Physical Layer Security: Wireless Location Verification and Secure Communications

Shihao Yan

A dissertation submitted to the Graduate Research School of
The University of New South Wales
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

School of Electrical Engineering and Telecommunications
Faculty of Engineering

April 2015

PLEASE TYPE

THE UNIVERSITY OF NEW SOUTH WALES
Thesis/Dissertation Sheet

Surname or Family name: **Yan**

First name: **Shihao** Other name/s:

Abbreviation for degree as given in the University calendar: **PhD**

School: **Electrical Engineering and Telecommunications** Faculty: **Faculty of Engineering**

Title: **Physical layer security: Wireless location verification and secure communications**

Abstract 350 words maximum: (PLEASE TYPE)

This thesis focuses on the utilization of reliable location information in wireless physical layer security. Specifically, new optimal Location Verification Systems (LVSs) are first developed to authenticate claimed locations, and then robust transmission strategies that utilize the verified locations are exploited in order to enhance physical layer security.

In the first half of this thesis, new optimal LVSs are developed and analyzed, leading to the following three main contributions. First, an information-theoretic framework for optimizing an LVS is developed and analyzed, in which the mutual information between the input and output data of the LVS is utilized as the optimization metric. Our analysis reveals that relative to more general frameworks the information-theoretic framework has a weaker dependence on critical unknown parameters of the system. Second, new optimal LVSs for a range of optimization metrics are proposed and examined under spatially correlated shadowing, with the conclusion that correlation in shadowing can lead to dramatic LVSs performance improvements. Third, analysis on an LVS under Rician fading channels discloses that the performance of the LVS increases significantly as the proportion of the line-of-sight component in the legitimate channel increases, or the tracking information on claimed locations accumulates. Surprisingly, our analysis also demonstrates that the performance limit of the LVS does not depend on the inherent properties of the channel between an adversary and the LVS.

In the second half of this thesis, robust transmission strategies utilizing verified location information are developed, leading to the following additional contributions. Fourth, an optimal location-based beamforming scheme that solely requires the locations of the intended receiver and the potential eavesdropper is proposed and analyzed under a Rician wiretap channel. Specifically, we provide the optimal location-based beamformer that minimizes the secrecy outage probability. Fifth, new antenna selection schemes which rely on verified locations are proposed. Our analysis reveals that the new antenna selection schemes enhance wireless physical layer security at the cost of only a minor increase in the feedback overhead. Sixth and finally, the optimization of wiretap code rates is investigated for a range of passive eavesdropping scenarios. Specifically, the optimal wiretap code rates for given locations of the eavesdropper are determined.

Declaration relating to disposition of project thesis/dissertation

I hereby grant to the University of New South Wales or its agents the right to archive and to make available my thesis or dissertation in whole or in part in the University libraries in all forms of media, now or here after known, subject to the provisions of the Copyright Act 1968. I retain all property rights, such as patent rights. I also retain the right to use in future works (such as articles or books) all or part of this thesis or dissertation.

I also authorise University Microfilms to use the 350 word abstract of my thesis in Dissertation Abstracts International (this is applicable to doctoral theses only).

Signature	Witness	Date
颜世豪	Chenxi Liu	10/04/2015

The University recognises that there may be exceptional circumstances requiring restrictions on copying or conditions on use. Requests for restriction for a period of up to 2 years must be made in writing. Requests for a longer period of restriction may be considered in exceptional circumstances and require the approval of the Dean of Graduate Research.

FOR OFFICE USE ONLY Date of completion of requirements for Award:

THIS SHEET IS TO BE GLUED TO THE INSIDE FRONT COVER OF THE THESIS

ORIGINALITY STATEMENT

'I hereby declare that this submission is my own work and to the best of my knowledge it contains no materials previously published or written by another person, or substantial proportions of material which have been accepted for the award of any other degree or diploma at UNSW or any other educational institution, except where due acknowledgement is made in the thesis. Any contribution made to the research by others, with whom I have worked at UNSW or elsewhere, is explicitly acknowledged in the thesis. I also declare that the intellectual content of this thesis is the product of my own work, except to the extent that assistance from others in the project's design and conception or in style, presentation and linguistic expression is acknowledged.'

Signed .....

Date 10/04/2015

ABSTRACT

This thesis focuses on the utilization of reliable location information in wireless physical layer security. Specifically, new optimal Location Verification Systems (LVSs) are first developed to authenticate claimed locations, and then robust transmission strategies that utilize the verified locations are exploited in order to enhance physical layer security.

In the first half of this thesis, new optimal LVSs are developed and analyzed, leading to the following three main contributions. First, an information-theoretic framework for optimizing an LVS is developed and analyzed, in which the mutual information between the input and output data of the LVS is utilized as the optimization metric. Our analysis reveals that relative to more general frameworks the information-theoretic framework has a weaker dependence on critical unknown parameters of the system. Second, new optimal LVSs for a range of optimization metrics are proposed and examined under spatially correlated shadowing, with the conclusion that correlation in shadowing can lead to dramatic LVSs performance improvements. Third, analysis on an LVS under Rician fading channels discloses that the performance of the LVS increases significantly as the proportion of the line-of-sight component in the legitimate channel increases, or the tracking information on claimed locations accumulates. Surprisingly, our analysis also demonstrates that the performance limit of the LVS does not depend on the inherent properties of the channel between an adversary and the LVS.

In the second half of this thesis, robust transmission strategies utilizing verified location information are developed, leading to the following additional contributions. Fourth, an optimal location-based beamforming scheme that solely requires the locations of the intended receiver and the potential eavesdropper is proposed and analyzed under a Rician wiretap channel. Specifically, we provide the optimal location-based beamformer that minimizes the secrecy outage probability. Fifth, new antenna selection schemes which rely on verified locations are proposed. Our analysis reveals that the new antenna selection schemes enhance wireless physical layer security at the cost of only a minor increase in the feedback overhead. Sixth and finally, the optimization of wiretap code rates is investigated for a range of passive eavesdropping scenarios. Specifically, the optimal wiretap code rates for given locations of the eavesdropper are determined.

ACKNOWLEDGEMENTS

My deepest and heartfelt gratitude goes first and foremost to my supervisor Prof. Robert Malaney for his constant encouragement, unambiguous guidance, and generous support given to me over the years. During my PhD study, I am always inspired by his wide knowledge and great patience, and thus I have acquired deep respect for his principles and philosophies about life and research. Specifically, I have learned many skills from him, such as how to think critically and write logically. Without his enthusiastic help, I would never have achieved academic progress or the completion of this thesis.

I would like to express my sincere appreciation to my co-supervisor, Prof. Jinhong Yuan, for his referral to my supervisor and his constructive suggestions on my research in physical layer security. I sincerely thank Dr. Ido Nevat of A*STAR, Singapore, for his inspiring discussions on location verification systems and also his encouragement given to me over the years. Special thanks go to Dr. Nan Yang of the Australian National University for his valuable guidance. I am very grateful to Dr. Gareth W. Peters of University College London, United Kingdom, who guided me in the world of statistics. Many thanks go to Dr. Ingmar Land and Dr. Ramanan Subramanian for their constructive comments on my research in physical layer security and their generous support on my visit to the University of South Australia. Also, I would like to thank Dr. Giovanni Geraci and Mr. Chenxi Liu for their contributions to my research in physical layer security.

My sincere thanks and lament go to my beloved mother who passed away in 2010 before witnessing my achievements. It was a hard time for me and my family to pass through. "One cannot forget the mother." It was she who inspired me to try my best to do everything. I would like to express my ultimate gratitude and love to my wife Jiaojiao, who marries me and then takes care of me and our son Zhengyu. She has been with me throughout the whole journey. Without her company and support, life would be much tougher. I am very grateful to my mother-in-law for her help and support dedicated to my young family in Australia. Many thanks go to my father, father-in-law, and sisters for the support given to me over the years.

Life in Electrical Engineering building (G17), The University of New South Wales (UNSW), was hard and enjoyable, and will never fade in my memory. Finally, I would like to express many thanks to my friends and colleagues at UNSW. Without their company, life would never be so enjoyable and fantastic.

Contents

Abbreviations

AOA	Angle of arrival
BS	Base station
cdf	cumulative distribution function
CSI	Channel state information
dB	decibel
DRSS	Differential received signal strength
FFA	Far field approximation
GPS	Global positioning system
i.i.d.	independent and identically distributed
KL	Kullback-leibler
LBB	Location-based beamforming
LOS	Line-of-sight
LRT	Likelihood ratio test
LVS	Location verification system
MAP	Maximum a posteriori probability
MD	Minimum distance
MRC	Maximal-ratio combining
MRT	Maximal-ratio transmission
MIMO	Multiple-input multiple output
NB	Non-beamforming
NMI	Normalized mutual information
OPA	Optimal power allocation

PC	Process center
pdf	probability density function
ROC	Receiver operating characteristic
RSS	Received signal strength
SC	Selection combining
SISOME	Single-input single-output multi-antenna eavesdropper
SNR	Signal-to-noise ratio
STBC	Space time block code
SVD	Singular value decomposition
TAS	Transmit antenna selection
TDMA	Time division multiple access
TDOA	Time difference of arrival
TOA	Time of arrival
UCA	Uniform circular array
UDA	Uniformly distributed approximation
ULA	Uniform linear array
VANET	Vehicular ad hoc network

List of Common Notations

$\lvert \cdot \rvert$	magnitude of an element
$\lVert \cdot \rVert$	Euclidean norm for vectors
$\mathbf{I}_n$	identity matrix with size $n \times n$
$(\cdot)^T$	transpose
$(\cdot)^\dagger$	conjugate transpose
$\log_2(\cdot)$	logarithm with base two
$\log_{10}(\cdot)$	logarithm with base ten
$\ln(\cdot)$	natural logarithm
$\lceil \cdot \rceil$	ceiling function
$\Gamma(\cdot)$	Gamma function
$\mathcal{Q}(\cdot)$	Q-function
$\mathrm{tr}(\cdot)$	trace of a matrix
$\mathrm{Re}\{\cdot\}$	real part of a complex number
$\mathbb{E}[\cdot]$	expectation
$\max\{\cdot\}$	maximization
$\min\{\cdot\}$	minimization
C_B	capacity of the main channel
C_E	capacity of the eavesdropper's channel
C_s	secrecy capacity
$\mathcal{H}_0$	null hypothesis
$\mathcal{H}_1$	alternative hypothesis

List of Figures

List of Publications

Journal Papers:

1. **S. Yan**, R. Malaney, I. Nevat, and G. Peters, "Location verification systems for VANETs in Rician fading channels," *IEEE Trans. Veh. Technol.*, accepted with minor revisions, arXiv:1412.2455, Mar. 2015.

2. **S. Yan**, G. Geraci, N. Yang, R. Malaney, and J. Yuan, "Optimization of code rates in SISOME wiretap channels," *IEEE Trans. Wireless Commun.*, accepted with minor revisions, Mar. 2015.

3. **S. Yan** and R. Malaney, "Secrecy performance analysis of location-based beamforming in Rician wiretap channels," arXiv:1412.6882, Dec. 2014.

4. **S. Yan**, R. Malaney, I. Nevat, and G. Peters, "Optimal information-theoretic wireless location verification," *IEEE Trans. Veh. Technol.*, vol. 63, no. 7, pp. 3410–3422, Sep. 2014.

5. **S. Yan**, I. Nevat, G. Peters, and R. Malaney, "Location verification systems under spatially correlated shadowing," arXiv:1410.5499, Sep. 2014.

6. **S. Yan**, N. Yang, R. Malaney, and J. Yuan, "Transmit antenna selection with Alamouti coding and power allocation in MIMO wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 13, no. 3, pp. 1656–1667, Mar. 2014.

7. **S. Yan** and R. Malaney, "Location verification systems in emerging wireless networks," *ZTE Communications*, vol. 11, no. 3, pp. 03–10, Sep. 2013 (**invited paper**).

Conference Papers:

1. **S. Yan**, R. Malaney, I. Nevat, and G. Peters, "Location spoofing detection systems for VANETs by a single base station in Rician fading channels," accepted by *IEEE VTC Spring*, arXiv:1410.2960, Jan. 2015.

2. **S. Yan**, N. Yang, R. Malaney, and J. Yuan, "Full-duplex wiretap channels: security enhancement via antenna switching," in *Proc. IEEE GlobeCOM TCPLS Workshop*, Dec. 2014, pp. 1412–1417.

3. **S. Yan** and R. Malaney, "Line-of-sight based beamforming for security enhancements in wiretap channels," in *Proc. ICITCS IEEE*, Oct. 2014, pp. 218–221.

4. **S. Yan**, G. Geraci, N. Yang, R. Malaney, and J. Yuan, "On the target secrecy rate for SISOME wiretap channels," in *Proc. IEEE ICC*, Jun. 2014, pp. 987–992.

5. **S. Yan**, R. Malaney, I. Nevat, and G. Peters, "Signal strength based location verification under spatially correlated shadowing," in *Proc. IEEE ICC*, Jun. 2014, pp. 2617–2623.

6. **S. Yan**, R. Malaney, I. Nevat, and G. Peters, "Timing information in wireless communications and optimal location verification frameworks," in *Proc. AusCTW*, Feb. 2014, pp. 144–149.

7. **S. Yan**, N. Yang, R. Malaney, and J. Yuan, "Transmit antenna selection with Alamouti scheme in MIMO wiretap channels," in *Proc. IEEE GlobeCOM*, Dec. 2013, pp. 687–692.

8. **S. Yan**, R. Malaney, I. Nevat, and G. Peters, "An information theoretic location verification system for wireless networks," in *Proc. IEEE GlobeCOM*, Dec. 2012, pp. 5415–5420.

Non-Lead-Author Papers (not included in this thesis):

1. N. Yang, **S. Yan**, J. Yuan, R. Malaney, R. Subramanian, and I. Land, "Artificial noise: Transmission optimization in Multi-Input Single-Output wiretap channels," *IEEE Trans. Commun.*, accepted, Mar. 2015.

2. C. Liu, N. Yang, **S. Yan**, J. Yuan, and R. Malaney, "Secure adaptive transmission in two-way relay wiretap channels," in *Proc. IEEE/CIC ICCC*, Oct. 2014, pp. 664–669.

Chapter 1

Introduction

As wireless services become increasingly ubiquitous, a growing amount of research effort has been devoted to the security issues pertaining to wireless networks. This is due to the fact that wireless networks suffer from security threats and vulnerabilities that are mainly caused by the broadcast nature of the wireless medium. Traditional cryptographic techniques require complex key distribution and management mechanisms. Also, the secrecy of cryptographic techniques is conditioned on the limited computational capability of attackers. Against this background, physical layer security is of growing importance since it eliminates the requirement of key distribution and management, and can guarantee secrecy regardless of an attacker's computational capability [1]. The core concept behind physical layer security is the exploitation of the inherent properties of wireless channels to realize secrecy [2].

This thesis focuses on the utilization of location information in enhancing physical layer security for wireless communications. Specifically, new optimal Location Verification Systems (LVSs) are first developed and analyzed, and then robust transmission strategies that utilize verified location information are explored to enhance physical layer security in wireless communications.

In this chapter, location verification and physical layer security in wireless communications are introduced in Section 1.1. Then, the motivations and challenging

research questions in location verification and physical layer security for wireless communications are outlined in Section 1.2. Finally, the thesis organization, together with our main contributions, is presented in Section 1.3.

1.1 Physical Layer Security in Wireless Networks

In this section, we first introduce location verification and physical layer security in wireless communications.

1.1.1 Location Verification

As location-based technologies and services become ubiquitous in emerging wireless networks, the authentication (verification) of location information has attracted considerable research interest in recent years [3–11]. In early wireless positioning systems, accuracy and performance issues were to the fore, with the authentication of location information relegated to a secondary concern. This is now changing. Many current mainstream wireless positioning systems, such as the now ubiquitous WiFi positioning systems, are highly vulnerable to location-spoofing attacks due to their openness and wide public availability [12, 13]. In particular, in many configurations wireless network positioning systems (e.g., GPS) are client-based [14, 15], meaning that only the client (the device whose location is to be verified) can obtain its location directly. The wider wireless networks can then only obtain the client's position through requesting the client to report its location. Such reported location information can be used to empower some functionalities of the wireless network such as in geographic routing protocols (e.g., [16–18]), to provide for location-based access control protocols (e.g., [19, 20]), and to provide some new location-based services (e.g., location-based key generation [21]). However, the use of such reported locations as an enabler of some functionalities or services within the wireless network, also provides ample opportunity to attack the system since any reported locations can be easily spoofed.

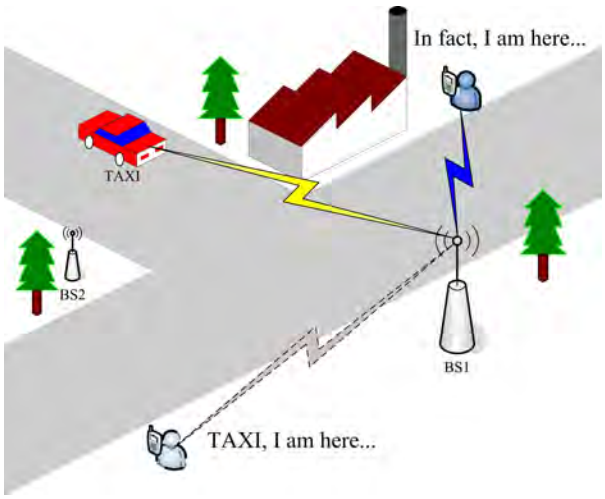

Figure 1.1: Illustration of a simple scenario of location spoofed attack.

LVSs are dedicated to detecting spoofed locations and eliminating the impact of such spoofed location information in wireless networks. The importance of location verification can be witnessed by the adverse effects that spoofed location information can have on a variety of network functions. For example, spoofed position information can lead to packet delivery rate in geographic routing protocols [18, 22, 23] being reduced dramatically [16, 17]. Performance of location-based access control can be decreased markedly by spoofed locations [19, 20, 24]. As mentioned in [25], WiFi, Cellular, and GPS position information within the E911 framework can be easily spoofed by clients, in order to maliciously attract emergency services to false locations. In addition, the adverse effects of location spoofing are arguably more severe in Vehicular Ad Hoc Networks (VANETs) [26–29]. Most importantly, location spoofing can lead to serious consequences in the collision avoidance aspects of VANETs. Beyond such critical effects, a malicious vehicle might spoof its position in order to cause serious service disruptions to other users [26–28], or to enhance in a selfish manner its own functionality within the network [30, 31]. Finally, we present a simple scenario of location spoofed attack in Fig. 1.1. In this figure, we can see that a user (not intend to take a taxi) can easily cheat a taxi driver to a fake location through reporting a spoofed location to the wireless network.

Location verification is different from the more general problem of locating a user in wireless networks [32]. A key difference between an LVS and a localization system is that we are provided some additional *a priori* (but potentially false) location information (i.e., a claimed location) in the LVS. Another key difference is that the output of an LVS is usually a binary decision, whereas in a localization system the output is usually an estimated location. An LVS aims at verifying a user's reported position based on observations and inferring whether the user is legitimate (reports its true position) or malicious (attempts to spoof its reported position). We focus on LVSs dedicated to physical layer, and thus the observations of such focused LVSs are obtained over wireless channels. From a statistical perspective, an location verification problem can be modeled as a binary hypotheses testing problem, where the null hypothesis $\mathcal{H}_0$ represents that the user is legitimate and alternative hypothesis $\mathcal{H}_1$ represents that the user is malicious. The output of an LVS are binary decisions, where $\mathcal{D}_0$ represents the decision that the user is legitimate and $\mathcal{D}_1$ represents the decision that the user is malicious. A statistical model for an LVS is presented in Fig. 1.2, where the binary realizations of the input X are $\mathcal{H}_0$ and $\mathcal{H}_1$, the binary realizations of the output Y are $\mathcal{D}_0$ and $\mathcal{D}_1$, and $P(\mathcal{D}_j|\mathcal{H}_i)$ $(i = 0, 1$ and $j = 0, 1)$ denotes the transition probability of deciding $\mathcal{D}_j$ for $\mathcal{H}_i$. In order to map X to Y, a binary decision rule has to be constructed based on observations and a claimed location in an LVS.

The traditional performance metrics of an LVS are false positive and detection rates. The false positive rate is the probability of deciding incorrectly that a legitimate user is malicious and is given by $\alpha = P(\mathcal{D}_1|\mathcal{H}_0)$. The detection rate is the probability of deciding correctly that a user is malicious and is given by $\beta = P(\mathcal{D}_1|\mathcal{H}_1)$. We are expecting an LVS to provide a high detection rate and a low false positive rate. But there is a tradeoff between the false positive and detection rates. The receiver operating characteristic (ROC) curve is used to demonstrate this tradeoff, and is constructed by plotting β versus α. However, the ROC curve by itself does not lead to an optimized setting in any sense (e.g., [33]).

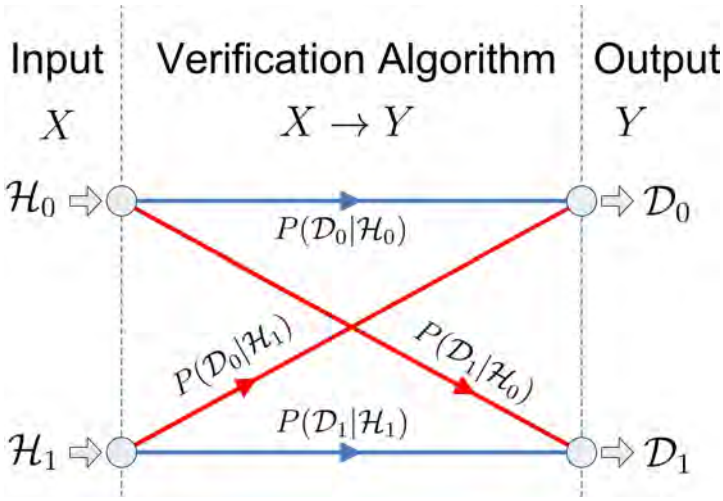

Figure 1.2: A Location Verification System (LVS) model.

To optimize an LVS, some unique evaluation criterion should be adopted as the performance metric. The transition probability $P(\mathcal{D}_j|\mathcal{H}_i)$ determines the performance of an LVS, thus the unique evaluation criterion should be a function of $P(\mathcal{D}_j|\mathcal{H}_i)$. One widely used metric is the Bayes' average cost, which is defined as [34]

$$\mathfrak{R} = \sum_{i=0}^{1}\sum_{j=0}^{1} C_{ji} P(\mathcal{D}_j|\mathcal{H}_i) P(\mathcal{H}_i), \tag{1.1}$$

where C_{ji} is the assigned cost associated with the decision $\mathcal{D}_j$ given the hypothesis $\mathcal{H}_i$, and $P(\mathcal{H}_0)$ and $P(\mathcal{H}_1)$ are the *a priori* probabilities of the occurrence of $\mathcal{H}_0$ and $\mathcal{H}_1$, respectively. In the Bayesian framework, the optimal LVS is the one which minimizes $\mathfrak{R}$. It is worthwhile to highlight that the Bayes' average cost requires that both C_{ji} and $P(\mathcal{H}_i)$ are known *a priori*. If the C_{ji}'s are unknown, the maximum a posteriori probability (MAP) criterion can be adopted [34], where the unique cost (i.e., total error [8]) is determined through

$$\mathfrak{R}_M = P(\mathcal{D}_1|\mathcal{H}_0)P(\mathcal{H}_0) + P(\mathcal{D}_0|\mathcal{H}_1)P(\mathcal{H}_1). \tag{1.2}$$

Comparing (1.1) and (1.2), we can see that $\mathfrak{R}_M$ is a special case of $\mathfrak{R}$ with $C_{00} = C_{11} = 0$, and $C_{10} = C_{01} = 1$. Thus, the MAP criterion is well suited for scenarios where the cost of rejecting a legitimate user is equal to that of accepting a malicious user.

In the following we first provide an overview on the state-of-the-art of LVS designs for generic wireless networks. Since collecting Received Signal Strength (RSS) does not require extra hardware, many LVSs for general wireless networks were developed based on RSS measurements. In [35], the authors proposed an algorithm to detect location spoofing attacks by matching the input instantaneous measurements with the normal signal fingerprints. Through exploiting experimental test results, the authors of [7] found that the RSSs follow a mixture of two Gaussian distributions if the prover (the user who provides the claimed location) and verifier are both equipped with two antennas. To perform the verification, [7] employed a likelihood ratio test constructed from the instantaneous measurements and expected normal profiles. An RSS fingerprints based location verification algorithm was also proposed in [5], where it was observed that solely analyzing the residual of RSS measurements can not robustly detect location spoofing attacks. However, if this residual is used referenced to a claimed location, it can provide for a verification algorithm robust against various forms of attacks. In [8], the location verification was formulated as a statistical significance testing problem. The authors analyzed the spatial correlation of RSS measurements to detect location attacks, and derived theoretic false positive and detection rates in 1-Dimension and 2-Dimension physical spaces. The algorithms of [5, 7, 8, 35] are representative of many similar RSS based wireless local verification algorithms.

Some generic challenge-response based location verification algorithms for wireless networks have been proposed in the literature (e.g., [6, 36, 37]). The well-known Echo protocol was proposed in [36], which is based on the delay of the two challenge-response messages sent through wireless and ultrasonic channels. The relative delay in the two channels is compared with the ideal theoretic delay, the latter of which is derived according to a prover's claimed location. A location verification protocol with hidden or mobile base stations was presented in [6]. The hidden or mobile base stations can securely estimate the distances to the prover since the locations of the hidden or mobile base stations are unknown to the prover. The distance error between

the estimated and claimed locations of a prover is compared with some threshold as a means to verification. In [37], several location verification algorithms were proposed based on power-modulated challenge-response method to detect malicious vehicles.

The authors of [38] proposed a probabilistic location verification algorithm for a wireless sensor network (WSN) with a high node density. In this WSN, the number of hops a packet (sent by a prover) traverses in order to reach a verifier, is shown to be probabilistically dependent on the Euclidean distance between the prover and the verifier. The proposed algorithm in [38] verifies a prover's claimed location by checking the correlation between the number of hops and the Euclidean distance (which is calculated based on the prover's claimed location). Assuming a high node density for the WSN, two location verification algorithms were proposed in [39]. These algorithms explored the inconsistencies between a prover's claimed location and the verifiers one-hop neighbor's determination that it can hear the prover.

We note that all the literature works discussed above are just representative (not exhaustive) of location verification algorithms proposed for generic wireless networks. We have tried to classify them into three classes, RSS-based, challenge-response based, and high-node-density based. Although the above discussed location verification algorithms can be applied to VANETs scenarios subject to some requirements (e.g., the vehicle density is high, the verifiers possess the ability to adjust their transmit power), many specific properties of VANETs were not explored in the above location verification algorithms. In the following, we review some location verification systems that are dedicated to VANETs.

By exploiting the specific properties of VANETs, such as high node density and mobility, the authors of [40] proposed an autonomous scheme and a cooperative scheme to detect and mitigate falsified locations. The acceptance range, mobility grade, and vehicle density are used in the binary decision rule in the autonomous scheme, where the thresholds are determined based on the maximum communication range, maximum velocity, and maximum density, respectively. The test statistics used in the cooperative scheme, such as neighbor tables, can only be obtained through co-

operating with other neighbor vehicles. The overall decision on a prover's claimed location is made by combining the local decisions with weight factors. Since the proposed location verification is applied in location-based routing protocols, in which it is assumed a malicious vehicle does not forward the packet to the correct next hop, the packet delivery ratio can be used as a performance criterion. The proposed schemes in [40] provide the basis of location verification in VANETs. Similar to [40], the authors of [41] also proposed location verification algorithms based on communication range, velocity, and density, but extended their test statistics to include traveled distance and map location.

To overcome the no line-of-sight (LOS) problem in LVSs, a cooperative location verification scheme was proposed in [42]. The proposed scheme focused on verifying a prover with no LOS to a verifier. To estimate the distance between the prover and verifier, this protocol requests help from a cooperative vehicle, which has LOS communications with both the prover and the verifier. The distances from the cooperator to the prover, and from the cooperator to the verifier, can be estimated, which then allows for the distance between the prover and verifier to be calculated. In addition, the claimed distance between the verifier and the prover's claimed location can be calculated. The main point of this protocol is its ability to verify vehicle locations that could not otherwise be verified due to obstacles.

A location verification solely based on messages exchange among neighbor vehicles was proposed in [43]. The authors focused on detecting a malicious vehicle which spoofs its position as the farthest one (within range) from the packet sender, so that it will be selected as the next hop in geographic routing protocols. In [43] it is assumed each vehicle is equipped with two directional antennas: forwards and backwards, and each vehicle constructs two corresponding tables of one-hop neighbors. The decision on a prover is made though exchanging and comparing such neighbor tables. The theoretic detection rate is derived as a function of the vehicle density. As expected, it is found that the larger the network density is, the higher the probability that malicious vehicles are detected by the proposed system will be.

A location verification algorithm based on a vehicle's direct connectivity (one-hop connectivity) with other vehicles was proposed in [44]. In this algorithm one-hop information is exchanged between vehicles so that each vehicle can build a two-hop neighborhood connectivity diagram. Using such diagrams, each vehicle can then attempt to verify the location information being passed to it. Each vehicle does this by constructing a *plausibility area*. Simply put, if a vehicle cannot hear directly from another vehicle, say vehicle A, at some location (since that vehicle is two hops away), then it should not be able to hear directly from a prover who claims to be further away than vehicle A. Similarly, in [45] a map-guided trajectory-based location verification algorithm was proposed, in which the plausibility area is constructed by using a prover's history location and map information (e.g., road dimensions).

In order to prevent the distance enlargement attack in VANETs, the authors of [46] proposed a cooperative verification algorithm to verify a prover's claimed location. In this scheme, both the verifier and cooperator can measure the TOA of the challenge-response messages from a prover. By using such TOA measurements, both the verifier and cooperator can conduct local verification on whether the prover launched distance reduction attacks. In such location verification algorithms, the test statistic is the difference between the TOA calculated distance and claimed distance derived from the prover's claimed location, and the threshold is determined using the processing delay of the challenge-response message. Since the cooperator is selected so as to locate the prover between the verifier and cooperator, the proposed cooperative algorithm is able to detect the distance enlargement attack.

In contrast to the previously reviewed works which focus on the one-hop location verification problem, the authors of [47] proposed a beacon-based trust managemen-t system, which combines the one-hop and multiple-hop verification algorithms to thwart internal attackers in VANETs. In the proposed system, the authors adopted the cosine similarity [48] between estimated vector (including position and velocity) and claimed vector in order to determine the beacon trustworthiness of a neighbor vehicle. The Tanimoto coefficient between history beacon messages and received event

messages is utilized to calculate the one-hop event trustworthiness, based on which an algorithm to determine the multiple-hop trustworthiness of an event message is also provided. Then, the Dempster-Shafer theory [49] is applied to combine all local event trustworthiness and determine the overall trustworthiness of an event message. Finally, the overall decision on the beacon message is made by comparing the overall trustworthiness with a predetermined threshold of trust degree.

Besides location spoofing attacks, Sybil attacks may also compromise some location-based services in VANETs. The Sybil attack refers to the scenario where a malicious vehicle illegitimately adopts multiple identities or locations to realize its attack purposes. This type of attacks is possibly launched by a selfish driver to mimic traffic congestion at some location on the road (used say as a mechanism to deter other vehicles from driving into his planned path). To detect such Sybil attacks, two location verification algorithms based on RSS measurements were proposed in [31]. In the first algorithm of [31], the verifier first estimates the prover's location through the Minimum Mean-Square Error on the distribution of RSS measurements. Then, the distance error between the estimated and claimed locations is utilized as the test statistic. In the second algorithm, the test statistic is derived from the distributions of such distance errors under $\mathcal{H}_0$ and $\mathcal{H}_1$, and the threshold is derived from a given false positive rate.

1.1.2 Physical Layer Security for Wireless Communications

The core concept behind physical layer security in wireless communications is to exploit the properties of wireless channels to perform secret data transmission [2]. In pioneering studies [50–52], a wiretap channel was characterized as the fundamental system model to protect information at the physical layer in wireless communications. As shown in Fig. 1.3, in the wiretap channel an eavesdropper (Eve) attempts to wiretap the communication between a transmitter (Alice) and an intended receiver (Bob). If Alice, Bob, and Eve are equipped with a single antenna, it was proved that

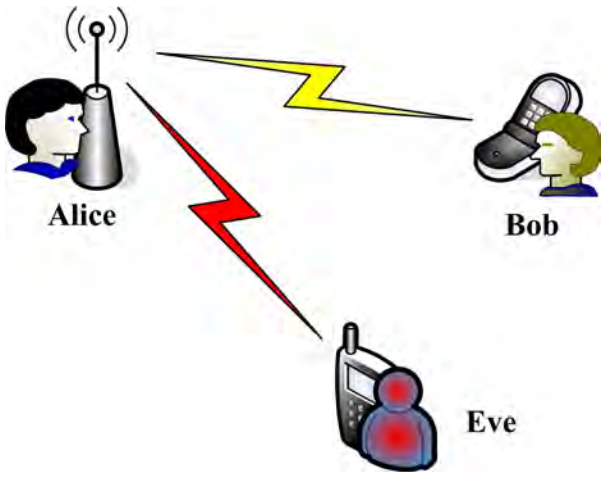

Figure 1.3: Illustration of the wiretap channel.

perfect secrecy can be achieved when the channel between Alice and Eve (henceforth referred to as the eavesdropper's channel) is worse than the channel between Alice and Bob (henceforth referred to as the main channel) [50–52]. As such, there are two methodologies to enhance physical layer security in wireless communications. The first one aims at enhancing the quality of the main channel. The second one aims at reducing the quality of the eavesdropper's channel.

Motivated by emerging multiple-input multiple-output (MIMO) techniques, physical layer security in MIMO wiretap channels is of growing interest [53, 54]. In the MIMO wiretap channel where Alice, Bob, and/or Eve are equipped with multiple antennas, physical layer security for wireless communications can be enhanced via many techniques, such as beamforming with and without artificial noise [53, 55–57] and transmit antenna selections [58–61]. The beamforming scheme (without artificial noise) was proposed and analyzed in [53], where the optimal beamformer that maximizes the secrecy capacity is achieved based on the generalized singular value decomposition of the main channel matrix and the eavesdropper's channel matrix. The beamforming with artificial noise scheme was proposed and analyzed in [55], in which Alice transmits artificial noise deliberately in the null space of the main channel matrix in order to confuse Eve. It is noted that beamforming with and without artificial

noise requires the precise channel state information (CSI) of the main channel and/or the eavesdropper's channel being fed back to Alice, which results in high feedback overhead and high signal processing cost [62]. In addition, it is shown in [57] that the secrecy performance of the beamforming with or without artificial scheme is highly dependent on the accuracy of the CSI of the main channel and/or the eavesdropper's channel.

To avoid the high feedback overhead and high signal processing cost required by beamforming, transmit antenna selection (TAS) was proposed to enhance physical layer security in MIMO wiretap channels [58–60]. In this TAS scheme, only one antenna is selected at Alice to maximize the instantaneous signal-to-noise ratio (SNR) of the main channel. Throughout this thesis, we refer to this scheme as *single TAS*. Single TAS significantly reduces the feedback overhead and hardware complexity, since only the index of the selected transmit antenna is fed back from Bob and only one radio-frequency chain is implemented at Alice. Motivated by this, [58] derived the secrecy outage probability of single TAS for the wiretap channel with multiple antennas at Alice and Eve but a single antenna at Bob. A general wiretap channel model with multiple antennas at Alice, Bob, and Eve was investigated in [59], in which the performance of single TAS with maximal-ratio combining (MRC) or selection combining (SC) was thoroughly examined in Rayleigh fading. Considering versatile Nakagami-m fading, [60] analyzed the secrecy performance of single TAS.

In a wiretap channel, the secrecy capacity, denoted as C_s, is defined as

$$C_s = \begin{cases} C_B - C_E, & \gamma_B > \gamma_E \\ 0, & \gamma_B \leq \gamma_E, \end{cases} \tag{1.3}$$

where $C_B = \log_2(1+\gamma_B)$ is the capacity of the main channel, $C_E = \log_2(1+\gamma_E)$ is the capacity of the eavesdropper's channel, γ_B and γ_E are the instantaneous SNRs of the main channel and the eavesdropper's channel, respectively. The secrecy capacity C_s is the metric to evaluate the secrecy performance of the wiretap channel when both C_B and C_E are achievable at Alice. However, in many practical application scenarios the eavesdropper is passive and C_E cannot be obtained. As such, the secrecy capacity

C_s cannot be used as the secrecy performance metric in such scenarios and the secrecy outage probability is adopted as a performance metric. The secrecy outage probability is defined as the probability of the secrecy capacity C_s being less than a specific target secrecy rate R_s (bits/channel-use) [63] and is given by

$$P_{out}(R_s) = \Pr(C_s < R_s). \tag{1.4}$$

In addition, the probability of non-zero secrecy capacity and the ε-outage secrecy capacity are also adopted as secrecy performance metrics for the scenarios in which C_s is intractable. The probability of non-zero secrecy capacity is defined as the probability that the secrecy capacity is positive and is given by

$$P_{non} = \Pr(C_s > 0) = \Pr(\gamma_B > \gamma_E). \tag{1.5}$$

We note that P_{non} is a function of $P_{out}(R_s)$ for $R_s = 0$, which is $P_{non} = 1 - P_{out}(0)$. The ε-outage secrecy capacity is defined as the maximum secrecy rate at which the secrecy outage probability is no larger than ε and is given by

$$C_{out}(\varepsilon) = \underset{P_{out}(R_s) \leq \varepsilon}{\operatorname{argmax}} R_s. \tag{1.6}$$

Based on the definitions of P_{non} and $C_{out}(\varepsilon)$, we know that $P_{out}(R_s)$ is the core secrecy performance metric when C_s is inapplicable.

1.2 Challenges and Motivations

In the context of LVSs, the core performance metrics are the false positive and detection rates, and the tradeoff between them is illustrated by the ROC curve. However, ROC curves are not always ideal in comparing performances of two LVSs [64,65]. For example, if the ROC curves of two LVSs intersect each other at a point, it is impossible to claim which one of these two LVSs is better. As such, a unique performance metric is required in order to compare performances of different LVSs or to optimize an LVS. As presented in the previous section, the Bayes' average cost is such a unique

performance metric widely adopted in the literature. However, the Bayes' average cost is subjective. This subjectivity arises through the necessity to pre-assign costs to all possible decisions. It has been discussed before how such subjectivity in Bayesian criteria can give rise to confusion when comparisons of detection performances are made [64, 65]. As such, although many of the previous works on LVSs have their own specific verification performance goals in mind, and their own advantages and disadvantages, none of these works identify an optimal LVS in any non-subjective sense. This leaves an important gap in objectively evaluating and optimizing an LVS. Filling this gap mainly forms the core of our work in Chapter 2.

The observations collected by an LVS obtained over wireless channels are related to location information, including (but not limited to) RSS, Time of Arrival (TOA), and Angle of Arrival (AOA). Among such location information metrics, RSS is the most desirable one in wireless networks due to its robustness, cost-effectiveness, and wide availability. In the literature, many LVSs that utilize RSS as input observations have been developed (e.g., [3–5, 7, 8, 35]). Most existing studies in the RSS-based systems simply assume that the shadowing at two different locations is independent. However, it is known from empirical studies that shadowing at different locations can be significantly correlated in some scenarios (e.g., the locations are close to each other, different locations possess similar terrain configurations [66–70]). Although some specific studies have investigated the performance of RSS-based localization systems under correlated shadowing [71, 72], the impact of spatially correlated shadowing on an LVS has not been previously explored. This leaves an important gap in the understanding on the performance levels of an LVS in a class of realistic wireless channel settings. As such, *"How does the correlated shadowing quantitatively impact the detection performance of an RSS-based LVS?"* is the main question answered in Chapter 3.

Motivated by the practical significance of location authentication in the context of VANETs, LVSs have been introduced to VANETs application scenarios and form part of the decision logic in the revocation of malicious-vehicle certificates within IEEE

1609.2 [74]. As such, many location verification protocols dedicated for VANETs have been proposed and studied in the literature (e.g., [31,32,40,42,46,48,75–77]). However, the quantitative impact of an inherent wireless channel property, the proportion of the line-of-sight (LOS) in a wireless channel, was not investigated. The proportion of the LOS in a wireless channel impacts the characteristics of observations obtained over wireless channels, such as the shadowing variance of RSS, the estimation error of TOA, and the statistics on AOA determinations. The follow-on impact of such effects on LVS performances is non-trivial. As such, examining the quantitative dependence between the optimal detection performance of an LVS and the proportion of the LOS of a wireless channel is our main objective in Chapter 4.

In the context of physical layer security for wireless communications, many techniques developed in the literature require precise CSI of the main channel and/or the eavesdropper's channel (e.g., [53, 55, 56, 60, 61]). However, such precise CSI may not be available in some practical application scenarios. For example, in massive MIMO techniques the CSI of a channel (e.g., the main channel, the eavesdropper's channel) cannot be precisely known to a receiver or transmitter due to pilot contamination issues [78–81]. In addition, it is well known that Alice cannot precisely know the CSI of the eavesdropper's channel if Eve is passive. Against this background, there are many circumstances where *location information* of Bob and Eve could be available. For example, in some specific military application scenarios, Alice may achieve Bob's location through direct requests, and Eve's location through some *a priori* surveillance. Such location information can be potentially verified by an LVS and then utilized to enhance physical layer security for wireless communications, which was not examined in the literature. Then, *"How does the location information of Bob and/or Eve quantitatively enhance physical layer security in wireless communications?"* is the main question we intend to explicitly answer in Chapter 5.

In the literature, single TAS was proposed to enhance physical layer security while avoiding the high feedback overhead and complex signal processing required by other techniques (e.g., beamforming) [58–60]. The cost paid by the low-complex

single TAS is the secrecy performance. The quantitative performance improvement brought by some specific increase in the complexity of TAS is of interest and was not explored in the literature. Specifically, in the context of TAS within MIMO wiretap channels, we are interested in the following question in Chapter 6: *"What is the secrecy performance if two antennas are selected at Alice?"*. Given the secrecy performance of the single TAS, answering the above question initiates the quantitative examine of the trade-off between feedback overhead and secrecy performance in the context of TAS schemes.

In wireless physical layer security, the capacities of the main channel and the eavesdropper's channel are required at Alice to determine wiretap code rates in order to guarantee perfect secrecy [82, 83]. In the case where either the capacity of the main channel C_B or the capacity of the eavesdropper's channel C_E is not available, wiretap code rates have to be set through guaranteing some given constraints. For example, the wiretap code rates can be set based on a given value of the secrecy outage probability given by (1.4) [58,60,63,84]. However, the use of the secrecy outage probability given by (1.4) in determining the wiretap code rates has the drawback that it requires a subjectively predetermined value of the secrecy outage probability. Then, in Chapter 7 from a new perspective we investigate the optimization of wiretap code rates for a range of passive eavesdropping scenarios, including the one where even Eve's location is unavailable.

1.3 Thesis Outline and Contributions

The outline of the remaining thesis, together with the main contributions, is summarized as follows.

In Chapter 2, we develop a new LVS focussed on network-based Intelligent Transport Systems and VANETs. The system we develop is based on an information theoretic framework in which the mutual information between the system's input and output data is maximized. Our system takes as inputs a user's claimed location and

base-station RSS measurements in order to form an optimal decision rule on the legitimacy of the claimed location. The scenario we consider is where a non-colluding malicious user alters his transmit power in an attempt to fool the LVS. We develop a practical threat model for this attack scenario, and investigate the performance of the LVS in terms of its input/output mutual information. We show how our LVS decision rule can be implemented straightforwardly with a performance that delivers near-optimality under realistic threat conditions. The practical advantages our new information-theoretic scheme delivers, relative to more traditional Bayesian verification frameworks, are discussed.

In Chapter 3, the verification of the location information utilized in wireless communication networks is a subject of growing importance. In this chapter we formally analyze, for the first time, the performance of a wireless LVS under the realistic setting of spatially correlated shadowing. Our analysis illustrates that anticipated levels of correlated shadowing can lead to a dramatic performance improvement of a RSS-based LVS. We also analyze the performance of an LVS that utilizes DRSS, formally proving the rather counter-intuitive result that a DRSS-based LVS has identical performance to that of an RSS-based LVS, for all levels of correlated shadowing. Even more surprisingly, the identical performance of RSS and DRSS-based LVSs is found to hold even when the adversary does not optimize his true location. Only in the case where the adversary does not optimize *all* variables under her control, do we find the performance of an RSS-based LVS to be better than a DRSS-based LVS. The results reported in this chapter are important for a wide range of emerging wireless communication applications whose proper functioning depends on the authenticity of the location information reported by a transceiver.

In Chapter 4, we propose and examine LVSs for VANETs in the realistic setting of Rician fading channels. In our LVSs, a single authorized Base Station (BS) equipped with multiple antennas aims to detect a malicious vehicle that is spoofing its claimed location. We first determine the optimal attack strategy of the malicious vehicle, which in turn allows us to analyze the optimal LVS performance as a function of the

Rician K-factor of the channel between the BS and a legitimate vehicle. Our analysis also allows us to formally prove that the LVS performance limit is independent of the properties of the channel between the BS and the malicious vehicle, provided the malicious vehicle's antenna number is above a specified value. We also investigate how tracking information on a vehicle quantitatively improves the detection performance of an LVS, showing how optimal performance is obtained under the assumption of the tracking length being randomly selected. The work presented here can be readily extended to multiple BS scenarios, and therefore forms the foundation for all optimal location authentication schemes within the context of Rician fading channels. Our study closes important gaps in the current understanding of LVS performance within the context of VANETs, and will be of practical value to certificate revocation schemes within IEEE 1609.2.

In Chapter 5, we develop a new optimal Location-Based Beamforming (LBB) scheme for the wiretap channel, where both the main channel and the eavesdropper's channel are subject to Rician fading. In our LBB scheme the two key inputs are the location of the legitimate receiver and the location of the potential eavesdropper. Notably, our scheme does not require as direct inputs any channel state information of the main channel or the eavesdropper's channel, making it easy to deploy in a host of application settings in which the location inputs are known. Our beamforming solution assumes a multiple-antenna transmitter, a multiple-antenna eavesdropper, and a single-antenna receiver, and its aim is to maximize the physical layer security of the channel. To obtain our solution we first derive the secrecy outage probability of the LBB scheme in a closed-form expression that is valid for arbitrary values of the Rician K-factors of the main channel and the eavesdropper's channel. Using this expression we then determine the location-based beamformer solution that minimizes the secrecy outage probability. To assess the usefulness of our new scheme, and to quantify the value of the location information to the beamformer, we compare our scheme to another scheme that does not utilize any location information. Our new beamformer solution provides optimal physical layer security for a wide range of

location-based applications.

In Chapter 6, we propose a new TAS scheme which examines the trade-off between feedback overhead and secrecy performance in MIMO wiretap channels. Our new scheme is carried out in two steps. First, the transmitter selects the first two strongest antennas to maximize the instantaneous SNR of the main channel. Second, Alamouti coding is employed at the selected antennas in order to perform secret data transmission. When equal power is applied to the selected antennas, we refer to our new scheme as TAS-Alamouti. To provide valuable insights into TAS-Alamouti, we derive new closed-form expressions for the secrecy performance metrics. In terms of these metrics, we show how in a Rayleigh fading channel that our TAS-Alamouti scheme outperforms the traditional single TAS scheme conditioned on the SNR of the main channel being larger than a specific value. We show how in some antenna configurations no additional feedback, relative to single TAS, is required in order to realize such performance enhancements. Furthermore, we show how optimal power allocation (OPA) across the selected antennas at the transmitter leads to a new scheme, which we refer to as TAS-Alamouti-OPA, that outperforms single TAS unconditionally. Relative to TAS-Alamouti, TAS-Alamouti-OPA requires only one additional feedback bit.

In Chapter 7, we develop a new framework for optimizing the wiretap code rates of single-input single-output multi-antenna eavesdropper (SISOME) wiretap channels when the capacity of the eavesdropper's channel is not available at the transmitter. In our framework we introduce the effective secrecy throughput as a new performance metric that explicitly captures the two key features of wiretap channels, namely, reliability and secrecy. Notably, the effective secrecy throughput measures the average rate of the confidential information transmitted from the transmitter to the intended receiver without being eavesdropped on. We optimize wiretap code rates for adaptive and fixed-rate transmission schemes when the capacity of the main channel is available and unavailable at the transmitter, respectively. Such optimizations are further extended into an absolute passive eavesdropping scenario where even the average S-

NR of the eavesdropper's channel is not available at the transmitter. Notably, our solutions for the optimal wiretap code rates do not require us to set reliability or secrecy constraints for the transmission in wiretap channels.

Chapter 2

Optimal Information-Theoretic Wireless Location Verification

2.1 Introduction

In an LVS, one aims at verifying a user's claimed position based on some input measurements so as to perform a binary decision on whether the user is *legitimate* (claims his true position) or *malicious* (spoofs his claimed position). In a binary decision rule embedded in an LVS, we have to determine both the test statistic and the corresponding threshold. In general, an LVS aims at obtaining a low false positive rate for legitimate users and a high detection rate for malicious users, leading to a tradeoff perhaps best illustrated by an ROC curve. However, it is established that ROCs are not always ideal in comparing performances of two separate systems (e.g., [64, 65]). It is also the case that the use of a ROC does not in any formal sense indicate what the *optimal* operating point of an LVS is. A possible direction to follow in attempting an optimization of an LVS is to utilize a Bayesian hypothesis test, which with uninformative priors contains the structure of a Likelihood Ratio Test (LRT) - which minimizes the input/output classification error in the scenario where the cost of all types of misclassifications are equal [8]. Additionally, if the costs of misclassifications

are not equal, then a variation of the LRT decision rule can be formed, namely the Bayesian criterion [34]. However, it is well known that these Bayes-decision criteria possess a weakness - they are *subjective*. This subjectivity arises through the necessity to pre-assign costs to the different types of misclassifications. It has been discussed before how such subjectivity in Bayesian criteria can give rise to confusion when comparisons of detector performances are made [64, 65]. As such, although many of the previous works on LVSs have their own specific verification performance goals in mind, and their own advantages and disadvantages, none of these works identify an optimal LVS in any non-subjective sense.

To make progress, what is actually required is an *objective* measure of detector performance, namely a single unified metric that takes into account all key aspects of intrusion detection in an objective fashion. As argued in [65], this metric should be the *mutual information*, and it is this approach we develop here in the context of location verification. More specifically, we develop here an information-theoretic framework for an LVS in which the mutual information between the input and output LVS data is used as the objective optimization criterion.

In general an LVS can be characterized as follows. The input data (a user to be verified) is represented by a binary random variable $X = x$, $x \in [0, 1]$, whose realized elements indicate legitimate ($x = 0$) or malicious ($x = 1$). Likewise the output data can be represented by a binary random variable $Y = y$, $y \in [0, 1]$, whose realized elements indicate the binary decisions made by the LVS, namely *verified* ($y = 0$) or *not verified* ($y = 1$). In the LVS, a *decision rule* is formed which indicates whether a user is malicious or not. This decision rule ultimately forms a test on whether some statistic (derived from network measurements and some prior information) is less than or equal to some *threshold*.

With these definitions in place, the contributions of this chapter can be specifically summarized as follows. (i) We develop for the first time an information-theoretic framework for an LVS, which allows us to utilize the mutual information between X and Y as a unique criterion to evaluate and optimize the performance of an LVS.

(*ii*) Under the assumption of *known* likelihood functions for the measurements, we prove that the likelihood ratio is the test statistic that produces the maximum mutual information between X and Y. (*iii*) Identifying the threshold value that maximizes the mutual information between X and Y, we then show how the LRT is the decision rule which maximizes the mutual information between X and Y, and leads to the optimal information-theoretic LVS. We take the further step of determining the likelihood functions under a series of threat models. This leads to a working LVS that will be an optimal information-theoretic approach under the given threat models. (*iv*) We show from our analysis how an effectively optimal LVS, which is simple to deploy in practice, can be developed. We show that our LVS leads to an optimal solution for most realistic attack scenarios in which a malicious user, who is outside a network region, is attempting to spoof that he is within the network region. We further show how optimality is approached as the malicious user moves further from the network region.

The remainder of this chapter is structured as follows. Section 2.2 presents both the general network system model and our information-theoretic LVS framework. The decision rule that maximizes mutual information is constructed in Section 2.3. In Section 2.4, analysis and simulations of our LVS are presented for a series of threat models. Discussion and results in relation to Bayesian frameworks are provided in Section 2.5. Section 2.6 concludes this chapter.

2.2 System Model of an LVS

In this section, we first present the general model of an LVS and the related assumptions. The values of the input data X can be represented as two hypotheses. The first of these is the null hypothesis, $\mathcal{H}_0$, which assumes the user to be verified is legitimate ($x = 0$). The second one is the alternative hypothesis, $\mathcal{H}_1$, which assumes the user to be verified is malicious ($x = 1$). Likewise, the possible values of the output data Y can be represented as two decisions, where $\mathcal{D}_0$ denotes verified ($y = 0$), and $\mathcal{D}_1$

denotes not verified ($y = 1$). We now outline the general LVS model, and detail the assumptions we use.

1. A *single* user (legitimate or malicious) reports his claimed location, $\mathbf{x}_c = (u_c, v_c) \in \mathbb{R}^2$, to a network with K ($K > 2$) Base Stations (BSs) in the communication range of the user (the K BSs are not in a line), where $\mathbf{x}_i = (u_i, v_i) \in \mathbb{R}^2$ is the location of the i-th BS, $i = 1, 2, ..., K$. Any one of the K BSs can be chosen as the Process Center (PC), and all other BSs will transmit the measurements collected from the user to that PC. Although any BS can be chosen as the PC, it would perhaps be wise to choose a BS which is not on the periphery of the network (i.e., is not poorly or intermittently connected to the network). The PC is to make decisions based on the user's claimed location and the measurements collected by all the K BSs. We assume all BSs are perfectly synchronized.

2. We assume a user (legitimate or malicious) knows the locations of the K BSs, and that $\mathbf{x}_c$ is supplied by the user to the PC.

3. For the legitimate user, we assume the true location is the same as his claimed location (here we will ignore the small location determination error, e.g., the GPS error[1]). We assume the malicious user's true location $\mathbf{x}_t = (u_t, v_t) \in \mathbb{R}^2$ is known exactly to him (i.e., again we ignore any small localization error), but is unknown to the network.

4. We assume $\mathbf{x}_t$ is a bivariate random variable following some distribution. The prior distribution, i.e., the conditional probability density function (pdf), for $\mathbf{x}_t$ under $\mathcal{H}_1$ is denoted as $p(\mathbf{x}_t|\mathcal{H}_1)$.

5. In general, the measurement (M_i) collected by the i-th BS from a legitimate user is dependent on $\mathbf{x}_i$ and the legitimate user's $\mathbf{x}_c$. In practice, a malicious user can impact the measurements collected by all BSs in order to avoid detection.

[1]When this error is much smaller than the average distance between BSs the effect on the results is negligible.

Thus, the measurement (M_i) collected by the i-th BS from a malicious user is some function of $\mathbf{x}_i$, the malicious user's $\mathbf{x}_t$, and his spoofed $\mathbf{x}_c$. Therefore, the measurement (M_i) collected by the i-th BS can be given by a composite model as below

$$\begin{cases} \mathcal{H}_0 : M_i = h_0\left(\mathbf{x}_i, \mathbf{x}_c, \omega\right), \\ \mathcal{H}_1 : M_i = h_1\left(\mathbf{x}_i, \mathbf{x}_c, \mathbf{x}_t, \omega\right), \end{cases} \tag{2.1}$$

where h_0 and h_1 are some functions yet to be specified (can involve additional parameters), and ω is random variable representing the communication system noise. Given the statistical nature of ω, the composite system model in (2.1) can produce the *likelihood functions* under $\mathcal{H}_0$ and $\mathcal{H}_1$, which are denoted as $p(\mathbf{m}|\mathcal{H}_0)$ and $p(\mathbf{m}|\mathcal{H}_1)$, respectively, where $\mathbf{m} = [m_1, m_2, ..., m_K]$ is a realization of the measurement vector $\mathbf{M} = [M_1, M_2, ..., M_K]$.

6. We also assume a user is legitimate with a known prior probability, which is $P_0 = P(x = 0)$. The probability of a user to be malicious is denoted as P_1, and $P_1 = 1 - P_0$. We note that the *a priori* probability (i.e., P_0 or P_1) can be estimated based on historical data records (e.g., verification results of previous LVSs). We also note that the *a priori* probability of a user being malicious is low in practice and as we show later our proposed information-theoretic framework is less sensitive to the estimation errors in the *a priori* probabilities (e.g., P_1) than the Bayesian framework. Finally, we note that if the historical data records are not available, the initial *a priori* probability can be set as $P_0 = P_1 = 0.5$ and updated sequentially based on neural network or machine learning methodologies.

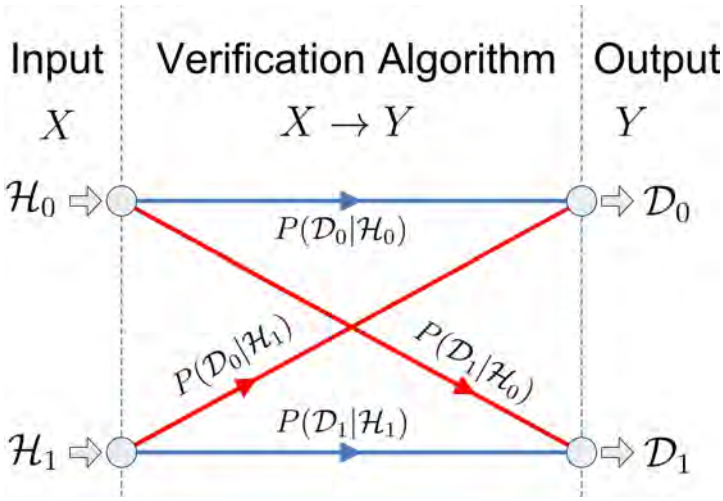

Figure 2.1: A Location Verification System (LVS) model.

2.3 Optimal Information-Theoretic Framework of an LVS

In this section, we first develop an information-theoretic framework for an LVS, which allows us to utilize the mutual information between X and Y as an unique criterion to evaluate and optimize an LVS. Then, based on the assumption of known likelihood functions under both $\mathcal{H}_0$ and $\mathcal{H}_1$, we take the additional step of identifying the optimal information-theoretic location verification algorithm, which produces the maximum $I(X;Y)$ relative to any other location verification algorithms.

2.3.1 Information-Theoretic Framework of an LVS

In general, the purpose of an LVS is to map the input data X to the output data Y, $X \to Y$, and can be represented as shown in Fig. 2.1. In this figure, the false positive rate, α, and the detection rate, β, are given as follows

$$\begin{aligned} \alpha &= P(\mathcal{D}_1|\mathcal{H}_0),\ 1-\alpha = P(\mathcal{D}_0|\mathcal{H}_0), \\ \beta &= P(\mathcal{D}_1|\mathcal{H}_1),\ 1-\beta = P(\mathcal{D}_0|\mathcal{H}_1), \end{aligned} \tag{2.2}$$

where $P(\cdot|\cdot)$ is the probability of an outcome conditional on a hypothesis. The mutual information between X and Y can be expressed as $I(X;Y) = H(X) - H(X|Y)$, where $H(X)$ is the entropy of X, and $H(X|Y)$ is the conditional entropy of X given Y. Given P_0, the entropy of the discrete binary random variable X can be written as $H(X) = -\sum_x P(X)\log_2 P(X) = -P_0\log_2 P_0 - (1-P_0)\log_2(1-P_0)$. With these definitions, the conditional entropy $H(X|Y)$ can be expressed as [64]

$$\begin{aligned} H(X|Y) &= -\sum_x \sum_y P(X,Y)\log_2 P(X|Y) \\ &= P_0(1-\alpha)\left(-\log_2 \frac{P_0(1-\alpha)}{P_0(1-\alpha)+(1-P_0)(1-\beta)}\right) \\ &\quad + P_0\alpha\left(-\log_2 \frac{P_0\alpha}{P_0\alpha+(1-P_0)\beta}\right) \\ &\quad + (1-P_0)(1-\beta)\left(-\log_2 \frac{(1-P_0)(1-\beta)}{P_0(1-\alpha)+(1-P_0)(1-\beta)}\right) \\ &\quad + (1-P_0)\beta\left(-\log_2 \frac{(1-P_0)\beta}{P_0\alpha+(1-P_0)\beta}\right). \end{aligned} \tag{2.3}$$

The mutual information $I(X;Y)$ measures the reduction of uncertainty of the input X given the output Y. For example, if we make verification decisions without any observations, X and Y will be independent of each other, and $I(X;Y)$ will be minimized (zero). However, based on some observations our LVS attempts to map X into Y so as to minimize the uncertainty of X given Y. An extreme example of this is when X and Y are identical and therefore $I(X;Y)$ is maximized (of course this would require infinite noisy observations or finite noiseless observations). More generally, given some finite noisy observations, maximizing on the mutual information $I(X;Y)$ leads to decisions which maximize the dependence between X and Y. As such, the mutual information is the natural optimization metric for an LVS from an information-theoretic viewpoint. The optimal information-theoretic location verification algorithm can be defined as the one that maximizes $I(X;Y)$.

2.3.2 Optimal Decision Rule

In the context of an LVS, a location verification algorithm must formulate a decision rule to infer whether the user is consistent with $\mathcal{H}_0$ or $\mathcal{H}_1$. The algorithm ultimately forms a comparison of some test statistic, $F(\mathbf{m})$, and a corresponding threshold, T_F, in the form of

$$F(\mathbf{m}) \underset{\mathcal{D}_0}{\overset{\mathcal{D}_1}{\gtrless}} T_F. \tag{2.4}$$

For a given $F(\mathbf{m})$, we will be interested in the value of T_F which maximizes $I(X;Y)$, i.e., $T_F^* = \arg\max_{T_F} I(X;Y)$. Furthermore, we will be interested in determining the functional form of $F(\mathbf{m})$ that maximizes $I(X;Y)$. This leads to our main result, which is stated in the following theorem.

***Theorem* 1** Given the decision rule

$$F(\mathbf{m}) \underset{\mathcal{D}_0}{\overset{\mathcal{D}_1}{\gtrless}} T_F^*, \tag{2.5}$$

the functional form of $F(\mathbf{m})$ that maximizes the mutual information $I(X;Y)$ is $\Lambda(\mathbf{m})$, where

$$\Lambda(\mathbf{m}) \triangleq \frac{p(\mathbf{m}|\mathcal{H}_1)}{p(\mathbf{m}|\mathcal{H}_0)}. \tag{2.6}$$

To prove Theorem 1, we first introduce two lemmas, of which the first one is the Neyman-Pearson Lemma [86].

***Lemma* 1** Consider two hypotheses $\mathcal{H}_0$ and $\mathcal{H}_1$, the decision rule to maximize a detection rate (β) for any given false positive rate (α) is

$$\Lambda(\mathbf{m}) \underset{\mathcal{D}_0}{\overset{\mathcal{D}_1}{\gtrless}} T_\Lambda, \tag{2.7}$$

where T_Λ is determined by the specified value of α.

For proof of Lemma 1, see [86]. Before proceeding, we note $\alpha < \beta$ will be a basic requirement for any useful LVS.

Lemma 2 Given the assumption $\alpha < \beta$, the mutual information $I(X;Y)$ is a monotonic increasing function of the detection rate β.

We now prove Lemma 2. Since $H(X)$ is not dependent on β, the first derivative of $I(X;Y)$ with respect to β can be expressed as

$$\begin{aligned}\frac{\partial I(X;Y)}{\partial \beta} &= \frac{\partial \left(H(X) - H(X|Y)\right)}{\partial \beta} = -\frac{\partial H(X|Y)}{\partial \beta} \\ &= (1-P_0)\left(\log_2 \frac{\beta[P_0(1-\alpha)+(1-P_0)(1-\beta)]}{(1-\beta)[P_0\alpha+(1-P_0)\beta]}\right) \\ &= (1-P_0)\log_2 \underbrace{\{\beta[P_0(1-\alpha)+(1-P_0)(1-\beta)]\}}_{V_0} \\ &\quad - (1-P_0)\log_2 \underbrace{\{[P_0\alpha+(1-P_0)\beta](1-\beta)\}}_{V_1}. \end{aligned} \tag{2.8}$$

Note, since $0 < P_0 < 1$, and the logarithm is a monotonic increasing function, then $\partial I(X;Y)/\partial\beta$ has the same sign as $(V_0 - V_1)$, where

$$\begin{aligned} V_0 - V_1 &= \beta[P_0(1-\alpha)+(1-P_0)(1-\beta)] - [P_0\alpha+(1-P_0)\beta](1-\beta) \\ &= P_0(\beta-\alpha). \end{aligned} \tag{2.9}$$

Thus, given the assumption $\alpha < \beta$, then $\partial I(X;Y)/\partial\beta > 0$, and Lemma 2 is proved.

Given Lemma 1 and Lemma 2, we now prove Theorem 1.

If the specified value of α in Lemma 1 is the one which results in the value T_F^* of (2.5), then by Lemma 2 the result presented in Theorem 1 follows.

2.3.3 Optimal Location Verification Algorithm

The optimal information-theoretic location verification algorithm is presented in Algorithm 2.1.

In order to apply the optimal information-theoretic location verification algorithm (Algorithm 2.1), we first have to construct the null and alternative hypotheses based

Algorithm 2.1 Optimal Location Verification Algorithm

Input: priori probability P_0, measurement model, measurements, a claimed location.

Output: binary decisions $\mathcal{D}_1$ and $\mathcal{D}_0$.

1: For a given specific observation model, determine the functional forms of h_0 and h_1 in (2.1).

2: Specify the prior distributions for $\mathbf{x}_t$, $p(\mathbf{x}_t|\mathcal{H}_0)$ and $p(\mathbf{x}_t|\mathcal{H}_1)$, and determine the likelihood functions $p(\mathbf{m}|\mathcal{H}_0)$ and $p(\mathbf{m}|\mathcal{H}_1)$.

3: With (2.7) as the general decision rule, derive the functional form of α and β. Note, α and β will be functions of T_Λ.

4: Using $I(X;Y)$ as the objective function, search for T_Λ^*, which is the value of T_Λ that maximizes $I(X;Y)$.

5: Collect measurements and calculate the likelihood ratio $\Lambda(\mathbf{m})$ according to the likelihood functions determined in step 2.

6: Form the optimal decision rule as

$$\Lambda(\mathbf{m}) \underset{\mathcal{D}_0}{\overset{\mathcal{D}_1}{\gtrless}} T_\Lambda^*. \tag{2.10}$$

on a given claimed location. The null hypothesis ($\mathcal{H}_0$) is constructed by presuming the claimed location is from a legitimate user (who utilizes his true location as the claimed location), and the alternative hypothesis ($\mathcal{H}_1$) is constructed by presuming the claimed location is from a malicious user (who utilizes a fake location as his claimed location). In step 2 of Algorithm 2.1, the final likelihood function $p(\mathbf{m}|\mathcal{H}_1)$ is obtained by averaging the conditional likelihood function $p(\mathbf{m}|\mathbf{x}_t, \mathcal{H}_1)$ over $\mathbf{x}_t$.

2.4 RSS-based Optimal Information-Theoretic Location Verifications

In order to implement the optimal location verification algorithm, in this section we take the further step of determining the likelihood functions under $\mathcal{H}_0$ and $\mathcal{H}_1$ with RSS as the system measurements, and we consider the algorithm under a series of threat models.

2.4.1 Observation Model and Threat Model

Although the framework we develop can be used for any network observation model (network location information metric), such as RSS, TOA, and TDOA (time difference of arrival), later in this chapter we focus on the RSS measurements. This choice is largely motivated by the fact that RSS measurements are the simplest network measurements to obtain (lowest hardware complexity). However, it is important to emphasize that other network metrics can be equally utilized within our framework, and indeed in some circumstances even lead to improved verification performance. For our claimed location information, we assume a GPS-based acquisition by the user device due to the ubiquitous deployment of such on-board systems. However, again we emphasize other sources of claimed location information could be utilized, as long as such information is independent of the network measurements that utilized for location verification. In the following, the measurement M_i is the RSS (in dB) collected by the i-th BS. We also assume that the legitimate user and all BSs are equipped with only a single omni-direction antenna.

Let us define the set of K BSs that are within the range of a legitimate user positioned at $\mathbf{x}_c$ as the *in-range* BSs. This set of BSs forms an effective perimeter for the network used in the location verification. We will assume a single malicious user has the technology that allows him to ensure (if required) that from some position outside the perimeter only the in-range K BSs receive a non-zero signal power. The

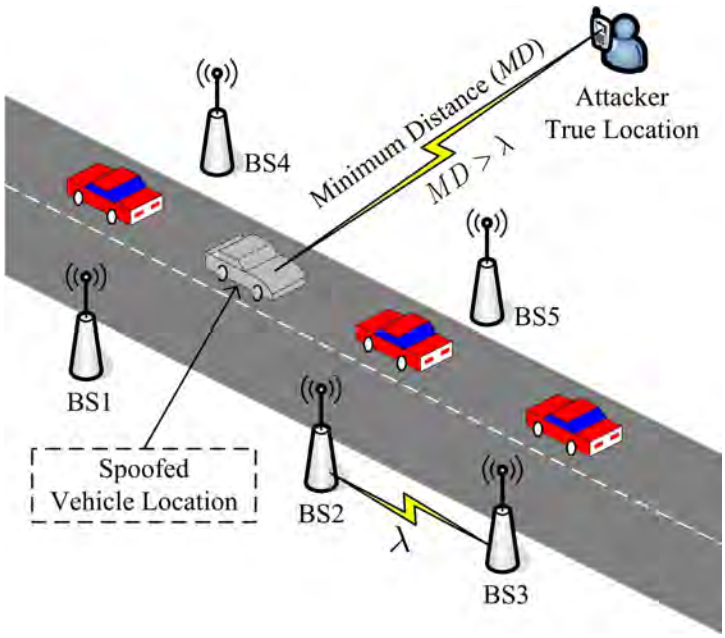

Figure 2.2: Illustration of the Minimum Distance (MD) threat model.

malicious user can set its transmit power. We do *not* allow an adversary to set multiple beams to different BSs via colluding malicious users (see later discussion).

The threat model we adopt can be applied to any true/spoofed location pair. The sole purpose of an attacker is to circumvent the LVS and thus be accepted as a legitimate user. This is in spite of the fact that the attacker's claimed position (provided to the LVS) and true position are significantly different. However, as the spoofed location approaches the true location, our detection rate will approach zero (as expected for any verification system). As such, in the following we will make the assumption that the true position of an attacker is some minimum distance (MD) from the spoofed position. We henceforth refer to our generic threat model as the MD threat model, a schematic of which is given in Fig. 2.2. In this scenario it is assumed the BSs that form the infrastructure part of the VANET, are placed alongside the highway (or on overhanging structures along the highway). This represents a realistic expectation for the physical deployment architecture for VANETs that is emerging from the ITS community. The scenario illustrated in Fig. 2.2 represents a generic

attack on an LVS from a malicious user, who can be stationary (e.g., a user within a building) or mobile on a different road.

Based on the log-normal propagation model [87], h_0 in (2.1) can be specified as (in the equations to follow we ignore some constants)

$$h_0(\mathbf{x}_i, \mathbf{x}_c, \omega) = -10\gamma \log_{10}(d_i^c) + \omega, \tag{2.11}$$

where γ is the path loss exponent, ω (in dB) is a zero-mean normal random variable with variance σ_{dB}^2, and d_i^c is the Euclidean distance from the i-th BS to the user's claimed location $\mathbf{x}_c$, which is given by

$$d_i^c = d(\mathbf{x}_c, \mathbf{x}_i) = \sqrt{(u_c - u_i)^2 + (v_c - v_i)^2}. \tag{2.12}$$

A malicious user can adjust his transmit power to impact the measurements collected by the BSs, thus h_1 in (2.1) can be expressed as

$$h_1(\mathbf{x}_i, \mathbf{x}_c, \mathbf{x}_t, \omega) = p_x - 10\gamma \log_{10}\left(d_i^t\right) + \omega, \tag{2.13}$$

where p_x is the additional transmit power (relative to the legitimate user's transmit power) boosted by the malicious user, and $d_i^t = d(\mathbf{x}_t, \mathbf{x}_i)$ is the Euclidean distance from the i-th BS to the user's true location $\mathbf{x}_t = (u_t, v_t)$. Assuming all M_i's are independent from each other, the likelihood function $p(\mathbf{m}|\mathcal{H}_0)$ can be expressed as

$$p(\mathbf{m}|\mathcal{H}_0) = \prod_{i=1}^{K} p(m_i|\mathcal{H}_0) = \prod_{i=1}^{K} \frac{1}{\sqrt{2\pi}\sigma_{dB}} \exp\left(\frac{-\left(m_i - \mu_i^c\right)^2}{2\sigma_{dB}^2}\right), \tag{2.14}$$

where

$$\mu_i^c = -10\gamma \log_{10}(d_i^c). \tag{2.15}$$

Moreover, the pdf of $\mathbf{m}$ conditional on $\mathbf{x}_t$ under $\mathcal{H}_1$, $p(\mathbf{m}|\mathbf{x}_t, \mathcal{H}_1)$, can be written as

$$p(\mathbf{m}|\mathbf{x}_t, \mathcal{H}_1) = \prod_{i=1}^{K} p(m_i|\mathbf{x}_t, \mathcal{H}_1) = \prod_{i=1}^{K} \frac{1}{\sqrt{2\pi}\sigma_{dB}} \exp\left(\frac{-\left(m_i - p_x + 10\gamma \log_{10}(d_i^t)\right)^2}{2\sigma_{dB}^2}\right). \tag{2.16}$$

A malicious user will utilize p_x in an attempt to impact the measurements collected by the BSs in order to avoid detection. We now discuss how to determine the 'optimal'

value of p_x from a malicious user's point of view. An LVS can be totally spoofed if the measurements collected from a malicious user follow exactly $p(\mathbf{m}|\mathcal{H}_0)$, which is given by (2.14). Therefore, in order to avoid detection a malicious user attempts to minimize the difference between $p(\mathbf{m}|\mathcal{H}_0)$ and $p(\mathbf{m}|\mathbf{x}_t, \mathcal{H}_1)$. This difference can be quantified through the Kullback-Leibler (KL)-divergence from $p(\mathbf{m}|\mathbf{x}_t, \mathcal{H}_1)$ to $p(\mathbf{m}|\mathcal{H}_0)$, which is defined as follows [88]

$$\begin{aligned} D_{KL}(p(\mathbf{m}|\mathbf{x}_t, \mathcal{H}_1)||p(\mathbf{m}|\mathcal{H}_0)) &= \int p(\mathbf{m}|\mathbf{x}_t, \mathcal{H}_1) \ln \frac{p(\mathbf{m}|\mathbf{x}_t, \mathcal{H}_1)}{p(\mathbf{m}|\mathcal{H}_0)} d\mathbf{m} \\ &= \sum_{i=1}^{K} \frac{\left(\mu_i^c - \mu_i^t - p_x\right)^2}{2\sigma_{dB}^2}, \end{aligned} \tag{2.17}$$

where

$$\mu_i^t = -10\gamma \log_{10}\left(d_i^t\right). \tag{2.18}$$

We note the fact that the relation between mutual information and KL-divergence can be written as $I(X;Y) = D_{KL}\left(P(X,Y)||P(X)P(Y)\right)$, where $P(X)$ and $P(Y)$ are the two marginal probability distributions obtained from the joint probability distribution $P(X,Y)$. This KL-divergence is the information loss when $p(\mathbf{m}|\mathcal{H}_0)$ is used to approximate $p(\mathbf{m}|\mathbf{x}_t, \mathcal{H}_1)$, and it becomes zero *if and only if* the two distributions are identical. From an information-theoretic point of view, the optimal value of p_x can be expressed as

$$p_x^* = \arg\min_{p_x} D_{KL}\left(p(\mathbf{m}|\mathbf{x}_t, \mathcal{H}_1)||p(\mathbf{m}|\mathcal{H}_0)\right) = \frac{1}{K}\sum_{i=1}^{K}\left(\mu_i^c - \mu_i^t\right). \tag{2.19}$$

We note that in (2.19) μ_i^c is a function of the malicious user's claimed location, and μ_i^t is a function of the malicious user's true location. As such, the malicious user optimizes his transmit power (equivalently, p_x) to compensate the path loss difference between his claimed location and his true location. However, it is important to emphasize that we have taken a conservative approach (worst case scenario) within our threat model, in which we have assumed the malicious user is in the possession of critical information which in practice will be quite difficult for him to obtain.

For example, the malicious user has to know the locations of all BSs, the path loss exponent to BSs, and the legitimate user's transmit power in order to optimize p_x. It is therefore unlikely in practice that the attacker can fully optimize the p_x as given by (2.19), making him even more likely to be detectable. Setting $p_x = p_x^*$ in (2.13), h_1 can be rewritten as

$$h_1(\mathbf{x}_i, \mathbf{x}_c, \mathbf{x}_t, \omega) = \bar{\mu}^c - \bar{\mu}^t - 10\gamma \log_{10}\left(d_i^t\right) + \omega, \tag{2.20}$$

where

$$\bar{\mu}^c = \frac{1}{K}\sum_{i=1}^{K} \mu_i^c, \text{ and } \bar{\mu}^t = \frac{1}{K}\sum_{i=1}^{K} \mu_i^t. \tag{2.21}$$

Although $\mathbf{x}_t$ is a known deterministic parameter for a malicious user, it is unknown for the network. This means h_1 is still unknown, and therefore the likelihood function $p(\mathbf{m}|\mathcal{H}_1)$ is unknown for the LVS in our MD threat model. To make progress, we will present some approximations of our MD threat model within which $p(\mathbf{m}|\mathcal{H}_1)$ becomes known. Although these approximations are not adopted in the MD threat model, they do allow for additional insight and analytical clarity. We will also show how the optimal threshold derived for the MD threat model is effectively the same as the optimal threshold derived under some of the simplifying approximations.

2.4.2 Far Field Approximation

In this subsection we propose the deployment of our LVS within a threat model where the Far Field Approximation (FFA) is made, meaning that the malicious user's distance from the highway is far enough that we can assume all RSS mean values received by all K BSs are equal. Although never achieved in practice this simplification will allow us some initial insights into the performance of the LVS. Under the FFA we can take the distance of a malicious user's true location to every BS to be approximated as a constant, i.e., $d_i^t = d(\mathbf{x}_t, \mathbf{x}_i) \cong constant, \forall i \in [1, 2, \ldots, K]$. Therefore, we will assume

$$\frac{1}{K}\sum_{i=1}^{K} 10\gamma \log_{10}\left(d_i^t\right) = 10\gamma \log_{10}\left(d_i^t\right). \tag{2.22}$$

Substituting (2.22) into (2.20), h_1 under the FFA can be expressed as

$$h_1\left(\mathbf{x}_i, \mathbf{x}_c, \omega\right) = \bar{\mu}^c + \omega. \tag{2.23}$$

Then, $p(\mathbf{m}|\mathcal{H}_1)$ (which now does not depend on $\mathbf{x}_t$) can be written as

$$p(\mathbf{m}|\mathcal{H}_1) = \prod_{i=1}^{K} \frac{1}{\sqrt{2\pi}\sigma_{dB}} \exp\left(\frac{-\left(m_i - \bar{\mu}^c\right)^2}{2\sigma_{dB}^2}\right). \tag{2.24}$$

Based on (2.6), (2.14), and (2.24), we construct the decision rule

$$\Lambda\left(\mathbf{m}\right) = \frac{\exp\left(\frac{-\sum_{i=1}^{K}(m_i-\bar{\mu}^c)^2}{2\sigma_{dB}^2}\right)}{\exp\left(\frac{-\sum_{i=1}^{K}(m_i-\mu_i^c)^2}{2\sigma_{dB}^2}\right)} \underset{\mathcal{D}_0}{\overset{\mathcal{D}_1}{\gtrless}} T_\Lambda. \tag{2.25}$$

In order to determine α and β analytically, (2.25) can be rewritten as

$$\digamma\left(\mathbf{m}\right) \underset{\mathcal{D}_0}{\overset{\mathcal{D}_1}{\gtrless}} \Gamma, \tag{2.26}$$

where

$$\digamma\left(\mathbf{m}\right) = \sum_{i=1}^{K} m_i(\bar{\mu}^c - \mu_i^c), \tag{2.27}$$

and

$$\Gamma = \frac{1}{2}\left(2\sigma_{dB}^2 \ln T_\Lambda - \sum_{i=1}^{K}\left((\mu_i^c)^2 - (\bar{\mu}^c)^2\right)\right). \tag{2.28}$$

Given (2.14) and (2.26), we have

$$p\left(\digamma\left(\mathbf{m}\right)|\mathcal{H}_0\right) = \mathcal{N}\left(\sum_{i=1}^{K}\mu_i^c\left(\bar{\mu}^c - \mu_i^c\right), \sum_{i=1}^{K}\left(\bar{\mu}^c - \mu_i^c\right)^2\sigma_{dB}^2\right), \tag{2.29}$$

where $\mathcal{N}(a, b)$ represents a normal distribution with a and b as the mean and variance, respectively. Likewise, given (2.24) and (2.26), we have

$$p\left(\digamma\left(\mathbf{m}\right)|\mathcal{H}_1\right) = \mathcal{N}\left(\sum_{i=1}^{K}\bar{\mu}^c\left(\bar{\mu}^c - \mu_i^c\right), \sum_{i=1}^{K}\left(\bar{\mu}^c - \mu_i^c\right)^2\sigma_{dB}^2\right). \tag{2.30}$$

The false positive and detection rates under the FFA can now be expressed analytically as

$$\alpha = P(\Lambda(\mathbf{m}) > T_\Lambda|\mathcal{H}_0) = P(\digamma(\mathbf{m}) > \Gamma|\mathcal{H}_0) = \mathcal{Q}\left(\frac{\Gamma - \sum_{i=1}^{K} \mu_i^c \left(\bar{\mu}^c - \mu_i^c\right)}{\sqrt{\sum_{i=1}^{K} \left(\bar{\mu}^c - \mu_i^c\right)^2 \sigma_{dB}^2}}\right), \quad (2.31)$$

$$\beta = P(\Lambda(\mathbf{m}) > T_\Lambda|\mathcal{H}_1) = P(\digamma(\mathbf{m}) > \Gamma|\mathcal{H}_1) = \mathcal{Q}\left(\frac{\Gamma - \sum_{i=1}^{K} \bar{\mu}^c \left(\bar{\mu}^c - \mu_i^c\right)}{\sqrt{\sum_{i=1}^{K} \left(\bar{\mu}^c - \mu_i^c\right)^2 \sigma_{dB}^2}}\right), \quad (2.32)$$

where $\mathcal{Q}(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty \exp^{-t^2/2}\, dt$.

Having determined α and β under the FFA, we can use these in (2) for the conditional entropy $H(X|Y)$. The value of Γ which maximizes $I(X;Y) = H(X) - H(X|Y)$, denoted as Γ^*, can be determined numerically. Using (2.28), the T_Λ^* can be determined by Γ^*. Then, the decision rule in (2.10) which leads to the optimal verification algorithm under the FFA can be formed, where $\Lambda(\mathbf{m})$ is specified in (2.25).

We verify the false positive and detection rates, given by (2.31) and (2.32), respectively, via detailed Monte Carlo simulations. The simulation settings are chosen so as to mimic a location verification test over an area spanning the intersection of several major freeways. The settings are detailed as follows.

- The K BSs are randomly distributed in a $200m \times 200m$ square area, $4 \leq K \leq 10$.
- The claimed locations of legitimate and malicious users are the same, which is $\mathbf{x}_c = [0, 0]$.
- The legitimate users are at $\mathbf{x}_c$. The malicious users are far away from $\mathbf{x}_c$, which in practice means the measurements collected are generated according to (2.23).
- Each BS collects L measurements from each user.

In the following, the simulation results are obtained through 10,000 Monte Carlo realizations of the measurement vector $\mathbf{M}$, and in all the specific results shown we have adopted the prior probability $P_0 = 0.9$, and the path loss exponent $\gamma = 3$. Also

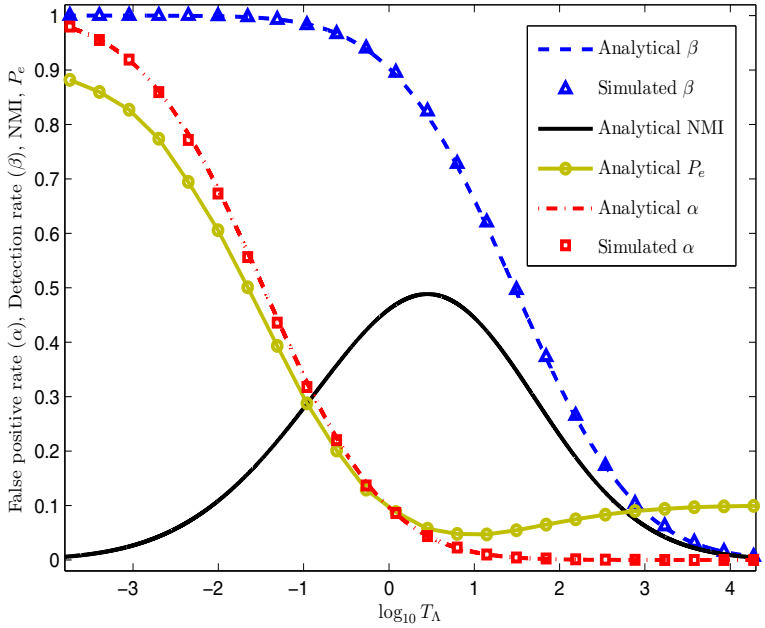

Figure 2.3: Analytical and simulated α, β, Normalized Mutual Information (NMI), and the probability of misclassification (P_e) versus T_Λ, where $K = 10$, $L = 1$, and $\sigma_{dB} = 5$.

note, we denote the Normalized Mutual Information (NMI) as

$$\text{NMI} = I(X;Y)/H(X). \tag{2.33}$$

In Fig. 2.3, the analytical α and β are directly derived from (2.31) and (2.32), respectively, and the analytical NMI is calculated using (2.3), (2.31), (2.32), and (2.33). In order to obtain the simulated α, we randomly generate $\mathbf{M}$ according to (2.11), from which we get a specific realization of $\Lambda(\mathbf{m})$, and for each value of T_Λ we decide whether the user is legitimate or malicious by (2.25). To obtain the simulated β, we randomly generate $\mathbf{M}$ according to (2.23), and follow the same procedure as above for α. The simulated NMI is calculated using (2.3) and (2.33) by adopting the simulated α and β. In Fig. 2.3 we have set $K = 10$, $L = 1$, and $\sigma_{dB} = 5$. From Fig. 2.3, we can see that the comparison between simulation and analysis shows excellent agreement, which verifies the analysis we have provided under the FFA. As we can see from Fig. 2.3, relatively high false positive rates are found at low thresholds. This is a consequence of the LVS operating at a point far from the optimal threshold.

In Fig. 2.3 we can find that the value of the threshold, T_Λ, that maximizes the NMI (solid curve) is given by $\log_{10} T_\Lambda = 0.45$. The false positive rate (dash-dotted curve) corresponding to $\log_{10} T_\Lambda = 0.45$ is given by $\alpha \approx 0.044$. This strong dependence on the threshold (also seen in all our other results), re-emphasizes the critical importance of always operating the LVS at the optimal threshold.

In Fig. 2.3 we also present the probability of misclassification, P_e, which is defined as $P_e = P_0\alpha + (1 - P_0)(1 - \beta)$. Note that the optimal threshold determined by the NMI method is given by $\log_{10} T_\Lambda = 0.45$ (set by the *maximum* value of NMI) and the optimal threshold determined by the P_e method is given by $\log_{10} T_\Lambda = 0.95$ (set by the *minimum* value of P_e). Both these values occur in a region where the false positive rate is approximately flat, but where the detection rate is steep. Due to this, relative to the P_e method, the NMI method results in a ~ 0.25 improvement in the detection rate at the cost of only a ~ 0.01 degradation in the false positive rate. Such results are typical of a comparison between the two methods, but to a large extent do not quantify the main benefits of NMI over the P_e method. The real practical benefits of the NMI method over other traditional methods can best be summarized as: (i) no subjective determination of the false positive rate required, (ii) no predetermined costs required, and (iii) less sensitivity to the unknown *a priori* probability that the user is legitimate. These practical advantages are discussed in more details in Section 2.5.2.

Fig. 2.4 plots β and NMI versus α for different values of P_0. Based on (2.31) and (2.32), we note that β is independent of P_0. We observe that for different values of P_0 the curves for NMI are maximized at different values of α. For example, for $P_0 = 0.9$ the NMI is maximized when $\alpha = 0.044$ (and where $\beta = 0.816$). With the α and β (that maximize NMI) determined, we can then set the optimal threshold in the binary decision rule.

We have investigated a range of other values of K, L, and σ_{dB}. Some of these results are presented in Fig. 2.5, where the maximum NMI is shown as a function of σ_{dB} for different values of K. In Fig. 2.5, we first observe that the simulations precisely

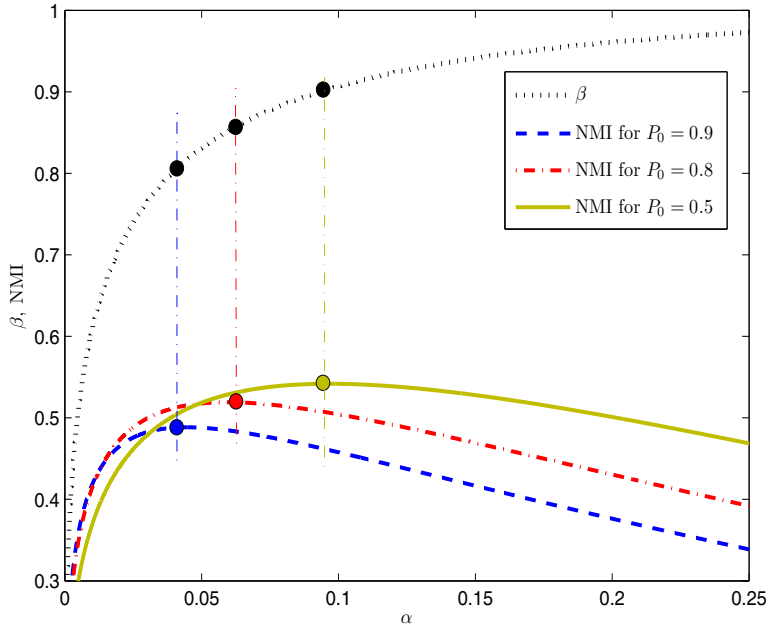

Figure 2.4: Detection rate and Normalized Mutual Information (NMI) versus α for different values of P_0, where $K = 10$, $L = 1$, and $\sigma_{dB} = 5$.

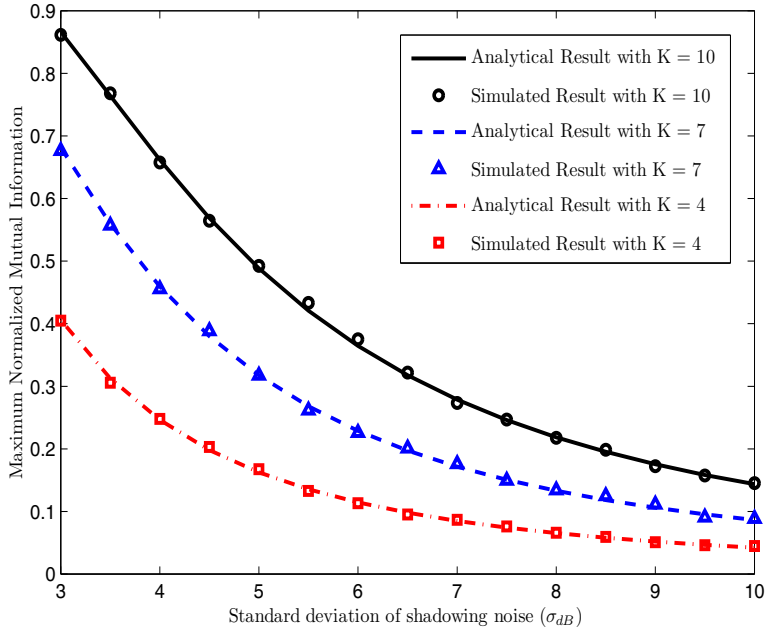

Figure 2.5: Maximum Normalized Mutual Information (NMI) versus σ_{dB} for different values of K, where $L = 1$.

match the analytical results. As expected, we also observe that the maximum NMI increases as K increases, and the maximum NMI decreases as σ_{dB} increases. In practice, RSS values are obtained by averaging multiple received symbols over time or frequency. This leads to that the effect of small-scale fading is negligeable in RSS observation model. In the simulations of Fig. 2.5 we have assumed that such averaging has been done sufficiently well that the impact of the small-scale fading and the receiver SNR can be neglected. However, it is important to understand that as the path loss increases, the amount of averaging symbols must increase if the receiver SNR is to remain unimportant. Ultimately, when the path loss becomes large enough, the ratio of the SNR receiver noise to the shadowing noise increases, and as this ratio grows the verification performance of the system degrades.

2.4.3 Uniformly Distributed Approximation

In this subsection we propose the Uniformly Distributed Approximation (UDA), where the malicious users are assumed to be uniformly distributed on a circle. Again, although never achievable in practice this simplification will allow us additional insights. More specifically, the malicious user's true location is uniformly distributed on a circle, whose radius and center are R and $\mathbf{x}_c$, respectively, where $R > r$ and $r = \max(d_i^c)$.

The main purpose of this model is to commence our probe of how reliable the use of the FFA will be when its assumptions are violated. To this end, we note that if the maximum mean difference between any two measurements collected from a malicious user, M_i and M_j $(i \neq j)$, is no larger than σ_{dB}, the scale R at which this occurs provides a *natural* distance at which we could anticipate the FFA and the UDA to be approximately equivalent. To quantify this let us introduce $\rho \triangleq R/r$. Under the UDA, the mean difference between M_i and M_j can be written as

$$\mathbb{E}\left[|M_i - M_j|\right] = \left|10\gamma \log_{10}\left(d_i^t\right) - 10\gamma \log_{10}\left(d_j^t\right)\right|. \tag{2.34}$$

Given that for a malicious user, we have $|d_i^t - d_j^t| \leq 2r$ and $d_i^t \geq R - r$, we can write

(2.34) as

$$\mathbb{E}\left[|M_i - M_j|\right] \leq \frac{10\gamma}{\ln 10} \ln\left(\frac{d_i^t + 2r}{d_i^t}\right) \leq \frac{10\gamma}{\ln 10} \ln\left(1 + \frac{2r}{R-r}\right), \tag{2.35}$$

where without loss of generality we have assumed $d_j^t > d_i^t$. In order to guarantee the required constraint, $\max \mathbb{E}\left[|M_i - M_j|\right] \leq \sigma_{dB}$, we should have

$$\frac{10\gamma}{\ln 10} \ln\left(1 + \frac{2r}{R-r}\right) \leq \sigma_{dB}, \tag{2.36}$$

which results in

$$\rho \geq \rho^* \triangleq \frac{2}{\exp\left\{\frac{\sigma_{dB} \ln 10}{10\gamma}\right\} - 1} + 1, \tag{2.37}$$

where $\rho^\star$ is a reference value that will be utilized when comparison under the FFA is made. Such a comparison is achieved by using the FFA decision rule in (2.25) but under the UDA. In such a set up we would anticipate that the optimal thresholds under the FFA and UDA would be very similar at ρ^*.

To proceed with a comparison under the FFA and UDA, we conduct Monte Carlo simulations. In these simulations, although $p(\mathbf{m}|\mathcal{H}_0)$ given by (2.14) is used, the likelihood function $p(\mathbf{m}|\mathcal{H}_1)$, which is given by

$$p(\mathbf{m}|\mathcal{H}_1) = \int p(\mathbf{m}|\mathbf{x}_t, \mathcal{H}_1) p(\mathbf{x}_t|\mathcal{H}_1) d\mathbf{x}_t, \tag{2.38}$$

must be determined numerically. The other simulation settings are the same as that under the FFA, except the malicious users are uniformly distributed on a circle, whose radius and center are R and $\mathbf{x}_c$, respectively. The measurements collected from the legitimate and malicious users are generated according to (2.11) and (2.20), respectively. To obtain the true numerical NMI under the UDA, we use (2.14) and (2.38) to calculate $p(\mathbf{m}|\mathcal{H}_0)$ and $p(\mathbf{m}|\mathcal{H}_1)$, respectively, and utilize (2.7) as the decision rule. To simulate the NMI obtained from the use of the FFA decision rule (but under the UDA) we use (2.14) and (2.24) in order to implement the decision rule in (2.25).

From our results, shown in Fig. 2.6, we can see that at values of $\rho << \rho^*$ the optimal thresholds (the values of T_Λ which maximize the NMI) for the two cases are

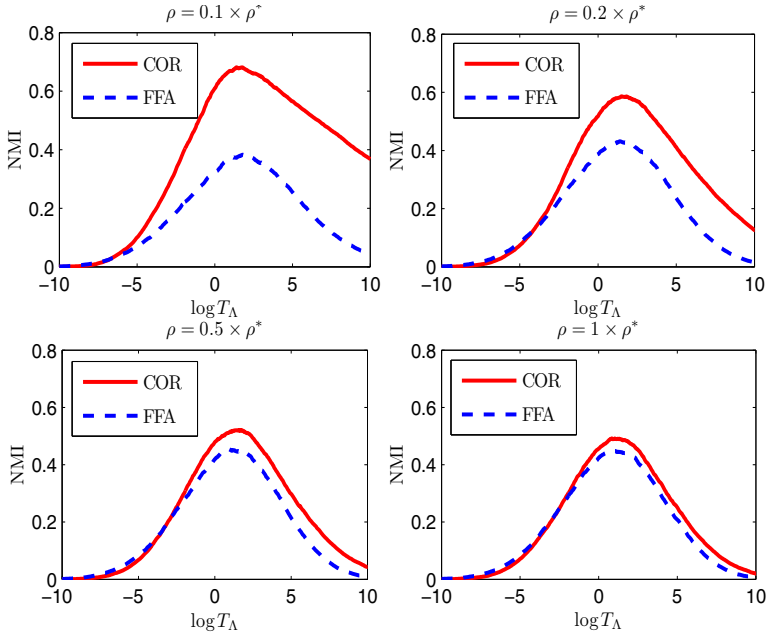

Figure 2.6: NMI versus T_Λ for different values of ρ, where $K = 10, L = 1$, $\sigma_{dB} = 5$, and $\rho^* = 5.275$. The solid curves (COR curves) represent the NMI achieved under the correct decision rule (2.7). The dashed curves (FFA curves) represent the NMI achieved under the FFA decision rule (2.25).

very different. However, as $\rho \to \rho^*$ the optimal threshold obtained under blindly adopting the FFA decision rule (even though the malicious user is not at infinity) is effectively the optimal value. Note also, the maximum values of the two NMIs and the corresponding T_Λ^* are coincident when $\rho = \rho^*$, which verifies that the reference value of ρ presented in (2.37) is reasonable.

2.4.4 Laplace Approximation in MD Threat Model

In this subsection we implement the optimal location verification algorithm under our adopted threat model - the MD threat model. We will assume that $MD > \lambda$, where λ is the mean separation distance between BSs. Pragmatically, this assumption also means that, in effect, the attacker will be placed at some minimum distance *off the highway*, since we find that if he is on the highway, he is trivially detectable for $MD > \lambda$. A malicious user (vehicle) on the highway claiming to be at a position

which is at $MD > \lambda$, must boost its transmissions significantly. However, since the user is on the actual highway, the nearest BS to its true location will easily detect an attack. This is confirmed by our analysis, and as such we will henceforth consider the attacker to be sophisticated enough to realize that to have any reasonable chance of remaining undetected he must launch his attacks from a position at some minimum distance from the closest BS of the VANET (e.g., off the highway). More generally, the value of MD in our threat model is set as $MD = \lambda/a$, where a is a constant that sets the scale for which an attacker on the highway is trivially detected. For λ's anticipated for ITS infrastructures say we find from simulations $a \approx 2$. However for simplicity, we henceforth adopt $a = 1$.

In our MD threat model $p(\mathbf{x}_t|\mathcal{H}_1)$ is assumed to be uniform over the annulus formed by two concentric circles, whose finite radii are R_1 and R_2 ($R_1 < R_2$), respectively, and whose mutual center is $\mathbf{x}_c$. The use of an annulus setting allows us to cover more general settings (beyond just single highways/freeways) such as freeway intersection regions where the the freeways can have multiple directions. In any scenario (single or intersecting roads) it will be assumed that the malicious user will not enter into any region (we assume the malicious users knows the locations of all BSs) where he is less than some distance R_1 from any of the VANET's infrastructure BSs (see footnote 2). This implies $p(\mathbf{x}_t|\mathcal{H}_1) = 1/\pi(R_2^2 - R_1^2)$, where $\mathbf{x}_t \in \{\mathbf{x}_t|R_1^2 \leq (u_t - u_c)^2 + (v_t - v_c)^2 \leq R_2^2\}$. Under this model, $p(\mathbf{m}|\mathcal{H}_0)$ is also the same as in (2.14), and $p(\mathbf{m}|\mathcal{H}_1)$ is as given in (2.38) but with the modified prior distribution. Again, no closed form solution is available for (2.38).

We present new Monte Carlo simulations where the settings are again the same as that under the FFA, except that now the malicious users are uniformly distributed in the annulus. Again, the measurements collected from the legitimate and malicious users are generated according to (2.11) and (2.20), respectively. To obtain the true numerical NMI under the MD threat model, we use (2.14) and (2.38) to calculate $p(\mathbf{m}|\mathcal{H}_0)$ and $p(\mathbf{m}|\mathcal{H}_1)$, respectively, and utilize (2.7) as the decision rule. To simulate the NMI obtained from the use of the FFA decision rule (but under the MD threat

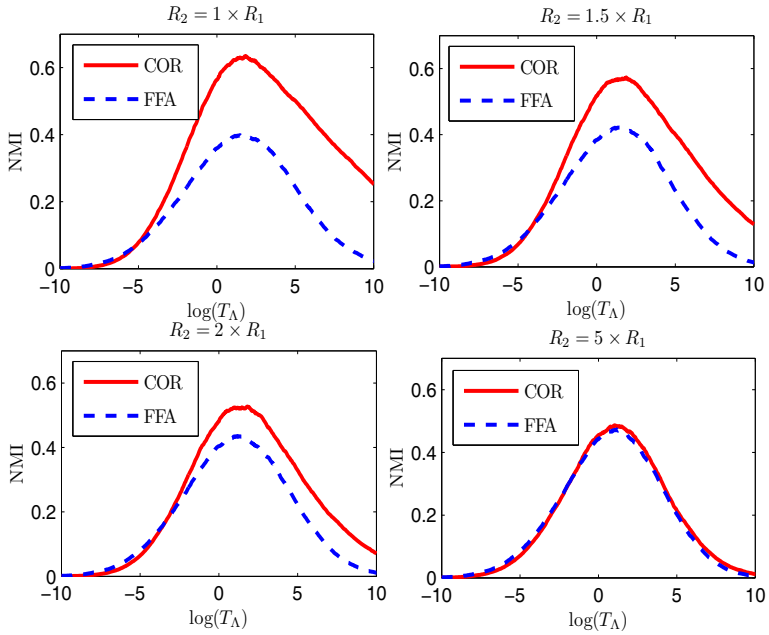

Figure 2.7: Numerical and IFA approximated NMI versus T_Λ for different values of R_2, where $\rho^* = 5.275, \rho = 0.2 \times \rho^*$, and $\sigma_{dB} = 5$. The solid curves (COR curves) represent the NMI achieved under the correct decision rule (2.7). The dashed curves (FFA curves) represent the NMI achieved under the FFA decision rule (2.25).

model) we use (2.14) and (2.24) in order to implement the decision rule in (2.25). The results of our simulations are shown in Fig. 2.7, where $\rho = 0.2\rho^*$, and ρ is redefined as $\rho = R_1/r$.

In the top left plot of Fig. 2.7, we have set $R_2 = R_1$, so in this specific plot the MD threat model is equivalent to that under the UDA (the result is the same as that shown in the top right plot of Fig. 2.6). However, again we see that as R_2 increases the optimal threshold obtained under blindly adopting the FFA decision rule (even though the malicious users are constrained within an annulus) is effectively the optimal value. Note also, that in the MD threat model, as R_2 increases this results holds for cases when $\rho << \rho^*$ (which was not the case under the UDA).

As a final point, we note that instead of numerically solving (2.38), it may be useful to find an approximate closed-form solution to (2.38) (e.g., this would allow for an approximate closed-form for the false positive and detection rates under this

threat model). We can approximate $p(\mathbf{m}|\mathcal{H}_1)$ via an application of the Laplace approximation, which can approximate integrals through a series expansion by using local information about the integrand around its maximum [89, 90]. The details are as follows. First, let us define a quantity as

$$h\left(\mathbf{x}_t|\mathcal{H}_1\right) \triangleq \ln\left(p\left(\mathbf{m}|\mathbf{x}_t,\mathcal{H}_1\right)p\left(\mathbf{x}_t|\mathcal{H}_1\right)\right). \tag{2.39}$$

In fact, $h\left(\mathbf{x}_t|\mathcal{H}_1\right)$ can be expanded using a Taylor series around its MAP estimate, denoted by $\widehat{\mathbf{\Theta}} = \arg\max_{\mathbf{x}_t}\{p(\mathbf{m}|\mathbf{x}_t,\mathcal{H}_1)p(\mathbf{x}_t|\mathcal{H}_1)\}$. This is the point where the posterior density is maximized, i.e., the mode of the posterior distribution. Hence, we obtain

$$\begin{aligned} h\left(\mathbf{x}_t|\mathcal{H}_1\right) = h\left(\widehat{\mathbf{\Theta}}|\mathcal{H}_1\right) + \left(\mathbf{x}_t-\widehat{\mathbf{\Theta}}\right)^T \underbrace{\frac{\partial h\left(\widehat{\mathbf{\Theta}}|\mathcal{H}_1\right)}{\partial \mathbf{x}_t}}_{(=0)\text{ at MAP location}} \\ +\frac{1}{2}\left(\mathbf{x}_t-\widehat{\mathbf{\Theta}}\right)^T \frac{\partial^2 h\left(\widehat{\mathbf{\Theta}}|\mathcal{H}_1\right)}{\partial^2 \mathbf{x}_t}\left(\mathbf{x}_t-\widehat{\mathbf{\Theta}}\right). \end{aligned} \tag{2.40}$$

The second term in (2.40) is zero, because the first derivative is zero at the maximum of $h\left(\mathbf{x}_t|\mathcal{H}_1\right)$. Replacing $h\left(\mathbf{x}_t|\mathcal{H}_1\right)$ by the truncated second-order Taylor series yields

$$h\left(\mathbf{x}_t|\mathcal{H}_1\right) \approx h\left(\widehat{\mathbf{\Theta}}|\mathcal{H}_1\right) + \frac{1}{2}\left(\mathbf{x}_t-\widehat{\mathbf{\Theta}}\right)^H \mathbf{H}\left(\mathbf{x}_t-\widehat{\mathbf{\Theta}}\right), \tag{2.41}$$

where $\mathbf{H}$ is the Hessian of the ln posterior, evaluated at $\widehat{\mathbf{\Theta}}$:

$$\mathbf{H} \triangleq \left.\frac{\partial^2 h\left(\widehat{\mathbf{\Theta}}|\mathcal{H}_1\right)}{\partial^2 \mathbf{x}_t}\right|_{\mathbf{x}_t=\widehat{\mathbf{\Theta}}} = \left.\frac{\partial^2 h\left(\mathbf{x}_t|\mathcal{H}_1\right)}{\partial \mathbf{x}_t \partial \mathbf{x}_t^H}\right|_{\mathbf{x}_t=\widehat{\mathbf{\Theta}}}. \tag{2.42}$$

Using the above approximation, we have

$$\begin{aligned} \ln p\left(\mathbf{m}|\mathcal{H}_1\right) &= \ln \int p\left(\mathbf{m}|\mathbf{x}_t,\mathcal{H}_1\right)p\left(\mathbf{x}_t|\mathcal{H}_1\right)d\mathbf{x}_t \\ &= \ln \int \exp^{h\left(\mathbf{x}_t|\mathcal{H}_1\right)} d\mathbf{x}_t \\ &\approx \ln \int \exp^{h\left(\widehat{\mathbf{\Theta}}|\mathcal{H}_1\right)+\frac{1}{2}\left(\mathbf{x}_t-\widehat{\mathbf{\Theta}}\right)^T\mathbf{H}\left(\mathbf{x}_t-\widehat{\mathbf{\Theta}}\right)} d\mathbf{x}_t \\ &= h\left(\widehat{\mathbf{\Theta}}|\mathcal{H}_1\right) + \ln \int \exp^{\frac{1}{2}\left(\mathbf{x}_t-\widehat{\mathbf{\Theta}}\right)^T\mathbf{H}\left(\mathbf{x}_t-\widehat{\mathbf{\Theta}}\right)} d\mathbf{x}_t \\ &= h\left(\widehat{\mathbf{\Theta}}|\mathcal{H}_1\right) + \frac{1}{2}\ln\left|2\pi\mathbf{H}\right| \\ &= \ln p\left(\widehat{\mathbf{\Theta}}|\mathcal{H}_1\right) + \ln p\left(\mathbf{m}|\widehat{\mathbf{\Theta}},\mathcal{H}_1\right) + \ln\left|2\pi\mathbf{H}^{-1}\right|^{1/2}. \end{aligned} \tag{2.43}$$

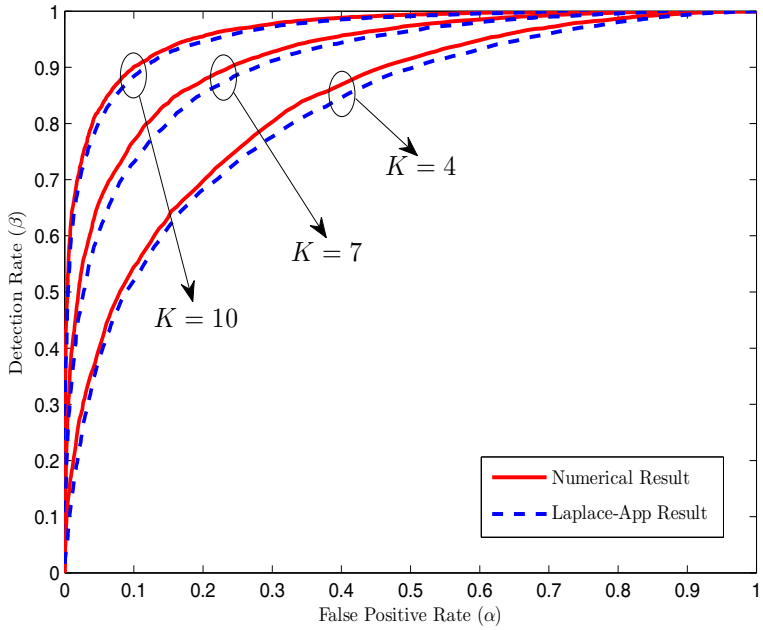

Figure 2.8: Numerical and Laplace approximated ROC curves for different values of K, where $\sigma_{dB} = 5, L = 1, R_1 = 100\text{m}$, and $R_2 = 500\text{m}$.

Finally, the marginal likelihood estimate can be written as

$$\widehat{p}\left(\mathbf{m}|\mathcal{H}_1\right) = p\left(\widehat{\boldsymbol{\Theta}}|\mathcal{H}_1\right) p\left(\mathbf{m}|\widehat{\boldsymbol{\Theta}}, \mathcal{H}_1\right) \left|2\pi\mathbf{H}^{-1}\right|^{1/2}. \tag{2.44}$$

In (2.44), $p\left(\widehat{\boldsymbol{\Theta}}|\mathcal{H}_1\right)$ and $|2\pi\mathbf{H}^{-1}|^{1/2}$ are both constant for a specific $\widehat{\boldsymbol{\Theta}}$; thus the Laplace approximated likelihood function, $\widehat{p}\left(\mathbf{m}|\mathcal{H}_1\right)$, is a K dimensional normal distribution with the same variance as $p(\mathbf{m}|\mathcal{H}_0)$ (because the variances of $p(\mathbf{m}|\mathcal{H}_0)$ and $p(\mathbf{m}|\mathbf{x}_t, \mathcal{H}_1)$ are the same). Under the Laplace approximation the decision rule in (2.7) is approximated by

$$\widehat{\Lambda}\left(\mathbf{m}\right) = \frac{\widehat{p}\left(\mathbf{m}|\mathcal{H}_1\right)}{p\left(\mathbf{m}|\mathcal{H}_0\right)} \underset{\mathcal{D}_0}{\overset{\mathcal{D}_1}{\gtrless}} T_\Lambda. \tag{2.45}$$

To study the performance our Laplace approximation we calculate ROC curves for both the numerical Monte Carlo calculation of $p(\mathbf{m}|\mathcal{H}_1)$ and the Laplace approximation of $p(\mathbf{m}|\mathcal{H}_1)$. These different forms are then used in the same decision rule (2.7) in order to form the ROC curves. The results of these simulations are shown in Fig. 2.8, and as we can see the approximation is a good one for the parameters used.

We have further investigated the accuracy of the approximation over a range of other parameters, finding similar results to those shown in Fig. 2.8.

2.5 Discussion and Results in Relation to Bayesian Frameworks

2.5.1 Discussion

In the preceding sections we have looked at a general attack scenario under specific threat models. The attack scenario we have focussed on is that of a non-colluding adversary who is attempting to spoof he is within the perimeter of some wireless network, when in reality he is some distance beyond the network boundary. A non-colluding adversary who is within the network region will be in general easily identified due to his inability to set different RSS values at different BSs. An attack from outside the network region is the perhaps most realistic and likely scenario one can imagine for the emerging ITS scenario. For example, a single adversary who is some distance from the highway (so as not to be easily identified or caught) is attempting to disrupt proper functioning of the ITS.

What we have shown through our investigations of specific threat models under our general attack scenario, is that an optimal LVS can be developed for each threat model, but in a non-straightforward manner in most cases - i.e., no closed-form solutions for the detection and false positive rates are available. Without such closed-form solutions for these rates, one must resort to complex and time consuming Monte Carlo simulations in order to determine the optimal threshold. However, from considerations of the FFA, and how other threat models can be approximated under the FFA, we have shown how a straightforward LVS algorithm can be deployed which is effectively optimal for most circumstances. More specifically, using analytical solutions for the detection and false positive rates in the FFA setting, which are then used in easily determining the optimal threshold value, a straightforward LVS is developed

whose performance is near-optimal when the adversary is close to the network, and optimal as the adversary moves to a large distance from the network.

However, of course more sophisticated attacks than those highlighted above are possible.[2] The most obvious of these is that of *colluding* adversaries who can communicate and cooperate with each other so as to form collective attacks on the LVS. An example of such an attack would be colluding adversaries who set different RSS values at different BSs. On the defensive side, the network could also deploy beamforming techniques to help the LVS thwart these types of attacks. The LVS could also deploy tracking algorithms and physical layer security techniques to assist in its defense. These more sophisticated forms of attacks and their corresponding defensive strategies will be exploited in the following chapters.

In our system model, we assumed zero calibration error in the measured RSS values at all the BSs. However, we note that the calibration error can exist in practice since a user may not be able to follow the calibration standard exactly due to hardware issues (e.g., transmit power fluctuations) or around interferences. We note that the impact of the calibration error can be examined through incorporating the calibration error in the shadowing noise (e.g., increasing the variance of the shadowing according to the scale of the calibration error). We conducted such examinations and our general result is that a percentage error of 15% in the variance of shadowing noise (i.e., σ_{dB}) leads to an approximately 10% percentage error in our normalized mutual information for the far field approximation. We also note that the variance of the calibration at different BSs may be different. This can result in biased errors in the RSS values observed at all the BSs, and thus can possibly decrease the detection performance of an LVS (e.g., increase the false positive rate).

[2]Throughout this thesis we will assume physical sabotage attacks (e.g., partially cover an antenna with RF-absorbant material) are not possible.

2.5.2 Results in Relation to Bayesian Frameworks

Location verification has been an active research area, and many verification algorithms have been proposed for VANETs (e.g., [36, 40, 42, 43, 75, 91–93]), WSNs (e.g., [4, 39]), and generic wireless networks (e.g., [5, 6, 8, 10, 25, 32, 37, 94, 95]).

Perhaps the most closely related works to ours are those which propose optimizing the system's threshold by minimizing the probability of misclassification (P_e) [8]. Of course, a direct comparison between such systems and ours is not entirely meaningful, due to the different optimization metrics being used. Further to this, it is important to note the complex interplay between the entropy of a random variable, $H(X)$, and the probability of misclassification. Although it may seem at first counter-intuitive, the fact is that there is not a one-to-one relationship between $H(X)$ and P_e. That is, two random variables with the same entropy can have different P_e [96]. This same issue extends to NMI and P_e, and in the context of our LVS, it is important to recognize this fact. As such, if optimization of P_e is the system objective, then use of a Bayesian framework, where the costs of all types of classifications are equal, will suffice.[3] But again we must stress that in the context of real-world LVS deployments this represents a strong *subjective* decision on the costs of misclassifications. Given the complexity, and the many different roles of location information within the ITS scenario (crash avoidance, vehicle-congestion avoidance, vehicle-to-vehicle communication protocols *etc.*), proper determination of misclassification costs will be, at best, extremely complex in nature. It is for this reason we have approached optimization of our LVS from an *objective* information-theoretic viewpoint. Our guiding light has been the well-known Infomax principle [97], which states an optimal system must transfer as much information as possible from its input to its output - i.e., maximize

[3] In a more general Bayesian framework, ignoring the costs of correct decisions the Bayes' average cost is given by $\mathfrak{R} = P_0\alpha C_0 + (1 - P_0)(1 - \beta)C_1$, where C_0 is the pre-assigned cost of rejecting a legitimate user, and C_1 is the pre-assigned cost of accepting a malicious user [34]. If C_0 and C_1 are known or can be set, the Bayesian framework is optimal for an LVS in the sense that it minimizes the Bayes' average cost (P_e is the special case of C with $C_0 = C_1 = 1$).

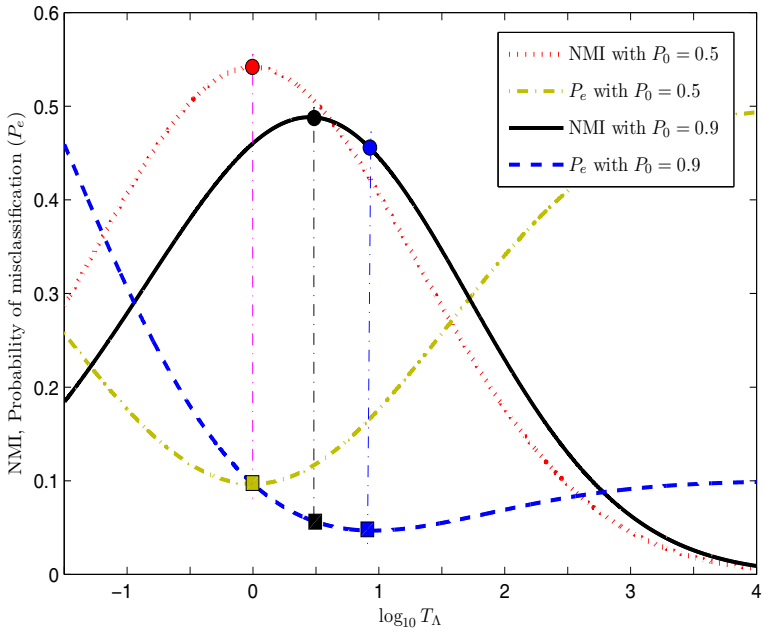

Figure 2.9: Normalized mutual information (NMI) and probability of misclassification (P_e) versus T_Λ for different values of P_0 (Note here the system and network parameters are same as those utilized in Fig. 2.3).

the mutual information between its inputs and outputs.

Notwithstanding the above discussion, we compare the optimal thresholds for NMI and P_e, as shown in Fig. 2.9. From this figure, we can see that for $P_0 = 0.5$ the optimal threshold ($T_\Lambda = 1$) is the same for both algorithms. However, the optimal thresholds for the two algorithms are different when $P_0 = 0.9$. Further, we see that in the $P_0 = 0.9$ case, the change in P_e, if the optimal NMI threshold is used instead of the optimal P_e threshold, is significantly less than the change in NMI if the optimal P_e threshold is used instead of the optimal NMI threshold.

We illustrate this last point (the information-theoretic framework is less sensitive to P_0 than the Bayesian framework) in Fig. 2.10 where the optimal thresholds and performance metrics of the information-theoretic framework and the Bayesian framework are plotted as functions of $P_1 = 1 - P_0$. In reality, the base rate of intrusions (P_1) is an unknown parameter *for all* LVS systems, which can be estimated through historical data records while suffering from estimation errors. We can see

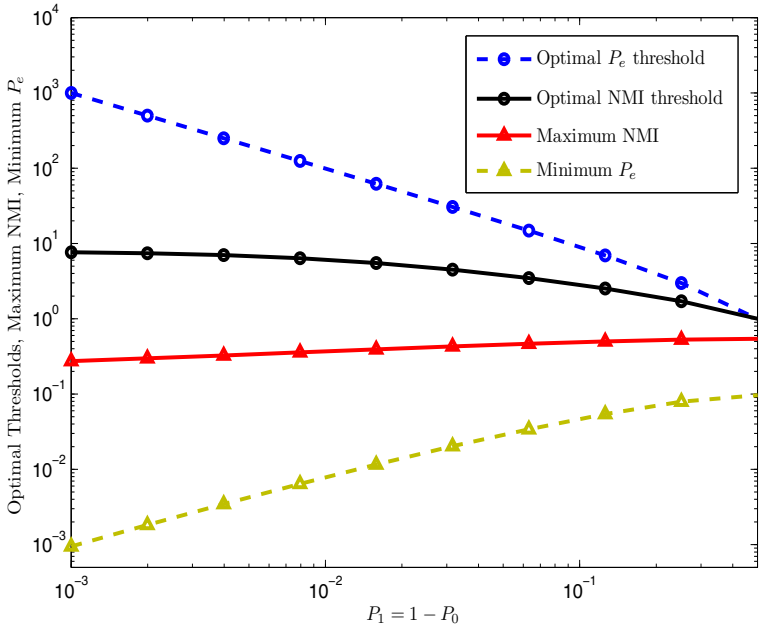

Figure 2.10: Optimal NMI and P_e thresholds, maximum NMI, and minimum P_e versus $P_1 = 1 - P_0$ (Note here the system and network parameters are same as those utilized in Fig. 2.3).

from Fig. 2.10 that the use of NMI results in a more robust system. As the true value of P_1 approaches small values (in any real situation it will be small) the NMI threshold and the corresponding maximum NMI are insensitive to the assumed P_1. This means that when using NMI as the optimization metric, any mismatch between true P_1 and assumed P_1 has little impact on system performance. In the Bayesian framework, however, the optimal threshold for minimizing P_e and the minimum P_e remain very sensitive (close to linear) to the assumed value of P_1. Therefore, in the Bayesian framework any mismatch between the true P_1 and the assumed P_1 results in poor system performance.

2.6 Summary

In this chapter, we developed an information-theoretic framework for an LVS, utilizing the mutual information between input and output data of the LVS as the

objective optimization criterion. We investigated our new optimal LVS under a realistic threat model, showing how in a straightforward implementation of an LVS, information-theoretic optimality is approached as the non-colluding adversary moves further from the network region that it is claiming to be within. This straightforward implementation makes our new algorithm an ideal candidate for the LVS that will be needed in emerging network-based and safety-enhanced transportation systems.

Chapter 3

Location Verification Systems in Spatially Correlated Shadowing

3.1 Introduction

In the previous chapter, after developing an optimal information-theoretic framework for an LVS, we focused on an LVS that utilizes RSS as input measurements and analyzed its detection performance under different threat models. This is mainly due to the fact that RSS measurements can be easily obtained in wireless networks. In addition, RSS can be readily combined with other location information metrics in order to improve the performance of a localization system [98, 99]. Many location verification algorithms that utilize RSS as input observations have been developed in the literature (e.g., [5, 7, 8, 33, 85]). Shadowing is one of the most influential and unavoidable factors in RSS-based LVSs. Our work presented in Chapter 2, together with all other existing studies in RSS-based LVSs, has made a simplified assumption that the shadowing at two different locations is uncorrelated. However, as per many empirical studies the shadowing at different locations will be significantly correlated when the locations are close to each other or different locations possess similar terrain configurations (e.g., [66–68]). Spatial correlation of the shadowing is more common in

VANETs relative to other wireless networks (e.g., cellular networks). This is due to the following two facts. In VANETs, two base stations (BSs) are more likely to share similar terrain configurations. Likewise, authorized vehicles (that potentially could be used to verify the position of a yet-to-be authorized vehicle) are likely to be close to each other. Indeed, such spatially correlated shadowing in VANETs is confirmed by recent empirical studies [100, 101]. Although some specific studies have investigated the performance of RSS-based localization systems under correlated shadowing [71, 102, 103], the impact of spatially correlated shadowing on RSS-based LVSs under realistic threat models has not been previously explored. This leaves an important gap in our understanding on the performance levels of RSS-based LVSs in realistic wireless channel settings and under realistic threat models. The main purpose of this chapter is to close this gap.

Further to our considerations of RSS-based LVSs, we note that there could be circumstances when the use of Differential Received Signal Strength (DRSS) in the LVS context may be beneficial. Indeed it is well known that there are a range of scenarios in which the use of DRSS is more suitable for wireless location acquisition [73]. One example is where users do not have a common transmit power setting on all devices. However, the performances of DRSS-based LVSs have not yet been analyzed in the literature. This chapter also closes this gap, extending our analysis of DRSS-based LVSs to the correlated shadowing regime. This will allow us to provide a detailed performance comparison between RSS-based LVSs and DRSS-based LVSs under correlated shadowing - a comparison that provides for a few surprising results.

The main contributions of this chapter are summarized as follows. (i) Under spatially correlated log-normal shadowing, we analyze the detection performance of an RSS-based LVS in terms of false positive and detection rates. Our analysis demonstrates that the spatial correlation of the shadowing can lead to a significant performance improvement for the RSS-based LVS relative to the case with uncorrelated shadowing (a doubling of the detection rate for a given false positive rate for anticipated correlation levels). (ii) We analyze the detection performance of a DRSS-based

LVS under spatially correlated shadowing, proving that the detection performance of the DRSS-based LVS is identical to that of the RSS-based LVS. As we discuss later, this result is rather surprising. (iii) We analyze our systems under a relaxed threat model scenario in which the adversary whose actual location is physically constrained (e.g., constrained within a building) and therefore cannot optimize his location for the attack. We show that even in these circumstance the performances of the RSS-based LVS and the DRSS-based LVS remain identical. (iv) Finally, we illustrate the case where the RSS-based LVS do have advantages over the DRSS-Based LVS, namely, when the adversary does not (or cannot) optimize his boosted transmit power level.

The rest of this chapter is organized as follows. Section 3.2 details our system model. In Section 3.3, the detection performance of an RSS-based LVS is analyzed under spatially correlated shadowing. In Section 3.4, the detection performance of a DRSS-based LVS is analyzed. In Section 3.5, a thorough performance comparison between the RSS-based LVS and the DRSS-based LVS is provided. Section 3.6 provides numerical results to verify the accuracy of our analysis. Finally, Section 3.7 draws concluding remarks.

3.2 System Model

3.2.1 Observation Model

We first outline the system model and state the assumptions adopted in this chapter.

1. A *single* user (legitimate or malicious) reports his claimed location, which is denoted as $\mathbf{x}_c = (x_c^1, x_c^2) \in \mathbb{R}^2$, to a network with N Base Stations (BSs) in the communication range of the user, where the publicly known location of the i-th BS is $\mathbf{x}_i = (x_i^1, x_i^2) \in \mathbb{R}^2$ $(i = 1, 2, \ldots, N)$. One of the N BSs is the PC, and all other BSs will transmit the measurements collected from the user to the PC. The PC is to make decisions based on the user's claimed location and the measurements collected by all the N BSs.

2. A user (legitimate or malicious) can obtain his true position, $\mathbf{x}_t = (x_t^1, x_t^2)$, from his localization equipment (e.g., GPS), and that the localization error is zero. Thus, a legitimate user's claimed location, $\mathbf{x}_c$, is exactly the same as his true location. However, a malicious user will falsify (spoof) his claimed position in an attempt to fool the LVS. We assume the spoofed claimed location of the malicious user is also $\mathbf{x}_c$.

3. We adopt the minimum distance model as our threat model, in which the distance between the malicious user's true location and his claimed location is greater or equal to r, i.e., $\|\mathbf{x}_c - \mathbf{x}_t\| \geq r$.

4. We denote the null hypothesis where the user is legitimate as $\mathcal{H}_0$, and denote the alternative hypothesis where the user is malicious as $\mathcal{H}_1$. The *a priori* knowledge at the LVS can be summarized as

$$\begin{cases} \mathcal{H}_0 : \ \mathbf{x}_c = \mathbf{x}_t \ \ \text{(legitimate user)}, \\ \mathcal{H}_1 : \ \|\mathbf{x}_c - \mathbf{x}_t\| \geq r \ \ \text{(malicious user)}. \end{cases} \tag{3.1}$$

We note that RSS values are obtained by averaging multiple symbols over time or frequency such that the small-scale fading is averaged out from RSS measurements and its impact is negligeable. Based on the log-normal propagation model, the RSS (in dB) received by the i-th BS from a legitimate user, y_i, is given by

$$y_i = u_i + \omega_i, \ \ i = 1, 2, \ldots, N, \tag{3.2}$$

where

$$u_i = p - 10\gamma \log_{10}\left(\frac{d_i^c}{d}\right), \tag{3.3}$$

and p is a reference received power corresponding to a reference distance d, γ is the path loss exponent, ω_i is a zero-mean normal random variable with variance σ_{dB}^2, and d_i^c is the Euclidean distance from the i-th BS to the legitimate user's claimed location (also his true location) given by $d_i^c = \|\mathbf{x}_c - \mathbf{x}_i\|$. In practice, in order to determine

the values of a pair of p and d we have to know the transmit power of a legitimate user. Under spatially correlated shadowing, ω_i is correlated to ω_j $(j = 1, 2, \ldots, N)$, and the $N \times N$ covariance matrix of $\boldsymbol{\omega} = [\omega_1, \ldots, \omega_N]^T$ is denoted as $\mathbf{R}$. Adopting the well-known spatially correlated shadowing model of [9, 66], the (i, j)-th element of $\mathbf{R}$ is given by

$$R_{ij} = \sigma_{dB}^2 \exp\left(-\frac{d_{ij}}{D_c} \ln 2\right), \ j = 1, 2, \ldots, N, \tag{3.4}$$

where $d_{ij} = ||\mathbf{x}_i - \mathbf{x}_j||$ is the Euclidean distance from the i-th BS to the j-th BS, and D_c is a constant in units of distance, at which the correlation coefficient reduces to 1/2 (in this chapter all distances are in meters). From (3.4), we can see that the correlation between ω_i and ω_j decreases as d_{ij} increases ($R_{ij} = \sigma_{dB}^2$ when $i = j$, and $R_{ij} \to 0$ as $d_{ij} \to \infty$). We also note that R_{ij} increases as D_c increases for a given d_{ij}. As such, D_c is a parameter that indicates the degree of shadowing correlation in some specific environment (for a given d_{ij}, a larger D_c means that the shadowing is more correlated).

Based on (3.2), we can see that under $\mathcal{H}_0$ the N-dimensional observation vector $\mathbf{y} = [y_1, \ldots, y_N]^T$ follows a multivariate normal distribution, which is

$$f(\mathbf{y}|\mathcal{H}_0) = \mathcal{N}(\mathbf{u}, \mathbf{R}), \tag{3.5}$$

where $\mathbf{u} = [u_1, u_2, \ldots, u_N]^T$ is the mean vector.

Again, in this chapter we assume that the malicious user is equipped with a single omnidirectional antenna since in some scenarios a low-complexity transceiver structure is more relevant (e.g., low-cost sensor devices). However, we do allow the malicious user to control its transmit power in order to launch location spoofing attacks. Therefore, in addition to spoofing the claimed location, the malicious user can also adjust his transmit power to impact the RSS values received by all BSs in order to minimize the probability of being detected. As such, the RSS received by the i-th BS from a malicious user, y_i, is given by

$$y_i = p_x + v_i + \omega_i, \tag{3.6}$$

where

$$v_i = p - 10\gamma \log_{10}\left(\frac{d_i^t}{d}\right), \tag{3.7}$$

d_i^t is the Euclidean distance from the i-th BS to the malicious user's true location given by $d_i^t = ||\mathbf{x}_t - \mathbf{x}_i||$, and p_x is the additional boosted transmit power. Based on (3.6), under $\mathcal{H}_1$ the N-dimensional observation vector $\mathbf{y}$, conditioned on known p_x and $\mathbf{x}_t$, also follows a multivariate normal distribution, which is

$$f\left(\mathbf{y}|p_x, \mathbf{x}_t, \mathcal{H}_1\right) = \mathcal{N}\left(p_x \mathbf{1}_N + \mathbf{v}, \mathbf{R}\right), \tag{3.8}$$

where $\mathbf{1_N}$ is a $N \times 1$ vector with all elements set to unity and $\mathbf{v} = [v_1, v_2, \ldots, v_N]^T$. We note that in practice p_x and $\mathbf{x}_t$ are set by the malicious user.

3.2.2 Adopted Decision Rule

We adopt the LRT as the decision rule since it is known that the LRT achieves the highest detection rate for any given false positive rate [86]. Therefore, the LRT can achieve the minimum Bayes' average cost and the maximum mutual information between the input and output of an LVS as we have shown in the last chapter. The LRT decision rule is given by

$$\Lambda\left(\psi(\mathbf{y})\right) \triangleq \frac{f\left(\psi(\mathbf{y})|\mathcal{H}_1\right)}{f\left(\psi(\mathbf{y})|\mathcal{H}_0\right)} \underset{\mathcal{D}_0}{\overset{\mathcal{D}_1}{\gtrless}} \lambda, \tag{3.9}$$

where $\Lambda\left(\psi(\mathbf{y})\right)$ is the test statistic, $\psi(\mathbf{y})$ is a predefined transformation of $\mathbf{y}$ (to be determined in a specific LVS, e.g., RSS or DRSS), $f\left(\psi(\mathbf{y})|\mathcal{H}_1\right)$ is the marginal likelihood function (probability density function of $\psi(\mathbf{y})$) under $\mathcal{H}_1$, $f\left(\psi(\mathbf{y})|\mathcal{H}_0\right)$ is the marginal likelihood function under $\mathcal{H}_0$, λ is the threshold corresponding to $\Lambda\left(\psi(\mathbf{y})\right)$, $\mathcal{D}_0$ and $\mathcal{D}_1$ are the binary decisions that infer whether the user is legitimate or malicious, respectively. Given the decision rule in (3.9), the false positive and detection rates of an LVS are functions of λ. The specific value of λ can be set through minimizing the Bayes' average cost or maximizing the mutual information between the system

input and output in the information-theoretic framework. The intrinsic core performance metrics of an LVS are false positive and detection rates, and other potential performance metrics can be written as functions of these two rates. As such, in this chapter we adopt the false positive and detection rates as the performance metrics.

3.3 RSS-based Location Verification System

In this section, we analyze the performance of the RSS-based LVS in terms of the false positive and detection rates, based on which we examine the impact of the spatially correlated shadowing.

3.3.1 Attack Strategy of the Malicious User

We assume that the malicious user optimizes all the parameters under his control. This assumption is adopted in most threat models. The malicious user will therefore optimize his p_x and $\mathbf{x}_t$ such that the difference between $f(\mathbf{y}|\mathcal{H}_0)$ and $f(\mathbf{y}|p_x, \mathbf{x}_t, \mathcal{H}_1)$ is minimized in order to minimize the probability to be detected. Here, we adopt the KL-divergence from $f(\mathbf{y}|p_x, \mathbf{x}_t, \mathcal{H}_1)$ to $f(\mathbf{y}|\mathcal{H}_0)$ in order to quantify the difference between $f(\mathbf{y}|\mathcal{H}_0)$ and $f(\mathbf{y}|p_x, \mathbf{x}_t, \mathcal{H}_1)$.

Based on (3.5) and (3.8), the KL-divergence from $f(\mathbf{y}|p_x, \mathbf{x}_t, \mathcal{H}_1)$ to $f(\mathbf{y}|\mathcal{H}_0)$ is given by [104]

$$\begin{aligned}\phi(p_x, \mathbf{x}_t) &= D_{KL}\left[f(\mathbf{y}|p_x, \mathbf{x}_t\mathcal{H}_1)\,||f(\mathbf{y}|\mathcal{H}_0)\right] \\ &= \int_{-\infty}^{\infty} \ln \frac{f(\mathbf{y}|p_x, \mathbf{x}_t, \mathcal{H}_1)}{f(\mathbf{y}|\mathcal{H}_0)} f(\mathbf{y}|p_x, \mathbf{x}_t\mathcal{H}_1)\, d\mathbf{y} \\ &= \frac{1}{2}(p_x\mathbf{1}_N + \mathbf{v} - \mathbf{u})^T\mathbf{R}^{-1}(p_x\mathbf{1}_N + \mathbf{v} - \mathbf{u}). \end{aligned} \tag{3.10}$$

Then, the optimal values of p_x and $\mathbf{x}_t$ that minimize $\phi(p_x, \mathbf{x}_t)$ can be obtained through

$$(p_x^*, \mathbf{x}_t^*) = \underset{p_x, ||\mathbf{x}_t - \mathbf{x}_c|| \geq r}{\operatorname{argmin}} \phi(p_x, \mathbf{x}_t). \tag{3.11}$$

The closed-form expressions for p_x^* and $\mathbf{x}_t^*$ are intractable, but they can be obtained through numerical search. In order to simplify the numerical search, we first derive the optimal value of p_x for a given $\mathbf{x}_t$, which is presented in the following lemma.

***Lemma* 3** The optimal value of p_x that minimizes $\phi(p_x, \mathbf{x}_t)$ for any given $\mathbf{x}_t$ is

$$p_x^o(\mathbf{x}_t) = \frac{(\mathbf{u}-\mathbf{v})^T\mathbf{R}^{-1}\mathbf{1}_N}{\mathbf{1}_N^T\mathbf{R}^{-1}\mathbf{1}_N}. \tag{3.12}$$

We now prove Lemma 3. The first derivative of $\phi(p_x, \mathbf{x}_t)$ with respect to p_x is derived as

$$\begin{aligned}\frac{\partial\phi(p_x,\mathbf{x}_t)}{\partial p_x} &= \frac{\partial\phi(p_x,\mathbf{x}_t)}{\partial\left(p_x\mathbf{1}_N\right)}\frac{\partial\left(p_x\mathbf{1}_N\right)}{\partial p_x} \\ &= (p_x\mathbf{1}_N+\mathbf{v}-\mathbf{u})^T\mathbf{R}^{-1}\frac{\partial\left(p_x\mathbf{1}_N\right)}{\partial p_x} \\ &= (p_x\mathbf{1}_N+\mathbf{v}-\mathbf{u})^T\mathbf{R}^{-1}\mathbf{1}_N. \end{aligned}\tag{3.13}$$

Following (3.13), the second derivative of $\phi(p_x, \mathbf{x}_t)$ with respect to p_x is derived as

$$\frac{\partial^2\phi(p_x,\mathbf{x}_t)}{\partial^2 p_x} = \mathbf{1}_N^T\mathbf{R}^{-1}\mathbf{1}_N. \tag{3.14}$$

Based on the definition of $\mathbf{R}$ given by (3.4), we have $\partial^2\phi(p_x, \mathbf{x}_t)/\partial^2 p_x > 0$ as per (3.14), which indicates that $\phi(p_x, \mathbf{x}_t)$ is a convex function of p_x. As such, we obtain the desired result in (3.12) by setting $\partial\phi(p_x, \mathbf{x}_t)/\partial p_x = 0$. This completes the proof of Lemma 3.

From Lemma 3, we note that the malicious user optimizes his transmit power, i.e., $p_x = p_x^o(\mathbf{x}_t)$, to compensate the path-loss difference between his claimed location and his true location. We also note that $p_x^o(\mathbf{x}_t)$ is a function of $\mathbf{R}$ under spatial correlated shadowing. This is different from the scenario with uncorrelated shadowing, where $p_x^o(\mathbf{x}_t)$ is independent of the shadowing noise as we have shown in the last chapter. Substituting $p_x^o(\mathbf{x}_t)$ into (3.10), we have

$$\phi(p_x^o(\mathbf{x}_t), \mathbf{x}_t) = \frac{1}{2}(\mathbf{w}-\mathbf{u})^T\mathbf{R}^{-1}(\mathbf{w}-\mathbf{u}), \tag{3.15}$$

where

$$\mathbf{w} = \frac{(\mathbf{u}-\mathbf{v})^T\mathbf{R}^{-1}\mathbf{1}_N}{\mathbf{1}_N^T\mathbf{R}^{-1}\mathbf{1}_N}\mathbf{1}_N + \mathbf{v}. \tag{3.16}$$

Since we have shown that $\phi(p_x, \mathbf{x}_t)$ is a convex function of p_x in (3.14), $\mathbf{x}_t^*$ is given by

$$\mathbf{x}_t^* = \underset{||\mathbf{x}_t-\mathbf{x}_c||\geq r}{\operatorname{argmin}} \ \phi(p_x^o(\mathbf{x}_t), \mathbf{x}_t). \tag{3.17}$$

Substituting $\mathbf{x}_t^*$ into $p_x^o(\mathbf{x}_t)$, we obtain $p_x^* = p_x^o(\mathbf{x}_t^*)$. We note that Lemma 3 is of importance since it reduces a three-dimension numerical search in (3.11) into a two-dimension numerical search in (3.17).

Substituting p_x^* and $\mathbf{x}_t^*$ into (3.6), the RSS received by the i-th BS from a malicious user can be written as

$$\mathbf{y} = \mathbf{w}^* + \boldsymbol{\omega}, \tag{3.18}$$

where

$$\mathbf{w}^* = \frac{(\mathbf{u}-\mathbf{v}^*)^T\mathbf{R}^{-1}\mathbf{1}_N}{\mathbf{1}_N^T\mathbf{R}^{-1}\mathbf{1}_N}\mathbf{1}_N + \mathbf{v}*, \tag{3.19}$$

$\mathbf{v}^*$ is obtained by substituting $\mathbf{x}_t^*$ into $\mathbf{v}$. Based on (3.18), the likelihood function under $\mathcal{H}_1$ conditioned on p_x^* and $\mathbf{x}_t^*$ can be written as

$$f\left(\mathbf{y}|p_x^*, \mathbf{x}_t^*, \mathcal{H}_1\right) = \mathcal{N}(\mathbf{w}^*, \mathbf{R}). \tag{3.20}$$

3.3.2 Detection Performance of the RSS-based LVS

In some practical cases, the malicious user may not have the freedom to optimize his true location, e.g., if the malicious user is physically limited to be inside a building. However, the malicious user can still optimize his transmit power as per his true location. As such, without losing generality, we first analyze the performance of the RSS-based LVS for $p_x = p_x^o(\mathbf{x}_t)$, and then present the performance of the RSS-based LVS for $p_x = p_x^*$ and $\mathbf{x}_t = \mathbf{x}_t^*$ as a special case.

Following (3.9), the specific LRT decision rule of the RSS-based LVS for $p_x = p_x^o(\mathbf{x}_t)$ is given by

$$\Lambda^o\left(\mathbf{y}\right) \triangleq \frac{f\left(\mathbf{y}|p_x^o(\mathbf{x}_t), \mathbf{x}_t, \mathcal{H}_1\right)}{f\left(\mathbf{y}|\mathcal{H}_0\right)} \underset{\mathcal{D}_0}{\overset{\mathcal{D}_1}{\gtrless}} \lambda_R^o, \tag{3.21}$$

where $\Lambda^o(\mathbf{y})$ is the likelihood ratio of $\mathbf{y}$ for $p_x = p_x^o(\mathbf{x}_t)$, $f(\mathbf{y}|p_x^o(\mathbf{x}_t), \mathbf{x}_t, \mathcal{H}_1) = \mathcal{N}(\mathbf{w}, \mathbf{R})$, and λ_R^o is a threshold for $\Lambda^o(\mathbf{y})$. Substituting (3.5) and (3.20) into (3.21), we obtain $\Lambda^o(\mathbf{y})$ in the log domain as

$$\begin{aligned}\ln \Lambda^o(\mathbf{y}) &= \frac{1}{2}(\mathbf{y}-\mathbf{u})^T\mathbf{R}^{-1}(\mathbf{y}-\mathbf{u}) - \frac{1}{2}(\mathbf{y}-\mathbf{w})^T\mathbf{R}^{-1}(\mathbf{y}-\mathbf{w}) \\ &= (\mathbf{w}-\mathbf{u})^T\mathbf{R}^{-1}\mathbf{y} - \frac{1}{2}(\mathbf{w}-\mathbf{u})^T\mathbf{R}^{-1}(\mathbf{w}+\mathbf{u}). \end{aligned} \tag{3.22}$$

As such, for the theorem to follow, we can rewrite the decision rule in (3.21) as the following format

$$\mathbb{T}(\mathbf{y}) \underset{\mathcal{D}_0}{\overset{\mathcal{D}_1}{\gtrless}} \Gamma_R, \tag{3.23}$$

where $\mathbb{T}(\mathbf{y})$ is the test statistic given by

$$\mathbb{T}(\mathbf{y}) \triangleq (\mathbf{w}-\mathbf{u})^T\mathbf{R}^{-1}\mathbf{y}, \tag{3.24}$$

and Γ_R is the threshold for $\mathbb{T}(\mathbf{y})$ given by

$$\Gamma_R \triangleq \ln \lambda_R^o + \frac{1}{2}(\mathbf{w}-\mathbf{u})^T\mathbf{R}^{-1}(\mathbf{w}+\mathbf{u}+2p\mathbf{1}_N). \tag{3.25}$$

We then derive the false positive rate, α_R^o, and detection rate, β_R^o, of the RSS-based LVS for $p_x = p_x^o(\mathbf{x}_t)$ in the following theorem.

***Theorem* 2** For $p_x = p_x^o(\mathbf{x}_t)$, the false positive and detection rates of the RSS-based LVS are

$$\alpha_R^o(\mathbf{x}_t) = \mathcal{Q}\left[\frac{\Gamma_R - (\mathbf{w}-\mathbf{u})^T\mathbf{R}^{-1}(p\mathbf{1}_N+\mathbf{u})}{\sqrt{(\mathbf{w}-\mathbf{u})^T\mathbf{R}^{-1}(\mathbf{w}-\mathbf{u})}}\right] = \mathcal{Q}\left[\frac{\ln\lambda_R^o + \frac{1}{2}(\mathbf{w}-\mathbf{u})^T\mathbf{R}^{-1}(\mathbf{w}-\mathbf{u})}{\sqrt{(\mathbf{w}-\mathbf{u})^T\mathbf{R}^{-1}(\mathbf{w}-\mathbf{u})}}\right], \tag{3.26}$$

$$\beta_R^o(\mathbf{x}_t) = \mathcal{Q}\left[\frac{\Gamma_R - (\mathbf{w}-\mathbf{u})^T\mathbf{R}^{-1}(p\mathbf{1}_N+\mathbf{w})}{\sqrt{(\mathbf{w}-\mathbf{u})^T\mathbf{R}^{-1}(\mathbf{w}-\mathbf{u})}}\right] = \mathcal{Q}\left[\frac{\ln\lambda_R^o - \frac{1}{2}(\mathbf{w}-\mathbf{u})^T\mathbf{R}^{-1}(\mathbf{w}-\mathbf{u})}{\sqrt{(\mathbf{w}-\mathbf{u})^T\mathbf{R}^{-1}(\mathbf{w}-\mathbf{u})}}\right], \tag{3.27}$$

where $\mathcal{Q}[x] = \frac{1}{\sqrt{2\pi}}\int_x^\infty \exp(-t^2/2)dt$.

We now prove Theorem 2. Using (3.24), the distributions of $\mathbb{T}(\mathbf{y})$ under $\mathcal{H}_0$ and $\mathcal{H}_1$ are derived as follows

$$\begin{aligned}\mathbb{T}(\mathbf{y})|\mathcal{H}_0 &\sim \mathcal{N}\left((\mathbf{w}\text{–}\mathbf{u})^T\mathbf{R}^{-1}\mathbf{u}, (\mathbf{w}\text{–}\mathbf{u})^T\mathbf{R}^{-1}\mathbf{R}\left((\mathbf{w}\text{–}\mathbf{u})^T\mathbf{R}^{-1}\right)^T\right)\\ &\sim \mathcal{N}\left((\mathbf{w}\text{–}\mathbf{u})^T\mathbf{R}^{-1}\mathbf{u}, (\mathbf{w}\text{–}\mathbf{u})^T\mathbf{R}^{-1}(\mathbf{w}\text{–}\mathbf{u})\right), \qquad (3.28)\\ \mathbb{T}(\mathbf{y})|\mathcal{H}_1 &\sim \mathcal{N}\left((\mathbf{w}\text{–}\mathbf{u})^T\mathbf{R}^{-1}\mathbf{w}, (\mathbf{w}\text{–}\mathbf{u})^T\mathbf{R}^{-1}\mathbf{R}\left((\mathbf{w}\text{–}\mathbf{u})^T\mathbf{R}^{-1}\right)^T\right)\\ &\sim \mathcal{N}\left((\mathbf{w}\text{–}\mathbf{u})^T\mathbf{R}^{-1}\mathbf{w}, (\mathbf{w}\text{–}\mathbf{u})^T\mathbf{R}^{-1}(\mathbf{w}\text{–}\mathbf{u})\right). \qquad (3.29)\end{aligned}$$

As per the decision rule in (3.23), the false positive and detection rates are given by

$$\alpha_R^o(\mathbf{x}_t) \triangleq \Pr\left(\mathbb{T}(\mathbf{y}) \geq \Gamma_R|\mathcal{H}_0\right), \qquad (3.30)$$

$$\beta_R^o(\mathbf{x}_t) \triangleq \Pr\left(\mathbb{T}(\mathbf{y}) \geq \Gamma_R|\mathcal{H}_1\right). \qquad (3.31)$$

Substituting (3.28) and (3.29) into (3.30) and (3.31), respectively, we obtain the results in (3.33) and (3.34) after some algebraic manipulations. This completes the proof of Theorem 2.

For $p_x = p_x^*$ and $\mathbf{x}_t = \mathbf{x}_t^*$, the LRT decision rule of the RSS-based LVS is given by

$$\Lambda^*(\mathbf{y}) \triangleq \frac{f(\mathbf{y}|p_x^*, \mathbf{x}_t^*, \mathcal{H}_1)}{f(\mathbf{y}|\mathcal{H}_0)} \underset{\mathcal{D}_0}{\overset{\mathcal{D}_1}{\gtrless}} \lambda_R^*, \qquad (3.32)$$

where $\Lambda^*(\mathbf{y})$ is the likelihood ratio of $\mathbf{y}$ for $p_x = p_x^*$ and $\mathbf{x}_t = \mathbf{x}_t^*$, and λ_R^* is a threshold for $\Lambda^*(\mathbf{y})$. Following Theorem 2, the false positive and detection rates of the RSS-based LVS for $p_x = p_x^*$ and $\mathbf{x}_t = \mathbf{x}_t^*$ are given by

$$\alpha_R^* = \mathcal{Q}\left[\frac{\ln\lambda_R^* + \frac{1}{2}(\mathbf{w}^*\text{–}\mathbf{u})^T\mathbf{R}^{-1}(\mathbf{w}^*\text{–}\mathbf{u})}{\sqrt{(\mathbf{w}^*\text{–}\mathbf{u})^T\mathbf{R}^{-1}(\mathbf{w}^*\text{–}\mathbf{u})}}\right], \qquad (3.33)$$

$$\beta_R^* = \mathcal{Q}\left[\frac{\ln\lambda_R^* - \frac{1}{2}(\mathbf{w}^*\text{–}\mathbf{u})^T\mathbf{R}^{-1}(\mathbf{w}^*\text{–}\mathbf{u})}{\sqrt{(\mathbf{w}^*\text{–}\mathbf{u})^T\mathbf{R}^{-1}(\mathbf{w}^*\text{–}\mathbf{u})}}\right]. \qquad (3.34)$$

We note that the results provided in (3.26) and (3.27) are based on an arbitrary true location $\mathbf{x}_t$ of the malicious user, which are more general than that provided in

(3.33) and (3.34). That is, $\alpha_R^* = \alpha_R^o(\mathbf{x}_t^*)$ and $\beta_R^* = \beta_R^o(\mathbf{x}_t^*)$. By using (3.26) and (3.27), we can compare the performance of the RSS-based LVS with that of the DRSS-based LVS in a general scenario.

3.4 DRSS-based Location Verification System

In this section, we analyze the detection performance of the DRSS-based LVS under spatially correlated shadowing.

3.4.1 DRSS Observations

There are range of scenarios in location acquisition (determination) in which the use of DRSS can often lead to location accuracy improvement. One example is where (legitimate) users do not have a common transmit power setting on all devices. It is therefore useful then to extend our analysis and probe the performance level of an LVS based on DRSS. Note, that we do not expect, in general, such a DRSS-based LVS to possess performance levels better than an RSS-based LVS. The main reason for this is that in a DRSS system the signal subtractions lead to one less observation for the system to use in its decision rule. We also note that a pragmatic advantage for an attacker in a DRSS system is that the determination of his optimal transmit power is no longer required.

In general, we can obtain $N(N-1)/2$ DRSS values from N RSS values. The $N(N-1)/2$ DRSS values include $(N-1)$ basic DRSS values, and $(N-1)(N-2)/2$ redundant DRSS values, which means all the $N(N-1)/2$ DRSS values can be determined by linear combinations of the $(N-1)$ basic DRSS values. As such, the $(N-1)$ basic DRSS values include all the information embedded in the $N(N-1)/2$ DRSS values, and our DRSS-based LVS utilizes the $(N-1)$ basic DRSS values. We achieve the $(N-1)$ basic DRSS values from N RSS values by subtracting the N-th RSS value from all other $(N-1)$ RSS values. As such, the m-th DRSS value under

$\mathcal{H}_0$ is given by

$$\Delta y_m = \Delta u_m + \Delta \omega_m,\ m = 1, 2, \ldots, N-1, \tag{3.35}$$

where $\Delta u_m = u_m - u_N$ and $\Delta \omega_m = \omega_m - \omega_N$. We note that $\Delta \omega_m$ is Gaussian with zero mean and variance $2(\sigma_{dB}^2 - R_{mN})$. We denote the $(N-1) \times (N-1)$ covariance matrix of the $(N-1)$-dimensional DRSS vector $\mathbf{\Delta y} = [\Delta y_1, \ldots, \Delta y_{N-1}]^T$ as $\mathbf{D}$, whose (m, n)-th element is given by $(n = 1, 2, \ldots, N-1)$

$$D_{mn} = R_{NN} + R_{mn} - R_{mN} - R_{nN}. \tag{3.36}$$

As such, $\mathbf{\Delta y}$ under $\mathcal{H}_0$ follows a multivariate normal distribution, which is given by

$$f\left(\mathbf{\Delta y}|\mathcal{H}_0\right) = \mathcal{N}(\mathbf{\Delta u}, \mathbf{D}), \tag{3.37}$$

where $\mathbf{\Delta u} = [\Delta u_1, \ldots, \Delta u_{N-1}]^T$ is the mean vector.

Likewise, the m-th DRSS value under $\mathcal{H}_1$ is

$$\Delta y_m = \Delta v_m + \Delta \omega_m, \tag{3.38}$$

where $\Delta v_m = v_m - v_N$. Noting $\mathbf{\Delta v} = [\Delta v_1, \ldots, \Delta v_{N-1}]^T$, $\mathbf{\Delta y}$ under $\mathcal{H}_1$ follows another multivariate normal distribution, which is given by

$$f\left(\mathbf{\Delta y}|\mathbf{x}_t, \mathcal{H}_1\right) = \mathcal{N}(\mathbf{\Delta v}, \mathbf{D}). \tag{3.39}$$

3.4.2 Attack Strategy of the Malicious User

As per (3.3) and (3.7), we know that both p and d are constant at all elements of $\mathbf{u}$ and $\mathbf{v}$. As such, based on (3.35) and (3.38) we can see that $\mathbf{\Delta y}$ under both $\mathcal{H}_0$ and $\mathcal{H}_1$ are independent of p and d, and therefore both $f\left(\mathbf{\Delta y}|\mathcal{H}_0\right)$ and $f\left(\mathbf{\Delta y}|\mathbf{x}_t, \mathcal{H}_1\right)$ are independent of p and d. As such, in the DRSS-based LVS the malicious user does not need to adjust his transmit power in order to minimize the probability to be detected. In the DRSS-based LVS, the malicious user only has to optimize his true location through minimizing the KL-divergence from $f\left(\mathbf{\Delta y}|\mathbf{x}_t, \mathcal{H}_1\right)$ to $f\left(\mathbf{\Delta y}|\mathcal{H}_0\right)$,

which is given by

$$\begin{aligned}\varphi(\mathbf{x}_t) &= D_{KL}\left[f\left(\mathbf{\Delta y}|\mathbf{x}_t,\mathcal{H}_1\right)||f\left(\mathbf{\Delta y}|\mathcal{H}_0\right)\right]\\ &= \int_{-\infty}^{\infty}\ln\frac{f\left(\mathbf{\Delta y}|\mathbf{x}_t,\mathcal{H}_1\right)}{f\left(\mathbf{\Delta y}|\mathcal{H}_0\right)}f\left(\mathbf{\Delta y}|\mathbf{x}_t,\mathcal{H}_1\right)d\mathbf{\Delta y}\\ &= \frac{1}{2}(\mathbf{\Delta v}-\mathbf{\Delta u})^T\mathbf{D}^{-1}(\mathbf{\Delta v}-\mathbf{\Delta u}).\end{aligned} \tag{3.40}$$

The optimal value of $\mathbf{x}_t$ for the malicious user in the DRSS-based LVS can be obtained through

$$\mathbf{x}_t^{\ddagger} = \underset{||\mathbf{x}_t-\mathbf{x}_c||\geq r}{\operatorname{argmin}}\ \varphi(\mathbf{x}_t). \tag{3.41}$$

The likelihood function under $\mathcal{H}_1$ for $\mathbf{x}_t=\mathbf{x}_t^{\ddagger}$ is given by

$$f\left(\mathbf{\Delta y}|\mathbf{x}_t^{\ddagger},\mathcal{H}_1\right)=\mathcal{N}(\mathbf{\Delta v}^{\ddagger},\mathbf{D}), \tag{3.42}$$

where $\Delta v_m^{\ddagger}=v_m^{\ddagger}-v_N^{\ddagger}$ and $\mathbf{v}^{\ddagger}$ is obtained by substituting $\mathbf{x}_t^{\ddagger}$ into $\mathbf{v}$.

3.4.3 Detection Performance of the DRSS-based LVS

In this subsection, we again consider the case where the true location of the malicious user is physically constrained. Specifically, we first analyze the performance of the DRSS-based LVS for an arbitrary $\mathbf{x}_t$, and then present the performance of the DRSS-based LVS for $\mathbf{x}_t=\mathbf{x}_t^{\ddagger}$ as a special case.

Following (3.9), the specific LRT decision rule of the DRSS-based LVS for any $\mathbf{x}_t$ is given by

$$\Lambda\left(\mathbf{\Delta y}\right)\triangleq\frac{f\left(\mathbf{\Delta y}|\mathbf{x}_t,\mathcal{H}_1\right)}{f\left(\mathbf{\Delta y}|\mathcal{H}_0\right)}\underset{\mathcal{D}_0}{\overset{\mathcal{D}_1}{\gtrless}}\lambda_D, \tag{3.43}$$

where $\Lambda\left(\mathbf{\Delta y}\right)$ is the likelihood ratio of $\mathbf{\Delta y}$ and λ_D is a threshold for $\Lambda\left(\mathbf{\Delta y}\right)$. Substituting (3.37) and (3.42) into (3.43), we obtain $\Lambda\left(\mathbf{\Delta y}\right)$ in log domain as

$$\begin{aligned}\ln\Lambda\left(\mathbf{\Delta y}\right) &= \frac{1}{2}(\mathbf{\Delta y}-\mathbf{\Delta u})^T\boldsymbol{D}^{-1}(\mathbf{\Delta y}-\mathbf{\Delta u})-\frac{1}{2}(\mathbf{\Delta y}-\mathbf{\Delta v})^T\boldsymbol{D}^{-1}(\mathbf{\Delta y}-\mathbf{\Delta v})\\ &= (\mathbf{\Delta v}-\mathbf{\Delta u})^T\boldsymbol{D}^{-1}\mathbf{\Delta y}-\frac{1}{2}(\mathbf{\Delta v}-\mathbf{\Delta u})^T\boldsymbol{D}^{-1}(\mathbf{\Delta v}+\mathbf{\Delta u}).\end{aligned} \tag{3.44}$$

Then, we can rewrite the decision rule given in (3.43) as

$$\mathbb{T}(\mathbf{\Delta y}) \underset{\mathcal{D}_1}{\overset{\mathcal{D}_0}{\gtrless}} \Gamma_D, \tag{3.45}$$

where $\mathbb{T}(\mathbf{\Delta y})$ is the test statistic given by

$$\mathbb{T}(\mathbf{\Delta y}) \triangleq (\mathbf{\Delta v} - \mathbf{\Delta u})^T \boldsymbol{D}^{-1} \mathbf{\Delta y}, \tag{3.46}$$

and Γ_D is the threshold for $\mathbb{T}(\mathbf{\Delta y})$ given by

$$\Gamma_D \triangleq \ln \lambda_D + \frac{1}{2}(\mathbf{\Delta v} - \mathbf{\Delta u})^T \boldsymbol{D}^{-1}(\mathbf{\Delta v} + \mathbf{\Delta u}). \tag{3.47}$$

We then derive the false positive rate, $\alpha_D(\mathbf{x}_t)$, and the detection rate, $\beta_D(\mathbf{x}_t)$, of the DRSS-based LVS for any $\mathbf{x}_t$ in the following theorem.

***Theorem* 3** The false positive and detection rates of the DRSS-based LVS for any $\mathbf{x}_t$ are given by

$$\begin{aligned}
\alpha_D(\mathbf{x}_t) &= \mathcal{Q}\left[\frac{\Gamma_D - (\mathbf{\Delta v}–\mathbf{\Delta u})^T \mathbf{D}^{-1} \mathbf{\Delta u}}{\sqrt{(\mathbf{\Delta v}–\mathbf{\Delta u})^T \mathbf{D}^{-1} (\mathbf{\Delta v}–\mathbf{\Delta u})}}\right] \\
&= \mathcal{Q}\left[\frac{\ln \lambda_D + \frac{1}{2}(\mathbf{\Delta v}–\mathbf{\Delta u})^T \mathbf{D}^{-1} (\mathbf{\Delta v}–\mathbf{\Delta u})}{\sqrt{(\mathbf{\Delta v}–\mathbf{\Delta u})^T \mathbf{D}^{-1} (\mathbf{\Delta v}–\mathbf{\Delta u})}}\right], \qquad (3.48) \\
\beta_D(\mathbf{x}_t) &= \mathcal{Q}\left[\frac{\Gamma_D - (\mathbf{\Delta v}–\mathbf{\Delta u})^T \mathbf{D}^{-1} \mathbf{\Delta v}}{\sqrt{(\mathbf{\Delta v}–\mathbf{\Delta u})^T \mathbf{D}^{-1} (\mathbf{\Delta v}–\mathbf{\Delta u})}}\right] \\
&= \mathcal{Q}\left[\frac{\ln \lambda_D - \frac{1}{2}(\mathbf{\Delta v}–\mathbf{\Delta u})^T \mathbf{D}^{-1} (\mathbf{\Delta v}–\mathbf{\Delta u})}{\sqrt{(\mathbf{\Delta v}–\mathbf{\Delta u})^T \mathbf{D}^{-1} (\mathbf{\Delta v}–\mathbf{\Delta u})}}\right]. \qquad (3.49)
\end{aligned}$$

We now prove Theorem 3. Using (3.37), (3.42), and (3.46), the distributions of $\mathbb{T}(\mathbf{\Delta y})$ under $\mathcal{H}_0$ and $\mathcal{H}_1$ are derived as follows

$$\mathbb{T}(\mathbf{\Delta y})|\mathcal{H}_0 \sim \mathcal{N}\left((\mathbf{\Delta v}–\mathbf{\Delta u})^T \mathbf{D}^{-1} \mathbf{\Delta u}, (\mathbf{\Delta v}–\mathbf{\Delta u})^T \mathbf{D}^{-1} (\mathbf{\Delta v}–\mathbf{\Delta u})\right), \tag{3.50}$$

$$\mathbb{T}(\mathbf{\Delta y})|\mathcal{H}_1 \sim \mathcal{N}\left((\mathbf{\Delta v}–\mathbf{\Delta u})^T \mathbf{D}^{-1} \mathbf{\Delta v}, (\mathbf{\Delta v}–\mathbf{\Delta u})^T \mathbf{D}^{-1} (\mathbf{\Delta v}–\mathbf{\Delta u})\right). \tag{3.51}$$

As per the decision rule in (3.45), the false positive and detection rates are given by

$$\alpha_D(\mathbf{x}_t) \triangleq \Pr\left(\mathbb{T}(\boldsymbol{\Delta}\mathbf{y}) \geq \Gamma_D | \mathcal{H}_0\right), \tag{3.52}$$

$$\beta_D(\mathbf{x}_t) \triangleq \Pr\left(\mathbb{T}(\boldsymbol{\Delta}\mathbf{y}) \geq \Gamma_D | \mathcal{H}_1\right). \tag{3.53}$$

Substituting (3.50) and (3.51) into (3.52) and (3.53), respectively, we obtain the results in (3.48) and (3.49) after some algebraic manipulations. This completes the proof of Theorem 3.

For $\mathbf{x}_t = \mathbf{x}_t^{\ddagger}$, the LRT decision rule of the DRSS-based LVS is given by

$$\Lambda^*\left(\boldsymbol{\Delta}\mathbf{y}\right) \triangleq \frac{f\left(\boldsymbol{\Delta}\mathbf{y}|\mathbf{x}_t, \mathcal{H}_1\right)}{f\left(\boldsymbol{\Delta}\mathbf{y}|\mathcal{H}_0\right)} \underset{\mathcal{D}_0}{\overset{\mathcal{D}_1}{\gtrless}} \lambda_D^*, \tag{3.54}$$

where $\Lambda^*\left(\boldsymbol{\Delta}\mathbf{y}\right)$ is the likelihood ratio of $\boldsymbol{\Delta}\mathbf{y}$ for $\mathbf{x}_t = \mathbf{x}_t^{\ddagger}$ and λ_D^* is a threshold for $\Lambda^*\left(\boldsymbol{\Delta}\mathbf{y}\right)$. Following Theorem 3, the false positive and detection rates of the DRSS-based LVS for $\mathbf{x}_t = \mathbf{x}_t^{\ddagger}$ are given by

$$\alpha_D^* = \mathcal{Q}\left[\frac{\ln\lambda_D^* + \frac{1}{2}\left(\boldsymbol{\Delta}\mathbf{v}^{\ddagger} - \boldsymbol{\Delta}\mathbf{u}\right)^T \mathbf{D}^{-1}\left(\boldsymbol{\Delta}\mathbf{v}^{\ddagger} - \boldsymbol{\Delta}\mathbf{u}\right)}{\sqrt{\left(\boldsymbol{\Delta}\mathbf{v}^{\ddagger} - \boldsymbol{\Delta}\mathbf{u}\right)^T \mathbf{D}^{-1}\left(\boldsymbol{\Delta}\mathbf{v}^{\ddagger} - \boldsymbol{\Delta}\mathbf{u}\right)}}\right], \tag{3.55}$$

$$\beta_D^* = \mathcal{Q}\left[\frac{\ln\lambda_D^* - \frac{1}{2}\left(\boldsymbol{\Delta}\mathbf{v}^{\ddagger} - \boldsymbol{\Delta}\mathbf{u}\right)^T \mathbf{D}^{-1}\left(\boldsymbol{\Delta}\mathbf{v}^{\ddagger} - \boldsymbol{\Delta}\mathbf{u}\right)}{\sqrt{\left(\boldsymbol{\Delta}\mathbf{v}^{\ddagger} - \boldsymbol{\Delta}\mathbf{u}\right)^T \mathbf{D}^{-1}\left(\boldsymbol{\Delta}\mathbf{v}^{\ddagger} - \boldsymbol{\Delta}\mathbf{u}\right)}}\right]. \tag{3.56}$$

Again, note that the results provided in (3.48) and (3.49) are for any $\mathbf{x}_t$, which are more general than that provided in (3.55) and (3.56). That is, $\alpha_D^* = \alpha_D(\mathbf{x}_t^{\ddagger})$ and $\beta_D^* = \beta_D(\mathbf{x}_t^{\ddagger})$. By using (3.48) and (3.49), we can compare the performance of the DRSS-based LVS with that of the RSS-based LVS in a general scenario.

3.5 Comparison between RSS-based LVS and DRSS-based LVS

In this section, we conduct a thorough comparison between the RSS-based LVS and the DRSS-based LVS. We now present the following theorem with regard to this comparison for a given $\mathbf{x}_t$.

***Theorem* 4** For any $\mathbf{x}_t$, we have $\alpha_R^o(\mathbf{x}_t) = \alpha_D(\mathbf{x}_t)$ and $\beta_R^o(\mathbf{x}_t) = \beta_D(\mathbf{x}_t)$ for $\lambda_R = \lambda_D$. That is, for any $\mathbf{x}_t$ the performance of the RSS-based LVS with $p_x = p_x^o(\mathbf{x}_t)$ is identical to the performance of the DRSS-based LVS.

The proof of Theorem 4 is provided in Appendix A.

We note that the result provided in Theorem 4 is valid for any $\mathbf{R}$, i.e., for any kind of shadowing (correlated or uncorrelated). We also note that in Theorem 4 the condition to guarantee the RSS-based LVS being identical to the DRSS-based LVS is that $p_x = p_x^o(\mathbf{x}_t)$. This condition forces the malicious user to optimize his transmit power based on the given $\mathbf{x}_t$ in the RSS-based LVS, but not in the DRSS-based LVS. Without this condition, the comparison result between the RSS-based LVS and the DRSS-based LVS is present in the following corollary.

***Corollary* 1** For any $\mathbf{x}_t$, the performance of the RSS-based LVS with $p_x \neq p_x^o(\mathbf{x}_t)$ is better than the performance of the DRSS-based LVS.

We now prove Corollary 1. For any p_x and $\mathbf{x}_t$, the LRT decision rule of the RSS-based LVS is given by

$$\Lambda(\mathbf{y}) \triangleq \frac{f(\mathbf{y}|p_x, \mathbf{x}_t, \mathcal{H}_1)}{f(\mathbf{y}|\mathcal{H}_0)} \underset{\mathcal{D}_0}{\overset{\mathcal{D}_1}{\gtrless}} \lambda_R, \tag{3.57}$$

where $\Lambda(\mathbf{y})$ is the likelihood ratio of $\mathbf{y}$ and λ_R is a threshold for $\Lambda(\mathbf{y})$. Following Theorem 2, the false positive and detection rates of the RSS-based LVS for any p_x and $\mathbf{x}_t$ are given by

$$\alpha_R(p_x, \mathbf{x}_t) = \mathcal{Q}\left[\frac{\ln\lambda_R + \frac{1}{2}(\mathbf{v}-\mathbf{u})^T \mathbf{R}^{-1}(\mathbf{v}-\mathbf{u})}{\sqrt{(\mathbf{v}-\mathbf{u})^T \mathbf{R}^{-1}(\mathbf{v}-\mathbf{u})}}\right], \tag{3.58}$$

$$\beta_R(p_x, \mathbf{x}_t) = \mathcal{Q}\left[\frac{\ln\lambda_R - \frac{1}{2}(\mathbf{v}-\mathbf{u})^T \mathbf{R}^{-1}(\mathbf{v}-\mathbf{u})}{\sqrt{(\mathbf{v}-\mathbf{u})^T \mathbf{R}^{-1}(\mathbf{v}-\mathbf{u})}}\right]. \tag{3.59}$$

Then, Corollary 1 can be presented in math as that given $p_x \neq p_x^o(\mathbf{x}_t)$, we have $\beta_R(p_x, \mathbf{x}_t) > \beta_D(\mathbf{x}_t)$ for $\alpha_R(p_x, \mathbf{x}_t) = \alpha_D(\mathbf{x}_t)$ or $\alpha_R(p_x, \mathbf{x}_t) < \alpha_D(\mathbf{x}_t)$ for $\beta_R(p_x, \mathbf{x}_t) =$

$\beta_D(\mathbf{x}_t)$. Given the proof of Theorem 4, in order to prove Corollary 1 we only have to prove the following equation

$$(\mathbf{v}–\mathbf{u})^T \mathbf{R}^{-1} (\mathbf{v}–\mathbf{u}) > (\mathbf{\Delta v}–\mathbf{\Delta u})^T \mathbf{D}^{-1} (\mathbf{\Delta v}–\mathbf{\Delta u}) . \tag{3.60}$$

Following similar manipulations in (A.3), for $\mathbf{R} = \mathbf{I}_N$ we have

$$(\mathbf{v}–\mathbf{u})^T \mathbf{R}^{-1} (\mathbf{v}–\mathbf{u}) = \sum_{i=1}^{N} g_i^2. \tag{3.61}$$

Since the malicious user's true location cannot be the same as his claimed location, i.e., $\mathbf{x}_t \neq \mathbf{x}_c$, we have $\mathbf{v} \neq \mathbf{u}$ and $\left(\sum_{i=1}^{N} g_i\right)^2 > 0$. As such, as per (A.3) and (3.61) we have

$$(\mathbf{v}–\mathbf{u})^T \mathbf{R}^{-1} (\mathbf{v}–\mathbf{u}) > (\mathbf{w}–\mathbf{u})^T \mathbf{R}^{-1} (\mathbf{w}–\mathbf{u}) . \tag{3.62}$$

Based on (A.1) and (3.62), we have proved (3.60), which completes the proof of Corollary 1.

We note that Corollary 1 presents a fair comparison between the RSS-based LVS and the DRSS-based LVS when the malicious user does not know the transmit power of the legitimate user and thus cannot optimize his transmit power.

Under the best attack strategies of the malicious user, the comparison result between the RSS-based LVS and the DRSS-based LVS is present in the following corollary.

Corollary 2 We have $\alpha_R^* = \alpha_D^*$ and $\beta_R^* = \beta_D^*$ for $\lambda_R^* = \lambda_D^*$. That is, the performance of the RSS-based LVS for $p_x = p_x^*$ and $\mathbf{x}_t = \mathbf{x}_t^*$ is identical to the performance of the DRSS-based LVS for $\mathbf{x}_t = \mathbf{x}_t^\ddagger$.

We now prove Corollary 2. Based on Theorem 4, in order to prove Corollary 2 we only have to prove $\mathbf{x}_t^* = \mathbf{x}_t^\ddagger$. We note that $\mathbf{x}_t^*$ and $\mathbf{x}_t^\ddagger$ are obtained through minimizing $\phi(p_x^o(\mathbf{x}_t), \mathbf{x}_t)$ and $\varphi(\mathbf{x}_t)$, respectively. As such, in order to prove $\mathbf{x}_t^* = \mathbf{x}_t^\ddagger$, it suffices to prove $\phi(p_x^o(\mathbf{x}_t), \mathbf{x}_t) = \varphi(\mathbf{x}_t)$. As per (3.15) and (3.40), we can see that we have proved $\phi(p_x^o(\mathbf{x}_t), \mathbf{x}_t) = \varphi(\mathbf{x}_t)$ in (A.1).

We note that Corollary 2 presents a comparison between the performance limits of the RSS-based LVS and the DRSS-based LVS. In the proof of Corollary 2, we also proved that the malicious user's optimal true location for the RSS-based LVS is the same as that for the DRSS-based LVS. We also note that the analysis and results reported in this chapter are not directly applicable to the colluding threat scenario (where multiple colluding adversaries attack the LVS). Future studies may wish to explore these more sophisticated attacks in the context of correlated fading channels. However, although such sophisticated attacks will obviously lead to poorer LVS performance, a conjecture is that the trends discovered here with regard to the impact of correlated shadowing on LVS performance will persist.

3.6 Numerical and Simulation Results

We now present numerical results to verify the accuracy of our provided analysis in this chapter. We also provide some insights on the impact of the spatially correlated shadowing on the performance of the RSS-based LVS and the DRSS-based LVS.

Although we have simulated a wide range of system settings, the associated settings for the results shown in this chapter (unless otherwise stated) are as follows. We carry out simulations that resemble settings anticipated for emerging VANETs. In the simulations specifically shown here, the BSs and the claimed locations are deployed in a rectangular area 500m by 20m. The origin is set at the center of the rectangular area, with the x-coordinate taken along the length, and the y-coordinate taken along the width. The claimed location of a user (legitimate or malicious) is set such as $\mathbf{x}_c = (50, 5)$, which is also the true location of the legitimate user. The locations of all BSs are provided in the caption of each figure, and all BSs collect measurements from the legitimate and malicious users. The path loss exponent is set to $\gamma = 3$, and the reference power is set to $p = -10$ dB at $d = 1$m.

In Fig. 3.1, we present the ROC curves of the RSS-based LVS. In order to obtain this figure, we have set the BSs at regular intervals (250m) on each side of the

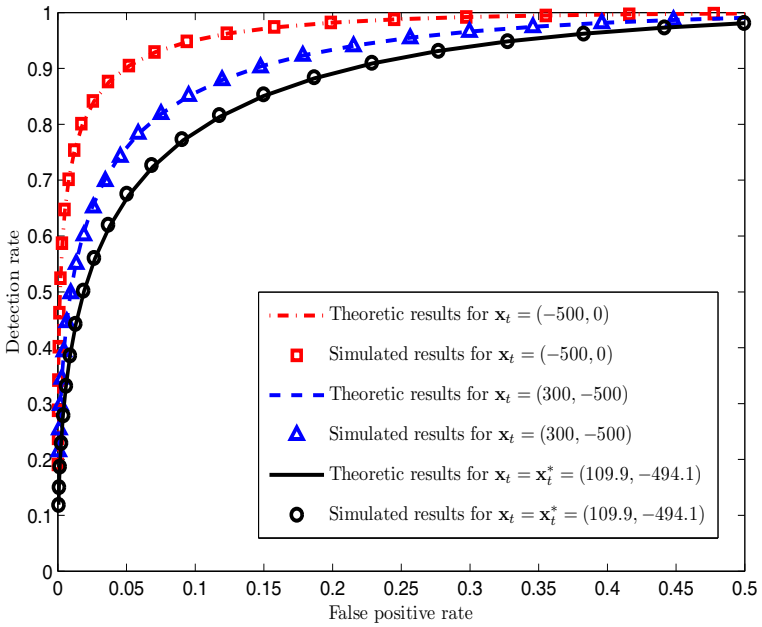

Figure 3.1: ROC curves of the RSS-based LVS for $\sigma_{dB} = 7.5$, $D_c = 50$m, $r = 500$m, $p_x = p_x^o(\mathbf{x}_t)$, and $N = 3$ $\big(\mathbf{x}_1 = (-250, 10)$, $\mathbf{x}_2 = (0, -10)$, and $\mathbf{x}_3 = (250, 10)\big)$.

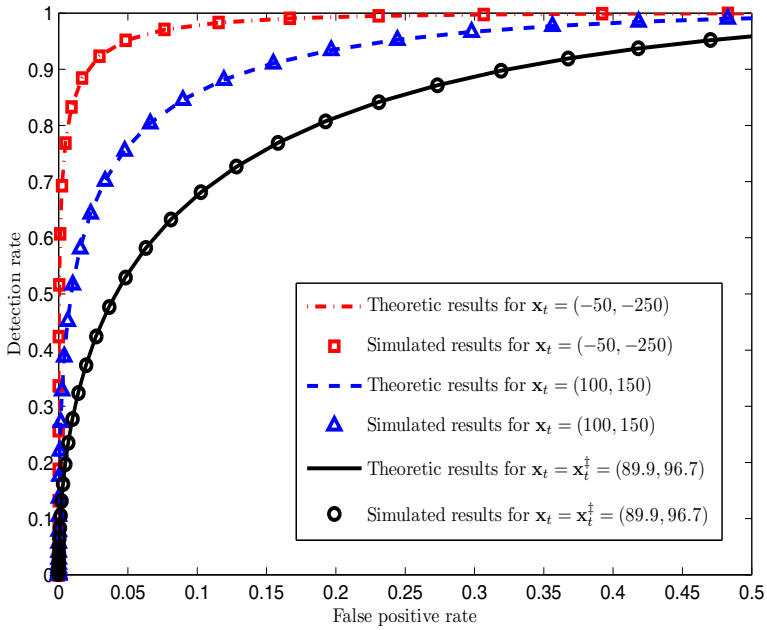

Figure 3.2: ROC curves of the DRSS-based LVS for $\sigma_{dB} = 5$, $D_c = 50$m, $r = 100$m, and $N = 4$ $\big(\mathbf{x}_1 = (201.4, -9.0)$, $\mathbf{x}_2 = (-161.7, 9.3)$, $\mathbf{x}_3 = (-97.4, 1.2)$, and $\mathbf{x}_4 = (91.5, 2.4)\big)$.

rectangular area. In this figure, we first observe that the Monte Carlo simulations precisely match the theoretic results, confirming our analysis in Theorem 2. We also observe that the ROC curves for $\mathbf{x}_t \neq \mathbf{x}_t^*$ dominate the ROC curve for $\mathbf{x}_t = \mathbf{x}_t^*$. This observation indicates that if the malicious user does not optimize his true location, it will be easier for the RSS-based LVS to detect the malicious user. In summary, the ROC curve for $\mathbf{x}_t = \mathbf{x}_t^*$ (analysis presented in (3.33) and (3.34)) provides a lower bound for the performance of the RSS-based LVS.

In Fig. 3.2, we present the ROC curves of the DRSS-based LVS. In order to obtain this figure, we have deployed the BSs randomly inside the rectangular area, which relates to a scenario where authorized vehicles represent the BSs. In this scenario the authorized vehicles already have their locations authenticated, and they are used as anchor points in authenticating the positions of yet-to-be authorized vehicles. In this figure, we first observe that the Monte Carlo simulations precisely match the theoretic results, confirming our analysis in Theorem 3. We also observe that the ROC curves for $\mathbf{x}_t \neq \mathbf{x}_t^\ddagger$ dominate the ROC curve for $\mathbf{x}_t = \mathbf{x}_t^\ddagger$. Again, this observation demonstrates the importance of optimally choosing the true location for the malicious user. To conclude, the ROC curve for $\mathbf{x}_t = \mathbf{x}_t^\ddagger$ (analysis presented in (3.55) and (3.56)) provides a lower bound for the performance of the DRSS-based LVS.

In Fig. 3.3, we present the ROC curves of the RSS-based LVS and the DRSS-based LVS. In order to obtain this figure, we have set one of the BSs at one side of the rectangular area and deployed the other two BSs randomly inside the rectangular area. This mimics the scenario in which only one fixed BS is available and we have to conduct location verification with the help of two already-authorized vehicles. In this figure, we first observe that the RSS-based LVS for $p_x = p_x^o(\mathbf{x}_t)$ and the DRSS-based LVS achieve identical performance (identical ROC curves). This demonstrates that as long as the malicious user optimizes his transmit power (as per his true location) the RSS-based LVS is identical to the DRSS-based LVS, which confirms the analytical comparison between the RSS-based LVS and the DRSS-based LVS presented in Theorem 4. We also observe that the ROC curves of the RSS-based LVS

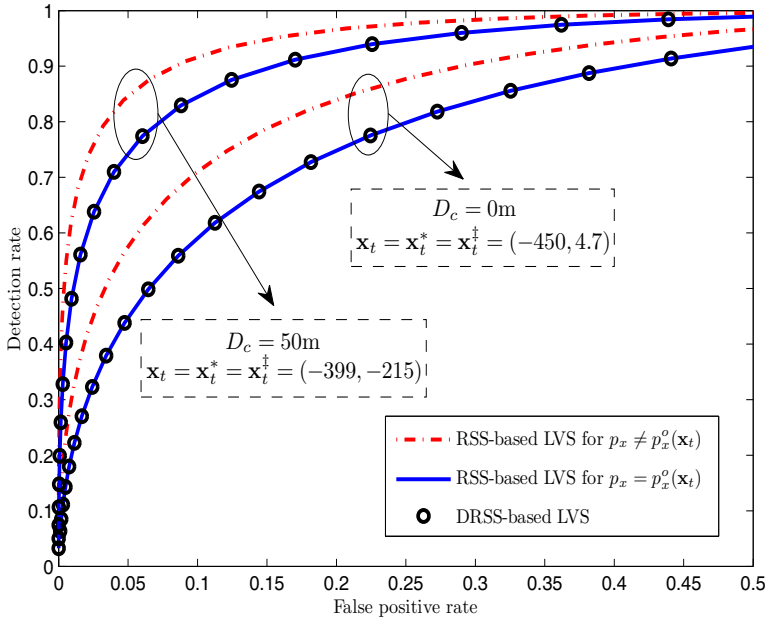

Figure 3.3: ROC curves of the RSS-based LVS and the DRSS-based LVS for $\sigma_{dB} = 5$, $D_c = 50$m, $r = 100$m, and $N = 3$ $\big(\mathbf{x}_1 = (0, 10)$, $\mathbf{x}_2 = (131.4, -9.3)$, and $\mathbf{x}_3 = (20.6, -0.9)\big)$.

for $p_x \neq p_x^o(\mathbf{x}_t)$ dominate the ROC curves of the DRSS-based LVS. This observation confirms that if the malicious user does not optimize his transmit power, the RSS-based LVS achieves a better performance than the DRSS-based LVS, which is provided in Corollary 1. This indicates that the RSS-based LVS is subjectively better than the DRSS-based LVS since the performance of the DRSS-based LVS is independent of the malicious user's transmit power and the determination of the optimal transmit power for the malicious user is no longer required in the DRSS-based LVS. In the simulations of Fig. 3.3, we confirmed that the malicious user's optimal true location for the RSS-based LVS is the same as that for the DRSS-based LVS, i.e., $\mathbf{x}_t^* = \mathbf{x}_t^\ddagger$. As such, Fig. 3.3 also confirms our analysis provided in Corollary 2.

In Fig. 3.4 and Fig. 3.5, we investigate the impact of the spatial correlation of the shadowing on the performance of the RSS-based LVS and the DRSS-based LVS, where $D_c = 0$m corresponds to the case with uncorrelated shadowing. In Fig. 3.4, we set $p_x = p_x^*$ and $\mathbf{x}_t = \mathbf{x}_t^*$ for the RSS-based LVS. From (3.12) and (3.17), we can

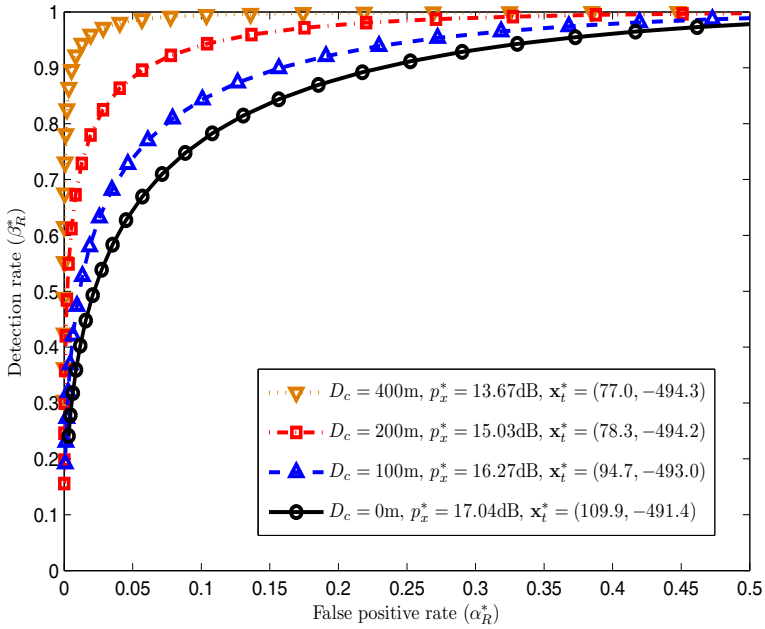

Figure 3.4: ROC curves of the RSS-based LVS for $\sigma_{dB} = 7.5$, $r = 500$m, $p_x = p_x^*$, $\mathbf{x}_t = \mathbf{x}_t^*$, and $N = 3$ $\big(\mathbf{x}_1 = (-250, 10)$, $\mathbf{x}_2 = (0, -10)$, and $\mathbf{x}_3 = (250, 10)\big)$.

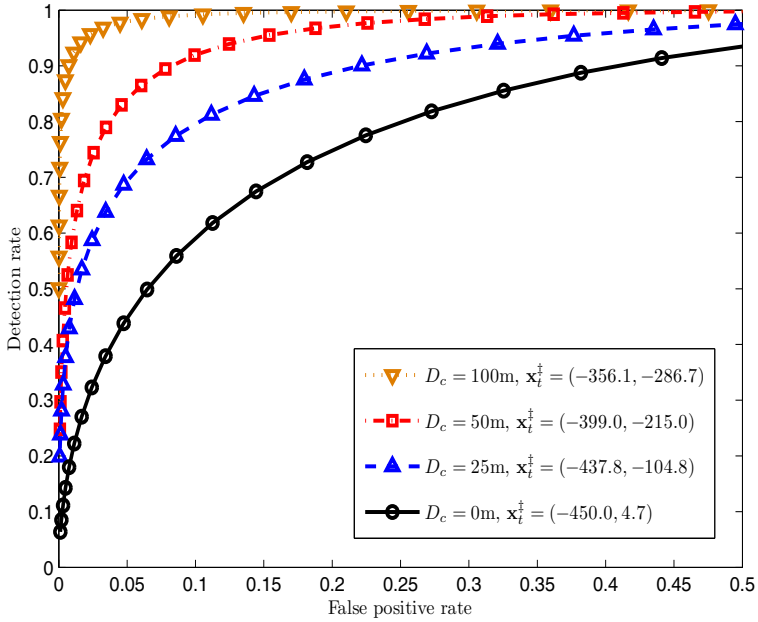

Figure 3.5: ROC curves of the DRSS-based LVS for $\sigma_{dB} = 5$, $D_c = 50$m, $r = 100$m, and $N = 3$ $\big(\mathbf{x}_1 = (0, 10)$, $\mathbf{x}_2 = (131.4, -9.3)$, and $\mathbf{x}_3 = (20.6, -0.9)\big)$.

see that both p_x^* and $\mathbf{x}_t^*$ are dependent on the spatial correlation of the shadowing (they are both functions of D_c), and the exact values of p_x^* and $\mathbf{x}_t^*$ corresponding to each D_c are also provided in Fig. 3.4. In this figure, we first observe the ROC curve moves toward the upper left corner (i.e., the area under the ROC curve increases) as D_c increases, which shows that the performance of the RSS-based LVS becomes better as D_c increases. This observation demonstrates that the spatial correlation of the shadowing improves the detection performance of the RSS-based LVS under the specific settings. We note that the above performance improvement due to the spatial correlation of the shadowing is only achieved under the condition $p_x = p_x^*$ and $\mathbf{x}_t = \mathbf{x}_t^*$. If the malicious user is physically limited at some specific location $\mathbf{x}_t$ and he optimizes his transmit power as per $\mathbf{x}_t$, i.e., $p_x = p_x^o(\mathbf{x}_t)$, the spatial correlation of the shadowing does not have a monotonic impact on the performance of the RSS-based LVS. As per Theorem 4 and Corollary 2, the ROC curves provided in Fig. 3.4 are also valid for the DRSS-based LVS, in which we have to set $\mathbf{x}_t = \mathbf{x}_t^\ddagger$. As such, we can conclude that the spatial correlation of the shadowing can also improve the detection performance of the DRSS-based LVS. Also, for a determined $\mathbf{x}_t$ the spatial correlation does not have a monotonic impact on the performance of the DRSS-based LVS. For confirmation, we also provide the ROC curves for the DRSS-based LVS in Fig. 3.5 under different settings. The same conclusion on the impact of spatial correlation of the shadowing can be drawn from Fig. 3.5.

In Fig. 3.6, we examine the impact of the parameter r on the performance of both the RSS-based LVS and the DRSS-based LVS. We note that r is the minimum distance between the claimed location and the malicious user's true location. As such, the disc determined by $\mathbf{x}_c$ and r can be interpreted as the area protected by some physical boundaries. In Fig. 3.6, we observe that the ROC curve moves toward the upper left corner as r increases, which indicates that the malicious user will be easier to detect if he is further away from his claimed location. We also observe that the performance improvement due to increasing r is not significant when r is larger than some specific value (e.g., $r > 250$m).

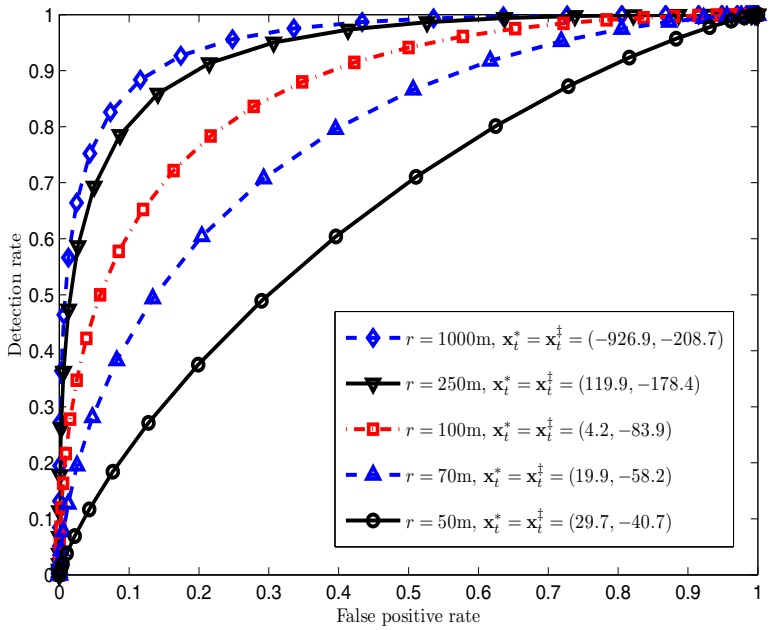

Figure 3.6: ROC curves of the RSS-based LVS ($p_x = p_x^*$) and the DRSS-based LVS for $\sigma_{dB} = 5$, $D_c = 50$m, $\mathbf{x}_t = \mathbf{x}_t^* = \mathbf{x}_t^\ddagger$, and $N = 3$ $\big(\mathbf{x}_1 = (0, 10)$, $\mathbf{x}_2 = (131.4, -9.3)$, and $\mathbf{x}_3 = (20.6, -0.9)\big)$.

3.7 Summary

In this chapter we have formally analyzed for the first time, the performances of two important types of LVSs, RSS and DRSS-based, in the regime of spatially correlated shadowing. Although generally applicable to a range of wireless networks, our analysis illustrates that for anticipated levels of correlated shadowing in a VANETs environment, both types of LVSs will have much improved performance. In addition, we formally proved that in fact the DRSS-based LVS has identical performance to that of the RSS-based LVS, for all levels of correlated shadowing. Even more surprisingly, the identical performance of RSS and DRSS-based LVSs was found to hold even when the adversary cannot optimize his true location. We found the performance of the RSS-based LVS to be better than that of the DRSS-based LVS only in the case where the adversary cannot optimize *all* variables under her control. The results presented here will be important for all practical location authentication systems deployed in support of emerging VANETs applications.

Chapter 4

Location Verification Systems in Rician Fading Channels

4.1 Introduction

The adverse effects of location spoofing can be more severe in VANETs due to the wide utilization of location information in VANETs. The integrity of claimed locations in VANETs is therefore important, and motivates the introduction of an LVS to VANETs. In Chapter 2 and Chapter 3, we developed optimal RSS-based LVSs for general wireless networks by considering uncorrelated and spatially correlated shadowing. Although these developed LVSs can be deployed in VANETs, some specific properties of VANETs (e.g., dedicated wireless channel conditions) were not explicitly explored.

In this chapter, we develop and analyze an optimal LVS for VANETs under Rician channels. This is motivated by the fact that in VANETs environments Rician channels are anticipated to dominate the channel characteristics [105, 106]. In addition, how the detection performance of an LVS is dependent on some properties of these Rician channels was not explicitly explored in the literature. For example, in [48] the authors utilized on-board radar systems to verify a vehicle's claimed location

(obtained through a GPS system). Considering the system noise, the authors first determined the GPS position tolerance shadow and radar position tolerance shadow, separately. The threshold and performance of the proposed location verification algorithm is determined by the accuracy of the GPS and radar systems. The time required to detect a malicious user is used as the evaluation criterion. However, the dependence between detection performance of the proposed LVS and the specific channel properties was not analyzed. In VANETs several important gaps in our knowledge of LVS performances and reliabilities under Rician channels remain. Among these are, (i) the optimal performance of an LVS as a function of the wireless channel conditions, and (ii) the optimal performance of an LVS as a function of the tracking information on a vehicle. These two open issues are of particular relevance to the VANETs environment, and the resolution of them forms the core of the work presented in this chapter. We note that how the detection performance of an LVS depends on the tracking information on a vehicle was investigated in [32]. A wireless intrusion detection system based on the utilization of position tracking and the localization error bounds of Extended Kalman Filters is developed in [32]. It is shown in [32] that the detection errors of the system with tracking information can be an order of magnitude smaller relative to that of the system with only a static location. However, the optimality of the location spoofing detection system with tracking was not discussed in [32].

With regard to our first issue, the specific question we wish to answer is *"How does the optimal detection performance of an LVS quantitatively depend on the proportion of the LOS (line-of-sight) relative to non-LOS in a wireless channel?"*. The proportion of the LOS relative to non-LOS in a wireless channel impacts the characteristics of observations obtained over wireless channels, such as the shadowing variance of RSS, the estimation error of TOA, and the statistics on AOA determinations. The follow-on impact of such effects on LVS performances is non-trivial. Our approach in addressing this question will be to first determine the optimal attack strategy of the malicious vehicle, and then to use that in order to conduct a formal theoretical

analysis on the LVS performance. With regard to our second issue, we pose the specific question: *How does the tracking information on a vehicle quantitatively improve the detection performance of an LVS?* This question is of practical significance since under some channel conditions the detection performance of an LVS with a only single claimed location (no tracking) is unfavorable. We address this issue by first formally developing the optimal decision rule of an LVS via an LRT based on the track of claimed locations and then analyze the detection performance of an LVS when such tracking information is available.

In order to explicitly answer the above two questions, the directions and some specific contributions of this chapter are summarized as follows. We first determine the optimal attack strategy of a malicious vehicle. To this end, after deriving the optimal transmit power and the optimal beamformer for the malicious vehicle at an arbitrary location, we identify the optimal locations of the malicious vehicle (best locations to launch an attack). Our analysis indicates that these optimal locations are determined solely by a single direction (due to the ability of the malicious vehicle to vary his transmit power and beamformer). Our analysis also reveals that the detection performance of an LVS will not be a function of the number of antennas held by the malicious vehicle once this number is above a derived bound. We next establish that the optimal attack direction is that set by the direction from the claimed location to the BS, and show how the malicious vehicle can perfectly imitate the signals expected from a legitimate vehicle if the malicious vehicle can find a location in this optimal direction with non-zero LOS. However, given a constraint imposed that the true location of the malicious vehicle should be some minimum distance from its claimed location, such an optimal attack direction may not be viable. Considering unlimited resources possessed by the malicious vehicle (e.g., unlimited number of antennas), the LVS can determine the actual (now sub-optimal) best attack location given the constraint. We present how all of these findings allow us to establish lower bounds (worst-case scenario) on the detection performance of the LVS. We next extend our analysis to a tracking version of the LVS where multiple claimed locations

and observations are utilized, showing how an extension of our previous analysis can lead to a range of similar outcomes, but with improved detection performance. A key part of the tracking LVS which allows for these findings is that the number of claimed locations and observations used for the decision-making process is randomly selected. Additional constraints on the tracking LVS solutions, imposed by speed limitations of the malicious vehicle, are presented. Finally, we present extensions of our analysis that take into account non-linear antenna arrays, and discuss the detection performance of the LVS in the presence of colluding attacks.

The rest of this chapter is organized as follows. Section 4.2 details our system model. In Section 4.3, the optimal attack strategy of the malicious vehicle is determined, based on which the detection performance of the LVS is analyzed. Section 4.4 formalizes the optimal decision rule of the LVS when tracking information of the claimed location is available. In Section 4.5, we present numerical results to verify our analysis and we also draw some important insights based on our analysis. In Section 4.6, we discuss potential extension directions of our analysis and the impact of colluding attacks on an LVS. Finally, Section 4.7 draws concluding remarks.

4.2 System Model

4.2.1 System Assumptions

We represent the inputs of an LVS as binary hypotheses, the null hypothesis $\mathcal{H}_0$ and the alternative hypothesis $\mathcal{H}_1$. Under $\mathcal{H}_0$ the vehicle is legitimate and provides to the LVS a claimed location equal to its true location. Under $\mathcal{H}_1$ the vehicle is malicious[1] and provides to the LVS a claimed location which is not its true location (a spoofed location). We consider a VANETs application scenario, where the BS, the

[1]Note, although we will often refer to the attacker as the *malicious vehicle*, we should bear in mind that in reality the attacker may not be a vehicle (e.g., could be a generic device/user situated anywhere).

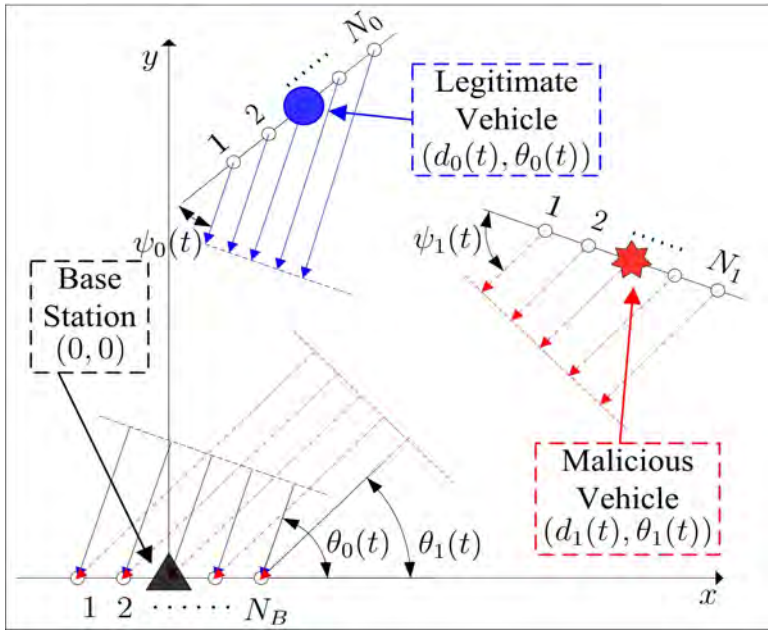

Figure 4.1: Illustration of the orientations of the three ULAs and the geometry of the BS, the legitimate vehicle, and the malicious vehicle. We note that N_1, $d_1(t)$, $\theta_1(t)$, and $\psi_1(t)$ are not assumed to be known to the LVS.

legitimate vehicle, and the malicious vehicle are all equipped with Uniform Linear Arrays (ULAs). We discuss later the impact of non-linear antenna arrays. The number of antenna elements of the ULAs at the BS, the legitimate vehicle, and the malicious vehicle are N_B, N_0, and N_1, respectively. Utilizing observations obtained over wireless channels, the BS is to verify whether the vehicle is indeed at its claimed location or not, thus inferring whether the vehicle is legitimate or malicious. In the first instance we will assume the presence of only one malicious vehicle (we discuss colluding attacks later).

We adopt the polar coordinate system (d_k, θ_k) in this chapter ($k \in \{0, 1\}$), where d_0 (d_1) is the distance from the origin to the center of the legitimate (malicious) vehicle's ULA, and θ_0 (θ_1) represents the angle measured counterclockwise from the x-axis to the line connecting the center of the legitimate (malicious) vehicle's ULA to the origin. The location of the BS is selected as the origin, and the BS's ULA is aligned with the x-axis (antenna elements all on x-axis). A schematic of our assumed set-up is

shown in Fig. 4.1. The claimed location of a vehicle (legitimate or malicious) at time slot t ($t = 1, 2, \ldots, T$) is denoted as $\mathbf{x}_c(t) = (d_c(t), \theta_c(t))$, which is supplied to the LVS and to be verified (note, the LVS may be embedded in the BS). The true location of the vehicle under $\mathcal{H}_0$ (the legitimate vehicle's true location) at t is denoted as $\mathbf{x}_0(t) = (d_0(t), \theta_0(t))$. The true location of the vehicle under $\mathcal{H}_1$ (the malicious vehicle's true location) at t is denoted as $\mathbf{x}_1(t) = (d_1(t), \theta_1(t))$. Since the legitimate vehicle reports its true location to the LVS, we have $\mathbf{x}_c(t) = \mathbf{x}_0(t)$. We adopt a practical threat model, in which the distance between the malicious vehicle's true location and its claimed location is larger than some specific value r_l (i.e., $\|\mathbf{x}_1(t) - \mathbf{x}_c(t)\| > r_l$). We note that this assumption is reasonable since the malicious vehicle does not need to spoof its claimed location if $\|\mathbf{x}_1(t) - \mathbf{x}_c(t)\|$ is very small. The value of r_l can be predetermined based on some specific application scenario and in general it is larger than a vehicle's intrinsic position uncertainty. The angles $\psi_0(t)$ and $\psi_1(t)$ as shown in Fig. 4.1 are under the control of the legitimate and malicious vehicles, respectively. We note that $\psi_0(t)$ ($\psi_1(t)$) represents the angle measured counterclockwise from the orientation of the ULA at the legitimate (malicious) vehicle to the line connecting the center of the legitimate (malicious) vehicle's ULA to the origin. Without other statements, we assume all information available to the LVS, BS, and legitimate vehicle is also known to the malicious vehicle. We assume N_1, $\mathbf{x}_1(t)$, and $\psi_1(t)$ are known only by the malicious vehicle. We will assume that N_1 is unbounded (of course in practice this number is constrained by the communication wavelength and the physical dimensions of the vehicle). If in practice the malicious vehicle possesses less than a critical number of antenna elements (to be derived later), then the results presented here represent conservative lower bounds on the LVS performance.

In this chapter we will consider observations collected by only one BS. In general, this represents the most likely (default) scenario for many real-world VANETs. As such, the analysis we provide here should be widely applicable. The analysis for the single BS also forms the basis from which other more complicated scenarios can be built upon. For example, in instances where additional BSs are within range

of claimed positions, the work presented in this chapter can be readily adapted to account for that.[2] A conceptually simple method of doing this would be for each additional BS to be allocated a separate LVS which can then cooperate with other LVSs (BSs) in order to make optimally-joint decisions.

4.2.2 Channel Model

We assume the channel from a vehicle (legitimate or malicious) to the BS is subject to Rician fading. Then, the $N_B \times N_k$ channel matrix at t under $\mathcal{H}_k$ is given by

$$\mathbf{H}_k(t) = \sqrt{\frac{K_k(t)}{1+K_k(t)}}\overline{\mathbf{H}}_k(t) + \sqrt{\frac{1}{1+K_k(t)}}\widetilde{\mathbf{H}}_k(t), \tag{4.1}$$

where $K_k(t)$ is the Rician K-factor of the channel under $\mathcal{H}_k$ (we assume $K_k(t)$ is a function the vehicle's true location), $\overline{\mathbf{H}}_k(t)$ is the LOS component of $\mathbf{H}_k(t)$, and $\widetilde{\mathbf{H}}_k(t)$ is the scattered component of $\mathbf{H}_k(t)$. The entries of $\widetilde{\mathbf{H}}_k(t)$ are independent and identically distributed (i.i.d.) circularly-symmetric complex Gaussian random variables with zero mean and unit variance. We assume that $\widetilde{\mathbf{H}}_k(t)$ is i.i.d. in different time slots. Denoting ρ_B as the space between two adjacent antenna elements of the ULA at the BS, $\overline{\mathbf{H}}_k(t)$ can be written as $\overline{\mathbf{H}}_k(t) = \mathbf{r}_k(t)\mathbf{t}_k(t)$ [107], where $\mathbf{r}_k(t)$ and $\mathbf{t}_k(t)$ are given by

$$\mathbf{r}_k(t) = \left[1, \cdots, \exp(j(N_B-1)\tau_B \cos\theta_k(t))\right]^T, \tag{4.2}$$

$$\mathbf{t}_k(t) = \left[1, \cdots, \exp(-j(N_k-1)\tau_k \cos\psi_k(t))\right]. \tag{4.3}$$

In (4.2) and (4.3), we have $\tau_B = 2\pi f_c \rho_B / c$ and $\tau_k = 2\pi f_c \rho_k / c$, where f_c is the carrier frequency, c is the speed of propagation of the plane wave, ρ_0 is the space between two antenna elements of the ULA at the legitimate vehicle, and ρ_1 is the space between two antenna elements of the ULA at the malicious vehicle. We note that we assume

[2] We note that other trusted vehicles within range of the claimed position could also be used as additional reference stations. Indeed, vehicles which are considered legitimate (e.g., by consistently passing all LVS decisions over a length of time) can be used to dynamically create/update the K map for a particular BS, at least with regard to all locations on the road.

the LVS knows $K_0(t)$ (e.g., through a predetermined measurement campaign in the vicinity of the BS). We assume $K_1(t)$ is known by the malicious vehicle but not known by the LVS. Note that we will assume that the time dependence for all our variables arises solely from the fact that the vehicle is in general moving (i.e., the variables are functions of location). The exception to this is $\widetilde{\mathbf{H}}_k(t)$, for which the time dependence is also due to the movement of scatterers. Our channel model covers the entire range of conditions from a pure Rayleigh channel ($K = 0$) to a pure LOS channel ($K = \infty$).

4.2.3 Observation Model

The composite observation model is given by

$$\mathcal{H}_k : \mathbf{y}(t) = \sqrt{p_k(t)\mathrm{g}(d_k(t))}\mathbf{H}_k(t)\mathbf{b}_k(t)s + \mathbf{n}_k(t), \tag{4.4}$$

where $p_k(t)$ is the transmit power of the vehicle under $\mathcal{H}_k$,[3] $\mathrm{g}(d_k(t))$ is the path loss gain under $\mathcal{H}_k$ given by $\mathrm{g}(d_k(t)) = (c/4\pi f_c d_r)^2 (d_r/d_k(t))^{\xi}$, d_r is a reference distance, ξ is the path loss exponent, $\mathbf{b}_k(t)$ is the beamformer adopted by the vehicle under $\mathcal{H}_k$ that satisfies $\|\mathbf{b}_k(t)\| = 1$, s is the publicly known pilot symbol satisfying $\|s\| = 1$, and $\mathbf{n}_k(t)$ is the additive white Gaussian noise vector at t under $\mathcal{H}_k$, of which the entries are i.i.d. circularly-symmetric complex Gaussian random variables with zero mean and variance σ_k^2. We note that for simplicity we assume that ξ is independent of a vehicle's location and is the same for all power components (i.e., $\overline{\mathbf{H}}_k(t)$ and $\widetilde{\mathbf{H}}_k(t)$) since we have assumed that $K_k(t)$ is a function of a vehicle's location [108]. As we show later, our analysis still holds even if ξ is a function of a vehicle's location and is different for $\overline{\mathbf{H}}_k(t)$ and $\widetilde{\mathbf{H}}_k(t)$. We assume that the legitimate vehicle adopts constant transmit power, i.e., $p_0(t) = p_0$. However, we note that $p_1(t)$ varies. This is due to the fact that the malicious vehicle can adjust its transmit power based on each pair

[3]We will be conservative and assume the attacker has unlimited power resources. If a power constraint (on attacker) is introduced some of the attacks we describe later may not be possible, and in these circumstances the LVS performances shown can be considered lower bounds (worst-case scenarios).

of $\mathbf{x}_0(t)$ and $\mathbf{x}_1(t)$. We also assume that $\mathbf{n}_k(t)$ is i.i.d. in different time slots. We note that $\mathbf{b}_0(t)$ and p_0 are under the control of the legitimate vehicle. We assume that the legitimate vehicle cooperates with the BS to facilitate the location verification. To this end, the legitimate vehicle sets $\mathbf{b}_0(t) = \mathbf{t}_0^\dagger(t)/\|\mathbf{t}_0(t)\|$ so as to maximize $|\mathbf{t}_0(t)\mathbf{b}_0(t)|$. In addition, the legitimate vehicle sets its transmit power to the required value by the BS (we assume p_0 is publicly known). Again, we assume neither $p_1(t)$ nor $\mathbf{b}_1(t)$ is known to the LVS. According to (4.1) and (4.4), the likelihood function of $\mathbf{y}(t)$ conditioned on a known s under $\mathcal{H}_k$ is

$$f(\mathbf{y}(t)|\mathcal{H}_k) = \frac{1}{\pi^{N_B}\det(\mathbf{R}_k(t))}\exp\left[-(\mathbf{y}(t)-\mathbf{m}_k(t))^\dagger \mathbf{R}_k^{-1}(t)(\mathbf{y}(t)-\mathbf{m}_k(t))\right], \tag{4.5}$$

where $\mathbf{m}_k(t)$ and $\mathbf{R}_k(t)$ are the mean vector and covariance matrix of $\mathbf{y}(t)$ under $\mathcal{H}_k$, respectively, which are given by

$$\mathbf{m}_k(t) = \sqrt{\frac{p_k(t)\mathrm{g}(d_k(t))K_k(t)}{1+K_k(t)}}\overline{\mathbf{H}}_k(t)\mathbf{b}_k(t), \tag{4.6}$$

$$\mathbf{R}_k(t) = \left(\frac{p_k(t)\mathrm{g}(d_k(t))}{1+K_k(t)} + \sigma_k^2\right)\mathbf{I}_{N_B}. \tag{4.7}$$

We note that we have $\overline{\mathbf{H}}_0(t)\mathbf{b}_0(t) = \sqrt{N_0}\mathbf{r}_0(t)$ due to $\mathbf{b}_0(t) = \mathbf{t}_0^\dagger(t)/\|\mathbf{t}_0(t)\|$. We also note that $f(\mathbf{y}(t)|\mathcal{H}_1)$ is dependent on $p_1(t)$, $\mathbf{b}_1(t)$, and $\mathbf{x}_1(t)$. Thus, we also denote $f(\mathbf{y}(t)|\mathcal{H}_1)$ as $f\left(\mathbf{y}|p_1(t),\mathbf{b}_1(t),\mathbf{x}_1(t),\mathcal{H}_1\right)$. These parameters (i.e., $p_1(t)$, $\mathbf{b}_1(t)$, and $\mathbf{x}_1(t)$) are all under the control of the malicious vehicle and are unknown to the LVS. In the next section, we will discuss how the malicious vehicle optimally sets these parameters in order to minimize the probability of being detected by the LVS.

4.3 Location Verification System Without Tracking

In this section we examine the performance of the LVS by considering only one claimed location and one observation snapshot at the BS antennas (i.e., BS measurements made in one time slot, and $T = 1$). As such, we drop explicit reference to (t) for all

variables in this section. We first present the decision rule and performance metrics adopted in this LVS. We then discuss the optimal attack strategy of the malicious vehicle (i.e., how to optimally set p_1, $\mathbf{b}_1$, and $\mathbf{x}_1$) in order to minimize the probability to be detected. Finally, we analyze the detection performance of the LVS based on this optimal attack strategy.

4.3.1 Decision Rule of the LVS

We adopt the LRT as the decision rule of the LVS. This is due to the fact that the LRT achieves the highest detection rate for any given false positive rate [86]. The LRT decision rule is given by

$$\Lambda(\mathbf{y}) \triangleq \frac{f(\mathbf{y}|p_1, \mathbf{b}_1, \mathbf{x}_1, \mathcal{H}_1)}{f(\mathbf{y}|\mathcal{H}_0)} \underset{\mathcal{D}_0}{\overset{\mathcal{D}_1}{\gtrless}} \lambda, \tag{4.8}$$

where $\Lambda(\mathbf{y})$ is the likelihood ratio of $\mathbf{y}$, λ is the threshold for $\Lambda(\mathbf{y})$, and $\mathcal{D}_0$ and $\mathcal{D}_1$ are the binary decisions that infer whether the vehicle is legitimate or malicious, respectively. Given the decision rule in (4.8), the false positive and detection rates of the LVS are functions of λ. Note, the false positive rate is given by $\alpha(\lambda) = \Pr(\Lambda(\mathbf{y}) > \lambda|\mathcal{H}_0)$, and detection rate is given by $\beta(\lambda) = \Pr(\Lambda(\mathbf{y}) > \lambda|\mathcal{H}_1)$. The specific value of λ can be set through predetermining a false positive rate, minimizing the Bayes' average cost, or maximizing the mutual information between the system input and output as what we did in Chapter 2. In order to quantitatively examine the impact of some system parameters on the detection performance of the LVS, we have to adopt a unique metric to evaluate the LVS. When it is necessary, we adopt a special Bayes' average cost as the unique performance metric, which is the total error. The total error is obtained by setting the costs of correct and incorrect decisions as zeros and ones, respectively [34]. The total error can be expressed as

$$\epsilon(\lambda) = P_0\alpha(\lambda) + (1 - P_0)(1 - \beta(\lambda)), \tag{4.9}$$

where P_0 and $1 - P_0$ are the *a priori* probabilities that the vehicle is legitimate and malicious, respectively. Based on the Bayesian framework, the optimal value of λ

that minimizes $\epsilon(\lambda)$ is given by $\lambda^* = P_0/(1-P_0)$ [34]. Substituting λ^* into (4.9), we can obtain the minimum value of $\epsilon(\lambda)$, referred to as the *minimum total error* and denoted by ϵ^*.

4.3.2 Optimal Attack Strategy Against the LVS

Knowing (4.8), the malicious vehicle is to minimize the difference between $f(\mathbf{y}|\mathcal{H}_0)$ and $f(\mathbf{y}|p_1, \mathbf{b}_1, \mathbf{x}_1, \mathcal{H}_1)$ in order to minimize the detection rate. It can be shown that minimization of the KL divergence from $f(\mathbf{y}|p_1, \mathbf{b}_1, \mathbf{x}_1, \mathcal{H}_1)$ to $f(\mathbf{y}|\mathcal{H}_0)$ leads to the minimum detection rate [109]. This is due to that the KL divergence is also the expected log likelihood ratio when the alternative hypothesis $\mathcal{H}_1$ is true. The KL divergence from $f(\mathbf{y}|p_1, \mathbf{b}_1, \mathbf{x}_1, \mathcal{H}_1)$ to $f(\mathbf{y}|\mathcal{H}_0)$ is defined as [104]

$$D_{KL}\left(f(\mathbf{y}|p_1, \mathbf{b}_1, \mathbf{x}_1, \mathcal{H}_1)\,||f(\mathbf{y}|\mathcal{H}_0)\right) = \int \left[\ln \Lambda(\mathbf{y})\right] f(\mathbf{y}|p_1, \mathbf{b}_1, \mathbf{x}_1, \mathcal{H}_1)\, d\mathbf{y}. \tag{4.10}$$

Given this, the optimization problem for the malicious vehicle can be written as

$$(p_1, \mathbf{b}_1, \mathbf{x}_1)^* = \underset{\substack{p_1 \geq 0, \|\mathbf{b}_1\|=1, \\ \|\mathbf{x}_c - \mathbf{x}_1\| \geq r_l}}{\operatorname{argmax}} D_{KL}\left(f(\mathbf{y}|p_1, \mathbf{b}_1, \mathbf{x}_1, \mathcal{H}_1)\,||f(\mathbf{y}|\mathcal{H}_0)\right). \tag{4.11}$$

We present the solutions to (4.11) in two steps. We first derive the optimal values of p_1 and $\mathbf{b}_1$ for any given $\mathbf{x}_1$ in Theorem 5. Then, we search for the optimal value of $\mathbf{x}_1$ numerically, with the aid of Theorem 6.

***Theorem* 5** The optimal values of p_1 and $\mathbf{b}_1$ that minimize the detection rate for any given $\mathbf{x}_1$ are derived as

$$p_1^*(\mathbf{x}_1) = \frac{K_1 + 1}{g(d_1)} \left(\frac{p_0 g(d_0)}{1 + K_0} + \sigma_0^2 - \sigma_1^2 \right), \tag{4.12}$$

$$\mathbf{b}_1^*(\mathbf{x}_1) = \mathbf{U}_* \mathbf{p}^*, \tag{4.13}$$

where $\mathbf{U}_*$ is the left singular and orthogonal matrix of the Singular Value Decomposition (SVD) for $\mathbf{G}_*^\dagger \mathbf{G}_*$, $\mathbf{G}_* = \sqrt{p_1^*(\mathbf{x}_1) \mathrm{g}(d_1) K_1/(1+K_1)}\, \overline{\mathbf{H}}_1$, $\mathbf{p}^*[1] = \mathbf{U}_*^\dagger \mathbf{G}_*^\dagger \mathbf{m}_0[1]/\eta_*$, η_* is the unique eigenvalue of $\mathbf{G}_*^\dagger \mathbf{G}_*$, and $\mathbf{p}^*[i]$ for $i = 2, 3, \cdots, N_1$ can be any value which enables $\|\mathbf{p}^*\| = 1$.

The proof of Theorem 5 is provided in Appendix B.

***Theorem* 6** The optimal value of θ_1 that minimizes the detection rate can be obtained through

$$\theta_1^* = \underset{\|\mathbf{x}_c - \mathbf{x}_1\| \geq r_l}{\operatorname{argmax}} |\mathbf{r}_1^\dagger \mathbf{r}_0|^2. \tag{4.14}$$

We now provide the proof of Theorem 6. Substituting (4.12) and (4.13) into (B.1), we obtain the minimum value of the KL divergence provided in (B.1) for any given $\mathbf{x}_1$ as

$$D_{KL}\left(f\left(\mathbf{y}|p_1^*(\mathbf{x}_1), \mathbf{b}_1^*(\mathbf{x}_1), \mathbf{x}_1, \mathcal{H}_1\right) || f\left(\mathbf{y}|\mathcal{H}_0\right)\right) = \frac{p_0 g(d_0) K_0 N_0}{p_0 g(d_0) + \sigma_0^2(1+K_0)} \left(N_B - \frac{|\mathbf{r}_1^\dagger \mathbf{r}_0|^2}{N_B}\right). \tag{4.15}$$

The malicious vehicle will determine its optimal true location by finding the value of $\mathbf{x}_1$ that minimizes (4.15). We note that in (4.15) only the term $|\mathbf{r}_1^\dagger \mathbf{r}_0|^2$ is a function of θ_1. As such, the malicious vehicle needs only to maximize $|\mathbf{r}_1^\dagger \mathbf{r}_0|^2$ in order find the optimal θ_1. As such, we obtain (4.14).

Based on Theorem 5 and Theorem 6 we obtain the following important insights. (i) We note that once $N_1 = N_1^*$, further increases in N_1 offer no further benefit to the malicious vehicle. That is, the additional degrees of freedom offered by additional antennas beyond N_1^* serve no purpose (in the beamformer solution the malicious vehicle can set power allocated to these additional antennas - if it has them - to zero). (ii) We can see that the minimum KL divergence presented in (4.15) increases as p_0, $g(d_0)$, K_0, or N_0 increases. (iii) We note that the minimum KL divergence presented in (4.15) is zero when $K_0 = 0$, and thus the malicious vehicle can always perfectly imitate the legitimate vehicle (again this issue that could be neutralized by using additional BSs). (iv) We note that the minimum KL divergence provided in (4.15) is not a function of K_1 or σ_1^2. However, we highlight that as $K_1 \to 0$, $N_1^* \to \infty$, meaning $K_1 = 0$ represents the worst case for the malicious vehicle. (v) Based on Theorem 6 we note that θ_1^* is a function of only $\mathbf{r}_0$ (i.e., only depends on N_B and

θ_0). This indicates that the malicious vehicle can directly search for its true location as per Theorem 6, no need to calculate $p_1^*(\mathbf{x}_1)$ or $\mathbf{b}_1^*(\mathbf{x}_1)$ for each $\mathbf{x}_1$. (vi) We also note that θ_1^* is not a function of K_1 or σ_1^2 (except that θ_1^* not defined for $K_1 = 0$). This demonstrates that the optimal true location of the malicious vehicle does not depend on the inherent properties of the malicious channel (the channel between the malicious vehicle and the BS). (vii) Following Theorem 6, we note that there is no *unique* solution to the optimal true location of the malicious vehicle since (4.15) does not depend on d_1. This is due to the fact that the malicious vehicle can adjust its transmit power to counteract the change of d_1 (i.e., $p_1^*(\mathbf{x}_1)$ is a function of d_1).

Following (4.2), we have

$$|\mathbf{r}_1^\dagger \mathbf{r}_0|^2 = \begin{cases} N_B^2, & \cos\theta_0 = \cos\theta_1, \\ \left(\frac{\sin\left(\frac{1}{2}N_B\nu_\theta\right)}{\sin\left(\frac{1}{2}\nu_\theta\right)}\right)^2, & \cos\theta_0 \neq \cos\theta_1, \end{cases} \tag{4.16}$$

where $\nu_\theta = \tau_B(\cos\theta_0 - \cos\theta_1)$. To gain further insights, we plot $|\mathbf{r}_1^\dagger \mathbf{r}_0|^2$ and $N_B - |\mathbf{r}_1^\dagger \mathbf{r}_0|^2/N_B$ versus θ_1/π in Fig. 4.2. In Fig. 4.2 (a), we first observe that the optimal attack is indeed at $\theta_1^* = \pm\theta_0$ (i.e., $\theta_1^* = \pm\theta_c$ due to $\theta_c = \theta_0$). Following (4.16), we note that the minimum KL divergence presented in (4.15) is zero for $\theta_1^* = \pm\theta_c$. This indicates that the malicious vehicle can perfectly imitate the signals expected from a legitimate vehicle at $\mathbf{x}_c$ if the malicious vehicle can set $\theta_1^* = \pm\theta_c$.[4] In Fig. 4.2 (b) we also observe this effect, but this figure also illustrates that if $\theta_1^* = \pm\theta_c$ was not possible (as was the case in this simulation in which the malicious vehicle could not access this angle due to the presence of a non-accessible area) then $|\mathbf{r}_1^\dagger \mathbf{r}_0|^2$ does not necessarily increase as θ_1 approaches θ_0. This is due to the fact that θ_1 minimizes $|\mathbf{r}_1^\dagger \mathbf{r}_0|^2$ at $\arccos\left(\cos\theta_0 + \frac{2n_a\pi}{N_B\tau_a}\right)$ for $n_a = 1, \ldots, N_B - 1$. Comparing Fig. 4.2 (c) with

[4]If additional BSs are in range of the claimed location this form of perfect attack can be neutralized. However, even in the one BS scenario (as we discuss later), when tracking is brought to bear on this issue this type of attack can minimized and even completely neutralized if constraints on the threat model are assumed (e.g., if the attacker is assumed to be another vehicle physically on the same highway as the legitimate vehicle).

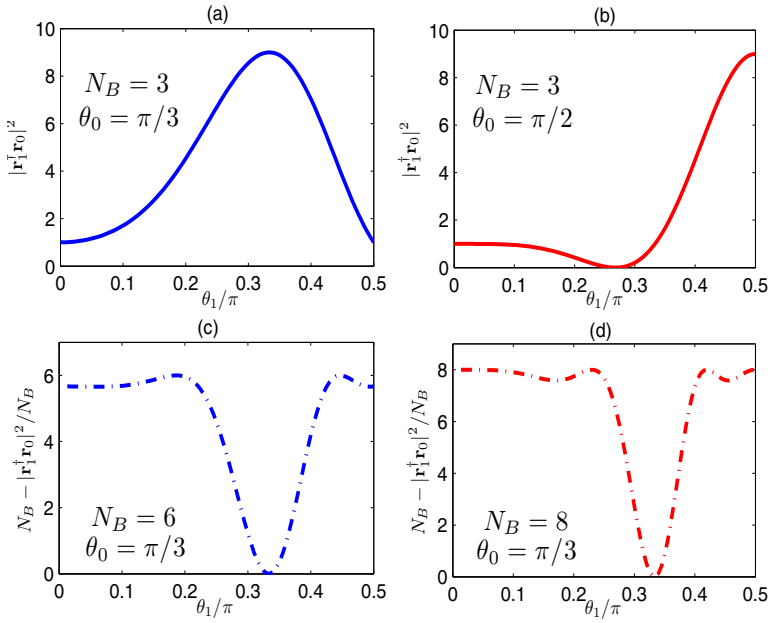

Figure 4.2: $|\mathbf{r}_1^\dagger\mathbf{r}_0|^2$ and $N_B - |\mathbf{r}_1^\dagger\mathbf{r}_0|^2/N_B$ versus θ_1/π for different values of N_B and θ_0, where $\tau_B = \pi$.

Fig. 4.2 (d), we can see that $N_B - |\mathbf{r}_1^\dagger\mathbf{r}_0|^2/N_B$ increases for the larger N_B case. This is consistent with the general rule that the minimum KL divergence presented in (4.15) increases as N_B increases, and thus indicates that the detection performance of the LVS increases as the number of antenna elements at the BS increases.

This above discussion also illustrates the very important role played by the constraint $\|\mathbf{x}_c - \mathbf{x}_1\| \geq r_l$ in (4.14) in limiting any attack. For example, if a claimed location is within r_l to the BS, and a building is between the claimed location and the malicious vehicle, then no LOS component to the BS at the angle $\theta_1^* = \pm\theta_c$ is available to the malicious vehicle. Its actual optimal (now sub-optimal) attack location is then set at another angle. Assuming the malicious vehicle can always access a $\theta_1^* = \pm\theta_c$ location, with a non-zero LOS component to the BS, is therefore the most conservative scenario (worst-case scenario from the LVS perspective).

4.3.3 Detection Performance of the LVS

Without loss of generality, we first analyze the detection performance of the LVS based on any given θ_1. Based on the proof of Theorem 5, we know that $\mathbf{R}_1 = \mathbf{R}_0$ when the malicious vehicle sets $p_1 = p_1^*(\mathbf{x}_1)$. Substituting (4.5), (4.12), and (4.13) into (4.8), the LRT decision rule presented in (4.8) can be written as

$$\mathbb{T}(\mathbf{y}) \underset{\mathcal{D}_0}{\overset{\mathcal{D}_1}{\gtrless}} \Gamma, \tag{4.17}$$

where $\mathbb{T}(\mathbf{y})$ is the test statistic given by

$$\mathbb{T}(\mathbf{y}) = 2\mathrm{Re}\{[\mathbf{m}_1^*(\theta_1) - \mathbf{m}_0]^\dagger \mathbf{R}_0^{-1}\mathbf{y}\}, \tag{4.18}$$

Γ is the threshold for $\mathbb{T}(\mathbf{y})$ given by

$$\Gamma = \ln\lambda + \mathrm{Re}\{[\mathbf{m}_1^*(\theta_1) - \mathbf{m}_0]^\dagger \mathbf{R}_0^{-1}[\mathbf{m}_1^*(\theta_1) + \mathbf{m}_0]\}, \tag{4.19}$$

and $\mathbf{m}_1^*(\theta_1)$ is obtained by substituting (4.12) and (4.13) into (4.6), which is given by

$$\mathbf{m}_1^*(\theta_1) = \sqrt{\frac{p_0 \mathrm{g}(d_0) K_0 N_0}{1 + K_0}} \frac{\mathbf{r}_1 \mathbf{r}_1^\dagger \mathbf{r}_0}{N_B}. \tag{4.20}$$

Next, we derive the false positive rate, $\alpha(\lambda, \theta_1)$, and the detection rate, $\beta(\lambda, \theta_1)$, of the LVS for any given θ_1 in the following theorem.

Theorem 7 The false positive and detection rates of the LVS with $p_1 = p_1^*(\mathbf{x}_1)$ and $\mathbf{b}_1 = \mathbf{b}_1^*(\mathbf{x}_1)$ for any given θ_1 are derived as

$$\alpha(\lambda, \theta_1) = \begin{cases} \tilde{\alpha}(\lambda, \theta_1), & \theta_1 \neq \pm\theta_c, \\ \mathbf{1}_A(-\Gamma) = \mathbf{1}_A(-\ln\lambda), & \theta_1 = \pm\theta_c, \end{cases} \tag{4.21}$$

$$\beta(\lambda, \theta_1) = \begin{cases} \tilde{\beta}(\lambda, \theta_1), & \theta_1 \neq \pm\theta_c, \\ \mathbf{1}_A(\Gamma) = \mathbf{1}_A(\ln\lambda), & \theta_1 = \pm\theta_c, \end{cases} \tag{4.22}$$

where

$$\tilde{\alpha}(\lambda,\theta_1)=\mathcal{Q}\left\{\frac{\Gamma-2\mathrm{Re}\{[\mathbf{m}_1^*(\theta_1)-\mathbf{m}_0]^\dagger\mathbf{R}_0^{-1}\mathbf{m}_0\}}{\sqrt{2[\mathbf{m}_1^*(\theta_1)-\mathbf{m}_0]^\dagger\mathbf{R}_0^{-1}[\mathbf{m}_1^*(\theta_1)-\mathbf{m}_0]}}\right\}=\mathcal{Q}\left\{\frac{\ln\lambda+D(\theta_1)}{\sqrt{2D(\theta_1)}}\right\}, \quad (4.23)$$

$$\tilde{\beta}(\lambda,\theta_1)=\mathcal{Q}\left\{\frac{\Gamma-2\mathrm{Re}\{[\mathbf{m}_1^*(\theta_1)-\mathbf{m}_0]^\dagger\mathbf{R}_0^{-1}\mathbf{m}_1^*(\theta_1)\}}{\sqrt{2[\mathbf{m}_1^*(\theta_1)-\mathbf{m}_0]^\dagger\mathbf{R}_0^{-1}[\mathbf{m}_1^*(\theta_1)-\mathbf{m}_0]}}\right\}=\mathcal{Q}\left\{\frac{\ln\lambda-D(\theta_1)}{\sqrt{2D(\theta_1)}}\right\}, \quad (4.24)$$

$\mathcal{Q}(x)=\frac{1}{\sqrt{2\pi}}\int_x^\infty \exp\left(-\frac{t^2}{2}\right)dt$, $D(\theta_1)$ is the minimum KL divergence for any θ_1 given by (following (4.15))

$$D(\theta_1)=[\mathbf{m}_1^*(\theta_1)-\mathbf{m}_0]^\dagger\mathbf{R}_0^{-1}[\mathbf{m}_1^*(\theta_1)-\mathbf{m}_0]=\frac{p_0g(d_0)K_0N_0}{p_0g(d_0)+\sigma_0^2(1+K_0)}\left(N_B-\frac{|\mathbf{r}_1^\dagger\mathbf{r}_0|^2}{N_B}\right), \quad (4.25)$$

and $\mathbf{1}_A(x)$ is a indicator function defined by

$$\mathbf{1}_A(x)=\begin{cases}1, & x\geq 0,\\ 0, & x<0.\end{cases} \quad (4.26)$$

We now prove Theorem 7. Following (4.18), we derive the distributions of the test statistic $\mathbb{T}(\mathbf{y})$ for $\theta_1\neq\pm\theta_c$ under $\mathcal{H}_0$ and $\mathcal{H}_1$ as follows

$$\mathbb{T}(\mathbf{y})|\mathcal{H}_0\sim\mathcal{N}\Big(2\mathrm{Re}\{[\mathbf{m}_1(\theta_1)-\mathbf{m}_0]^\dagger\mathbf{R}_0^{-1}\mathbf{m}_0\},2[\mathbf{m}_1^*(\theta_1)-\mathbf{m}_0]^\dagger\mathbf{R}_0^{-1}[\mathbf{m}_1^*(\theta_1)-\mathbf{m}_0]\Big), \quad (4.27)$$

$$\mathbb{T}(\mathbf{y})|\mathcal{H}_1\sim\mathcal{N}\Big(2\mathrm{Re}\{[\mathbf{m}_1(\theta_1)-\mathbf{m}_0]^\dagger\mathbf{R}_0^{-1}\mathbf{m}_1(\theta_1)\},2[\mathbf{m}_1^*(\theta_1)-\mathbf{m}_0]^\dagger\mathbf{R}_0^{-1}[\mathbf{m}_1^*(\theta_1)-\mathbf{m}_0]\Big). \quad (4.28)$$

Based on the decision rule in (4.17) and the definitions of the false positive and detection rates, we obtain the false positive and detection rates for $\theta_1\neq\pm\theta_c$ in (4.23) and (4.24) after some algebraic manipulations. For $\theta_1=\pm\theta_c$, following (4.18) and (4.19) we have $\mathbb{T}(\mathbf{y})=0$ and $\Gamma=\ln\lambda$. Then, based on the decision rule presented in (4.17) we obtain the desirable results for $\theta_1=\pm\theta_c$ as detailed in (4.21) and (4.22). This completes the proof of Theorem 7.

We note that both $\alpha(\lambda, \theta_1)$ and $\beta(\lambda, \theta_1)$ are functions of $D(\theta_1)$, which is the minimum KL divergence for a given θ_1 presented in (4.15). Based on the properties of $\mathcal{Q}(x)$ and the expressions for $\alpha(\lambda, \theta_1)$ and $\beta(\lambda, \theta_1)$, we know that the detection performance of the LVS increases as $D(\theta_1)$ increases (e.g., for a given $\alpha(\lambda, \theta_1)$, $\beta(\lambda, \theta_1)$ increases as $D(\theta_1)$ increases). This confirms that the malicious vehicle is to search for $\mathbf{x}_1^*$ through minimizing the minimum KL divergence presented in (4.15). By setting $\lambda = \lambda^*$, following (4.9) the minimum total error conditioned on a θ_1 can be expressed as [34]

$$\epsilon^*(\theta_1) = P_0\alpha(\lambda^*, \theta_1) + (1 - P_0)\left(1 - \beta(\lambda^*, \theta_1)\right). \tag{4.29}$$

We note that the detection performance of the LVS based on the malicious vehicle's optimal true location can be obtained by substituting θ_1^* into our derived $\alpha(\lambda, \theta_1)$ and $\beta(\lambda, \theta_1)$.

4.4 Location Verification System with Tracking

In this section, we examine the LVS when tracking information on the claimed location is available. That is, when claimed locations and BS measurements are available at multiple (sequential) time slots ($T \geq 2$). We refer to this LVS as the *tracking LVS*. We first present the decision rule adopted in this tracking LVS, and then present the optimal attack strategy of the malicious vehicle against the tracking LVS. Finally, we analyze the detection performance of the tracking LVS based on this optimal attack strategy.

4.4.1 Decision Rule of the Tracking LVS

In the tracking LVS we assume that we collect one $\mathbf{y}(t)$ for each claimed location $\mathbf{x}_c(t)$. There are several questions we could pose given the introduction of tracking information to the LVS. However, perhaps the most pragmatic question for a tracking LVS is how to make an optimal decision (e.g., minimize the total error) on whether

the vehicle is legitimate or malicious given the last sequence of observations at its disposal. An important system-model issue in tracking mode is that we will let the tracking LVS randomly select the number of time slots to be used prior to each LVS decision. That is, once a decision is made based on say T_a time slots, the next decision is made independently based on the next say T_b time slots, where T_a and T_b are specific realizations of the random variable T. Operationally, this means the specific realizations of T will always be unknown to the malicious vehicle.[5] Henceforth, when we use T we will mean a realization of the random variable T. Under such conditions the optimal decision rule (per decision) for the tracking LVS will be an expanded version of our previously utilized LRT, namely,

$$\Lambda_{track}\left(\mathbf{Y}(T)\right) \underset{\mathcal{D}_0}{\overset{\mathcal{D}_1}{\gtrless}} \lambda_{track}, \tag{4.30}$$

where $\mathbf{Y}(T) = [\mathbf{y}(1), \cdots, \mathbf{y}(T)]$, $\Lambda_{track}\left(\mathbf{Y}(T)\right)$ is the likelihood ratio of $\mathbf{Y}(T)$ given by

$$\Lambda_{track}\left(\mathbf{Y}(T)\right) = \frac{f\left(\mathbf{Y}(T)|\mathbf{p}_1(T), \mathbf{B}_1(T), \mathbf{X}_1(T), \mathcal{H}_1\right)}{f\left(\mathbf{Y}(T)|\mathcal{H}_0\right)}, \tag{4.31}$$

$\mathbf{p}_1(T) = [p_1(1), \cdots, p_1(T)]$, $\mathbf{B}_1(T) = [\mathbf{b}_1(1), \cdots, \mathbf{b}_1(T)]$, $\mathbf{X}_1(T) = [\mathbf{x}_1(1), \cdots, \mathbf{x}_1(T)]$, and λ_{track} is the threshold for $\Lambda_{track}\left(\mathbf{Y}(T)\right)$. Since $\mathbf{y}(t)$ are independent for different t, we further have

$$\Lambda_{track}\left(\mathbf{Y}(T)\right) = \frac{\prod_{t=1}^{T} f\left(\mathbf{y}(t)|p_1(t), \mathbf{b}_1(t), \mathbf{x}_1(t), \mathcal{H}_1\right)}{\prod_{t=1}^{T} f\left(\mathbf{y}(t)|\mathcal{H}_0\right)}. \tag{4.32}$$

Again, the false positive rate is given by $\alpha_{track}(\lambda_{track}) = \Pr\left(\Lambda_{track}\left(\mathbf{Y}(T)\right) > \lambda_{track}|\mathcal{H}_0\right)$, and the detection rate is given by $\beta_{track}(\lambda_{track}) = \Pr\left(\Lambda_{track}\left(\mathbf{Y}(T)\right) > \lambda_{track}|\mathcal{H}_1\right)$. The specific value of λ_{track} can be set based on a methodology similar to that used in setting λ. We again adopt the total error as the unique performance metric to evaluate

[5]The (non-tracking) LVS discussed earlier is now seen as a special case of the tracking LVS with the realization of T always set equal to one and without the additional constraint r_u. Note, due to the additional constraint r_u, the tracking solution in general is not identical to a solution derived from the direct use of individual unit ($T = 1$) timeslot decisions.

the tracking LVS. The optimal value of λ_{track} that minimizes the total error of the tracking LVS is given by $\lambda^*_{track} = P_0/(1-P_0)$ [34].

4.4.2 Optimal Attack Strategy Against the Tracking LVS

Knowing (4.30), in order to minimize the detection rate, the malicious vehicle is to minimize the following KL divergence [109]

$$\begin{aligned} &D_{KL}\left(f\left(\mathbf{Y}(T)|\mathbf{p}_1(T),\mathbf{B}_1(T),\mathbf{X}_1(T),\mathcal{H}_1\right)||\ f\left(\mathbf{Y}(T)|\mathcal{H}_0\right)\right) \\ &= \int \left[\ln \Lambda_{track}(\mathbf{Y}(T))\right] f\left(\mathbf{Y}(T)|\mathbf{p}_1(T),\mathbf{B}_1(T),\mathbf{X}_1(T),\mathcal{H}_1\right) d\mathbf{Y}(T) \\ &= \int \left[\sum_{t=1}^{T} \ln \Lambda(\mathbf{y}(t))\right] \prod_{t=1}^{T} f\left(\mathbf{y}(t)|p_1(t),\mathbf{b}_1(t),\mathbf{x}_1(t),\mathcal{H}_1\right) d\mathbf{Y}(T) \\ &= \sum_{t=1}^{T} D_{KL}\left(f\left(\mathbf{y}(t)|p_1(t),\mathbf{b}_1(t),\mathbf{x}_1(t),\mathcal{H}_1\right)||f\left(\mathbf{y}(t)|\mathcal{H}_0\right)\right). \end{aligned} \tag{4.33}$$

Based on (4.33), we know that the KL divergence for $t = 1, 2, \cdots, T$ is the sum of the KL divergence presented in (4.10) for each t. We also can see that the KL divergence at t is independent of the system settings at other time slots. This indicates that the malicious vehicle can optimize all the parameters under his control at t (e.g., $p_1(t)$, $\mathbf{b}_1(t)$, and $\mathbf{x}_1(t)$) by considering only the system settings for the current time slot t (e.g., the values of $\mathbf{x}_c(t)$, $\sigma_0^2(t)$, and $\sigma_1^2(t)$). As such, the optimal attack strategy for the malicious vehicle is to optimize all parameters under its control for the current time slot. To this end, for each t the malicious vehicle first optimizes $p_1(t)$ and $\mathbf{b}_1(t)$ according to Theorem 5 for any given $\mathbf{x}_1(t)$. Then, the malicious vehicle is to optimize $\mathbf{x}_1(t)$ under some constraints detailed in the following. For $\mathbf{x}_c(1)$, the malicious vehicle can optimize $\mathbf{x}_1(t)$ according to Theorem 6. We would like to highlight that in addition to $|\mathbf{x}_c(t) - \mathbf{x}_1(t)| \geq r_l$ there is another constraint on $\mathbf{x}_1(t)$ for $t \geq 2$, which is that $|\mathbf{x}^*_1(t-1) - \mathbf{x}_1(t)| \leq r_u$, where r_u can be determined through imposition of a realistic vehicle speed limitation. This is due to the fact that the malicious vehicle cannot move too far away from its previous location (i.e., its location in the previous time

slot). Then, the optimal $\theta_1(t)$ for $t \geq 2$ is given by

$$\theta_1^*(t) = \underset{\substack{\|\mathbf{x}_c(t)-\mathbf{x}_1(t)\| \geq r_l, \\ \|\mathbf{x}_1^*(t-1)-\mathbf{x}_1(t)\| \leq r_u}}{\operatorname{argmax}} |\mathbf{r}_1^\dagger(t)\mathbf{r}_0(t)|^2. \tag{4.34}$$

We note that the optimal attack strategy against the tracking LVS for the malicious vehicle is to find an angle $\theta_1^*(t) = \pm\theta_c(t)$ with a non-zero LOS component towards the BS for every time slot. Should the two distance constraints imposed on the malicious vehicle make $\theta_1^*(t) = \pm\theta_c(t)$ impossible, then a sub-optimal attack at $\theta_1^*(t) \neq \pm\theta_c(t)$ must take place at some of the time slots.

4.4.3 Detection Performance of the Tracking LVS

Without loss of generality, we analyze the detection performance of the tracking LVS for any given $\boldsymbol{\theta}_1(T) = [\theta_1(1), \cdots, \theta_1(T)]$ by considering $p_1(t) = p_1^*(\mathbf{x}_1(t))$ and $\mathbf{b}_1(t) = \mathbf{b}_1^*(\mathbf{x}_1(t))$. We denote the track of claimed locations as $\boldsymbol{\theta}_c(T) = [\theta_c(1), \cdots, \theta_c(T)]$. Following (4.32), the LRT decision rule presented in (4.30) can be rewritten as

$$\mathbb{T}_{track}(\mathbf{Y}(T)) \underset{\mathcal{D}_0}{\overset{\mathcal{D}_1}{\gtrless}} \Gamma_{track}, \tag{4.35}$$

where $\mathbb{T}_{track}(\mathbf{Y}(T))$ is the test statistic given by

$$\mathbb{T}_{track}(\mathbf{Y}(T)) = 2\mathrm{Re}\left\{\sum_{t=1}^{T}[\mathbf{m}_1^*(\theta_1(t)) - \mathbf{m}_0(t)]^\dagger \mathbf{R}_0^{-1}\mathbf{y}(t)\right\}, \tag{4.36}$$

and Γ_{track} is the threshold for $\mathbb{T}_{track}(\mathbf{Y}(T))$ given by

$$\Gamma_{track} = \ln \lambda_{track} + \mathrm{Re}\left\{\sum_{t=1}^{T}[\mathbf{m}_1^*(\theta_1(t)) - \mathbf{m}_0(t)]^\dagger \mathbf{R}_0^{-1}[\mathbf{m}_1^*(\theta_1(t)) + \mathbf{m}_0(t)]\right\}. \tag{4.37}$$

We then derive the false positive rate, $\alpha_{track}(\lambda_{track}, \boldsymbol{\theta}_1(T))$, and the detection rate, $\beta_{track}(\lambda_{track}, \boldsymbol{\theta}_1(T))$, of the tracking LVS for any given $\boldsymbol{\theta}_1(T)$ in the following theorem.

***Theorem* 8** The false positive rate and the detection rate of the tracking LVS for any given $\boldsymbol{\theta}_1(T)$ are derived as

$$\alpha_{track}(\lambda_{track}, \boldsymbol{\theta}_1(T)) = \begin{cases} \tilde{\alpha}_{track}(\lambda_{track}, \boldsymbol{\theta}_1(T)), & \boldsymbol{\theta}_1(T) \neq \pm\boldsymbol{\theta}_c(T), \\ \mathbf{1}_A(-\ln \lambda_{track}), & \boldsymbol{\theta}_1(T) = \pm\boldsymbol{\theta}_c(T), \end{cases} \tag{4.38}$$

$$\beta_{track}(\lambda_{track}, \boldsymbol{\theta}_1(T)) = \begin{cases} \tilde{\beta}_{track}(\lambda_{track}, \boldsymbol{\theta}_1(T)), & \boldsymbol{\theta}_1(T) \neq \pm\boldsymbol{\theta}_c(T), \\ \mathbf{1}_A(\ln \lambda_{track}), & \boldsymbol{\theta}_1(T) = \pm\boldsymbol{\theta}_c(T), \end{cases} \tag{4.39}$$

where

$$\tilde{\alpha}_{track}(\lambda_{track}, \boldsymbol{\theta}_1(T)) = \mathcal{Q}\left\{ \frac{\ln \lambda_{track} + D_{track}(\boldsymbol{\theta}_1(T))}{\sqrt{2D_{track}(\boldsymbol{\theta}_1(T))}} \right\}, \tag{4.40}$$

$$\tilde{\beta}_{track}(\lambda_{track}, \boldsymbol{\theta}_1(T)) = \mathcal{Q}\left\{ \frac{\ln \lambda_{track} - D_{track}(\boldsymbol{\theta}_1(T))}{\sqrt{2D_{track}(\boldsymbol{\theta}_1(T))}} \right\}, \tag{4.41}$$

and $D_{track}(\boldsymbol{\theta}_1(T))$ is the minimum KL divergence for any given $\boldsymbol{\theta}_1(T)$, which is given by (following (4.15) and (4.33))

$$\begin{aligned} D_{track}(\boldsymbol{\theta}_1(T)) &= \sum_{t=1}^{T} D_{KL}\left(f\left(\mathbf{y}(t)|p_1^*(t), \mathbf{b}_1^*(t), \mathbf{x}_1(t), \mathcal{H}_1\right) || f\left(\mathbf{y}(t)|\mathcal{H}_0\right)\right) \\ &= \sum_{t=1}^{T} \frac{p_0 g(d_0(t)) K_0(t) N_0}{p_0 g(d_0(t)) + \sigma_0^2(t)(1+K_0(t))} \left(N_B - \frac{|\mathbf{r}_1(t)^\dagger \mathbf{r}_0(t)|^2}{N_B} \right). \end{aligned} \tag{4.42}$$

The proof of Theorem 8 is very similar to that of Theorem 7, we therefore omit it here.

The minimum total error of the tracking LVS for any given $\boldsymbol{\theta}_1(T)$ is [34]

$$\epsilon_{track}^*(\boldsymbol{\theta}_1(T)) = P_0 \alpha_{track}(\lambda_{track}^*, \boldsymbol{\theta}_1(T)) + (1 - P_0)\left(1 - \beta_{track}(\lambda_{track}^*, \boldsymbol{\theta}_1(T))\right). \tag{4.43}$$

We note that the minimum KL divergence provided in (4.15) is greater than zero for any $\mathbf{x}_1(t)$ as long as $\theta_1(t) \neq \pm\theta_c(t)$. As such, $D_{track}(\boldsymbol{\theta}_1(T))$ monotonically increases as T increases for $\theta_1(t) \neq \pm\theta_c(t)$. This demonstrates that the detection performance of the tracking LVS increases as T increases as long as $\theta_1(t) \neq \pm\theta_c(t)$ (e.g., $\epsilon_{track}^*(\boldsymbol{\theta}_1(T))$ decreases as T increases).

In summarizing this section we note the following. The above analysis on the tracking LVS leads to the following key points. Under the assumption that T is

randomly selected *per decision* by the tracking LVS, the optimal decision framework is a reasonably extension of the non-tracking framework. The optimal attack scenario is for the malicious vehicle to be at $\theta_1^*(t) = \pm\theta_c(t)$. However, physical constraints (such as limited speed) may make this impossible. The next sub-optimal malicious vehicle location can then be calculated - and this location may not necessarily be the $\theta_1(t)$ closest to $\theta_0(t)$ with non-zero LOS components. The performance of the tracking LVS under any potential sequence of the malicious vehicle's locations is provided analytically.

4.5 Numerical Results

In this section, we present numerical simulations to verify the accuracy of our provided analysis on the LVS and the tracking LVS. We also provide some useful insights on the impact of p_0, θ_1^*, N_B, N_0, and K_0 on the detection performance of the LVS. We further examine the impact of K_1 and σ_1^2 on N_1^*.

4.5.1 Numerical Results for the LVS

We first consider the LVS (i.e., the non-tracking LVS) and thus we drop the index (t) in this subsection. In Fig. 4.3, we present the ROC curve of the LVS. In this figure, we first observe that the Monte Carlo simulations precisely match the theoretic results, which confirms our analysis presented in Theorem 7. We also observe that the ROC curves for $p_0 g(d_0)/\sigma_0^2 = 5$dB dominate the ROC curves for $p_0 g(d_0)/\sigma_0^2 = 0$dB. This observation demonstrates that the detection performance of the LVS increases as the SNR of the legitimate channel (the channel between the BS and the legitimate vehicle) increases. As expected, we further observe that the ROC curve shifts towards the right-lower corner as θ_1^* moves closer to θ_0.

In Fig. 4.4, we present the minimum total error $\epsilon(\theta_1^*)$ versus the number of antenna elements at the legitimate vehicle (N_0) and the number of antenna elements at the

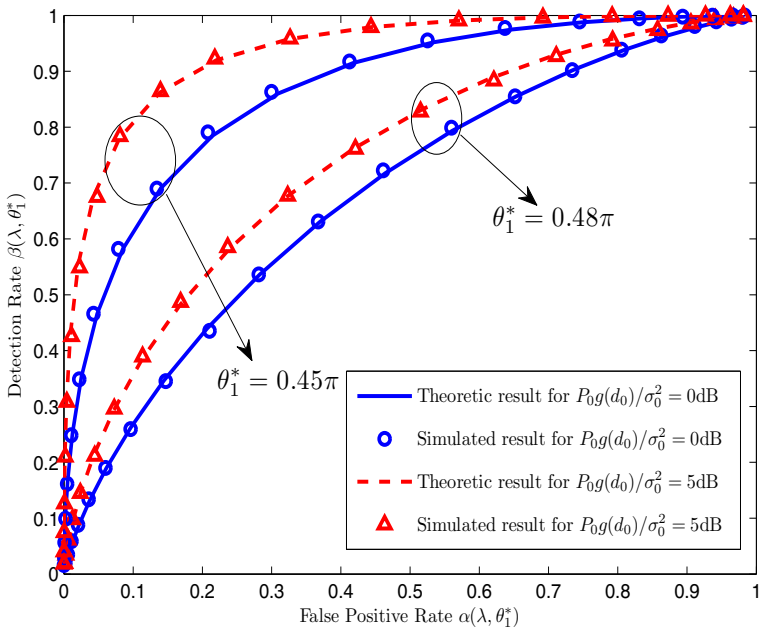

Figure 4.3: ROC curves of the LVS for $N_B = 4$, $N_0 = 3$, $N_1 \geq N_1^*$, $\theta_0 = \pi/2$, $K_0 = 1$dB, $\sigma_0^2 = \sigma_1^2 = 0$dB, $p_1 = p_1^*(\mathbf{x}_1)$, and $\mathbf{b}_1 = \mathbf{b}_1^*(\mathbf{x}_1)$.

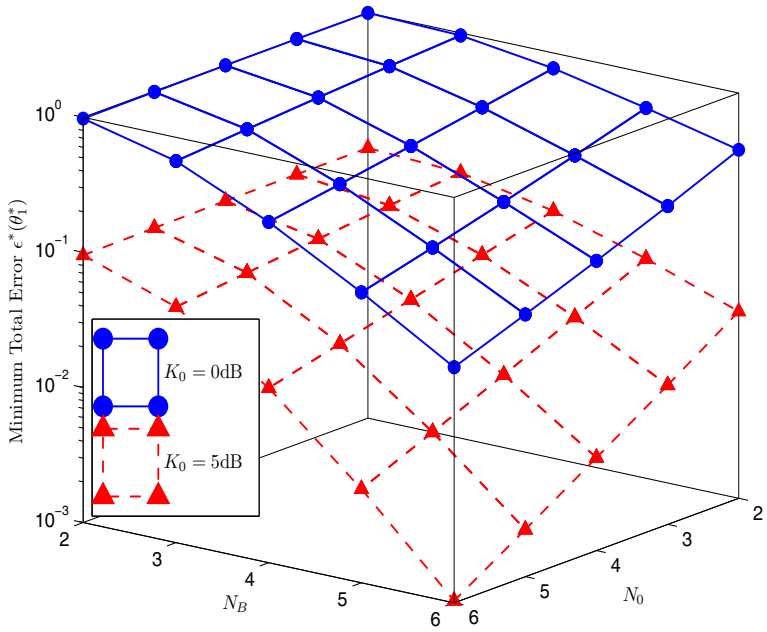

Figure 4.4: Minimum total error of the LVS versus N_B and N_0 for $P_0 = 0.9$, $\theta_0 = \pi/3$, $\theta_1^* = \pi/4$, $K_1 = 0$dB, $p_0 g(d_0)/\sigma_0^2 = 0$dB, $p_1 = p_1^*(\mathbf{x}_1)$, $\mathbf{b}_1 = \mathbf{b}_1^*(\mathbf{x}_1)$, and $N_1 \geq N_1^*$.

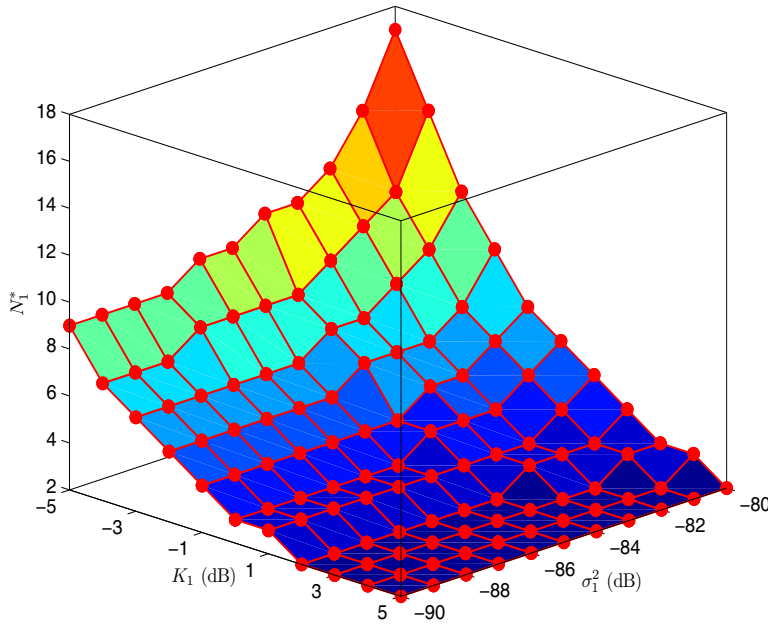

Figure 4.5: N_1^* versus K_1 and σ_1^2 for $N_0 = 3$, $p_0 g(d_0) = -75$dB, $\sigma_0^2 = -85$dB, and $K_0 = 0$dB.

BS (N_B). As expected, we first observe that $\epsilon(\theta_1^*)$ decreases as N_B or N_0 increases. We also observe that $\epsilon(\theta_1^*)$ decreases as the Rician K-factor of the legitimate channel (K_0) increases. From the simulations to obtain Fig. 4.4, we confirm N_1^* increases as N_0 or K_0 increases, but is not a function of N_B.

In Fig. 4.5, we plot N_1^* versus Rician K-factor of the malicious channel, K_1, and the noise variance of the malicious channel, σ_1^2. As expected from (B.10), we first observe that N_1^* increases as K_1 decreases or σ_1^2 increases. This demonstrates that N_1^* is highly dependent on the inherent properties of the malicious channel. We also observe that N_1^* is a reasonable value (e.g., 15) even when K_1 is small (e.g., -5dB).

4.5.2 Numerical Results for the Tracking LVS

In Fig. 4.6, we examine the impact of T on the detection performance of the tracking LVS. In the simulations to obtain Fig. 4.6, we have assumed the claimed location $\mathbf{x}_0(t)$ is moving towards the BS along a straight line with a constant velocity 20km/h and

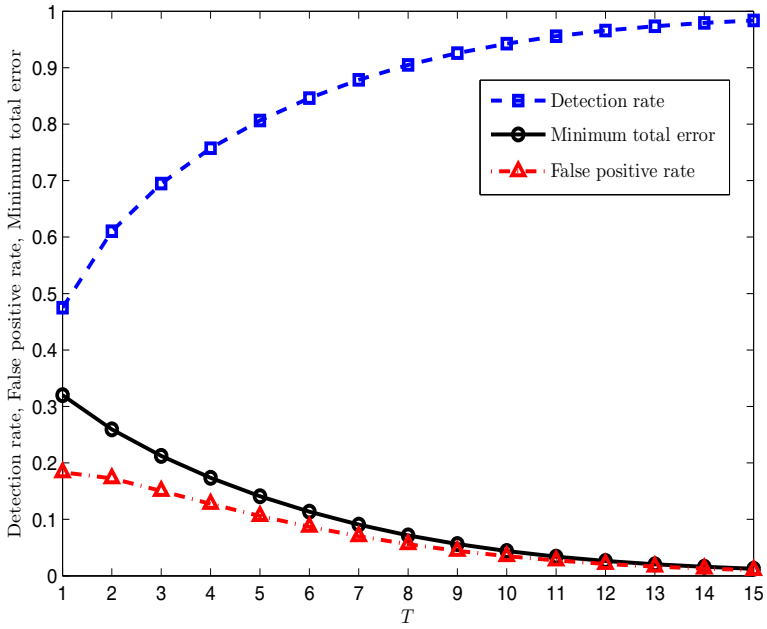

Figure 4.6: False positive rate, detection rate, and minimum total error of the tracking LVS versus T for $P_0 = 0.6$, $N_B = 3$, $N_0 = 2$, $N_1 \geq N_1^*$, $p_0 = 30$dB, $K_0 = -10$dB, $\xi = 3$, $c = 3 \times 10^8$m/s, $f_0 = 5.9$GHz, $r_l = 100$m, $r_u = 3$m, $\tau_B = \pi$, and $\mathbf{x}_1(t) = \mathbf{x}_1^*(t)$.

$\mathbf{x}_0(1) = [10\sqrt{2}, \pi/4]$. We have also assumed that $\mathbf{x}_1(t)$ is on the straight line and K_0 is a constant for all $\mathbf{x}_0(t)$. These settings mimic a practical VANETs scenario, where the BS is on the roadside, the legitimate vehicle is moving along the road towards the BS, and the malicious vehicle is also on the same road. The observation frequency and claimed-location reception are both set at 10 Hz (10 time slots per second). Other parameters adopted are specified in the caption of Fig. 4.6. As expected, we observe that the false positive rate and the minimum total error decrease as T increases and the detection rate increases as T increases. With the aid of the derived false positive and detection rates provided in (4.38) and (4.39), we can quantify the detection performance improvement brought by increased T. For example, the minimum total error for $T = 10$ is only about 30% of that for $T = 1$.

Finally, in this section we note the effect some of our channel and system model assumptions have on our results. More specifically, we probe circumstances where

non-zero errors on the claimed location are present (inclusion of location errors also probes the impact of other issues such as inaccuracies in the K map and potential shadowing effects). In general, we find such real-world effects have a limited impact on our results. For example, for the localization error (average distance between the estimated positions and the real positions) of 5 meters we find the results of Fig. 4.6 are impacted only at the 10% level (e.g., the false positive rate for this localization error is about 10% higher than that for the zero localization error).

4.6 Discussion

4.6.1 Other Antenna Arrays

Although we assumed that the malicious vehicle is equipped with a ULA, our main analysis provided in this chapter still holds if the ULA is replaced by other antenna arrays (e.g., non-uniform linear arrays, circular arrays, rectangle arrays). If the malicious vehicle is equipped with other antenna arrays, only (4.3) under $\mathcal{H}_1$ will be modified. For example, if the ULA at the malicious vehicle in Fig. 4.1 is replaced by a Uniform Circular Array (UCA) centered at the malicious vehicle, (4.3) under $\mathcal{H}_1$ will be replaced by the following equation (dropping the index t) [110]

$$\mathbf{t}_1 = [\exp(-j\tau_1^c \cos\phi_1), \cdots, \exp(-j\tau_1^c \cos\phi_{N_1})]\,, \tag{4.44}$$

where $\tau_1^c = 2\pi f_c a_1/c$, a_1 is the radius of the UCA at the malicious vehicle, and $\phi_m = 2\pi(m-1)/N_1 + \phi_1$ (where $m = 1, 2, \cdots, N_1$) is the angle measured counterclockwise from the reference line (the line connecting the center of the malicious vehicle's UCA and the center of the ULA at the BS) to the m-th antenna element of the UCA. Based on (4.44) and $\overline{\mathbf{H}}_1 = \mathbf{r}_1\mathbf{t}_1$ we can see that $\overline{\mathbf{H}}_1$ still only contains the directional information of the malicious channel (i.e., $\overline{\mathbf{H}}_1$ only depends on θ_1 and ϕ_1). Noting $\mathbf{Q} \propto \overline{\mathbf{H}}_1^{\dagger}\overline{\mathbf{H}}_1$, we know that the matrix $\mathbf{Q}$ involved in Theorem 5 is still a rank-1 matrix due to $\mathbf{r}_k^{\dagger}\mathbf{r}_k = N_B$. In addition, as we have shown in Theorem 7 the detection

performance of the LVS is not a function of $\mathbf{t}_1$ as long as the malicious vehicle adopts the optimal transmit power and beamformer. As such, all the analysis provided earlier still holds exactly for the case where the malicious vehicle is equipped with the UCA. That is, the use of a UCA provides the attacker no additional benefit. Finally, we note our analysis can be readily adapted to cases where antenna arrays under the control of the LVS (e.g., at the BS and legitimate vehicle) are also non-linear arrays.

4.6.2 Colluding Attacks

We note that in practice the malicious vehicle may launch colluding attacks to the LVS and the tracking LVS by cooperating with other malicious vehicles. However, colluding attacks of any form cannot bring any additional benefits to the malicious vehicle that can set $\theta_1^*(t) = \pm\theta_c(t)$ at every decision step. This is because the minimum KL divergence presented in (4.15) will always be zero when $\theta_1^*(t) = \pm\theta_c(t)$. This is the case for both the (non-tracking) LVS and the tracking LVS.

Considering the case where $\theta_1^*(t) \neq \pm\theta_c(t)$, there are two general specific attack strategies that can be adopted by the colluding malicious vehicles, single-transmission attack and multiple-transmission attack. In the single-transmission attack only one of the colluding malicious vehicles is active and transmitting signals. As such, the collusion in this type of attack takes the form of information-sharing and the subsequent decision of which vehicle is in the optimal location to launch an attack. The single-transmission attack can help a malicious vehicle against the tracking LVS (but not the non-tracking LVS). This is because the colluding malicious vehicles can potentially cooperatively select their true locations over different time slots in order to avoid the second constraint in (4.34), i.e. $\|\mathbf{x}_1^*(t-1) - \mathbf{x}_1(t)\| \leq r_u$. As the number of colluding malicious vehicles approach infinity, this constraint can be removed from (4.34) entirely. In the multiple-transmission attack, all the colluding malicious vehicles are active and transmitting signals simultaneously. As such, the collusion takes the form of information-sharing and the subsequent decisions on the optimal trans-

mit power, beamformer, and locations of the colluding malicious vehicles. Obviously such a sophisticated attack could outperform the single transmission attack in the general scenario. But again we stress that when $\theta_1^*(t) = \pm\theta_c(t)$ is allowed none of these colluding attacks are of importance. As such, adopting the detection rates for $\theta_1^*(t) = \pm\theta_c(t)$ always provides a worst-case bound for the LVS and the tracking LVS.

4.7 Summary

In this chapter we have proposed a generic LVS framework for multi-antenna communication systems, and conducted a detailed analysis of the framework's location authentication performance. Although our work is general and can cover many application scenarios, we have focussed here on the emerging VANETs paradigm under the assumption of Rician channels. Such channels are anticipated to dominate real-world VANETs communication conditions. The LVS solution we have proposed is very general and provides a foundation for all optimal location authentication schemes in the VANETs scenario. Taking as inputs a claimed location and raw observations across the receiving BS antennas, our LVS checks its knowledge of the Rician channel conditions in its vicinity, forms a view as to the optimal attack location (from the attacker's viewpoint), and then outputs a binary decision on whether a vehicle is providing a legitimate location. Our analysis quantifies the dependence between the detection performance limit of the LVS and the Rician K-factor of the legitimate channel, and formally reveals that the LVS performance limit is independent of the properties of the malicious channel. In addition, our analysis discloses that once the malicious vehicle's number of antennas reaches a derived bound, further increase in this number does not reduce the detection rate. We also formalized the optimal decision rule when tracking information is added to the LVS. The work presented in this chapter will be of importance to emerging intelligent vehicular network scenarios, particularly in relation to certificate revocation schemes within IEEE 1609.2.

Chapter 5

Location-based Beamforming for Wireless Physical Layer Security

5.1 Introduction

In the last three chapters (Chapter 2, Chapter 3, and Chapter 4), new optimal LVSs were developed in order to verify claimed location information. In this chapter, we propose and analyze robust transmission schemes that utilize such verified location information in enhancing physical layer security for wireless communications. As mentioned in Chapter 1, many of the works in MIMO wiretap channels assume that the (instantaneous) CSI of the main channel is perfectly known by Alice or Bob (e.g., [53, 55, 56]). This assumption is usually very difficult to justify in practice (e.g., in massive MIMO techniques the CSI of a channel cannot be perfectly known even to a receiver due to pilot contamination issues [78–81]). Another assumption adopted in the literature is that the CSI of the eavesdropper's channel is known to Alice, which is even harder to justify in practice.

However, there are many circumstances where location information of Bob and Eve could be available. For example, in some specific military application scenarios, Alice may obtain Bob's location through direct communications, and Eve's location

through some (possibly *a priori*) surveillances. Other circumstances could be where Eve, in a previous communication round, was a valid user in which her location information was provided to the system (so as to optimize communications to her), whereas, in the next communication round she no longer is the intended receiver. Example applications where this latter circumstance could play-out are in vehicular networks or wireless social-media applications.

Regardless of the application scenario, the main point we focus on here is that if there is an LOS component in the main channel or the eavesdropper's channel, it is possible to utilize location information directly in order to enhance the physical layer security. More specifically, we propose and analyze a new LBB scheme in the wiretap channel, where both the main channel and the eavesdropper's channel are subject to Rician fading. Our scheme does not require the CSI of either the main channel or the eavesdropper's channel - thus making it quite general, as well as pragmatic. The basic *modus operandi* of the scheme we propose is that given the input locations of Bob and Eve, we output the optimal beamformer solution and the security level (the secrecy outage probability) associated with this solution. Detailing how these outputs are determined forms the core of this chapter.

Surprisingly, there has been little previous work in this area, with the closest works perhaps those of [111] and [112]. In [111], the ergodic secrecy rate was examined for multiple-antenna wiretap channels with Rician fading. However, in [111] it was assumed that the CSI of the main channel was perfectly known by Alice. The work of [112] analyzed the secrecy performance of orthogonal space-time block codes when the main channel is assumed to be subject to Rician fading. But the eavesdropper's channel was assumed to be subject to Rayleigh fading in [112] and therefore Eve's location information was not that useful.

The direction of this chapter and our contributions are summarized as follows. (i) We first derive the secrecy outage probability of the LBB scheme in a closed-form expression, which is valid for arbitrary values of the Rician K-factors of the main channel and the eavesdropper's channel. (ii) We then determine the optimal location-

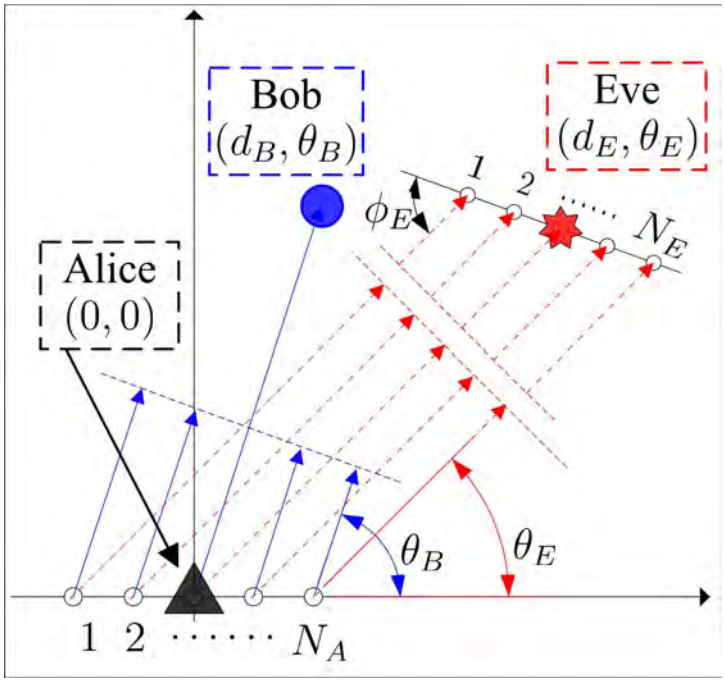

Figure 5.1: Illustration of the Rician wiretap channel of interest.

based beamformer and the minimum secrecy outage probability for the scheme. (iii) In order to fully appreciate the gains of the LBB scheme, we also analyze, for comparison, the secrecy performance of a Non-Beamforming (NB) scheme.

The rest of this chapter is organized as follows. Section 5.2 details our system model; Section 5.3 provides our analytical solutions; Section 5.4 presents the secrecy performance of the NB scheme; Section 5.5 provides numerical simulations; and Section 5.6 draws concluding remarks.

5.2 System Model

We examine the LBB scheme by considering generic and realistic channel conditions. That is, we will assume $K_B > 0$ and $K_E > 0$, where K_B and K_E are the Rician K-factors of the main channel and the eavesdropper's channel, respectively. The wiretap channel of interest is illustrated in Fig. 5.1, where Alice and Eve are equipped with

Uniform Linear Arrays (ULAs) with N_A and N_E antenna elements,[1] respectively; and Bob is equipped with a single antenna. As we will show later, our analysis provided in this chapter is also valid for other antenna arrays beyond ULAs at Eve. We assume that Alice, Bob, and Eve are static. We note that we assume that the antenna gains at all the transceivers (i.e., Alice, Bob, and Eve) are the same. The antenna gains and other factors (excluding the instantaneous CSI) that can impact the quality of a channel can be incorporated into the average SNR of the channel. As such, in our system model the SNRs at Bob and Eve are solely governed by the average SNRs and instantaneous CSI of the main channel and the eavesdropper's channel, respectively.

As shown in Fig. 5.1, we adopt the polar coordinate system, where Alice's location is selected as the origin, Bob's location is denoted as (d_B, θ_B), and Alice's location is denoted as (d_E, θ_E). For presentation convenience, without other statements we assume that the coordinate system is set up such that $0 \leq \theta_B \leq \pi$ and $0 \leq \theta_E \leq \pi$. The orientation of the ULA at Alice is also shown in this figure. We also assume that the main channel and the eavesdropper's channel are subject to quasi-static Rician fading with equal block length but different (can be equal) Rician K-factors, and that a K-factor map (K as a function of locations) is known in the vicinity of Alice via some *a priori* measurement campaigns. We further assume that the CSI of the main channel is unknown to Alice, but that Bob's location is known to Alice. We note that using Bob's location saves feedback overhead relative to use of the CSI of the main channel. This is due to the following two facts: (i) the CSI varies during different fading blocks and has to be fed back for each fading block, meanwhile the location

[1]We will assume N_E is also known to Alice. This is reasonable in circumstances where Alice can determine physical constraints on the size of an eavesdropper's antenna, knowledge of which, coupled to the known frequency of transmission, can allow for a reliable upper bound on N_E to be set. If an upper bound on N_E is set, then our solutions become bounds (worst case scenarios). In other circumstances, where Eve is at times a legitimate user, we can assume N_E is known. We note that in practice it is possible that Eve possesses more resources than Alice or Bob (e.g., N_E is greater than N_A). From a conservative point of view, it is better to overestimate N_E than underestimating it and we will examine the case where $N_E > N_A$ in the numerical section of this chapter.

information only has to be fed back once for a static Bob; and (ii) the CSI is an N_A-dimension complex vector ($2N_A$ variables embedded), meanwhile Bob's location is determined by only two real numbers. Additional assumptions are that Eve knows the CSI of the eavesdropper's channel and the beamformer adopted by Alice; that Eve applies MRC in order to maximize the probability of successful eavesdropping [60,61]; and that Eve's location is known to Alice. As we discuss later, our analysis also covers the case where Eve's location is unavailable at Alice.

As per the aforementioned assumptions, the $1 \times N_A$ main channel vector is given by

$$\mathbf{h} = \sqrt{\frac{K_B}{1+K_B}}\mathbf{h}_o + \sqrt{\frac{1}{1+K_B}}\mathbf{h}_r, \tag{5.1}$$

where $\mathbf{h}_o$ is the LOS component, and $\mathbf{h}_r$ is the scattered component. The entries of $\mathbf{h}_r$ are i.i.d. circularly-symmetric complex Gaussian random variables with zero mean and unit variance, i.e., $\mathbf{h}_r \sim \mathcal{CN}(0, \mathbf{I}_{N_A})$. Denoting ρ_A as the space between two antenna elements of the ULA at Alice, $\mathbf{h}_o$ is given by [113]

$$\mathbf{h}_o = \left[1, \cdots, \exp(j(N_A - 1)\tau_A \cos\theta_B)\right], \tag{5.2}$$

where $\tau_A = 2\pi f_0 \rho_A / c$, f_0 is the carrier frequency, and c is the speed of propagation of the plane wave. The $N_E \times N_A$ eavesdropper's channel matrix is given by

$$\mathbf{G} = \sqrt{\frac{K_E}{1+K_E}}\mathbf{G}_o + \sqrt{\frac{1}{1+K_E}}\mathbf{G}_r, \tag{5.3}$$

where $\mathbf{G}_o$ is the LOS component, and $\mathbf{G}_r$ is the scattered component represented by a matrix with i.i.d. circularly-symmetric complex Gaussian random variables with zero mean and unit variance. Given the locations of Alice and Eve, $\mathbf{G}_o$ can be written as [107]

$$\mathbf{G}_o = \mathbf{r}_o^T \mathbf{g}_o \tag{5.4}$$

where $\mathbf{r}_o$ and $\mathbf{g}_o$ are the array responses at Eve and Alice, respectively, which are

given by

$$\mathbf{r}_o = [1, \cdots, \exp(-j(N_E - 1)\tau_E \cos\phi_E)], \tag{5.5}$$

$$\mathbf{g}_o = [1, \cdots, \exp(j(N_A - 1)\tau_A \cos\theta_E)]. \tag{5.6}$$

In (5.5), we have $\tau_E = 2\pi f_0 \rho_E / c$, where ρ_E is the space between two antenna elements of the ULA at Eve, and ϕ_E is the direction of arrival from Eve to Alice which is dependent on the orientation of the ULA at Eve. As we show later, the SNR of the eavesdropper's channel is independent of ϕ_E when Eve utilizes MRC to combine the received signals. As such, the secrecy performance of the LBB scheme does not depend on ϕ_E and thus Alice does not have to know ϕ_E.

The received signal at Bob is given by

$$y = \sqrt{g(d_B)}\mathbf{h}\mathbf{b}x + n_B, \tag{5.7}$$

where $g(d_B)$ is the path loss component of the main channel given by $g(d_B) = (c/4\pi f_0 d_0)^2 (d_0/d_B)^{\eta_B}$ (d_0 is a reference distance and η_B is the path loss exponent[2] of the main channel), $\mathbf{b}$ is a normalized beamformer (i.e., $\|\mathbf{b}\| = 1$), x is the Gaussian distributed information bearing signal satisfying $\mathbb{E}[|x|^2] = P$ (P is the total transmit power of Alice[3]), and n_B is the additive white Gaussian noise of the main channel with zero mean and variance σ_B^2. Likewise, the received signal at Eve is given by

$$\mathbf{z} = \sqrt{g(d_E)}\mathbf{G}\mathbf{b}x + \mathbf{n}_E, \tag{5.8}$$

where $g(d_E)$ is the path loss component of the eavesdropper's channel given by $g(d_E) = (c/4\pi f_0 d_0)^2 (d_0/d_E)^{\eta_E}$ (η_E is the path loss exponent of the eavesdropper's

[2]The path loss exponent η_B is dependent on the Rician K-factor K_B. For example, $\eta_B \to 2$ as $K_B \to \infty$. For simplicity, we assume η_B is known to Alice since K_B is known. This declaration also applies to the path loss exponent of the eavesdropper's channel η_E and the Rician K-factor K_E.

[3]It is straightforward to prove that the secrecy outage probability is a monotonically decreasing function of Alice's transmit power for given locations of Bob and Eve. As such, we assume that Alice always sets her transmit power at the maximum value P.

channel), and $\mathbf{n}_E$ is the additive white Gaussian noise vector of the eavesdropper's channel with zero mean and variance matrix $\sigma_E^2\mathbf{I}_{N_E}$, i.e., $\mathbf{n}_E \sim \mathcal{CN}(\mathbf{0}, \sigma_E^2\mathbf{I}_{N_E})$

Then, the SNR of the main channel is given by

$$\gamma_B = \frac{Pg(d_B)|\mathbf{hb}|^2}{\sigma_B^2} = \overline{\gamma}_B|\mathbf{hb}|^2, \tag{5.9}$$

where $\overline{\gamma}_B$ is defined as $\overline{\gamma}_B \triangleq Pg(d_B)/\sigma_B^2$. Assuming Eve applies MRC to combine the received signals at different antennas, the SNR of the eavesdropper's channel is given by

$$\gamma_E = \frac{Pg(d_E)\|\mathbf{Gb}\|^2}{\sigma_E^2} = \overline{\gamma}_E\|\mathbf{Gb}\|^2, \tag{5.10}$$

where $\overline{\gamma}_E$ is defined as $\overline{\gamma}_E \triangleq Pg(d_E)/\sigma_E^2$.

5.3 Location-based Beamforming Scheme

In this section, we first examine the secrecy performance of our proposed LBB scheme in terms of the secrecy outage probability and the probability of non-zero secrecy capacity. We then determine the optimal location-based beamformer of the LBB scheme that minimizes the secrecy outage probability.

5.3.1 Statistical Properties of the SNRs

In order to derive the secrecy performance metrics of our scheme (e.g., the secrecy outage probability), we first derive the pdfs of γ_B and γ_E. Without loss of generality, we derive such pdfs for a general $\mathbf{b}$, which is independent of $\mathbf{h}_r$ and $\mathbf{G}_r$. To this end, we first determine the distribution type of $|\mathbf{hb}|$. As per (5.1), we have

$$\mathbf{hb} = \underbrace{\sqrt{\frac{K_B}{1+K_B}}\mathbf{h}_o\mathbf{b}}_{\tilde{h}_o} + \underbrace{\sqrt{\frac{1}{1+K_B}}\mathbf{h}_r\mathbf{b}}_{\tilde{h}_r}. \tag{5.11}$$

Since $\mathbf{b}$ is independent of $\mathbf{h}_r$, $\tilde{h}_r$ is still a circularly-symmetric complex Gaussian random variable. Noting that $\tilde{h}_o$ is deterministic, we conclude that $|\mathbf{hb}|$ follows a

Rician distribution. We next determine the parameters of this Rician distribution. Following (5.11), we have

$$|\tilde{h}_o|^2 = \frac{K_B}{1+K_B}|\mathbf{h}_o\mathbf{b}|^2 \tag{5.12}$$

and

$$\mathbb{E}[|\tilde{h}_r|^2] = \frac{1}{1+K_B}\mathbb{E}[|\mathbf{h}_r\mathbf{b}|^2] = \frac{1}{1+K_B}. \tag{5.13}$$

We note that $|\tilde{h}_o|^2$ is the power of the LOS (deterministic) component and $\mathbb{E}[|\tilde{h}_r|^2]$ is the average power of the non-LOS (random) component. As such, we conclude that $|\mathbf{hb}|$ follows a Rician distribution with $\widetilde{K}_B$ and $\widetilde{\overline{\gamma}}_B$ as the Rician K-factor and total power, respectively, where $\widetilde{K}_B$ and $\widetilde{\overline{\gamma}}_B$ are given by

$$\widetilde{K}_B \triangleq \frac{|\tilde{h}_o|^2}{\mathbb{E}[|\tilde{h}_r|^2]} = |\mathbf{h}_o\mathbf{b}|^2 K_B, \tag{5.14}$$

$$\widetilde{\overline{\gamma}}_B \triangleq \mathbb{E}[\gamma_B] = \overline{\gamma}_B\left(|\tilde{h}_o|^2 + \mathbb{E}[|\tilde{h}_r|^2]\right) = \frac{(K_B|\mathbf{h}_o\mathbf{b}|^2+1)\,\overline{\gamma}_B}{1+K_B}. \tag{5.15}$$

The pdf of a Rician random variable involves the zero-order modified Bessel function of the first kind, which is not suitable for further analysis (e.g., deriving the secrecy outage probability). To make progress, it is convenient to interpret the Rician fading as a special case of Nakagami fading. As such, the pdf of γ_B is approximated as [87]

$$f_{\gamma_B}(\gamma) = \left(\frac{\widetilde{m}_B}{\widetilde{\overline{\gamma}}_B}\right)^{\widetilde{m}_B} \frac{\gamma^{\widetilde{m}_B-1}}{\Gamma(\widetilde{m}_B)} \exp\left(\frac{-\widetilde{m}_B\gamma}{\widetilde{\overline{\gamma}}_B}\right), \tag{5.16}$$

where $\widetilde{m}_B$ is the Nakagami fading parameter given by $\widetilde{m}_B = (\widetilde{K}_B+1)^2/(2\widetilde{K}_B+1)$ and $\Gamma(\mu) = \int_0^\infty e^{-t}t^{\mu-1}dt$, $\mathrm{Re}(\mu) > 0$, is the Gamma function.

Following (5.10), the SNR of the eavesdropper's channel can be rewritten as

$$\gamma_E = \sum_{i=1}^{N_E} \gamma_{E,i}, \tag{5.17}$$

where $\gamma_{E,i} = \overline{\gamma}_E|\mathbf{g}_i\mathbf{b}|^2$, $\mathbf{g}_i$ is the $1 \times N_A$ channel vector between Eve's i-th antenna and Alice, i.e., $\mathbf{g}_i$ is the i-th row of $\mathbf{G}$. As per (5.3), we have

$$\mathbf{g}_i = \sqrt{\frac{K_E}{1+K_E}}\epsilon_i\mathbf{g}_o + \sqrt{\frac{1}{1+K_E}}\mathbf{g}_{r,i}, \tag{5.18}$$

where $\epsilon_i = e^{-j(i-1)\tau_E \cos\phi_E}$ and $\mathbf{g}_{r,i}$ is the i-th row of $\mathbf{G}_r$. For any value of i ($i = 1, 2, \ldots, N_E$), we have

$$|\epsilon_i \mathbf{g}_o \mathbf{b}| = |\mathbf{g}_o \mathbf{b}|. \tag{5.19}$$

As such, following a procedure similar to that used in obtaining $f_{\gamma_B}(\gamma)$, the pdf of $\gamma_{E,i}$ can be approximated as

$$f_{\gamma_{E,i}}(\gamma) = \left(\frac{\widetilde{m}_E}{\widetilde{\overline{\gamma}}_E}\right)^{\widetilde{m}_E} \frac{\gamma^{\widetilde{m}_E - 1}}{\Gamma(\widetilde{m}_E)} \exp\left(\frac{-\widetilde{m}_E \gamma}{\widetilde{\overline{\gamma}}_E}\right), \tag{5.20}$$

where $\widetilde{m}_E$ is given by $\widetilde{m}_E = (\widetilde{K}_E + 1)^2/(2\widetilde{K}_E + 1)$, $\widetilde{K}_E$ is given by $\widetilde{K}_E = |\mathbf{g}_o \mathbf{b}|^2 K_E$, and $\widetilde{\overline{\gamma}}_E$ is given by

$$\widetilde{\overline{\gamma}}_E \triangleq \mathbb{E}[\gamma_E] = \frac{(K_E |\mathbf{g}_o \mathbf{b}|^2 + 1)\, \overline{\gamma}_E}{1 + K_E}. \tag{5.21}$$

Since the $\gamma_{E,i}$ are independent, following (5.21) the pdf of γ_E can be approximated as

$$f_{\gamma_E}(\gamma) = \left(\frac{\widetilde{m}_E}{\widetilde{\overline{\gamma}}_E}\right)^{N_E \widetilde{m}_E} \frac{\gamma^{N_E \widetilde{m}_E - 1}}{\Gamma(N_E \widetilde{m}_E)} \exp\left(\frac{-\widetilde{m}_E \gamma}{\widetilde{\overline{\gamma}}_E}\right). \tag{5.22}$$

Following (5.19), we note that γ_E is independent of $\mathbf{r}_o$. This indicates that the SNR at Eve is independent of ϕ_E when Eve adopts MRC to combine the received signals (we do not need to know the orientation of the ULA at Eve for our analysis). This also reveals that the SNR at Eve is independent of the type of antenna array at Eve (e.g., other antenna arrays beyond ULAs) since different antenna arrays only impact $\mathbf{r}_o$. As such, our following analysis is also valid for other antenna arrays at Eve (e.g., non-uniform linear arrays, circular arrays, rectangle arrays).

5.3.2 Secrecy Performance of the LBB Scheme

Since the capacity of the eavesdropper's channel C_E is unavailable at Alice, the perfect secrecy cannot be guaranteed in the wiretap channel of interest. For this reason we adopt the secrecy outage probability and the probability of non-zero secrecy capacity

as our secrecy performance metrics. The secrecy outage probability is defined as the probability of the secrecy capacity C_s being less than the target secrecy rate R_s (bits/channel-use), which can be formulated as [60, 61]

$$P_{out}\left(R_s\right) = \Pr\left(C_s < R_s\right) = \int_0^{\infty} f_{\gamma_E}(\gamma_E) \left[\int_0^{2^{R_s}(1+\gamma_E)-1} f_{\gamma_B}(\gamma_B) d\gamma_B \right] d\gamma_E. \quad (5.23)$$

The secrecy outage probability is the most common metric used in physical layer security when the CSI of the eavesdropper's channel is unavailable at Alice. However, it is important to note this metric does not distinguish between reliability and security [114]. This secrecy outage probability consists of the reliability outage probability and the pure secrecy outage probability. The reliability outage probability is represented as the transmission outage probability in the on-off transmission scheme, which is the probability that the capacity of the main channel is less than the target secrecy rate [115]. The on-off transmission scheme is the only practical transmission scheme in which the transmission outage probability (i.e., the reliability outage probability) exists. We note that the capacity of the main channel is required in order to determine the wiretap code rates or design wiretap codes in the on-off transmission scheme. Therefore, secrecy outage probability is a valid and meaningful performance metric only when the capacity of the main channel is available at Alice.

With regard to the secrecy performance of the LBB scheme, we first provide the following theorem.

***Theorem* 9** The secrecy outage probability of the LBB scheme for a given R_s is

$$\begin{aligned} P_{out}\left(R_s\right) = & \frac{\widetilde{m}_B^{\widetilde{m}_B} \widetilde{m}_E^{N_E \widetilde{m}_E} 2^{\widetilde{m}_B R_s}}{\Gamma(N_E \widetilde{m}_E) \widetilde{\overline{\gamma}}_B^{-N_E \widetilde{m}_E} \widetilde{\overline{\gamma}}_E^{-\widetilde{m}_B}} \sum_{n=0}^{+\infty} \frac{2^{nR_s} \exp\left(-\frac{\widetilde{m}_B \left(2^{R_s}-1\right)}{\widetilde{\overline{\gamma}}_B} \right)}{\widetilde{m}_B^{n} \widetilde{\overline{\gamma}}_B^{n} \Gamma(\widetilde{m}_B + n + 1)} \times \\ & \sum_{l=0}^{+\infty} \frac{\binom{\widetilde{m}_B+n}{l} \left(2^{R_s}-1\right)^l \left(\widetilde{\overline{\gamma}}_B \widetilde{\overline{\gamma}}_E\right)^{n-l} \Gamma_G(\widetilde{m}_B + N_E \widetilde{m}_E + n - l)}{2^{lR_s} \left(2^{R_s} \widetilde{m}_B \widetilde{\overline{\gamma}}_E + \widetilde{m}_E \widetilde{\overline{\gamma}}_B\right)^{\widetilde{m}_B + N_E \widetilde{m}_E + n - l}}, \end{aligned} \quad (5.23)$$

where $\Gamma_G(\cdot)$ is the generalized gamma function (also valid for negative integers), which

is given by [116]

$$\Gamma_G(\alpha)=\begin{cases}\frac{(-1)^{-\alpha}}{(-\alpha)!}\left(\sum_{i=1}^{-\alpha}\frac{1}{i}+\alpha\right), & \alpha \text{ is a negative integer,}\\ \Gamma(\alpha), & \text{otherwise.}\end{cases} \tag{5.24}$$

The proof of Theorem 9 is provided in Appendix C.

We first note that the secrecy outage probability derived in (5.23) is a function of Bob and Eve's locations and the beamformer $\mathbf{b}$, all of which are embedded in the parameters $\widetilde{m}_B$, $\widetilde{m}_E$, $\widetilde{\overline{\gamma}}_B$, and $\widetilde{\overline{\gamma}}_E$. We also note that (5.23) is valid for arbitrary $\widetilde{m}_B$ and $\widetilde{m}_E$ ($\widetilde{m}_B$ and $\widetilde{m}_E$ can be equal), and thus (5.23) is valid for arbitrary K_B and K_E. As such, our derived expression for the secrecy outage probability is of more generality than that presented in [60], which is only valid for integral $\widetilde{m}_B$ and $\widetilde{m}_E$. Although the expression presented in (5.23) involves two infinite series, they both can be approximated by finite series accurately. We approximate the infinite series $\sum_{n=0}^{+\infty}$ and $\sum_{l=0}^{+\infty}$ by truncating them at finite numbers. As we will show in Section 5.5, the accuracy of such approximations is acceptable as long as the truncating numbers are larger than approximately one hundred.

An important performance parameter associated with the secrecy outage probability is the secrecy diversity order, which determines the slope of the curve for the secrecy outage probability (in dB) versus $\overline{\gamma}_B$ (in dB) as $\overline{\gamma}_B \to \infty$ for finite $\overline{\gamma}_E$. Mathematically, the secrecy diversity order is defined as

$$\Phi = \lim_{\overline{\gamma}_B\to\infty} \frac{\log_{10} P_{out}\left(R_s\right)}{\log_{10}(1/\overline{\gamma}_B)}. \tag{5.25}$$

The secrecy diversity order of the LBB scheme is presented in the following corollary.

***Corollary* 3** The secrecy diversity order of the LBB scheme is $\widetilde{m}_B$.

Following a procedure similar to that used in deriving the secrecy diversity order of the antenna selection schemes presented in [60,61], we can obtain in a straightforward manner the secrecy diversity order of the LBB scheme as $\widetilde{m}_B$. As such, we omit the

proof of the above corollary here. We note that maximum value of $\widetilde{m}_B$ is $(N_A K_B + 1)^2/(2N_A K_B + 1)$ due to $|\mathbf{h}_o\mathbf{b}|^2 \leq \|\mathbf{h}_o\|^2\|\mathbf{b}\|^2 = N_A$.

The probability of non-zero secrecy capacity is defined as the probability that a positive secrecy capacity is achieved. As per the definition of C_s provided in Chapter 1, the probability of non-zero secrecy capacity can be formulated as

$$P_{non} = \Pr(C_s > 0) = 1 - \int_0^\infty f_{\gamma_E}(\gamma_E) \left(\int_0^{\gamma_E} f_{\gamma_B}(\gamma_B) d\gamma_B \right) d\gamma_E. \tag{5.26}$$

Then, the probability of non-zero secrecy capacity of the LBB scheme is presented in the following corollary.

***Corollary* 4** The probability of non-zero secrecy capacity of the LBB scheme is given by

$$\begin{aligned} P_{non} = 1 - & \frac{\widetilde{m}_B^{\widetilde{m}_B} \widetilde{m}_E^{N_E \widetilde{m}_E}}{\Gamma(N_E \widetilde{m}_E) \widetilde{\overline{\gamma}}_E^{-\widetilde{m}_B} \widetilde{\overline{\gamma}}_B^{-N_E \widetilde{m}_E}} \sum_{n=0}^{+\infty} \frac{\widetilde{m}_B^n \widetilde{\overline{\gamma}}_E^n}{\Gamma(\widetilde{m}_B + n + 1)} \\ & \times \frac{\Gamma\left(\widetilde{m}_B + N_E \widetilde{m}_E + n\right)}{\left(\widetilde{m}_B \widetilde{\overline{\gamma}}_E + \widetilde{m}_E \widetilde{\overline{\gamma}}_B\right)^{\widetilde{m}_B + N_E \widetilde{m}_E + n}}. \end{aligned} \tag{5.27}$$

The proof of Corollary 4 is provided in the following. As per (5.26), the probability of non-zero secrecy capacity can also be formulated as

$$P_{non} = 1 - P_{out}(R_s = 0). \tag{5.28}$$

Substituting $R_s = 0$ into (5.23), we obtain the desirable result in (5.27).

We note that the expression for the probability of non-zero secrecy capacity is simpler than that for the secrecy outage probability and it only involves one infinite series. This infinite series can also be approximated by truncating it at a finite number. This approximation is very accurate even when the truncating number is small (e.g., 10).

5.3.3 Optimal Location-based Beamformer

A location-based beamformer can be written as

$$\mathbf{b} = \frac{1}{\sqrt{N_A}} \left[1, \cdots, \exp(-j(N_A - 1)\tau_A \cos\psi)\right]^T, \tag{5.29}$$

where ψ ($0 \leq \psi \leq \pi$) is the beamforming direction. In this chapter we define the optimal location-based beamformer, $\mathbf{b}^*$, as the one that minimizes the secrecy outage probability for a given R_s. Therefore, defining

$$\psi^* = \underset{0 \leq \psi \leq \pi}{\operatorname{argmin}} P_{out}\left(R_s\right), \tag{5.30}$$

and setting $\psi = \psi^*$ in (5.29) completely determine the optimal beamformer $\mathbf{b}^*$. We note that the value range of ψ is selected based on the symmetric property of the ULA (e.g., $\psi = \pi/3$ and $\psi = -\pi/3$ lead to the same beamformer $\mathbf{b}$). We note that (5.30) is a one-dimensional optimization problem, which can be solved through numerical search. Substituting $\mathbf{b}^*$ into (5.23), we achieve the minimum secrecy outage probability of the LBB scheme, which is denoted as $P^*_{out}(R_s)$. We would like to highlight that ψ^* can be analytically determined in some special cases as detailed in the following corollaries.

***Corollary* 5** For $K_B > 0$, the solution to (5.30) is $\psi^* = \theta_B$ in the following cases: (i) when $\overline{\gamma}_B \to \infty$ for finite $\overline{\gamma}_E$, (ii) when $K_E = 0$, or (iii) when θ_E is unavailable at Alice.

We provide the proof of Corollary 5 in the following. In Case (i), as $\overline{\gamma}_B \to \infty$ the secrecy diversity order determines the secrecy outage probability. As such, as $\overline{\gamma}_B \to \infty$ the optimal location-based beamformer is to maximize the secrecy diversity order given in Corollary 3 (i.e., $\widetilde{m}_B$) in order to minimize the secrecy outage probability. To this end, ψ^* is to maximize $\widetilde{K}_B$. Following (5.14), ψ^* finally is to maximize $|\mathbf{h}_o\mathbf{b}|^2$. In Case (ii), there is no LOS component in the eavesdropper's channel due to $K_E = 0$ and ψ does not impact γ_E. As such, ψ^* is to maximize γ_B in order to minimize the secrecy outage probability. Following (5.9), ψ^* finally is to maximize $|\mathbf{h}_o\mathbf{b}|^2$ in this case. In Case (iii), Alice is not sure how ψ impacts γ_E since θ_E is unknown. Then, ψ is to maximize γ_B and thus to maximize $|\mathbf{h}_o\mathbf{b}|^2$ based on (5.9).

As we can see from the above discussion, in all three cases of the corollary the value of ψ^* is the one that maximizes $|\mathbf{h}_o\mathbf{b}|^2$. So, to complete the proof we now prove

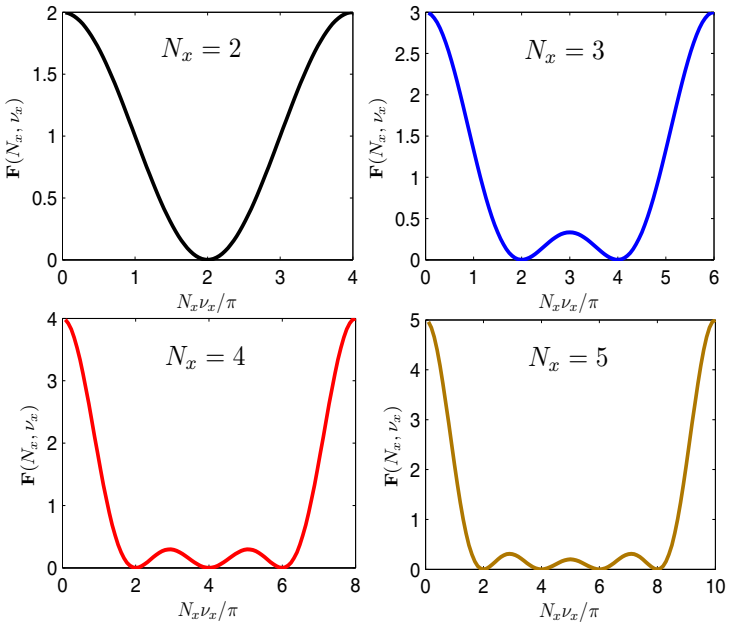

Figure 5.2: $\mathbf{F}(N_x, \nu_x)$ versus $N_x\nu_x/\pi$ for different values of N_x.

that this value is indeed θ_B. Denoting $\nu_A = \tau_A(\cos\theta_B - \cos\psi)$, as per (5.2) and (5.29), for $\nu_A \neq 0$ we have

$$\begin{aligned}\mathbf{h}_o\mathbf{b} &= \frac{1}{\sqrt{N_A}}\frac{\exp(jN_t\nu_A)-1}{\exp(j\nu_A)-1} \\ &= \frac{1}{\sqrt{N_A}}\frac{-e^{jN_A\nu_A/2}\left(-e^{-jN_A\nu_A/2}-e^{jN_A\nu_A/2}\right)}{-e^{j\nu_A/2}\left(-e^{-j\nu_A/2}-e^{j\nu_A/2}\right)} \\ &= \frac{1}{\sqrt{N_A}}\frac{\sin\left(\frac{1}{2}N_A\nu_A\right)}{\sin\left(\frac{1}{2}\nu_A\right)}e^{j\nu_A(N_A-1)/2}.\end{aligned} \tag{5.31}$$

For $\nu_A = 0$, we have $\mathbf{h}_o\mathbf{b} = \sqrt{N_A}$. Then, following (5.31) we have

$$|\mathbf{h}_o\mathbf{b}|^2 = \mathbf{F}(N_A, \nu_A), \tag{5.32}$$

where $\mathbf{F}(\cdot,\cdot)$ is defined as

$$\mathbf{F}(N_x, \nu_x) = \begin{cases} N_x, & \nu_x = 0, \\ \frac{1}{N_x}\left(\frac{\sin\left(\frac{1}{2}N_x\nu_x\right)}{\sin\left(\frac{1}{2}\nu_x\right)}\right)^2, & 0 \leq \nu_x < 2\pi. \end{cases} \tag{5.33}$$

It is straightforward to prove that the maximum value of $\mathbf{F}(N_x, \nu_x)$ is N_x, which is achieved for $\nu_x = 0$. This is also confirmed by Fig. 5.2, where we plot $\mathbf{F}(N_x, \nu_x)$

versus $N_x\nu_x/\pi$ for different value of N_x. As such, $|\mathbf{h}_o\mathbf{b}|^2$ is maximized when $\nu_A = 0$ and thus we have $\psi^* = \theta_B$ (we ignore the negative solutions due to $0 \leq \psi \leq \pi$) in order to maximize $|\mathbf{h}_o\mathbf{b}|^2$. This completes the proof of Corollary 5.

We note that for $\psi^* = \theta_B$ we have $\mathbf{b}^* = \mathbf{h}_o^\dagger/\sqrt{N_A}$ and $|\mathbf{h}_o\mathbf{b}|^2 = N_A$. As such, we have $\widetilde{K}_B = N_A K_B$ and $\widetilde{\overline{\gamma}}_B = (N_A K_B + 1)\overline{\gamma}_B/(1 + K_B)$. We denote the secrecy outage probability of the LBB scheme with unknown Eve's location (i.e., $\psi^* = \theta_B$) as $P_{out}^b(R_s)$.

***Corollary* 6** For $K_E > 0$, the solution to (5.30) is $\psi^* = \arccos\left(\cos\theta_E + \frac{2n_A\pi}{N_A\tau_A}\right)$, $n_A = 1, \ldots, N_A - 1$, in the following cases: (i) when $\overline{\gamma}_E \to \infty$ for finite $\overline{\gamma}_B$, (ii) when $K_B = 0$, or (iii) when θ_B is unavailable at Alice.

We now prove Corollary 6. Following similar arguments to those used in the proof of Corollary 5, we know that ψ^* is to minimize $|\mathbf{g}_o\mathbf{b}|^2$ for all three cases in Corollary 6. The value of $|\mathbf{g}_o\mathbf{b}|^2$ is given by

$$|\mathbf{g}_o\mathbf{b}|^2 = \mathbf{F}(N_A, \nu_E), \tag{5.34}$$

where $\nu_E = \tau_A(\cos\theta_E - \cos\psi)$. We note that the minimum value of $\mathbf{F}(N_x, \nu_x)$ is achieved when $\nu_x = 2n_x\pi$ for $n_x = 1, \ldots, N_x - 1$, which is also confirmed by Fig. 5.2. As such, $|\mathbf{g}_o\mathbf{b}|^2$ is minimized when $\nu_E = 2n_A\pi$ for $n_A = 1, \ldots, N_A - 1$, and thus we obtain Corollary 6.

5.4 Non-Beamforming Scheme

In this section, we analyze the secrecy performance of the NB scheme as a benchmark to understand the LBB scheme.

5.4.1 Statistical Properties of the Instantaneous SNRs

In the NB scheme, Alice distributes her total transmit power uniformly among the N_A orthogonal independent transmit directions (i.e., the covariance matrix of $\mathbf{b}x$ is

$P\mathbf{I}_{N_A}/N_A$) [117, 118]. Then, the SNR at Bob is given by [117, 118]

$$\gamma_B^{\mathbf{NB}} = \frac{\overline{\gamma}_B ||\mathbf{h}||^2}{N_A}. \tag{5.35}$$

Interpreting Rician fading as a special case of Nakagami fading, the pdf of $\gamma_B^{\mathbf{NB}}$ can be approximated by

$$f_{\gamma_B^{\mathbf{NB}}}(\gamma) = \frac{m_B^{N_A m_B} \gamma^{N_A m_B - 1} e^{-\frac{N_A m_B \gamma}{\overline{\gamma}_B}}}{\Gamma(N_A m_B)(\overline{\gamma}_B/N_A)^{N_A m_B}}, \tag{5.36}$$

where $m_B = (K_B+1)^2/(2K_B+1)$. We assume that Eve applies MRC to combine the received signals at different antenna elements. As such, the SNR at Eve is given by

$$\gamma_E^{\mathbf{NB}} = \frac{\overline{\gamma}_E ||\mathbf{s}_0^\dagger \mathbf{G}||^2}{N_A} = \frac{\overline{\gamma}_E \lambda_0^2}{N_A}, \tag{5.37}$$

where $\mathbf{s}_0$ is the $N_E \times 1$ eigenvector for the largest eigenvalue λ_0 of $\mathbf{G}$. The theoretical expression for the distribution of λ_0^2 has been derived in [119]. However, this expression is too complicated to be used for further analysis. To make progress, we adopt the simple approximation for the pdf of λ_0^2 proposed in [120]. As such, the pdf of $\gamma_E^{\mathbf{NB}}$ can be approximated by

$$f_{\gamma_E^{\mathbf{NB}}}(\gamma) = \frac{(N_A m_E)^{N_A N_E m_E} \gamma^{N_A N_E m_E - 1}}{\Gamma(N_A N_E m_E)(\overline{\gamma}_E \overline{\lambda}_0)^{N_A N_E m_E}} \exp\left(-\frac{N_A m_E \gamma}{\overline{\gamma}_E \overline{\lambda}_0}\right), \tag{5.38}$$

where $m_E = (K_E+1)^2/(2K_E+1)$ and $\overline{\lambda}_0$ is the mean of the per-branch largest eigenvalue (i.e., $\overline{\lambda}_0 = \mathbb{E}[\lambda_0]/N_A N_E$). The value of $\overline{\lambda}_0$ can be approximated by [120]

$$\overline{\lambda}_0 = \begin{cases} \frac{K_E}{K_E+1} + \frac{1}{K_E+1}\frac{N_A+N_E}{N_A N_E+1}, & K_E \geq 0.5, \\ \left(\frac{N_A+N_E}{N_A N_E+1}\right)^{\frac{4-K_E}{6}}, & K_E < 0.5. \end{cases} \tag{5.39}$$

We note that we have $\overline{\lambda}_0 = 1$ for arbitrary K_E when $N_E = 1$.

5.4.2 Secrecy Performance of the NB Scheme

Following a similar procedure to that used in deriving $P_{out}(R_s)$ in Theorem 9, the secrecy outage probability of the NB scheme is derived as

$$\begin{aligned} P_{out}^{\mathbf{NB}}(R_s) &= \int_0^{\infty} f_{\gamma_E^{\mathbf{NB}}}(\gamma_E)\left[\int_0^{2^{R_s}(1+\gamma_E)-1} f_{\gamma_B^{\mathbf{NB}}}(\gamma_B)d\gamma_B\right]d\gamma_E \\ &= \frac{m_B^{N_A m_B} m_E^{N_A N_E m_E} 2^{N_A m_B R_s}}{\Gamma(N_A N_E m_E)\overline{\gamma}_B^{-N_A N_E m_E}(\overline{\gamma}_E\overline{\lambda}_0)^{-N_A m_B}}\times \\ &\quad \sum_{n=0}^{+\infty} \frac{m_B^n 2^{nR_s}\exp\left(-\frac{N_A m_B\left(2^{R_s}-1\right)}{\overline{\gamma}_B}\right)}{\overline{\gamma}_B^n\Gamma(N_A m_B+n+1)}\times \\ &\quad \sum_{l=0}^{+\infty} \frac{\binom{N_A m_B+n}{l}\left(2^{R_s}-1\right)^l}{N_A^{-l}2^{lR_s}}\times \\ &\quad \frac{\left(\overline{\gamma}_B\overline{\gamma}_E\overline{\lambda}_0\right)^{n-l}\Gamma_G(N_A m_B+N_A N_E m_E+n-l)}{\left(2^{R_s}m_B\overline{\gamma}_E\overline{\lambda}_0+m_E\overline{\gamma}_B\right)^{N_A m_B+N_A N_E m_E+n-l}}. \end{aligned} \tag{5.40}$$

As per (5.40), we can see that the secrecy outage probability of the NB scheme is independent of θ_B and θ_E. However, (5.40) is a function of $\overline{\gamma}_B$ and $\overline{\gamma}_E$, which are dependent on d_B and d_E, respectively. We note that the secrecy diversity order of the NB scheme is $N_A m_B$, which is the full secrecy diversity order. Also, following a similar procedure to that used in deriving P_{non} in Corollary 4, the probability of non-zero secrecy capacity of the NB scheme is derived as

$$\begin{aligned} P_{non}^{\mathbf{NB}} = 1 &- \frac{m_B^{N_A m_B} m_E^{N_A N_E m_E}\overline{\gamma}_B^{N_A N_E m_E}}{\Gamma(N_A N_E m_E)(\overline{\gamma}_E\overline{\lambda}_0)^{-N_A m_B}}\times \\ &\sum_{n=0}^{+\infty}\frac{m_B^n\left(\overline{\gamma}_E\overline{\lambda}_0\right)^n}{\Gamma(N_A m_B+n+1)}\frac{\Gamma\left(N_A m_B+N_A N_E m_E+n\right)}{\left(m_B\overline{\gamma}_E\overline{\lambda}_0+m_E\overline{\gamma}_B\right)^{N_A m_B+N_A N_E m_E+n}}. \end{aligned} \tag{5.41}$$

5.5 Numerical and Simulation Results

In this section we present numerical simulations to verify our secrecy performance analysis of the LBB scheme, and examine the impact of different system parameters (e.g., K_B, K_E, $\overline{\gamma}_B$, and $\overline{\gamma}_E$) on the LBB scheme. To better illustrate the gains obtained by our scheme, we will also present simulations of the secrecy performance

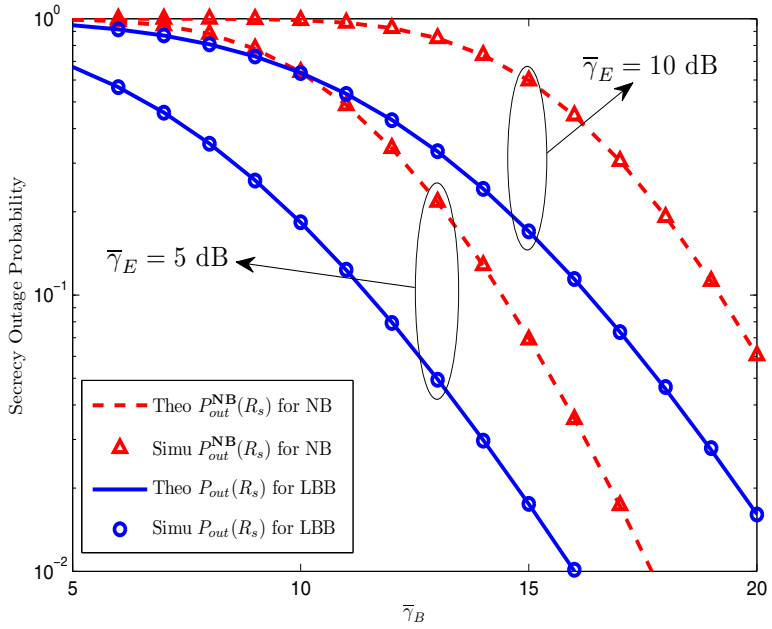

Figure 5.3: Secrecy outage probabilities versus different values of $\overline{\gamma}_B$, where $m_B = 1.35, m_E = 1.33, \overline{\lambda}_0 = 0.85, N_A = 3, N_E = 2$, and $R_s = 1$.

of the NB (non-beamforming) scheme. This latter scheme represents the case when an isotropic beamforming pattern is produced by Alice. To conduct simulations, we deploy Bob and Eve at specific locations and then map such locations into $\overline{\gamma}_B$ and $\overline{\gamma}_E$, respectively. Such a mapping is based on Alice's transmit power (i.e., P) and path loss exponents of the main channel and the eavesdropper's channel (i.e., η_B and η_E). For presentation convenience, we only specify the values of $\overline{\gamma}_B$ and $\overline{\gamma}_E$ adopted in our following simulations. We note that in the following figures provided in this chapter we use "Theo" and "Simu" as the abbreviations of "Theoretic" and "Simulated", respectively.

In Fig. 5.3 we first verify our derived secrecy outage probabilities for Nakagami fading channels. To this end, we generate channel realizations as per the Nakagami fading channel, where we have set $\widetilde{m}_B = 2m_B$, $\widetilde{m}_E = m_E$, $\widetilde{\overline{\gamma}}_B = 3\overline{\gamma}_B$, and $\widetilde{\overline{\gamma}}_E = \overline{\gamma}_E$. The theoretic secrecy outage probability of the LBB scheme, $P_{out}\,(R_s)$, and the secrecy outage probability of the NB scheme, denoted as $P_{out}^{\mathbf{NB}}(R_s)$, are obtained through (5.23) and (5.40), respectively, where relevant infinite series are truncated at 100. In

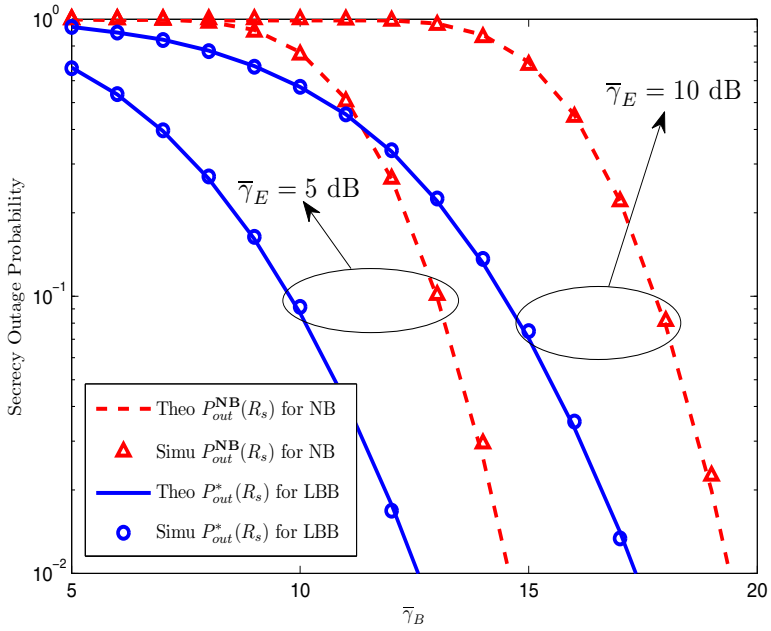

Figure 5.4: Secrecy outage probabilities of the LBB and NB schemes versus different values of $\overline{\gamma}_B$, where $N_A = 3, N_E = 2, K_B = 10$ dB, $K_E = 5$ dB, $\theta_b = \pi/3, \theta_e = \pi/4$, and $R_s = 1$.

this figure, we observe that the theoretic $P_{out}(R_s)$ and $P_{out}^{\mathbf{NB}}(R_s)$ precisely match the simulated $P_{out}(R_s)$ and $P_{out}^{\mathbf{NB}}(R_s)$, respectively. This confirms the correctness of our derived secrecy outage probabilities.

Recall that for mathematical convenience, our analysis approximates a Rician channel with a Nakagami channel. To see the effect of this, in Fig. 5.4 we again plot the secrecy outage probabilities of the LBB scheme and the NB scheme, but this time for specific Rician fading channels. In this figure, we observe that the simulated minimum secrecy outage probability of the LBB scheme, $P_{out}^{*}(R_s)$, and the secrecy outage probability of the NB scheme, $P_{out}^{\mathbf{NB}}(R_s)$, match extremely well the theoretic $P_{out}^{*}(R_s)$ and $P_{out}^{\mathbf{NB}}(R_s)$, respectively, thus confirming the validity of our channel approximation. We note that we have set θ_E very close to θ_B in Fig. 5.4 (i.e., $\theta_B = \pi/3$ and $\theta_E = \pi/4$). The gap between $P_{out}^{*}(R_s)$ and $P_{out}^{\mathbf{NB}}(R_s)$ can even be larger when θ_E is not so close to θ_B.

In Fig. 5.5, we plot the minimum secrecy outage probability of the LBB scheme,

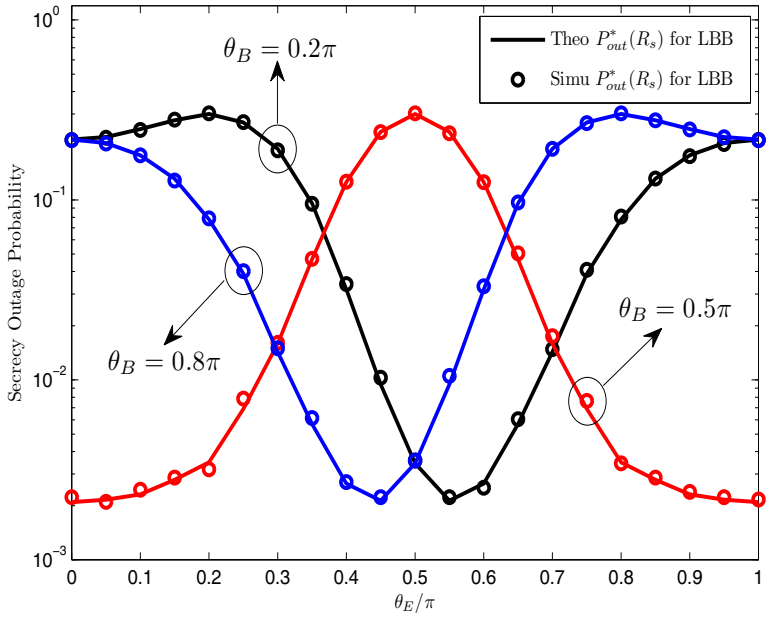

Figure 5.5: Minimum secrecy outage probability of the LBB scheme versus different values of θ_E, where $N_A = 2, N_E = 2, K_B = 10$ dB, $K_E = 10$ dB, $\overline{\gamma}_B = 10$ dB, $\overline{\gamma}_E = 10$ dB, and $R_s = 1$.

$P^*_{out}(R_s)$, versus different values of θ_E. Again we observe that the theoretic $P^*_{out}(R_s)$ matches extremely well the simulated $P^*_{out}(R_s)$, which again confirms the validity of our analysis. Fig. 5.5 is also useful in that it more visually represents how the minimum secrecy outage probability of the LBB scheme depends on the locations of Bob and Eve. For example, $P^*_{out}(R_s)$ is maximized when $\theta_B = \theta_E$. In addition, we also can see how the secrecy performance of our LBB scheme is sensitive to the accuracy of provided location information. For instance, we observe that $P^*_{out}(R_s)$ is very sensitive to θ_E when $\theta_B = 0.8\pi$ and θ_E is around 0.2π (e.g., $0.1\pi < \theta_E < 0.3\pi$). We also observe $P^*_{out}(R_s)$ is not sensitive to θ_E when $\theta_B = 0.8\pi$ and θ_E is around 0.45π (e.g., $0.4\pi < \theta_E < 0.5\pi$). These two observations illustrate that the sensitivity of the secrecy performance of our LBB scheme with respect the location accuracy of Bob or Eve is highly dependent on the geometry of all the transceivers (i.e., Alice, Bob, and Eve). In the simulations to obtain Fig. 5.5, we also observe that the optimal beamforming direction ψ^* shifts away from θ_B as θ_E approaches to θ_B.

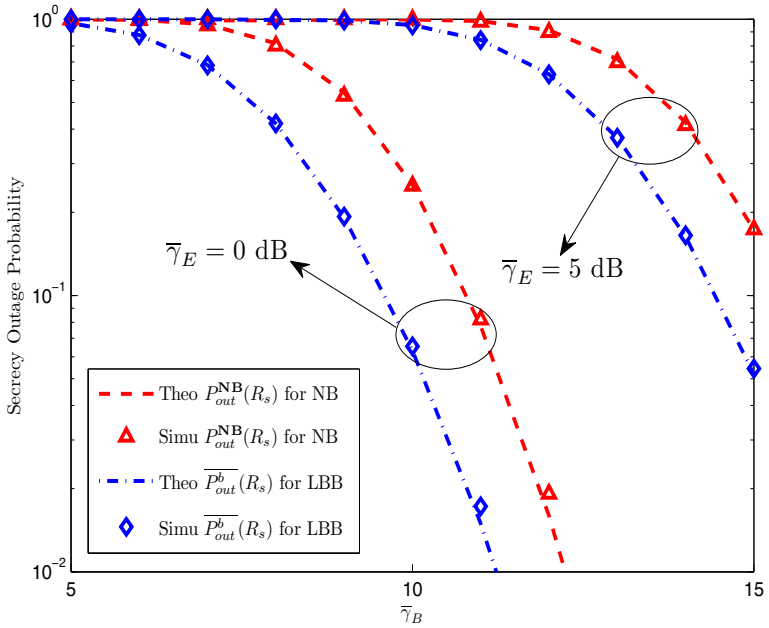

Figure 5.6: Secrecy outage probabilities of the LBB and NB schemes versus different values of $\overline{\gamma}_B$, where $N_A = 3, N_E = 4, K_B = 10$ dB, $K_E = 5$ dB, $\theta_b = \pi/3$, and $R_s = 1$.

In Fig. 5.6, we examine the secrecy outage probability of the LBB scheme without knowing Eve's location, $P_{out}^{b}(R_s)$. As per Corollary 5, we know that $\mathbf{b}^* = \mathbf{h}^\dagger/\|\mathbf{h}\|$ when Eve's location is unavailable at Alice. In Fig. 5.6 we also compare the the solution with no information on Eve's location to the NB scheme. To conduct a fair comparison, we assume Eve's location is uniformly distributed on a circle centered at Alice, i.e., θ_E uniformly distributes between 0 and 2π, $\theta_E \sim \mathcal{U}[0, 2\pi]$. We then average $P_{out}^{b}(R_s)$ over θ_E to obtain the average secrecy outage probability, denoted as $\overline{P_{out}^{b}}(R_s)$. As expected, we observe that $\overline{P_{out}^{b}}(R_s)$ is lower than $P_{out}^{\mathbf{NB}}(R_s)$, which demonstrates that the LBB scheme still outperforms the NB scheme *on average*, even when Eve's location is unavailable at Alice. This is due to the fact that the LBB scheme improves the quality of the main channel based on Bob's location, which on average reduces the secrecy outage probability. However, the most important result obtained from the simulations of Fig. 5.6 is that the secrecy outage probability of the LBB scheme without Eve's location increases (e.g., by approximately a factor of 5 for

$\overline{\gamma}_B = 10$dB) relative to that of the LBB scheme with Eve's location.

It is worth mentioning how the relaxation of some assumptions we have made (e.g., zero error in the location information of Bob and Eve) impacts our results. Of course, in reality it will never be the case that all reported locations, all K map information, and all path loss exponents are known with zero error. Errors in these quantities are intermingled in the sense that an error in one leads to an error in another. We have attempted to encompass such correlated errors in a range of additional simulations. Our general result is that a percentage error of 15% in any of these inputs leads to an approximately 10% percentage error in our reported outage probabilities. For anticipated error inputs, we can therefore say that our analysis remains reasonably accurate.

5.6 Summary

We proposed and analyzed a novel beamforming scheme in the wiretap channel where both the main channel and the eavesdropper's channel are subject to Rician fading. Our new LBB scheme solely requires as inputs the location information of Bob and Eve, and does not require the CSI of the main channel or the eavesdropper's channel. We derived the secrecy outage probability of the LBB scheme in a closed-form expression valid for arbitrary values of K_B and K_E. We then determined the optimal location-based beamformer that minimizes the secrecy outage probability. Comparisons with the NB scheme were then carried out so as to better understand the performance gains offered by our location-based solution. The work we presented in this chapter will be important for a range of application scenarios in which Rician channels are expected to be dominant and where location information of potential users and adversaries are known.

Chapter 6

TAS with Alamouti Coding and Power Allocation

6.1 Introduction

In Chapter 5, an optimal LBB scheme was analyzed in the context of physical layer security for wireless communications. By comparing the LBB scheme with the Non-Beamforming scheme, the trade-off between feedback overhead and secrecy performance in wiretap channels was investigated. Following on from Chapter 5, we further examine the trade-off between feedback overhead and secrecy performance in the context of transmit antenna selections. In our examination, we consider MIMO wiretap channels, in which location information (which potentially can be verified by our developed LVSs in Chapter 2, Chapter 3, and Chapter 4) is required to provide the average SNR of the main channel or the eavesdropper's channel. As discussed in Chapter 1, to avoid high feedback overhead and complex signal processing, a single TAS scheme was proposed in wiretap channels [58–60]. In this scheme, only one antenna is selected at Alice to maximize the instantaneous SNR of the main channel. Throughout this thesis, we refer to this scheme as *single TAS*. Notably, single TAS incurs low feedback overhead and low implementation complexity since only the

index of the strongest transmit antenna is fed back from the receiver to the transmitter and only one radio-frequency chain is implemented at the transmitter. We note that [58–60, 121] considered the scenario where the instantaneous CSI of the eavesdropper's channel is not available at the transmitter. In this scenario, perfect secrecy between Alice and Bob cannot be guaranteed and secrecy outage probability [63] is adopted as a practical and important metric to evaluate the secrecy performance.

In the context of TAS within the MIMO wiretap channel, a natural question that arises is "*What is the secrecy performance if two antennas are selected at the transmitter?*". This is the main question we intend to answer in this chapter. When two antennas are selected at the transmitter, an effective coding strategy needs to be incorporated in order to maximize secrecy performance. Here, we adopt Alamouti coding since it achieves full rate (one symbol per time slot) using linear encoding and decoding algorithms [122]. Henceforth, we refer to two-antenna selection with Alamouti coding as the *TAS-Alamouti* scheme. We note that the Alamouti code is the only space time block code (STBC) that achieves full rate and full diversity with linear receiver algorithms. The selection of more than 2 antennas and an appropriate STBC can achieve a lower secrecy outage probability at the cost of reducing the rate (or increasing the decoding complexity). This is the main reason that we focus on Alamouti code with two transmit antennas in this work. In our TAS-Alamouti scheme, Alice selects the first two strongest antennas based on the feedback from Bob, which maximizes the instantaneous SNR of the main channel. After this, Alice employs Alamouti coding at the selected transmit antennas in order to perform secret data transmission. At Bob, MRC is applied in order to combine the received signals to fully exploit the benefits of multiple receive antennas. We assume that Eve also uses MRC to maximize the probability of successful eavesdropping.

The specific contributions of this chapter are summarized as follows. (i) We derive a closed-form expression for the secrecy outage probability of the TAS-Alamouti scheme. Based on the secrecy outage probability, we present the probability of non-zero secrecy capacity of TAS-Alamouti and numerically determine the ε-outage secre-

cy capacity. (ii) We derive a more compact closed-form expression for the asymptotic secrecy outage probability of TAS-Alamouti in the high SNR regime of the main channel. (iii) We apply optimal power allocation (OPA) within the TAS-Alamouti scheme, henceforth referred as TAS-Alamouti-OPA, and derive a closed-form expression for the secrecy outage probability of TAS-Alamouti-OPA. The main observations we draw from this chapter are summarized as follows. (i) The proposed TAS-Alamouti scheme achieves a lower secrecy outage probability than single TAS for the medium and high SNRs of the main channel. (ii) TAS-Alamouti-OPA achieves a lower secrecy outage probability than single TAS for *all* the SNRs of the main channel.

The rest of this chapter is organized as follows. Section 6.2 details the system model and the proposed TAS-Alamouti scheme. In Section 6.3, the secrecy performance of TAS-Alamouti is analyzed. In Section 6.4, a performance comparison between TAS-Alamouti and single TAS is presented. In Section 6.5, TAS-Alamouti-OPA is detailed and its secrecy performance is analyzed. Numerical results that demonstrate the performance improvement of TAS-Alamouti-OPA over TAS-Alamouti are presented in Section 6.6. Finally, Section 6.7 draws concluding remarks and suggests future directions.

6.2 System Model

We assume a Time Division Multiple Access (TDMA) system. The MIMO wiretap channel of interest is illustrated in Fig. 6.1, where the transmitter (Alice), the receiver (Bob), and the eavesdropper (Eve) are equipped with N_A, N_B, and N_E antennas, respectively. We assume that the main channel and the eavesdropper's channel are subject to quasi-static Rayleigh fading, the block length is the same for all channels, and Alice, Bob, and Eve are static. We assume that one fading block covers two time slots within which Alamouti coding is applied. We assume that the full CSI of the main channel is known to Bob, and that Bob applies MRC to combine the received signals. This allows Bob to exploit the N_B-antenna diversity and maximize

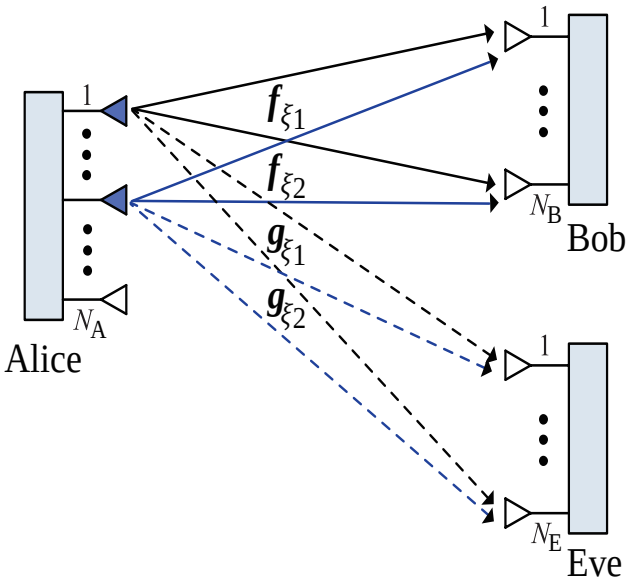

Figure 6.1: Illustration of a MIMO wiretap channel with N_A, N_B, and N_E antennas at Alice, Bob, and Eve, respectively.

the probability of secret transmission. We also assume that the full CSI of the eavesdropper's channel is known to Eve, and that Eve applies MRC in order to exploit the N_E-antenna diversity and to maximize the probability of successful eavesdropping.

In addition to the indices of the two strongest antennas, we assume that Bob feeds back the average SNR of the main channel, $\overline{\gamma}_B$, to Alice. We note that feeding back $\overline{\gamma}_B$ leads to a lower feedback relative to feeding back the full CSI of the main channel. The reason for this is that $\overline{\gamma}_B$ needs to be fed back only once, since the distance between Alice and Bob stays constant. This is to be compared with CSI knowledge which has to be fed back for each fading block. We also note the full CSI of the main channel is an $N_B \times N_A$ complex matrix, whereas $\overline{\gamma}_B$ is a real number. As such, feeding back the full CSI incurs a higher feedback overhead relative to feeding back $\overline{\gamma}_B$.

A final assumption is that the average SNR of the eavesdropper's channel, $\overline{\gamma}_E$, is known to Alice[1]. This assumption can be justified in several practical scenarios. For

[1]This means that Eve's distance from Alice is known and the path loss exponent is known. Note, the assumption that $\overline{\gamma}_E$ is known at Alice has been adopted elsewhere (e.g. [58–60]), and is a relaxed assumption relative to the assumption of full CSI feedback from Eve adopted elsewhere, e.g. [11,12].

example, Eve may be a regular user served by Alice in a previous time slot. Being a regular user at some time, the true $\overline{\gamma}_E$ must be fed back to Alice by Eve (otherwise Eve will not receive information at the full transmit rate). Another example in which $\overline{\gamma}_E$ may be known is where Eve is likely to be at some known fixed distance away from Alice, such as on the perimeter of a building or fence. In this case, the average SNR of the eavesdropper's channel is upper bounded by the SNR at the perimeter of a building or fence. In this situation, the derived secrecy outage probability in this chapter is still valid, as it represents a worst case when information is leaked. A final scenario we suggest is the military one where the enemy's position is *a priori* ascertained (e.g. via reconnaissance).

The proposed TAS-Alamouti scheme is performed in two steps, which are detailed in the following two subsections.

6.2.1 Transmit Antenna Selection

In the first step, the first two strongest antennas out of N_A antennas are selected at Alice based on the feedback from Bob. This feedback is the indices of the two antennas at Alice which result in the strongest signals at Bob. These two antennas maximize the instantaneous SNR of the main channel. Given that Bob employs MRC to combine the received signals, the index of the first strongest antenna is given by

$$\xi_1 = \underset{0\leq\xi\leq N_A}{\operatorname{argmax}} \|\boldsymbol{f}_\xi\|\,, \tag{6.1}$$

and the index of the second strongest antenna is determined by

$$\xi_2 = \underset{0\leq\xi\leq N_A,\xi\neq\xi_1}{\operatorname{argmax}} \|\boldsymbol{f}_\xi\|\,, \tag{6.2}$$

where $\boldsymbol{f}_\xi = [f_{\xi,1}, f_{\xi,2}, ..., f_{\xi,N_B}]^T$ is the $N_B \times 1$ channel vector between the ξ-th antenna at Alice and the N_B antennas at Bob with i.i.d. Rayleigh fading entries.

To conduct transmit antenna selection, Alice sends Bob pilot symbols prior to data transmission. Using these symbols, Bob determines the CSI of the main channel and

determines ξ_1 and ξ_2 according to (6.1) and (6.2), respectively. After this, Bob feeds back ξ_1 and ξ_2 to Alice via a low-rate feedback channel. As such, TAS-Alamouti reduces the feedback overhead compared with beamforming, since only $\left\lceil \log_2 \frac{N_A(N_A-1)}{2} \right\rceil$ bits are required to feed back the antenna indices. Comparing with single TAS, TAS-Alamouti requires $\left(\left\lceil \log_2 \frac{N_A(N_A-1)}{2} \right\rceil - \lceil \log_2 N_A \rceil \right)$ extra feedback bits. For example, when $N_A = 3$ TAS-Alamouti requires no extra feedback bit. For $4 \leq N_A \leq 6$, TAS-Alamouti requires only one extra feedback bit. We note that the antenna indices ξ_1 and ξ_2 are entirely dependent on the main channel. Due to the independence of the main channel and the eavesdropper's channel, it follows that our proposed TAS-Alamouti scheme improves the quality of main channel relative to the eavesdropper's channel, which in turn promotes the secrecy of the MIMO wiretap channel.

6.2.2 Alamouti Coding

In the second step, Alice adopts Alamouti coding to perform secret transmission. During the transmission, Alice allocates a percentage α of its total transmit power to the first strongest antenna, and allocates a percentage β of its total transmit power to the second strongest antenna. Due to the total power constraint, we have $\beta = 1 - \alpha$.

As per the rules of Alamouti coding, the $N_B \times 1$ received signal vectors at Bob in the first and second time slots are given by

$$\boldsymbol{y}_B(1) = \left[\sqrt{\alpha} \boldsymbol{f}_{\xi_1}, \sqrt{\beta} \boldsymbol{f}_{\xi_2} \right] \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} + \boldsymbol{n}(1), \tag{6.3}$$

and

$$\boldsymbol{y}_B(2) = \left[\sqrt{\alpha} \boldsymbol{f}_{\xi_1}, \sqrt{\beta} \boldsymbol{f}_{\xi_2} \right] \begin{bmatrix} -x_2^\dagger \\ x_1^\dagger \end{bmatrix} + \boldsymbol{n}(2), \tag{6.4}$$

respectively, where $[\boldsymbol{f}_{\xi_1}, \boldsymbol{f}_{\xi_2}]$ is the $N_B \times 2$ main channel matrix after TAS, $[x_1, x_2]^T$ is the transmit signal vector in the first time slot, $[-x_2^\dagger, x_1^\dagger]^T$ is the transmit signal vector in the second time slot, $\boldsymbol{n}$ is the zero-mean circularly symmetric complex Gaussian

noise vector satisfying $\mathbb{E}[\boldsymbol{n}\boldsymbol{n}^{\dagger}] = \boldsymbol{I}_{N_B}\sigma_{AB}^2$, σ_{AB}^2 is the noise variance for each receive antenna at Bob. Under the power constraint, we have $\mathbb{E}[|x_1|^2] = \mathbb{E}[|x_2|^2] = P_A$, where P_A is the total transmit power at Alice.

By performing MRC and space-time signal processing, the signals containing x_1 and x_2 at Bob can be expressed as

$$y_B(x_1) = \left(\alpha \boldsymbol{f}_{\xi_1}^{\dagger}\boldsymbol{f}_{\xi_1} + \beta \boldsymbol{f}_{\xi_2}^{\dagger}\boldsymbol{f}_{\xi_2}\right) x_1 + \sqrt{\alpha}\boldsymbol{f}_{\xi_1}^{\dagger}\boldsymbol{n}(1) + \sqrt{\beta}\boldsymbol{n}(2)^{\dagger}\boldsymbol{f}_{\xi_2}, \tag{6.5}$$

and

$$y_B(x_2) = \left(\alpha \boldsymbol{f}_{\xi_1}^{\dagger}\boldsymbol{f}_{\xi_1} + \beta \boldsymbol{f}_{\xi_2}^{\dagger}\boldsymbol{f}_{\xi_2}\right) x_2 + \sqrt{\alpha}\boldsymbol{f}_{\xi_2}^{\dagger}\boldsymbol{n}(1) - \sqrt{\beta}\boldsymbol{n}(2)^{\dagger}\boldsymbol{f}_{\xi_1}, \tag{6.6}$$

respectively. The instantaneous SNR at Bob is written as

$$\gamma_B = \frac{(\alpha\|\boldsymbol{f}_{\xi_1}\|^2 + \beta\|\boldsymbol{f}_{\xi_2}\|^2)P_A}{\sigma_{AB}^2}. \tag{6.7}$$

Likewise, the instantaneous SNR at Eve is written as

$$\gamma_E = \frac{(\alpha\|\boldsymbol{g}_{\xi_1}\|^2 + \beta\|\boldsymbol{g}_{\xi_2}\|^2)P_A}{\sigma_{AE}^2}, \tag{6.8}$$

where $[\boldsymbol{g}_{\xi_1}, \boldsymbol{g}_{\xi_2}]$ is the $N_E \times 2$ eavesdropper's channel matrix after TAS, σ_{AE}^2 is the noise variance for each receive antenna at Eve, and $\boldsymbol{g}_{\xi} = [g_{\xi,1}, g_{\xi,2}, ..., g_{\xi,N_E}]^T$ denotes the $N_E \times 1$ channel vector between the ξ-th antenna at Alice and the N_E antennas at Eve with i.i.d. Rayleigh fading entries. In the following two sections, we assume equal power allocation to the selected antennas, i.e., $\alpha = \beta = 0.5$ (optimal power allocation is discussed in Section 6.5).

6.3 Secrecy Performance of TAS-Alamouti

In this section, we quantify the secrecy performance of the proposed TAS-Alamouti scheme. Specifically, we derive a closed-form expression for the secrecy outage probability. Based on the secrecy outage probability, we present the probability of non-zero secrecy capacity and numerically determine the ε-outage secrecy capacity. In addition,

we derive a more compact closed-form expression for the secrecy outage probability as $\overline{\gamma}_B$ approaches high values. This expression determines the secrecy diversity order and the secrecy array gain.

6.3.1 Secrecy Outage Probability

The secrecy outage probability is defined as the probability of the secrecy capacity C_s being less than a specific transmission rate R_s (bits/channel-use) [63]. According to the definition, the secrecy outage probability is formulated as

$$P_{out}\left(R_s\right) = \Pr\left(C_s < R_s\right). \tag{6.9}$$

We commence our analysis by presenting the pdf of γ_B, $f_{\gamma_B}\left(\gamma_B\right)$, and the pdf of γ_E, $f_{\gamma_E}\left(\gamma_E\right)$. Specifically, we adopt [123, Eq. (15)] with $L_t = N_A$ and $L_r = N_B$ as $f_{\gamma_B}\left(\gamma_B\right)$ for TAS-Alamouti, and define $\overline{\gamma}_B = \mathbb{E}[\gamma_B]/N_B$. We then adopt [123, Eq. (15)] with $L_t = 2$ and $L_r = N_E$ as $f_{\gamma_E}\left(\gamma_E\right)$, and define $\overline{\gamma}_E = \mathbb{E}[\gamma_E]/N_E$. The derived expression for the secrecy outage probability is presented in the following theorem.

***Theorem* 10** The secrecy outage probability of the TAS-Alamouti scheme is

$$P_{out}(R_s) = 1 - \frac{N_A(N_A-1)\left[A_1 - A_2 + A_3 - A_4\right]}{\left[(N_B-1)!\,(N_E-1)!\right]^2}, \tag{6.10}$$

where

$$A_1 = -\mathbb{S}_i\mathbb{S}_j\mathbb{S}_t\mathbb{S}_m\mathbb{S}_k\mathbb{S}_u e_1 \varphi_0^{\omega_1}\left(\frac{\overline{\gamma}_E}{2}\right)^u \left[\frac{\mathbb{S}_n\mathbf{F}(\eta_1,1,\lambda_1,\varphi_1)}{2^{N_E-m-2}} + \frac{\mathbb{S}_q\mathbf{F}(\eta_2,1,\lambda_2,\varphi_1)}{2^{N_E+q-1}(N_E+q)}\right], \tag{6.11}$$

$$A_2 = \mathbb{S}_j\mathbb{S}_m\mathbb{S}_p\bar{\mathbb{S}}_u e_2 \varphi_0^{2N_B-j-1}\frac{2^{N_B-j-p-u}\overline{\gamma}_E^u}{N_B+p}\left[\frac{\mathbb{S}_n\mathbf{F}(\eta_1,1,\lambda_1,\varphi_2)}{2^{N_E-m-1}} + \frac{\mathbb{S}_q\mathbf{F}(\eta_2,1,\lambda_2,\varphi_2)}{2^{N_E+q}(N_E+q)}\right], \tag{6.12}$$

$$A_3 = \bar{\mathbb{S}}_i\mathbb{S}_j\mathbb{S}_t\mathbb{S}_m\bar{\mathbb{S}}_k\mathbb{S}_u e_1 \varphi_0^{\omega_1}\frac{2^{\omega_1-\omega_2}\overline{\gamma}_E^u}{\imath^{k+1}}\left[\frac{\mathbb{S}_n\mathbf{F}(\eta_1,1,\lambda_1,\varphi_1)}{2^{N_E-m-2}} + \frac{\mathbb{S}_q\mathbf{F}(\eta_2,1,\lambda_2,\varphi_1)}{2^{N_E+q-1}(N_E+q)}\right], \tag{6.13}$$

$$A_4 = -\bar{\mathbb{S}}_i\mathbb{S}_j\mathbb{S}_t\mathbb{S}_m\mathbb{S}_p\hat{\mathbb{S}}_u\rho e_2 \varphi_0^{\omega_3}\frac{2^{\omega_3-u}\overline{\gamma}_E^u}{\imath^{N_B+p+t}}\left[\frac{\mathbb{S}_n\mathbf{F}(\eta_1,1,\lambda_1,\varphi_2)}{2^{N_E-m-2}} + \frac{\mathbb{S}_q\mathbf{F}(\eta_2,1,\lambda_2,\varphi_2)}{2^{N_E+q-1}(N_E+q)}\right]. \tag{6.14}$$

In A_1, A_2, A_3 and A_4, we define the symbols used as

$$\mathbb{S}_i \equiv \sum_{i=0}^{N_A-2} (-1)^i \binom{N_A-2}{i}, \tag{6.15}$$

$$\mathbb{S}_j \equiv \sum_{j=0}^{N_B-1} j! \binom{N_B-1}{j}, \tag{6.16}$$

$$\mathbb{S}_t \equiv \sum_{t=0}^{(N_B-1)i} a_t(N_B, i), \tag{6.17}$$

$$\mathbb{S}_m \equiv \sum_{m=0}^{N_E-1} m! \binom{N_E-1}{m}, \tag{6.18}$$

$$\mathbb{S}_k \equiv \sum_{k=0}^{2N_B+t-j-2} \frac{k! \binom{2N_B+t-j-2}{k}}{(i+2)^{k+1}}, \tag{6.19}$$

$$\mathbb{S}_u \equiv \sum_{u=0}^{2N_B+t-j-k-2} \frac{\binom{2N_B+t-j-k-2}{u}}{(1-2^{-R_s})^{-(2N_B+t-j-k-u-2)}}, \tag{6.20}$$

$$\mathbb{S}_n \equiv \sum_{n=0}^{2N_E-m-2} n! \binom{2N_E-m-2}{n}, \tag{6.21}$$

$$\mathbb{S}_q \equiv \sum_{q=0}^{N_E-m-1} (-1)^q \binom{N_E-m-1}{q}, \tag{6.22}$$

$$\mathbb{S}_p \equiv \sum_{p=0}^{N_B-j-1} (-1)^p \binom{N_B-j-1}{p}, \tag{6.23}$$

$$\bar{\mathbb{S}}_u \equiv \sum_{u=0}^{2N_B-j-1} \frac{\binom{2N_B-j-1}{u}}{(1-2^{-R_s})^{-(2N_B-j-u-1)}}, \tag{6.24}$$

$$\bar{\mathbb{S}}_i \equiv \sum_{i=1}^{N_A-2} (-1)^i \binom{N_A-2}{i}, \tag{6.25}$$

$$\bar{\mathbb{S}}_k \equiv \sum_{k=0}^{N_B+t+p-1} k! \binom{N_B+t+p-1}{k}, \tag{6.26}$$

$$\hat{\mathbb{S}}_u \equiv \sum_{u=0}^{N_B-j-p-1} \frac{\binom{N_B-j-p-1}{u}}{(1-2^{-R_s})^{-(N_B-j-p-u-1)}}, \tag{6.27}$$

where $a_t(N_B, i)$ in $\mathbb{S}_t$ is the coefficient of z^t in the expansion of $\left(\sum_{j=0}^{N_B-1} z^j/j!\right)^i$. In A_1, A_2, A_3 and A_4, we define $\omega_1 = 2N_B + t - j - k - 2$, $\omega_2 = N_B + p + t - k - 1$, $\omega_3 = \omega_1 - \omega_2$, $\lambda_1 = 2N_E + u - m - n - 3$, $\lambda_2 = 2N_E + u - m - 2$, $\eta_1 = 2N_E - m - n - 2$,

$\eta_2 = 2N_E - m - 1$, $\varphi_0 = \frac{2^{R_s}}{\overline{\gamma}_B}$, $\varphi_1 = \frac{\overline{\gamma}_B + 2^{R_s-1}(i+2)\overline{\gamma}_E}{\overline{\gamma}_B}$, $\varphi_2 = \frac{\overline{\gamma}_B + 2^{R_s}\overline{\gamma}_E}{\overline{\gamma}_B}$, $e_1 = e^{-\frac{(i+2)(2^{R_s}-1)}{\overline{\gamma}_B}}$, $e_2 = e^{-\frac{(2^{R_s+1}-2)}{\overline{\gamma}_B}}$, $\rho = (N_B + t + p - 1)!$, and

$$\mathbf{F}(\eta, \tau, \lambda, \varphi) = \eta \mathbf{W}(\lambda, \varphi) - \tau \mathbf{W}(\lambda + 1, \varphi), \tag{6.28}$$

where $\mathbf{W}(r, \varphi)$, $r \in \{\lambda, \lambda + 1\}$, is defined as

$$\mathbf{W}(r, \varphi) = \int_0^\infty x^r e^{-\varphi x} dx = \begin{cases} r! \varphi^{-r-1}, & \text{if } r = 0, 1, 2, ... \\ 0, & \text{if } r = -1. \end{cases} \tag{6.29}$$

We now prove Theorem 10. Based on the definition of the secrecy outage probability, $P_{out}(R_s)$ can be rewritten as

$$P_{out}(R_s) = \underbrace{\Pr(C_s < R_s | \gamma_B > \gamma_E) \Pr(\gamma_B > \gamma_E)}_{V_1} + \underbrace{\Pr(\gamma_B < \gamma_E)}_{V_2}, \tag{6.30}$$

where V_1 is

$$\begin{aligned} V_1 &= \int_0^\infty \int_{\gamma_E}^{2^{R_s}(1+\gamma_E)-1} f_{\gamma_E}(\gamma_E) f_{\gamma_B}(\gamma_B) d\gamma_B d\gamma_E \\ &= \underbrace{\int_0^\infty f_{\gamma_E}(\gamma_E) \left[\int_0^{2^{R_s}(1+\gamma_E)-1} f_{\gamma_B}(\gamma_B) d\gamma_B \right] d\gamma_E}_{U_1} \\ &\quad - \underbrace{\int_0^\infty f_{\gamma_E}(\gamma_E) \left[\int_0^{\gamma_E} f_{\gamma_B}(\gamma_B) d\gamma_B \right] d\gamma_E}_{U_2}. \end{aligned} \tag{6.31}$$

We note that $V_2 = \int_0^\infty \int_0^{\gamma_E} f_{\gamma_E}(\gamma_E) f_{\gamma_B}(\gamma_B) d\gamma_B d\gamma_E = U_2$. As such, $P_{out}(R_s) = U_1$. To calculate the integrations in U_1, we first substitute $f_{\gamma_B}(\gamma_B)$ into U_1 and solve the inner integral with the aid of [124, Eq. (3.351.1)]. We then substitute $f_{\gamma_E}(\gamma_E)$ into U_1 and solve the resultant integral with the aid of [124, Eq. (3.351.3)]. By performing some algebraic manipulations, the secrecy outage probability is derived as in (6.10). This completes the proof of Theorem 10.

It is highlighted that our new expression in (6.10) is in closed form as it involves finite summations of exponential and power functions only. Again, we note that (6.10)

is only valid for $\alpha = 0.5$. The probability of non-zero secrecy capacity is defined as the probability that the secrecy capacity is larger than zero. We present the probability of non-zero secrecy capacity of TAS-Alamouti in the following corollary.

***Corollary* 7** The probability of non-zero secrecy capacity of TAS-Alamouti is

$$P_{non} = \Pr\left(C_s > 0\right) = \Pr\left(\gamma_B > \gamma_E\right). \tag{6.32}$$

Using our expression for the secrecy outage probability, the probability of non-zero secrecy capacity is obtained as $P_{non} = 1 - P_{out}\left(0\right)$.

The ε-outage secrecy capacity is defined as the maximum secrecy rate at which the secrecy outage probability is no larger than ε. Specifically, the ε-outage secrecy capacity of TAS-Alamouti is given in the following corollary.

***Corollary* 8** The ε-outage secrecy capacity of TAS-Alamouti is given by

$$C_{out}\left(\varepsilon\right) = \underset{P_{out}(R_s)\leq\varepsilon}{\operatorname{argmax}}\ R_s. \tag{6.33}$$

Using the closed-form expression for $P_{out}\left(R_s\right)$ in (6.10), we can find $C_{out}\left(\varepsilon\right)$ numerically.

6.3.2 Asymptotic Secrecy Outage Probability

We now derive a simpler expression for the secrecy outage probability in the asymptotic limit $\overline{\gamma}_B \to \infty$. To this end, we present the following theorem.

***Theorem* 11** As $\overline{\gamma}_B \to \infty$, $P_{out}(R_s) \to P_{out}^{\infty}(R_s)$, where the asymptotic secrecy outage probability $P_{out}^{\infty}(R_s)$ is

$$P_{out}^{\infty}(R_s) = \left(\Psi\overline{\gamma}_B\right)^{-\Phi} + o\left(\overline{\gamma}_B^{-\Phi}\right), \tag{6.34}$$

where $\Phi = N_A N_B$,

$$\Psi = \Bigg\{ \frac{\mathbb{C}(N_A, N_B)}{(2^{R_s+1}-2)^{-N_A N_B}} + \frac{\mathbb{C}(N_A, N_B)\mathbb{S}_m}{[(N_E-1)!]^2 \left(2^{R_s}\overline{\gamma}_E\right)^{-N_A N_B}} \times \sum_{k=1}^{N_A N_B} k \binom{N_A N_B}{k} \left(\frac{2-2^{1-R_s}}{\overline{\gamma}_E}\right)^{N_A N_B - k} \times \left[\frac{\mathbb{S}_n(\eta_1+k-1)!}{2^{2N_E-m-2}} + \frac{\mathbb{S}_q(\eta_2+k-1)!}{2^{N_E+q-1}(N_E+q)}\right] \Bigg\}^{-\frac{1}{N_A N_B}}, \tag{6.35}$$

and $o(\cdot)$ denotes the higher order terms.

To derive $P_{out}^{\infty}(R_s)$, we need to determine the cumulative distribution function (cdf) of γ_B, $F_{\gamma_B}(\gamma_B)$, which is a function of $\overline{\gamma}_B$. In this function, we expand the exponential function using $e^{-x} = \sum_{k=0}^{\infty}(-x)^k/k!$. If we take the limit $\overline{\gamma}_B \to \infty$, we keep the first non-zero order term in the expansion and ignore the higher order terms. This results in

$$F_{\gamma_B}^{\infty}(\gamma_B) = \mathbb{C}(N_A, N_B) \left(\frac{2\gamma_B}{\overline{\gamma}_B}\right)^{N_A N_B}, \tag{6.36}$$

where $\mathbb{C}(N_A, N_B)$ is given by

$$\begin{aligned} \mathbb{C}(N_A, N_B) = \frac{N_A(N_A-1)}{[(N_B-1)!]^2} \times & \\ \Bigg[-\mathbb{S}_i\mathbb{S}_j\mathbb{S}_t \frac{(-1)^{N_A N_B}(i+2)^{N_A N_B} 2^{-N_A N_B - 2N_B - t + j + k + 2}}{(N_A N_B - 2N_B - t + j + k + 2)!} & \\ -\mathbb{S}_j\mathbb{S}_p \frac{(-1)^{N_A N_B} 2^{-N_B - p}(N_B+p)^{-1}}{(N_A N_B - 2N_B + j + 1)!} & \\ +\bar{\mathbb{S}}_i\mathbb{S}_j\mathbb{S}_t\mathbb{S}_p \frac{(-1)^{N_A N_B}(i+2)^{N_A N_B} 2^{-N_A N_B - N_B - t - p + k + 1}}{i^{k+1}(N_A N_B - 2N_B - t + j + k + 2)!} & \\ -\bar{\mathbb{S}}_i\mathbb{S}_j\mathbb{S}_t\mathbb{S}_p\rho \frac{(-1)^{N_A N_B} i^{-N_B - p - t}}{(N_A N_B - N_B + j + p + 1)!} \Bigg]. & \end{aligned} \tag{6.37}$$

We note that $\mathbb{C}(N_A, N_B)$ can be simplified in some special cases. For example, $\mathbb{C}(2, N_B) = 1/[2N_B(2N_B-1)!]$ and $\mathbb{C}(N_A, 1) = 1/2^{N_A-1}$. Using (6.30) and (6.31), we then find that

$$P_{out}^{\infty}(R_s) = \int_0^{\infty} f_{\gamma_E}(\gamma_E) F_{\gamma_B}^{\infty}\left(2^{R_s}(1+\gamma_E)-1\right) d\gamma_E. \tag{6.38}$$

We substitute (6.36) into (6.38), and then rewrite the product of $F_{\gamma_B}^{\infty}\left(2^{R_s}(1+\gamma_E)-1\right)$ and $f_{\gamma_E}(\gamma_E)$ with the aid of [124, Eq.(1.111)]. Finally, the resultant integral with respect to γ_E is solved with the aid of [124, Eq.(3.351.3)], which leads to the desired asymptotic secrecy outage probability in (6.34). This proves Theorem 11.

We refer to Φ as the secrecy diversity order, and Ψ as the secrecy array gain of TAS-Alamouti. We observe that the secrecy diversity order of TAS-Alamouti is the same as that of single TAS, which is $N_A N_B$ [59]. Furthermore, we later show that the TAS-Alamouti scheme achieves a higher secrecy array gain than single TAS.

6.4 Comparison between TAS-Alamouti and single TAS

In this section, we conduct a thorough performance comparison between the proposed TAS-Alamouti scheme and the single TAS scheme proposed in [59]. Moreover, we present numerical results to examine the impact of the number of antennas (N_A, N_B, and N_E) and the average SNRs on the secrecy performance of TAS-Alamouti. This comparison highlights the superiority of TAS-Alamouti relative to single TAS.

6.4.1 Secrecy Outage Probability

We first examine the impact of N_A on the secrecy outage probability. Fig. 6.2 plots the secrecy outage probability versus $\overline{\gamma}_B$ for different values of N_A. In this figure, $P_{out}(R_s)$ and $P_{out}^{\infty}(R_s)$ of TAS-Alamouti are generated from (6.10) and (6.34), respectively. The secrecy outage probability of single TAS, $P_{out}^{s}(R_s)$, and the asymptotic secrecy outage probability of single TAS, $P_{out}^{s,\infty}(R_s)$, are generated from [59, Eq. (13)] and [59, Eq. (18)], respectively. We first observe that $P_{out}(R_s)$ of TAS-Alamouti matches precisely with Monte Carlo simulations. This demonstrates the correctness of our analysis. Monte Carlo simulations are omitted in other figures to avoid cluttering. We further observe that $P_{out}^{\infty}(R_s)$ approaches $P_{out}(R_s)$ as $\overline{\gamma}_B$ increases, which verifies our

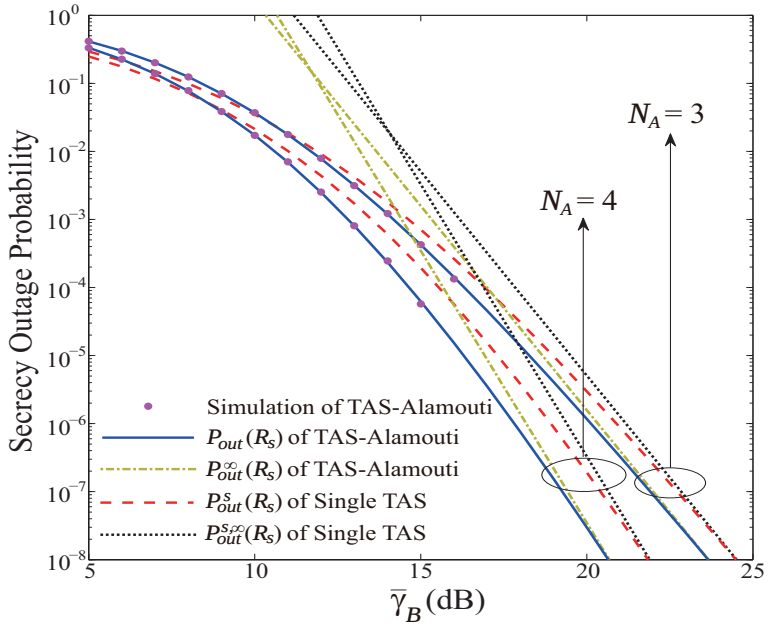

Figure 6.2: Secrecy outage probability versus $\overline{\gamma}_B$ for $R_s = 1$, $\overline{\gamma}_E = 5$ dB, $N_B = 2$, and $N_E = 1$.

asymptotic analysis. In Fig. 6.2, we also observe that $P_{out}(R_s)$ significantly decreases as N_A increases. This can be explained by the fact that N_A increases the secrecy diversity order of TAS-Alamouti via $N_A N_B$. We note the asymptotic curves of single TAS and TAS-Alamouti are parallel, which confirms that the diversity order of the two schemes is the same. We observe that TAS-Alamouti has an SNR gain relative to single TAS at the same secrecy outage probability. This SNR gain is due to the fact that TAS-Alamouti has a higher secrecy array gain than single TAS. Notably, this SNR gain increases with N_A. We further observe that the *crossover point*, at which TAS-Alamouti and single TAS achieve the same secrecy outage probability, moves to a lower $\overline{\gamma}_B$ when N_A increases. Both of these observations demonstrate that the advantage of TAS-Alamouti over single TAS increases as N_A increases.

From Fig. 6.2, we observe that TAS-Alamouti achieves a lower secrecy outage probability than single TAS when $\overline{\gamma}_B > 11$ dB for $N_A = 3$. We note that it is a general result that TAS-Alamouti outperforms single TAS when $\overline{\gamma}_B$ is larger than some specific value. This general result is different from the comparison between TAS-

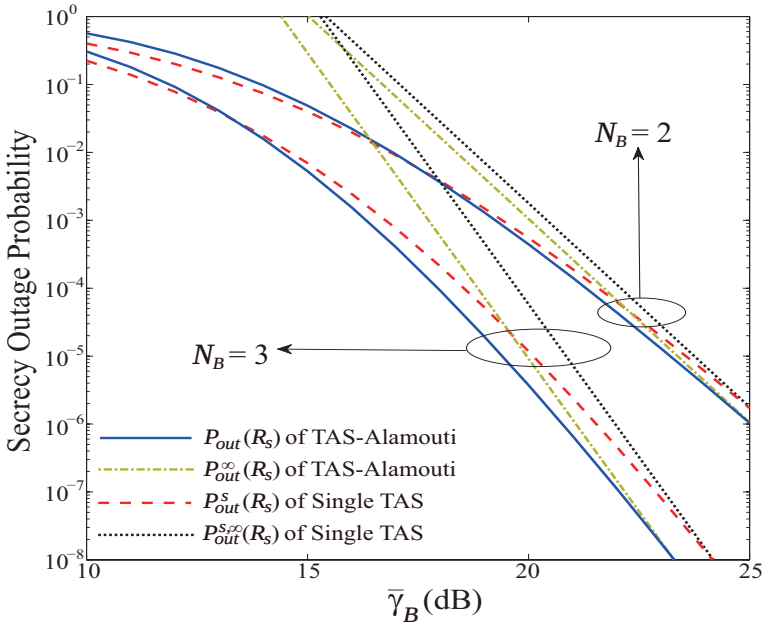

Figure 6.3: Secrecy outage probability versus $\overline{\gamma}_B$ for $R_s = 1$, $\overline{\gamma}_E = 5$ dB, $N_A = 3$, and $N_E = 2$.

Alamouti and single TAS in non-secrecy MIMO systems [123] where the performance of TAS-Alamouti is always worse than that of single TAS, which is due to the fact that the transmitter wastes some transmit power on the second strongest antenna in TAS-Alamouti. However, in MIMO wiretap channels there is a potential advantage in selecting two antennas at Alice. This is because that Eve's probability of countering the fading (matching the SNR at Bob) decreases as the number of selected antennas at Alice increases.

We next examine the impact of N_B on the secrecy outage probability. Fig. 6.3 plots the secrecy outage probability versus $\overline{\gamma}_B$ for different values of N_B. In this figure, we observe that $P_{out}(R_s)$ decreases as N_B increases, which is explained by the fact that N_B increases the secrecy diversity order via $N_A N_B$. We also observe that the SNR gain of TAS-Alamouti relative to single TAS increases with N_B. We further observe that the crossover point moves to a lower $\overline{\gamma}_B$ when N_B increases. These observations demonstrate that the advantage of TAS-Alamouti over single TAS increases as N_B increases.

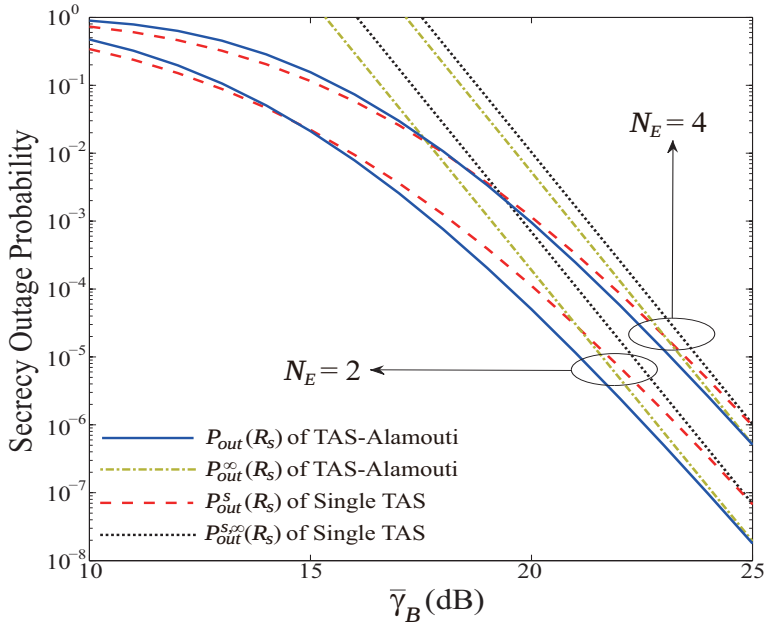

Figure 6.4: Secrecy outage probability versus $\overline{\gamma}_B$ for $R_s = 1$, $\overline{\gamma}_E =$ 5 dB, $N_A = 4$, and $N_B = 2$.

We now examine the impact of N_E on the secrecy outage probability. Fig. 6.4 plots the secrecy outage probability versus $\overline{\gamma}_B$ for different values of N_E. As expected, we observe that $P_{out}(R_s)$ increases as N_E increases. We note that the asymptotic curves of TAS-Alamouti for different values of N_E are parallel, which confirms that the diversity order is not affected by N_E. We also observe that the SNR gain of TAS-Alamouti relative to single TAS decreases as N_E increases. We further observe that the crossover point moves to a higher $\overline{\gamma}_B$ when N_E increases. These observations demonstrate that the advantage of TAS-Alamouti over single TAS decreases as N_E increases.

6.4.2 Probability of Non-Zero Secrecy Capacity

Fig. 6.5 plots the probability of non-zero secrecy capacity versus $\overline{\gamma}_B$ for different values of $\overline{\gamma}_E$. In this figure, P_{non} of TAS-Alamouti is generated from (6.32), and the probability of non-zero secrecy capacity of single TAS, P^{s}_{non}, is generated from [59, Eq.

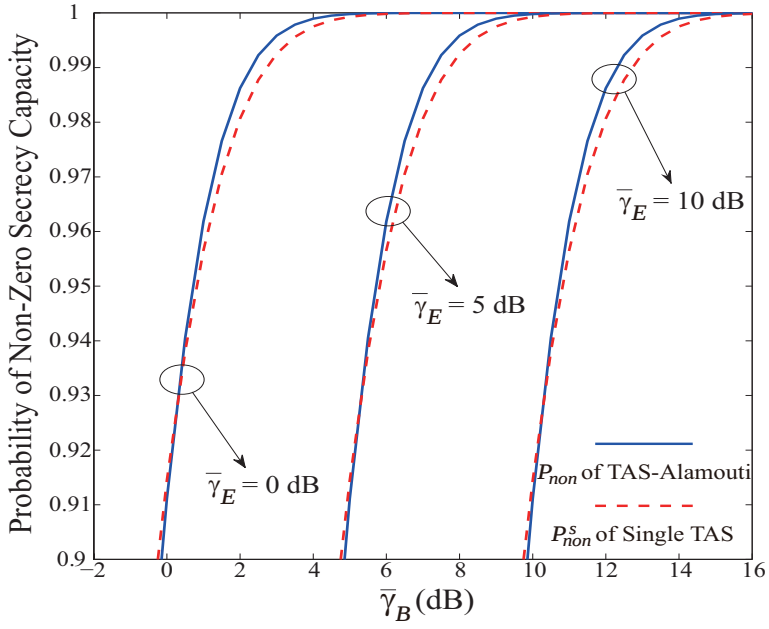

Figure 6.5: The probability of non-zero secrecy capacity versus $\overline{\gamma}_B$ for $N_A = 4$, $N_B = 3$, and $N_E = 2$.

(29)]. From Fig. 6.5, we observe that P_{non} of TAS-Alamouti is higher than that of single TAS when $\overline{\gamma}_B$ is larger than some specific value. We also observe that the crossover point moves to a higher $\overline{\gamma}_B$ when $\overline{\gamma}_E$ increases. This demonstrates that the advantage of TAS-Alamouti over single TAS increases as $\overline{\gamma}_E$ decreases.

6.4.3 ε-outage Secrecy Capacity

Fig. 6.6 plots the ε-outage secrecy capacity versus N_A for different values of N_E. In this figure, $C_{out}(\varepsilon)$ of TAS-Alamouti is generated from (6.33) and the ε-outage secrecy capacity of single TAS, $C^s_{out}(\varepsilon)$, is generated from [59, Eq. (31)]. From this figure, we observe that $C_{out}(\varepsilon)$ increases with N_A but decreases with N_E. We also observe that TAS-Alamouti achieves a higher ε-outage secrecy capacity than single TAS when N_A is larger than some specific value. Notably, the ε-outage secrecy capacity advantage of TAS-Alamouti over single TAS increases with N_A but decreases with N_E.

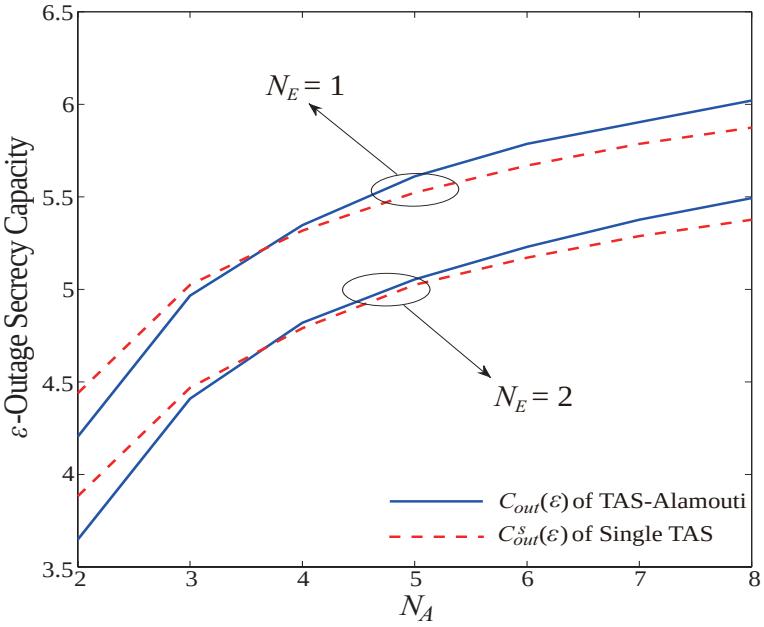

Figure 6.6: The ε-outage secrecy capacity versus N_A for $\varepsilon = 0.01$, $\overline{\gamma}_B = 20$ dB, $\overline{\gamma}_E = 0$ dB, and $N_B = 2$.

6.5 Secrecy Performance of TAS-Alamouti-OPA

In this section, we optimize power allocation for the TAS-Alamouti scheme. To this end, we derive a closed-form expression for the secrecy outage probability of TAS-Alamouti with general power allocation, i.e., $0.5 \leq \alpha \leq 1$. Based on this expression, we determine the optimal power allocation for TAS-Alamouti and obtain the secrecy performance of TAS-Alamouti-OPA. In TAS-Alamouti-OPA, the optimal α that minimizes the secrecy outage probability is determined at Alice based on the knowledge of $\overline{\gamma}_B$ and $\overline{\gamma}_E$. In order to determine the optimal α, Alice requires to know her strongest and second strongest antennas. This is different from TAS-Alamouti in which Alice only requires to know her two strongest antennas, but does not need to know which of these two is the strongest. As such, TAS-Alamouti-OPA requires one extra feedback bit relative to TAS-Alamouti. Other than this small change in the feedback overhead, the steps of TAS-Alamouti-OPA are the same as those outlined in Section 6.2.

6.5.1 Secrecy Outage Probability of TAS-Alaouti with PA

We note that when $\alpha = 0.5$, the secrecy outage probability of TAS-Alamouti, $P_{out}(R_s)$, is derived in (6.10). As such, we focus on $0.5 < \alpha \leq 1$ and commence our analysis by deriving the pdfs of γ_B and γ_E.

We first derive the pdf of γ_B, $f^{\alpha}_{\gamma_B}(\gamma_B)$. Recall that $\|\boldsymbol{f}_{\xi}\|^2$ is a chi-squared variable with $2N_B$ degrees of freedom. Denoting $\chi\|\boldsymbol{f}_{\xi_\varrho}\|^2$ as Y_ϱ, $(\chi, \varrho) \in \{(\alpha, 1), (\beta, 2)\}$, the cdf and pdf of Y_ϱ are given by [125]

$$F_{Y_\varrho}(y_\varrho) = 1 - e^{-\frac{y_\varrho}{\chi}} \sum_{k=0}^{N_B-1} \frac{y_\varrho^k}{\chi^k k!}, \tag{6.39}$$

and

$$f_{Y_\varrho}(y_\varrho) = \frac{1}{\chi(N_B-1)!} \left(\frac{y_\varrho}{\chi}\right)^{N_B-1} e^{-\frac{y_\varrho}{\chi}}, \tag{6.40}$$

respectively. We note that γ_B in (6.7) can be expressed as $\gamma_B = \overline{\gamma}_B(Y_1 + Y_2)$. The joint pdf of Y_1 and Y_2 can be written as [126]

$$\begin{aligned} f_{Y_1Y_2}(y_1, y_2) &= \frac{N_A!}{(N_A-2)!} \left[F_{Y_2}(y_2)\right]^{N_A-2} f_{Y_1}(y_1) f_{Y_2}(y_2) \\ &= \frac{N_A(N_A-1)}{\alpha\beta[(N_B-1)!]^2} \sum_{i=0}^{N_A-2} (-1)^i \binom{N_A-2}{i} \sum_{t=0}^{(N_B-1)i} a_t(N_B, i) \\ &\quad \times \left(\frac{y_1}{\alpha}\right)^{N_B-1} e^{-\frac{y_1}{\alpha}} \left(\frac{y_2}{\beta}\right)^{N_B+t-1} e^{-(1+i)\frac{y_2}{\beta}}. \end{aligned} \tag{6.41}$$

As such, the cdf of γ_B can be expressed as

$$\begin{aligned} F^{\alpha}_{\gamma_B}(\gamma_B) &= \Pr\left(\overline{\gamma}_B(Y_0 + Y_1) \leq \gamma_B\right) \\ &= \int_0^{\frac{\beta\gamma_B}{\overline{\gamma}_B}} \int_{\frac{\alpha}{\beta}y_2}^{\frac{\gamma_B}{\overline{\gamma}_B}-y_2} f_{Y_1Y_2}(y_1, y_2) dy_1 dy_2. \end{aligned} \tag{6.42}$$

Substituting (6.41) into (6.42) and solving the resultant integrals, we derive the closed-

form expression for $F^{\alpha}_{\gamma_B}(\gamma_B)$ as

$$F^{\alpha}_{\gamma_B}(\gamma_B) = \frac{N_A(N_A-1)}{[(N_B-1)!]^2}\mathbb{S}_i\mathbb{S}_j\mathbb{S}_t \left\{ \left[\bar{\rho} - \mathbb{S}_k \left(\frac{\gamma_B}{\overline{\gamma}_B}\right)^{\omega_1} e^{-\frac{(i+2)\gamma_B}{\overline{\gamma}_B}} \right] \right.$$
$$-\mathbb{S}_p \left[\rho \frac{\alpha^{N_B+t}\beta^p}{[(1+i)\alpha-\beta]^{N_B+t+p}} \left(\frac{\gamma_B}{\alpha\overline{\gamma}_B}\right)^{\omega_3} e^{-\frac{\gamma_B}{\alpha\overline{\gamma}_B}} \right.$$
$$\left. \left. -\bar{\mathbb{S}}_k \frac{\alpha^{N_B+t}\beta^p}{[(1+i)\alpha-\beta]^{k+1}} \left(\frac{\gamma_B}{\alpha\overline{\gamma}_B}\right)^{\omega_1} e^{-\frac{(i+2)\gamma_B}{\overline{\gamma}_B}} \right] \right\}, \tag{6.43}$$

where $\bar{\rho} = \frac{(2N_B+t-j-2)!}{(i+2)^{2N_B+t-j-1}}$. The pdf of γ_B, $f^{\alpha}_{\gamma_B}(\gamma_B)$, can then be derived.

We next derive the pdf of γ_E, $f^{\alpha}_{\gamma_E}(\gamma_E)$. We denote $\alpha\|\boldsymbol{g}_{\xi_1}\|^2$ and $\beta\|\boldsymbol{g}_{\xi_2}\|^2$ as Z_1 and Z_2, respectively. The cdf and pdf of Z_ϱ are given by [125]

$$F_{Z_\varrho}(z_\varrho) = 1 - e^{-\frac{z_\varrho}{\chi}} \sum_{k=0}^{N_E-1} \frac{z_\varrho^k}{\chi^k k!}, \tag{6.44}$$

and

$$f_{Z_\varrho}(z_\varrho) = \frac{1}{\chi(N_E-1)!}\left(\frac{z_\varrho}{\chi}\right)^{N_E-1} e^{-\frac{z_\varrho}{\chi}}, \tag{6.45}$$

respectively, where $(\chi,\varrho) \in \{(\alpha,1),(\beta,2)\}$. Since Z_1 and Z_2 are independent, the pdf of $\gamma_E = \overline{\gamma}_E(Z_1+Z_2)$ is expressed as

$$f^{\alpha}_{\gamma_E}(\gamma_E) = \int_0^{\frac{\gamma_E}{\overline{\gamma}_E}} f_{Z_1}(\gamma_E - z) f_{Z_2}(z) dz$$
$$= \frac{\bar{\mathbb{S}}_m\hat{\rho}}{\overline{\gamma}_E[(N_E-1)!]^2} \left[\frac{\alpha^{N_E-1}\beta^m}{(\alpha-\beta)^{N_E+m}} \left(\frac{\gamma_E}{\alpha\overline{\gamma}_E}\right)^{N_E-m-1} e^{-\frac{\gamma_E}{\alpha\overline{\gamma}_E}} \right.$$
$$\left. -\frac{\bar{\mathbb{S}}_q\alpha^{m-q}\beta^{N_E-1}}{(\alpha-\beta)^{N_E+m-q}} \left(\frac{\gamma_E}{\beta\overline{\gamma}_E}\right)^{N_E+q-m-1} e^{-\frac{\gamma_E}{\beta\overline{\gamma}_E}} \right], \tag{6.46}$$

where $\hat{\rho} = (N_E+m-1)!$,

$$\bar{\mathbb{S}}_m \equiv \sum_{m=0}^{N_E-1} (-1)^m \binom{N_E-1}{m}, \tag{6.47}$$

and

$$\bar{\mathbb{S}}_q \equiv \sum_{q=0}^{N_E+m-1} \frac{1}{q!}. \tag{6.48}$$

Based on $f^{\alpha}_{\gamma_B}(\gamma_B)$ and $f^{\alpha}_{\gamma_E}(\gamma_E)$, we present the secrecy outage probability of TAS-Alamouti with general power allocation in the following theorem.

***Theorem* 12** The secrecy outage probability of TAS-Alamouti with general power allocation is

$$P'_{out}(R_s) = \begin{cases} P_{out}(R_s), \text{ when } \alpha = 0.5, \\ P^{\alpha}_{out}(R_s), \text{ when } 0.5 < \alpha \leq 1, \end{cases} \tag{6.49}$$

where $P^{\alpha}_{out}(R_s)$ is derived as

$$P^{\alpha}_{out}(R_s) = \frac{N_A(N_A-1)\big[B_1+B_2+B_3+B_4\big]}{[(N_B-1)!]^2[(N_E-1)!]^2}, \tag{6.50}$$

and

$$B_1 = -\mathbb{S}_i\mathbb{S}_j\mathbb{S}_t\bar{\mathbb{S}}_m\mathbb{S}_k\mathbb{S}_u\hat{\rho}e_1\overline{\gamma}_E^u\varphi_0^{\omega_1}\left[\frac{T\alpha^{N_E+u}\beta^m}{(\alpha-\beta)^{N_E+m}\varphi_3^{\omega_4}} - \frac{\bar{\mathbb{S}}_q\bar{T}\alpha^{m-q}\beta^{N_E+u}}{(\alpha-\beta)^{N_E+m-q}\varphi_4^{\omega_4+q}}\right], \tag{6.51}$$

$$B_2 = \mathbb{S}_i\mathbb{S}_j\mathbb{S}_t\bar{\mathbb{S}}_m\bar{\rho}\hat{\rho}\left[\frac{\alpha^{N_E}\beta^m\omega_4!}{(\alpha-\beta)^{N_E+m}} - \frac{\bar{\mathbb{S}}_q\alpha^{m-q}\beta^{N_E}(\omega_4+q)!}{(\alpha-\beta)^{N_E+m-q}}\right], \tag{6.52}$$

$$\begin{aligned} B_3 = {} & \mathbb{S}_i\mathbb{S}_j\mathbb{S}_t\bar{\mathbb{S}}_m\mathbb{S}_p\bar{\mathbb{S}}_k\mathbb{S}_u\hat{\rho}e_1\frac{\alpha^{-N_B+j+k+2}\beta^p\overline{\gamma}_E^u\varphi_0^{\omega_1}}{[(i+2)\alpha-1]^{k+1}} \\ & \times\left[\frac{T\alpha^{N_E+u}\beta^m}{(\alpha-\beta)^{N_E+m}\varphi_3^{\omega_4}} - \frac{\bar{\mathbb{S}}_q\bar{T}\alpha^{m-q}\beta^{N_E+u}}{(\alpha-\beta)^{N_E+m-q}\varphi_4^{\omega_4+q}}\right], \end{aligned} \tag{6.53}$$

$$\begin{aligned} B_4 = {} & -\mathbb{S}_i\mathbb{S}_j\mathbb{S}_t\bar{\mathbb{S}}_m\mathbb{S}_p\hat{\mathbb{S}}_u\rho\hat{\rho}e_\alpha\frac{\alpha^{t+j+p+1}\beta^p\overline{\gamma}_E^u\varphi_0^{\omega_3}}{[(i+2)\alpha-1]^{N_B+t+p}} \\ & \times\left[\frac{T\alpha^{N_E+u}\beta^m}{(\alpha-\beta)^{N_E+m}\varphi_2^{\omega_4}} - \frac{\bar{\mathbb{S}}_q\bar{T}\alpha^{m-q}\beta^{N_E+u}}{(\alpha-\beta)^{N_E+m-q}\varphi_5^{\omega_4+q}}\right]. \end{aligned} \tag{6.54}$$

In B_1, B_2, B_3, and B_4, we define new variables used as $T = (N_E-m+u-1)!$, $\bar{T} = (N_E-m+u+q-1)!$, $\omega_4 = N_E-m+u$, $\omega_5 = N_E-m-1$, $\varphi_3 = \frac{(i+2)2^{R_s}\alpha\overline{\gamma}_E+\overline{\gamma}_B}{\overline{\gamma}_B}$, $\varphi_4 = \frac{(i+2)2^{R_s}\beta\overline{\gamma}_E+\overline{\gamma}_B}{\overline{\gamma}_B}$, $\varphi_5 = \frac{2^{R_s}\beta\overline{\gamma}_E+\alpha\overline{\gamma}_B}{\alpha\overline{\gamma}_B}$, and $e_\alpha = e^{-\frac{2^{R_s}-1}{\alpha\overline{\gamma}_B}}$.

To derive (6.50), we first substitute $f^{\alpha}_{\gamma_B}(\gamma_B)$ and $f^{\alpha}_{\gamma_E}(\gamma_E)$ into U_1 in (6.31). We then solve the resultant integrals with the aid of [124, Eq.(3.351.1)] and [124, Eq.(3.351.3)], which yields the desired result in (6.50).

We highlight that the expression in (6.50) is in closed form as it involves only finite summations of exponential functions and power functions. Again, we note that (6.50) is valid for $\alpha \in (0.5, 1]$, and when $\alpha = 1$ (6.50) reduces to the secrecy outage probability of single TAS, denoted as $P^s_{out}(R_s)$, which was derived in [59, Eq. (13)].

6.5.2 Secrecy Outage Probability of TAS-Alaouti-OPA

Algorithm 6.1 Bisection Algorithm to determine α^*

Input: upper bound and lower bound on α, $P_{out}(R_s)$, $g(\alpha)$

Output: α^*

1: Set the upper bound and lower bound on α as $\alpha_u = 1$ and $\alpha_l = 0.5+\epsilon$, respectively, where ϵ is an arbitrarily small positive quantity. Set the maximum iteration as I_m, and set the minimum step size as δ_m.

2: Estimate the root of $g(\alpha) = 0$, α_m, as the mid-point between α_u and α_l, i.e., $\alpha_m = (\alpha_u + \alpha_l)/2$. Initialize the iteration number as $I = 1$.

3: Check the following conditions to update the upper bound or lower bound. If $g(\alpha_l)g(\alpha_m) < 0$, the root lies between α_l and α_m; then $\alpha_l = \alpha_l$ and $\alpha_u = \alpha_m$. If $g(\alpha_l)g(\alpha_m) > 0$, the root lies between α_m and α_u; then $\alpha_l = \alpha_m$ and $\alpha_u = \alpha_u$. If $g(\alpha_l)g(\alpha_m) = 0$, the root is α_m; then set the temporary optimal value of α as $\alpha_t = \alpha_m$ and skip to step 6.

4: Update the root of $g(\alpha) = 0$ as $\alpha_m^{new} = (\alpha_u + \alpha_l)/2$ and calculate the step size as $\delta = |\alpha_m^{new} - \alpha_m|$. If $\delta \leq \delta_m$, then $\alpha_t = \alpha_m$ and skip to step 6. If $\delta > \delta_m$, then $I = I + 1$.

5: Check the iteration number. If $I < I_m$, then $\alpha_m = \alpha_m^{new}$ and skip to step 3. If $I = I_m$, then $\alpha_t = \alpha_m$ and skip to step 6.

6: Check $P_{out}^{\alpha}(R_s)$ conditioned on $\alpha = \alpha_t$ with $P_{out}(R_s)$. If $P_{out}^{\alpha}(R_s)$ conditioned on $\alpha = \alpha_t$ is larger than or equal to $P_{out}(R_s)$, then $\alpha^* = 0.5$. If $P_{out}^{\alpha}(R_s)$ conditioned on $\alpha = \alpha_t$ is less than $P^{\alpha}(R_s)$, then $\alpha^* = \alpha_t$.

Based on (6.49), the optimal value of α which minimizes $P'_{out}(R_s)$, α^*, is determined by

$$\alpha^* = \underset{0.5\leq\alpha\leq 1}{\operatorname{argmin}} P'_{out}(R_s). \tag{6.55}$$

To search α^*, we first derive $g(\alpha) = \partial P_{out}^{\alpha}(R_s)/\partial\alpha$, and then apply the Algorithm 6.1 to find α^*. Substituting α^* into (6.49), we obtain the secrecy outage probability of

TAS-Alamouti-OPA, denoted as $P^{*}_{out}(R_s)$.

6.6 Numerical and Simulation Results

In this section, we conduct a secrecy performance comparison among single TAS, TAS-Alamouti, TAS-Alamouti-OPA, and the beamforming scheme with all transmit antennas. In addition, we examine the impact of imperfect knowledge of $\overline{\gamma}_E$ and number of antennas (N_A, N_B, and N_E) on the secrecy outage probability.

6.6.1 Comparison Results

Fig. 6.7 plots the secrecy outage probabilities of single TAS, TAS-Alamouti and TAS-Alamouti-OPA. We observe that the analytical curves of TAS-Alamouti-OPA match precisely with the Monte Carlo simulations, which verifies our analysis. We also observe that TAS-Alamouti-OPA always achieves a better secrecy performance than TAS-Alamouti. Moreover, we observe that TAS-Alamouti-OPA always achieves a better secrecy performance than single TAS. Note that as $\overline{\gamma}_B \to 0$, TAS-Alamouti-OPA becomes the same as single TAS.

Fig. 6.8 plots and compares the secrecy outage probability of TAS-Alamouti-OPA with that of beamforming with N_A transmit antennas. In this figure, $P^{b}_{out}(R_s)$ is the secrecy outage probability of beamforming. First, we can see that the beamforming and TAS-Alamouti-OPA achieve the same secrecy diversity order. As expected, we also observe that beamforming outperforms TAS-Alamouti-OPA. This is due to the fact that Alice knows the full CSI of the main channel in beamforming and adopts the maximum ratio transmission (MRT) to maximize the SNR at Bob. We also observe that the gap between TAS-Alamouti-OPA and beamforming increases as N_A increases. The secrecy performance improvement of beamforming relative TAS-Alamouti-OPA comes as the cost of extra feedback bits required by beamforming. Only the indices of the two strongest antennas are fed back from Bob to Alice in

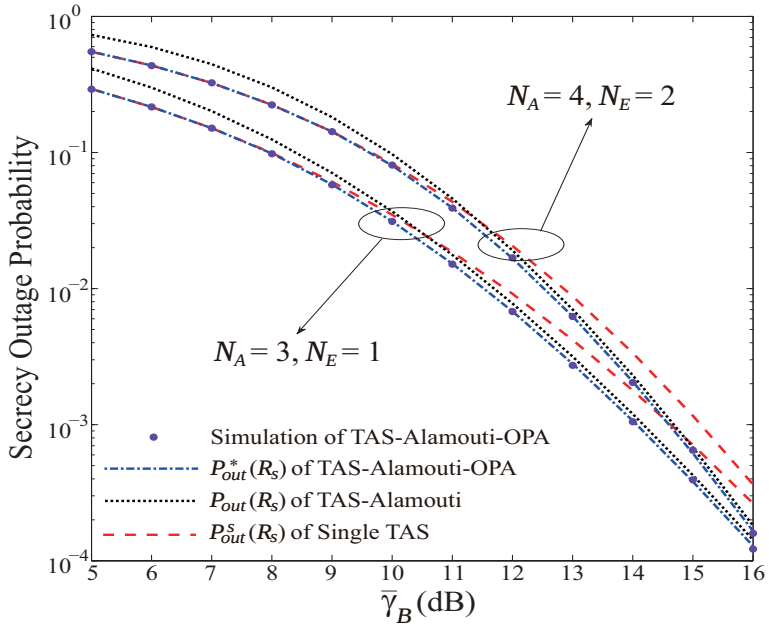

Figure 6.7: Secrecy outage probability versus $\overline{\gamma}_B$ for $R_s = 1$, $\overline{\gamma}_E = 5$ dB, and $N_B = 2$.

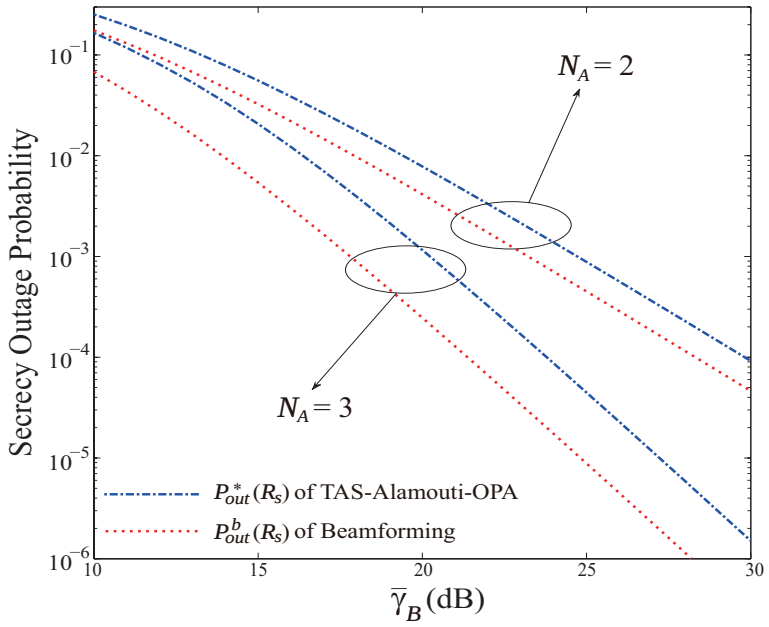

Figure 6.8: Secrecy outage probability versus $\overline{\gamma}_B$ for $R_s = 1$, $\overline{\gamma}_E = 5$ dB, $N_B = 1$, and $N_E = 1$.

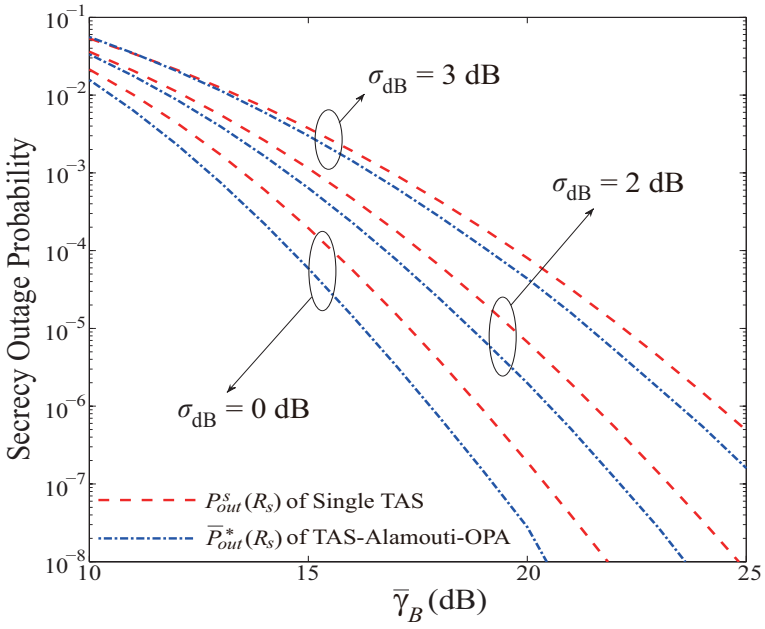

Figure 6.9: Secrecy outage probability versus $\overline{\gamma}_B$ for $R_s = 1$, $\mu_E = 5$ dB, $N_A = 4$, $N_B = 2$, and $N_E = 1$.

TAS-Alamouti-OPA, but an $N_B \times N_A$ complex matrix need to be quantified and fed back to Alice in beamforming. As such, beamforming incurs a much higher feedback overhead than TAS-Alamouti-OPA.

6.6.2 Impacts on Secrecy Outage Probability

In order to examine the impact of imperfect knowledge of $\overline{\gamma}_E$ on the secrecy outage probability, we assume that $\overline{\gamma}_E$ follows a log-normal distribution, i.e., $\overline{\gamma}_E \sim \mathcal{N}(\mu_E, \sigma^2_{dB})$, where μ_E is the mean and σ_{dB} is the standard deviation (where $\overline{\gamma}_E$, μ_E, and σ_{dB} are all in dB). The secrecy outage probabilities in Fig. 6.9, $\overline{P}^s_{out}(R_s)$ and $\overline{P}^*_{out}(R_s)$, are calculated using $\overline{P}^s_{out}(R_s) = \mathbb{E}_{\overline{\gamma}_E}[P^s_{out}(R_s)]$ and $\overline{P}^*_{out}(R_s) = \mathbb{E}_{\overline{\gamma}_E}[P^*_{out}(R_s)]$, respectively. In Fig. 6.9, we first observe that $\overline{P}^s_{out}(R_s)$ and $\overline{P}^*_{out}(R_s)$ with imperfect knowledge of $\overline{\gamma}_E$ ($\sigma_{dB} > 0$), are higher than the corresponding values with perfect knowledge of $\overline{\gamma}_E$ ($\sigma_{dB} = 0$). This confirms that imperfect knowledge degrades the secrecy performance. We also observe that $\overline{P}^s_{out}(R_s)$ and $\overline{P}^*_{out}(R_s)$ increase as σ_{dB}

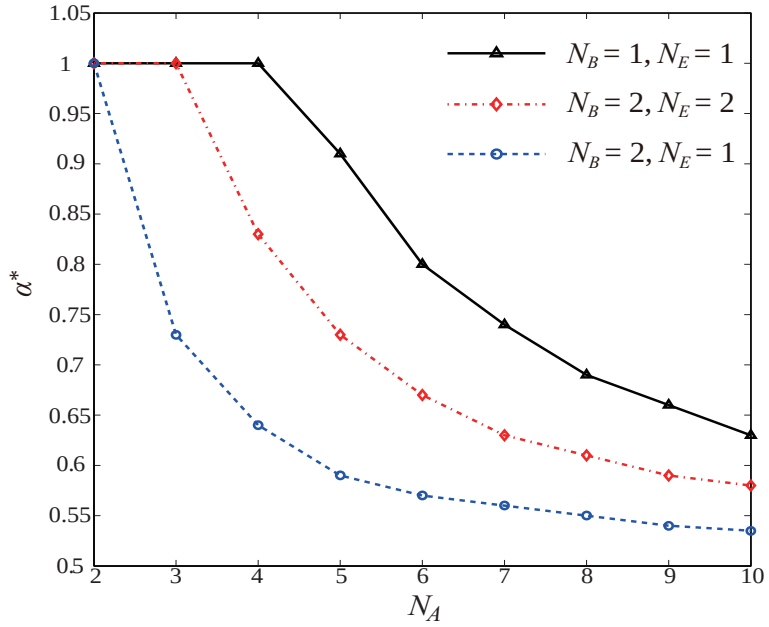

Figure 6.10: The value of α^* versus N_A for $R_s = 1$, $\overline{\gamma}_B = 10$ dB, and $\overline{\gamma}_E = 5$ dB.

increases. This indicates that the poorer the knowledge of $\overline{\gamma}_E$ is, the poorer the secrecy performance is. Furthermore, we observe that the gap between $\overline{P}^s_{out}(R_s)$ and $\overline{P}^*_{out}(R_s)$ decreases as σ_{dB} increases, which indicates that imperfect knowledge of $\overline{\gamma}_E$ degrades the superiority of TAS-Alamouti-OPA over single TAS.

We investigate the impact of the number of antennas (N_A, N_B, and N_E) on α^*. Fig. 6.10 plots α^* versus N_A for different values of N_B and N_E. In this figure, we observe that α^* decreases as N_A increases. This demonstrates that the power allocated to the second strongest antenna increases as N_A increases. As $N_A \to \infty$, $\alpha^* \to 0.5$. This result is expected because when N_A is large, the likelihood that the two selected antennas result in the same instantaneous SNR at Bob is increased.

We present 3D plots to compare the secrecy outage probability of single TAS with that of TAS-Alamouti-OPA in order to examine the joint impact of N_A, N_B, and N_E on the secrecy performance. In Fig. 6.11, Fig. 6.12, and Fig. 6.13, $P^s_{out}(R_s)$ is the secrecy outage probability of single TAS, and $P^*_{out}(R_s)$ is the secrecy outage probability of TAS-Alamouti-OPA. Fig. 6.11 plots the secrecy outage probabilities

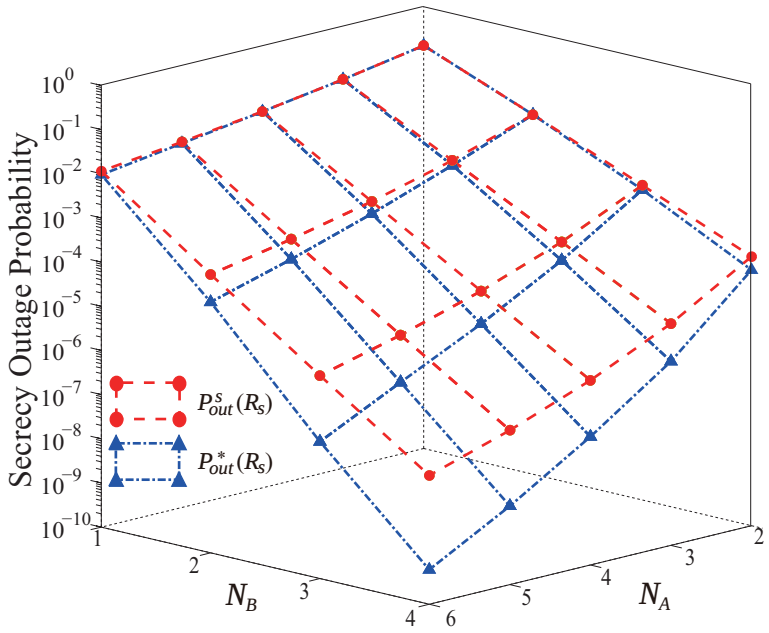

Figure 6.11: Secrecy outage probability versus N_A and N_B for $R_s = 1$, $\overline{\gamma}_B = 15$ dB, $\overline{\gamma}_E = 5$ dB, and $N_E = 2$.

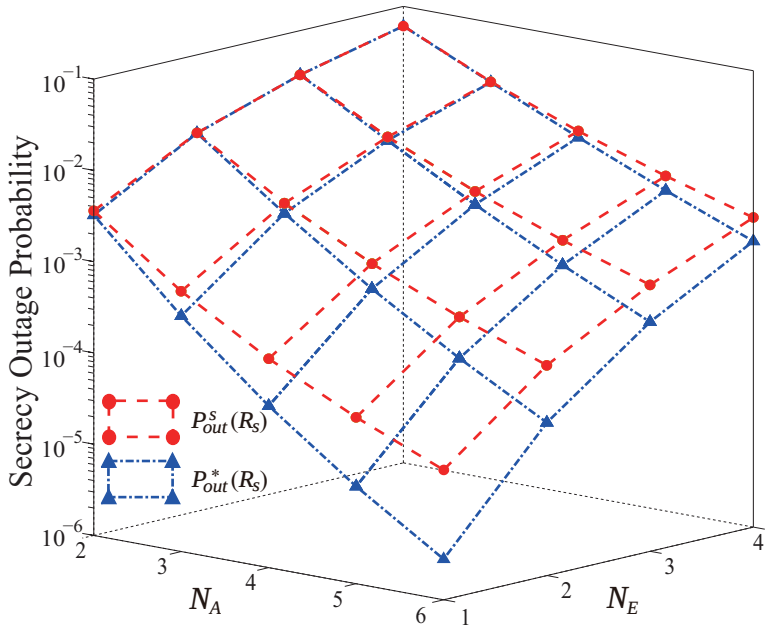

Figure 6.12: Secrecy outage probability versus N_A and N_E for $R_s = 1$, $\overline{\gamma}_B = 15$ dB, $\overline{\gamma}_E = 5$ dB, and $N_B = 2$.

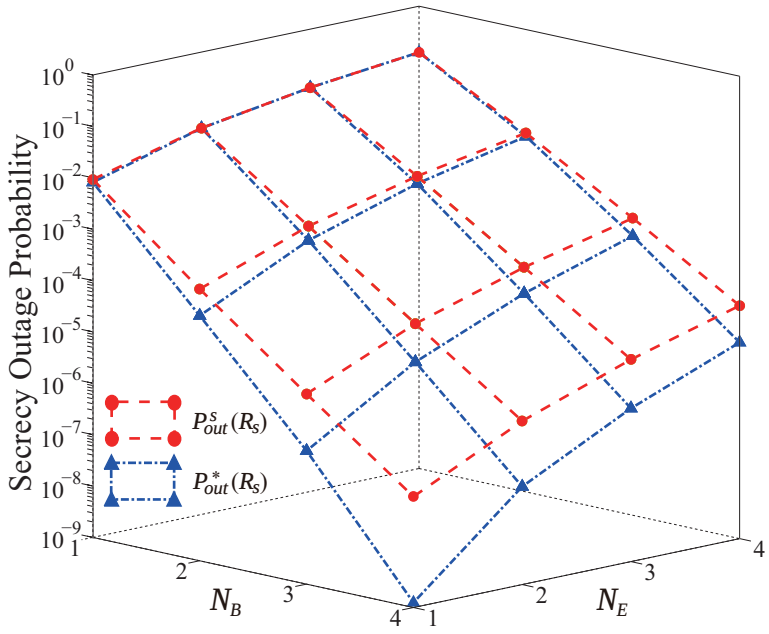

Figure 6.13: Secrecy outage probability versus N_B and N_E for $R_s = 1$, $\overline{\gamma}_B = 15$ dB, $\overline{\gamma}_E = 5$ dB, and $N_A = 4$.

of single TAS and TAS-Alamouti-OPA versus N_A and N_B. In Fig. 6.11, we first observe that when $N_B = 1, N_A < 6$ or $N_A = 2, N_B < 3$, TAS-Alamouti-OPA does not achieve a significantly lower secrecy outage probability relative to single TAS. We also observe that the gap between single TAS and TAS-Alamouti-OPA increases as N_A or N_B increases. Fig. 6.12 plots the secrecy outage probabilities of single TAS and TAS-Alamouti-OPA versus N_A and N_E. In Fig. 6.12, we first observe that when $N_A = 2, N_E > 1$ or $N_E = 4, N_A < 4$, TAS-Alamouti-OPA does not achieve a significantly lower secrecy outage probability relative to single TAS. We also observe that the gap between single TAS and TAS-Alamouti-OPA increases as N_A increases, but decreases as N_E increases. Fig. 6.13 plots the secrecy outage probabilities of single TAS and TAS-Alamouti-OPA versus N_B and N_E. In Fig. 6.13, we first observe that when $N_B = 1, N_E > 1$ or $N_E = 4, N_B < 2$, TAS-Alamouti-OPA does not achieve a significantly lower secrecy outage probability relative to single TAS. We also observe that the gap between single TAS and TAS-Alamouti-OPA increases as N_B increases but decreases as N_E increases. In summary, the observations in Fig. 6.11, Fig. 6.12,

and Fig. 6.13 demonstrate that the superiority of TAS-Alamouti-OPA over single TAS increases as N_A or N_B increases, and decreases as N_E increases.

6.6.3 Discussion

We note that it is possible to explore the trade-off between the feedback overhead and secrecy performance further. For example, one could probe the use of additional antennas combined with other coding schemes, at an increased cost in feedback overhead. Potential coding schemes that could be considered in this context include those discussed in [127, 128]. Another potential avenue of research along these lines could be a system in which Bob quantizes his CSI feedback using a predetermined number of bits. This estimate of the CSI could be modeled as quantization error on the true CSI of the main channel. Future work in this area may wish to consider such possibilities.

6.7 Summary

In this chapter we proposed a new TAS scheme for physical layer security enhancement in MIMO wiretap channels in which two antennas are selected. We derived new closed-form expressions for the exact and asymptotic secrecy outage probabilities of the scheme. When power at the selected antennas is equally distributed, our scheme was referred to as TAS-Alamouti, and we showed that such a scheme outperformed single TAS conditioned on the SNR at the intended receiver being above some threshold. A particularly interesting observation is that for $N_A = 3$, this enhanced performance of TAS-Alamouti required *no* additional feedback bits relative single TAS. We also determined the optimal power allocation for our proposed scheme – referred to TAS-Alamouti-OPA. We showed how TAS-Alamouti-OPA *always* outperformed the traditional single TAS scheme. TAS-Alamouti-OPA required only one extra feedback bit relative to TAS-Alamouti in order to provide improved secrecy

performance.

The useful trade-off trends discussed above for our schemes were also seen for $N_A > 3$. That is, for a minor increase in the feedback overhead, our two-antenna selection schemes allowed for significant security performance enhancement in MIMO wiretap channels relative to single TAS. The secrecy performance enhancements we found for our new schemes are surprising, because for non-secrecy MIMO systems it is known that the equivalent TAS-Alamouti schemes do not provide for any outage probability performance enhancement relative to single TAS.

Chapter 7

Optimization of Code Rates in SISOME Wiretap Channels

7.1 Introduction

Following our study of the role played by verified location information in enhancing physical layer security for wireless communications provided in Chapter 5 and Chapter 6, we examine the impact of such verified location information on the determination of wiretap code rates in this chapter. From the perspective of wiretap code design, the knowledge of the capacities of the main channel and the eavesdropper's channel is required at Alice in order to guarantee perfect secrecy [82]. In fact, perfect secrecy has two requirements: (i) the error probability at Bob decreases with increasing code length, and (ii) the fraction of information leakage to Eve decreases with increasing code length. These two requirements are denoted as the reliability constraint and the secrecy constraint, respectively [82, 83, 129]. A wiretap code can be designed by choosing two code rates, namely, the codeword rate, R_B, and the rate of transmitted confidential information (or equivalently, the target secrecy rate), R_s [82, 83]. The redundancy rate, $R_E = R_B - R_s$, is used to confuse Eve. In order to guarantee the reliability constraint of wiretap channels, the rate of transmitted

codewords has to be chosen as $R_B \leq C_B$, where C_B is the capacity of the main channel. In order to guarantee the secrecy constraint of wiretap channels, the redundancy rate has to be chosen as $R_E > C_E$, where C_E is the capacity of the eavesdropper's channel. If both C_B and C_E are available at Alice, the maximum target secrecy rate is achievable, which is referred to as the secrecy capacity of a wiretap channel and is given by $C_s = C_B - C_E$ [53, 54, 130, 131]. However, the assumption that C_E is available at Alice is too strong since in practice Eve may not feed back her CSI to Alice. In addition, in practice Alice may not know C_B since Bob may not feed back C_B to Alice due to the limited feedback overhead supported by the main channel[1].

We note that it is impossible for Alice to guarantee $R_E > C_E$ and fulfill the secrecy constraint in the case where only the statistical knowledge of the eavesdropper's channel is available at Alice. In this case, the performance of wiretap channels has been characterized in terms of the ergodic secrecy capacity [53, 130], and in terms of the existing secrecy outage probability (as what we did in Chapter 5 and Chapter 6), i.e., $\Pr(C_s < R_s)$ [58, 60, 63, 84, 121]. It is important to point out that the ergodic secrecy capacity is an average performance metric, and thus cannot be utilized to set R_B or R_E. We note that a proper definition of the ergodic secrecy capacity should consider specific coding strategies. The use of the secrecy outage probability given by (1.4) in determining R_B or R_E has the drawback that it does not separate the reliability from the security. The work of [114], focussed on an on-off transmission scheme for the wiretap channel, introduced a new metric that is motivated by a desire to disentangle reliability and secrecy features. The approach of [114] is based on a new secrecy outage probability defined through a *conditional* probability. We note that the legitimate approach of [114] explores the tradeoff between the quality of service and secrecy requirements. As we shown later, our approach (will be detailed below) is different from and can be complementary to the approach adopted in [114].

In this chapter, we propose a new framework to optimize the wiretap code rates

[1]The number of bits required to feed back C_B from Bob to Alice depends on the quantization accuracy of C_B.

when the capacity of the eavesdropper's channel is not available at Alice. Our framework is based on a new metric, referred to as the *effective secrecy throughput*, which explicitly captures both the reliability constraint and the secrecy constraint of wiretap channels. The effective secrecy throughput measures the average rate of the confidential information transmitted from Alice to Bob without being eavesdropped on by Eve. In the proposed framework, the optimal wiretap code rates maximize the effective secrecy throughput. Knowing the maximum average rate of confidential messages is of practical significance for the passive eavesdropping scenario, since it tells us on average how much secrecy data can be transmitted over a given period of time in a secret communication system. As we discuss in more details later, the key attribute of our new metric is that it encapsulates the main features of the wiretap channel, yet can be applied to a variety of transmission schemes.

By using our proposed framework, we optimize the wiretap code rates for two system models. (*i*) The first is a high complexity system model where Bob feeds back the capacity of the main channel to Alice. We refer to the transmission scheme under this system model as the adaptive transmission scheme since Bob can adaptively adjusts his wiretap code rates according to the fed back C_B. (*ii*) The second is a lower complexity system where Bob does not feed back the capacity of the main channel to Alice. We refer to the transmission scheme under this system model as the fixed-rate transmission scheme since Bob has to fix his wiretap code rates when both C_B and C_E are unavailable. In the above two system models, we assume that the average SNR of the eavesdropper's channel is available at Alice. In order to relax this assumption, we consider an absolute passive eavesdropping scenario where the average SNR of the eavesdropper's channel is not available at Alice. For this scenario, we derive closed-form expressions for the average effective secrecy throughput of the adaptive and the fixed-rate transmission schemes, based on which the wiretap code rates of these two schemes are optimized.

The rest of this chapter is organized as follows. Section 7.2 details the system model and the proposed new framework for optimizing the wiretap code rates. In

Section 7.3, the optimization of the redundancy rate R_E for the adaptive transmission scheme is presented. Section 7.4 presents the determination of the optimal (R_B, R_E) for the fixed-rate transmission scheme. In Section 7.5, we extend the optimization of the wiretap code rates into an absolute passive eavesdropping scenario based on the proposed annulus threat model. Numerical results are provided in Section 7.3, Section 7.4, and Section 7.5 in order to verify our analysis and provide useful insights into our optimal solutions. Finally, Section 7.6 draws some concluding remarks.

7.2 System Model and New Framework

In this section, we detail our system model and the new framework for optimizing wiretap code rates (e.g., R_B, R_E) by using the proposed effective secrecy throughput.

7.2.1 System Model

The wiretap channel of interest is where the transmitter (Alice) and the intended receiver (Bob) are equipped with a single antenna, and the eavesdropper (Eve) is equipped with N_E antennas. The above wiretap channel is referred to as the single-input single-output multi-antenna eavesdropper (SISOME) wiretap channel. We assume that the main channel and the eavesdropper's channel are subject to independent quasi-static Rayleigh fading with equal block length. We also assume that Bob possesses the full knowledge of the instantaneous CSI of the main channel, but Alice only knows the average SNR of the main channel. We further assume that Eve knows the instantaneous CSI of the eavesdropper's channel. As such, Eve applies MRC [87,132,133] to combine the received signals in order to exploit the N_E-antenna diversity and maximize the probability of successful eavesdropping.

The received signal at Bob is given by

$$y_B = hx + n_B, \tag{7.1}$$

where h is the complex gain of the main channel, x is the transmit signal, and n_B is the Gaussian noise of the main channel with zero mean and variance σ_B^2. The transmit power constraint is given by $\mathbb{E}[|x|^2] = P_A$, where P_A is the total transmit power. Based on (7.1), the instantaneous SNR at Bob is obtained as

$$\gamma_B = \frac{|h|^2 P_A}{\sigma_B^2}, \tag{7.2}$$

which indicates that γ_B follows an exponential distribution with $1/\overline{\gamma}_B$ as the rate parameter, where $\overline{\gamma}_B = \mathbb{E}[\gamma_B]$.

The $N_E \times 1$ received signal vector at Eve is given by

$$\mathbf{y}_E = \mathbf{g}x + \mathbf{n}_E, \tag{7.3}$$

where $\mathbf{g}$ is the $N_E \times 1$ eavesdropper's channel vector with i.i.d. Rayleigh fading entries, and $\mathbf{n}_E$ is circularly symmetric complex Gaussian noise vector of the eavesdropper's channel with zero mean and covariance matrix $\mathbf{I}_{N_E}\sigma_E^2$. Applying MRC to exploit the N_E-antenna diversity at Eve, the instantaneous SNR at Eve is obtained as

$$\gamma_E = \frac{\|\mathbf{g}\|^2 P_A}{\sigma_E^2}, \tag{7.4}$$

which indicates that γ_E follows a Gamma distribution with N_E and $\overline{\gamma}_E = \mathbb{E}[\gamma_E]/N_E$ as the shape and scale parameters, respectively.

7.2.2 New Framework for Optimizing Wiretap Code Rates

In wiretap channels, Alice intends to sent the confidential information to Bob with a high transmission rate while guaranteeing both the reliability constraint and secrecy constraint. However, if the capacity of the eavesdropper's channel is not available at Alice, the secrecy constraint cannot be guaranteed and a secrecy outage may incur. We define the secrecy outage probability in this chapter as [134]

$$\mathcal{O}_s(R_E) = \Pr(R_E < C_E). \tag{7.5}$$

We note that $\mathcal{O}_s(R_E)$ is different from the existing secrecy outage probability, $\Pr(C_s < R_s)$, since the latter includes not only the secrecy outage probability but also the reliability outage probability.

Likewise, if the capacity of the main channel is not available at Alice, the reliability constraint cannot be guaranteed and thus a reliability outage may incur. We define the reliability outage probability as [134]

$$\mathcal{O}_r(R_B) = \Pr(R_B > C_B). \tag{7.6}$$

Based on (7.6), we can see that the reliability constraint can be guaranteed if C_B is available at Alice.

Incorporating both the secrecy outage probability and reliability outage probability, we present the effective secrecy throughput in the following definition.

***Definition* 1** The effective secrecy throughput of a wiretap channel is defined as

$$\Psi(R_B, R_E) = (R_B - R_E)\left[1 - \mathcal{O}_r(R_B)\right]\left[1 - \mathcal{O}_s(R_E)\right]. \tag{7.7}$$

From (7.7), we can see that the effective secrecy throughput measures the average rate of the confidential information successfully transmitted from Alice to Bob excluding the information eavesdropped on by Eve. Maximizing the effective secrecy throughput presented in (7.7) will maximize the *real confidential information* (the confidential information that does not incur reliability outage or secrecy outage) received by Bob within a time period. As such, in wiretap channels Alice intends to maximize such effective secrecy throughput. Therefore, in the following sections we determine the optimal values of wiretap code rates (e.g., R_B, R_E) for the adaptive and fixed-rate transmission schemes in order to maximize the effective secrecy throughput of each scheme. In (7.7), $\mathcal{O}_r(R_B)$ and $\mathcal{O}_s(R_E)$ are functions of R_B and R_E, respectively. This allows us to jointly determine the optimal values of R_B and R_E that maximize $\Psi(R_B, R_E)$. The definition of $\Psi(R_B, R_E)$ provided in (7.7) is different from an sub-optimal strategy to obtain a value of $\Psi(R_B, R_E)$, in which the values of $\mathcal{O}_r(R_B)$ and $\mathcal{O}_s(R_E)$ are first predetermined (thus the values of R_B and R_E are also predetermined)

and then the value of $\Psi(R_B, R_E)$ is calculated via (7.7) by using the predetermined values of R_B, R_E, $\mathcal{O}_r(R_B)$, and $\mathcal{O}_s(R_E)$. The difference arises from that in the sub-optimal strategy the value of $\Psi(R_B, R_E)$ is not optimized.

We note that different from the approach adopted in [114] we directly optimize a key throughput rate of the wiretap channel - the effective secrecy throughput. Importantly, our technique is not targeted at any transmission scheme in particular and therefore is directly applicable to a wide range of schemes and system models. We optimize wiretap code rates by maximizing the effective secrecy throughput, a metric which implicitly captures both the quality of service (reliability) and secrecy constraints. This is also different from the approach pursued in [114], where the tradeoff between the quality of service and secrecy requirements is explored subjectively. As such, our approach and the approach of [114] are complementary and examine different trade-offs, and therefore in this sense one approach cannot be said to be better than the other.

7.3 Redundancy Rate for Adaptive Transmission Scheme

In this section, we first derive a closed-form expression for the effective secrecy throughput of the adaptive transmission scheme, based on which we optimize the redundancy rate R_E for this scheme. We note that applying the adaptive transmission scheme requires the capacity of the main channel be available at Alice. As such, the complexity of the system where the adaptive transmission scheme can be applied is high since Bob has to feed back C_B to Alice.

7.3.1 Adaptive Transmission Scheme

In the adaptive transmission scheme, C_B is available at Alice and R_B is chosen as $R_B = C_B$. As such, to design a wiretap code for the adaptive transmission scheme

we only need to determine the value of R_E. In the adaptive transmission scheme, R_E is adjusted within the constraint $0 < R_E < C_B$ according to each γ_B. Since R_B is chosen as $R_B = C_B$, the reliability constraint can always be guaranteed in the adaptive transmission scheme (reliability outage probability is zero). We note that a secrecy outage may incur since C_E is not available at Alice. In the following, we first present the secrecy outage probability of the adaptive transmission scheme.

As per the definition of $\mathcal{O}_s(R_E)$, the secrecy outage probability of the adaptive transmission scheme is

$$\mathcal{O}_{s,a}(R_E) = \Pr(R_E < C_E) = \Pr\left(\gamma_E > 2^{R_E} - 1\right) = 1 - F_{\gamma_E}\left(2^{R_E} - 1\right), \tag{7.8}$$

where $F_{\gamma_E}(\gamma_E)$ is the cdf of γ_E, which is

$$F_{\gamma_E}(\gamma_E) = 1 - e^{-\frac{\gamma_E}{\overline{\gamma}_E}} \sum_{j=0}^{N_E-1} \frac{1}{j!} \left(\frac{\gamma_E}{\overline{\gamma}_E}\right)^j. \tag{7.9}$$

As such, the effective secrecy throughput of the adaptive transmission scheme is given in the following lemma.

***Lemma* 4** The effective secrecy throughput of the adaptive transmission scheme is

$$\Psi_a(R_E) = (C_B - R_E)\left[1 - e^{-\frac{2^{R_E}-1}{\overline{\gamma}_E}} \sum_{j=0}^{N_E-1} \frac{1}{j!} \left(\frac{2^{R_E}-1}{\overline{\gamma}_E}\right)^j\right]. \tag{7.10}$$

The proof of Lemma 4 is provided in the following. Since the reliability outage probability of the adaptive transmission scheme is zero and R_B is set as $R_B = C_B$, based on (7.7) the effective secrecy throughput of the adaptive transmission scheme is given by

$$\Psi_a(R_E) = (C_B - R_E)\left[1 - \mathcal{O}_{s,a}(R_E)\right] = (C_B - R_E)\, F_{\gamma_E}\left(2^{R_E} - 1\right). \tag{7.11}$$

Substituting (7.9) into (7.11), we obtain the result in (7.10).

The optimal value of R_E that maximizes $\Psi_a(R_E)$ of the adaptive transmission scheme is provided in the following theorem.

***Theorem* 13** The optimal value of R_E that maximizes $\Psi_a(R_E)$ of the adaptive transmission scheme, $R_E^{\ddagger}$, can be obtained by solving the fixed-point equation given by

$$R_E^{\ddagger} = C_B - \frac{\overline{\gamma}_E (N_E-1)!}{2^{R_E^{\ddagger}} \ln 2} \left(\frac{\overline{\gamma}_E}{2^{R_E^{\ddagger}}-1} \right)^{N_E-1} \left[e^{\frac{2^{R_E^{\ddagger}}-1}{\overline{\gamma}_E}} - \sum_{j=0}^{N_E-1} \frac{1}{j!} \left(\frac{2^{R_E^{\ddagger}}-1}{\overline{\gamma}_E} \right)^j \right]. \quad (7.12)$$

We now prove Theorem 13. The first derivative of (7.10) with respect to R_E is obtained as

$$\begin{aligned} \frac{\partial \Psi_a(R_E)}{\partial R_E} = &- \left[1 - e^{-\frac{2^{R_E}-1}{\overline{\gamma}_E}} \sum_{j=0}^{N_E-1} \frac{1}{j!} \left(\frac{2^{R_E}-1}{\overline{\gamma}_E} \right)^j \right] \\ &+ (C_B - R_E) \left(\frac{2^{R_E} \ln 2}{\overline{\gamma}_E} \right) \frac{e^{-\frac{2^{R_E}-1}{\overline{\gamma}_E}}}{(N_E-1)!} \left(\frac{2^{R_E}-1}{\overline{\gamma}_E} \right)^{N_E-1}. \end{aligned} \quad (7.13)$$

By setting $\partial \Psi_a(R_E)/\partial R_E = 0$, we obtain the fixed-point equation in (7.12) after some algebraic manipulations. This completes the proof of Theorem 13.

Substituting $R_E^{\ddagger}$ into (7.10), we obtain the maximum value of $\Psi_a(R_E)$, which is denoted as Ψ_a^*. We now provide some valuable insights on $R_E^{\ddagger}$ for $N_E = 1$ by conducting the following asymptotic analysis.

***Corollary* 9** As $\overline{\gamma}_E \to 0$, we obtain $R_E^{\ddagger} \to 0$.

The proof of Corollary 9 is presented in the following. When $N_E = 1$, (7.10) reduces to

$$\Psi_a(R_E) = (C_B - R_E) \left[1 - e^{-\frac{2^{R_E}-1}{\overline{\gamma}_E}} \right]. \quad (7.14)$$

It is found from (7.14) that $\Psi_a(R_E)$ converges to $(C_B - R_E)$ as $\overline{\gamma}_E \to 0$. Therefore, due to the constraint $0 < R_E < C_B$, we have $R_E^{\ddagger} \to 0$.

It is indicated from Corollary 9 that Eve can be ignored if she is far from Alice.

***Corollary* 10** As $\overline{\gamma}_E \to \infty$, $R_E^{\ddagger}$ can be obtained by solving the fixed-point equation given by

$$R_E^{\ddagger} = C_B - \frac{1 - 2^{-R_E^{\ddagger}}}{\ln 2}. \quad (7.15)$$

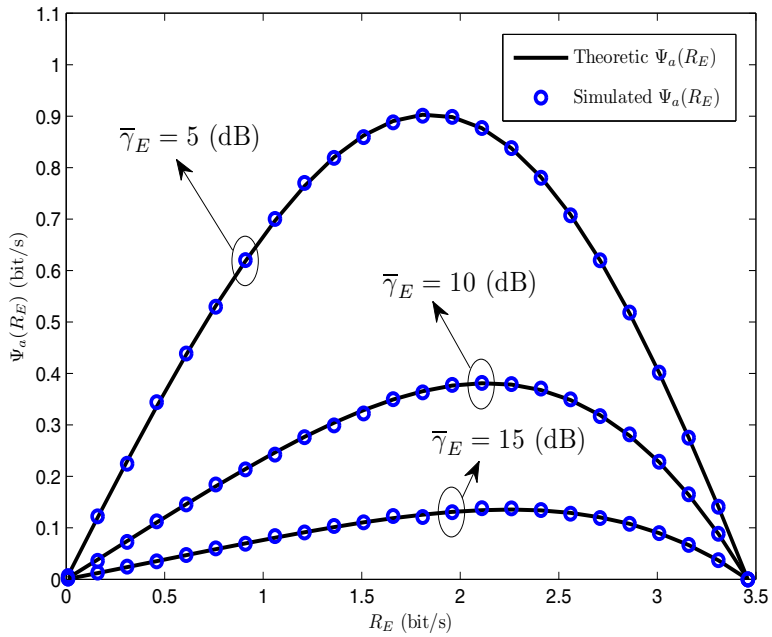

Figure 7.1: Effective secrecy throughput of the adaptive transmission scheme, $\Psi_a(R_E)$, versus R_E for $N_E = 1$, $\gamma_B = 10$ dB, and different values of $\overline{\gamma}_E$.

We now prove Corollary 10. Applying $\lim_{x\to 0} e^{-x} \approx 1 - x$ into (7.14), we obtain

$$\lim_{\overline{\gamma}_E \to \infty} (C_B - R_E) \left[1 - e^{-\frac{2^{R_E}-1}{\overline{\gamma}_E}}\right] \approx (C_B - R_E) \frac{2^{R_E}-1}{\overline{\gamma}_E}. \tag{7.16}$$

By setting the first derivative of (7.16) with respect to R_E as zero, we obtain the fixed-point equation in (7.15) after some algebraic manipulations.

From Corollary 10, we see that $R_E^{\ddagger}$ does not approach C_B as $\overline{\gamma}_E \to \infty$. Notably, $R_E^{\ddagger}$ approaches a constant value that is a function of C_B.

7.3.2 Numerical Results

In this subsection, we present numerical results to examine the impact of the number of antennas at Eve and the SNRs of the main channel and eavesdropper's channel, on the optimal redundancy rate $R_E^{\ddagger}$.

In Fig. 7.1, we plot the effective secrecy throughput of the adaptive transmission scheme, $\Psi_a(R_E)$, versus R_E for different values of $\overline{\gamma}_E$. The theoretic curve is obtained

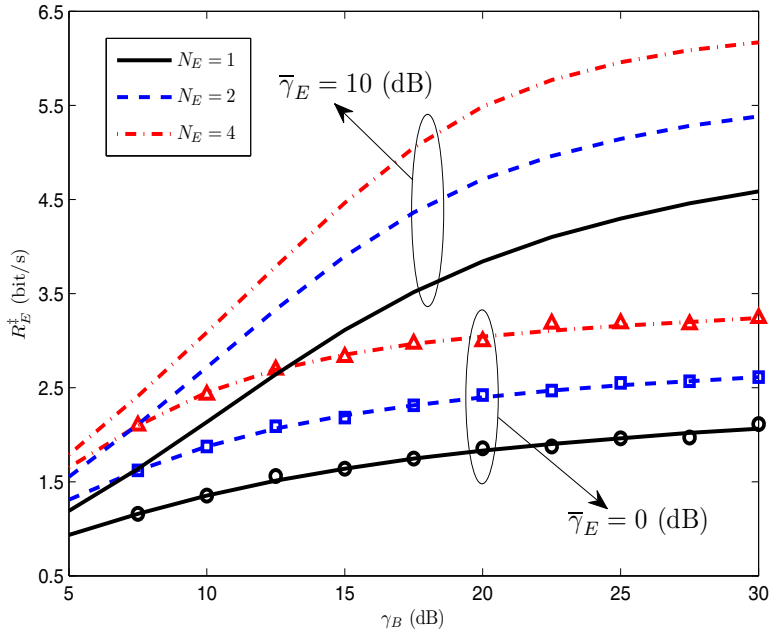

Figure 7.2: Optimal redundancy rate for the adaptive transmission scheme, $R_E^{\ddagger}$, versus γ_B for different values of N_E and $\overline{\gamma}_E$.

from (7.10). In this figure, we first observe that the Monte Carlo simulations precisely match the theoretic curves, which validates our analysis in Lemma 4. We also observe that $\Psi_a(R_E)$ increases as $\overline{\gamma}_E$ decreases, which demonstrates that the worse the eavesdropper's channel is the larger effective secrecy throughput the adaptive transmission scheme achieves. Moreover, we observe that a unique value of R_E exists which maximizes $\Psi_a(R_E)$ for a given γ_B. Focusing on the peaks of the three curves, we also observe that $R_E^{\ddagger}$ decreases as $\overline{\gamma}_E$ decreases, which demonstrates that the further Eve is from Alice the smaller redundancy rate we set in order to maximize the effective secrecy throughput.

In Fig. 7.2, we plot the optimal redundancy rate for the adaptive transmission scheme, $R_E^{\ddagger}$, versus γ_B for different values of N_E and $\overline{\gamma}_E$. The curves represent the theoretic results for $R_E^{\ddagger}$ are obtained from (7.12), and the symbols represent the simulated results for $R_E^{\ddagger}$ are obtained from Monte Carlo simulations. The accuracy of our analysis in Theorem 13 is demonstrated in this figure. As expected, we first observe that $R_E^{\ddagger}$ increases as $\overline{\gamma}_E$ increases. We also observe that $R_E^{\ddagger}$ first increases as γ_B in-

creases and then approaches a constant as γ_B approaches large values. Furthermore, we observe that $R_E^{\ddagger}$ increases as N_E increases. This can be explained by the fact that a higher N_E leads to the better quality of the eavesdropper's channel since Eve applies MRC to combine the received signals.

7.4 Wiretap Code Rates for Fixed-Rate Transmission Scheme

In this section, we first derive a closed-form expression for the effective secrecy throughput of the fixed-rate transmission scheme, based on which we jointly optimize the codeword rate R_B and redundancy rate R_E for this scheme. We note that the fixed-rate transmission scheme does not require the capacity of the main channel be available at Alice. As such, this scheme is to be a lower complexity system where there is no feedback from Bob to Alice.

7.4.1 Fixed-Rate Transmission Scheme

In the fixed-rate transmission scheme, both C_B and C_E are unavailable at Alice, so we have to jointly determine R_B and R_E for given $\overline{\gamma}_B$ and $\overline{\gamma}_E$. Therefore, both the reliability constraint and secrecy constraint cannot be guaranteed in the fixed-rate transmission scheme. In the following, we first present the reliability outage probability and secrecy outage probability.

As per the definition of $\mathcal{O}_r(R_B)$, the reliability outage probability of the fixed-rate transmission scheme is

$$\mathcal{O}_{r,f}(R_B) = \Pr(R_B > C_B) = F_{\gamma_B}\left(2^{R_B} - 1\right), \tag{7.17}$$

where $F_{\gamma_B}(\gamma_B)$ is the cdf of γ_B, which is

$$F_{\gamma_B}(\gamma_B) = 1 - e^{-\frac{\gamma_B}{\overline{\gamma}_B}}. \tag{7.18}$$

According to the definition of $\mathcal{O}_s(R_E)$, the secrecy outage probability of the fixed-rate transmission scheme is

$$\mathcal{O}_{s,f}(R_E) = \Pr(R_E < C_E) = 1 - F_{\gamma_E}\left(2^{R_E} - 1\right). \tag{7.19}$$

Then, the effective secrecy throughput of the fixed-rate transmission scheme is presented in the following lemma.

***Lemma* 5** The effective secrecy throughput of the fixed-rate transmission scheme is

$$\Psi_f(R_B, R_E) = (R_B - R_E)\, e^{-\frac{2^{R_B}-1}{\overline{\gamma}_B}} \left(1 - e^{-\frac{2^{R_E}-1}{\overline{\gamma}_E}} \sum_{j=0}^{N_E-1} \frac{1}{j!} \left(\frac{2^{R_E}-1}{\overline{\gamma}_E}\right)^j\right). \tag{7.20}$$

We present the proof of Lemma 5 in the following. As per the definition of $\Psi(R_B, R_E)$, the effective secrecy throughput of the fixed-rate transmission scheme can be written as

$$\begin{aligned} \Psi_f(R_B, R_E) &= (R_B - R_E)\left[1 - \mathcal{O}_{r,f}(R_B)\right]\left[1 - \mathcal{O}_{s,f}(R_E)\right] \\ &= (R_B - R_E)\left[1 - F_{\gamma_B}\left(2^{R_B} - 1\right)\right] F_{\gamma_E}\left(2^{R_E} - 1\right). \end{aligned} \tag{7.21}$$

Substituting (7.18) and (7.9) into (7.21), we obtain the result in (7.20) after some algebraic manipulations.

Using (7.21), the optimal (R_B, R_E) which maximizes $\Psi_f(R_B, R_E)$ can be obtained through

$$(R_B, R_E)^* = \underset{0<R_B, 0<R_E<R_B}{\operatorname{argmax}} \Psi_f(R_B, R_E). \tag{7.22}$$

The optimal values of R_B and R_E in $(R_B, R_E)^*$ are denoted as R_B^* and R_E^*, respectively. The explicit solutions to R_B^* and R_E^* are given in the following theorem.

***Theorem* 14** The value of R_B^* can be obtained through solving the following fixed-point equation

$$R_B^* = R_E^* + \frac{e^{\frac{2^{R_E^*}-1}{\overline{\gamma}_E}} - \mathbf{F}(N_E, R_E^*, \overline{\gamma}_E)}{\mathbf{G}(N_E, R_E^*, \overline{\gamma}_E)}, \tag{7.23}$$

where

$$R_E^* = R_B^* - \frac{\overline{\gamma}_B}{2^{R_B^*} \ln 2}, \tag{7.24}$$

and the value of R_E^* can be obtained by substituting R_B^* into (7.24). In (7.23) and (7.24), we define the two functions, $\mathcal{F}(\cdot)$ and $\mathcal{G}(\cdot)$, as follows

$$\begin{aligned}\mathcal{F}(N_E, R_E, \overline{\gamma}_E) &= \sum_{j=0}^{N_E-1} \frac{1}{j!} \left(\frac{2^{R_E}-1}{\overline{\gamma}_E}\right)^j, \\ \mathcal{G}(N_E, R_E, \overline{\gamma}_E) &= \frac{2^{R_E}\ln 2}{\overline{\gamma}_E (N_E-1)!} \left(\frac{2^{R_E}-1}{\overline{\gamma}_E}\right)^{N_E-1}.\end{aligned} \tag{7.25}$$

We now prove Theorem 14. We note that $1-\mathcal{F}(N_E, R_E, \overline{\gamma}_E)e^{-\frac{2^{R_E}-1}{\overline{\gamma}_E}}$ and $e^{-\frac{2^{R_B}-1}{\overline{\gamma}_B}}$ are both positive for $0 < R_E < R_B$ and finite N_E. Setting the first partial derivative of (7.20) with respect to R_B as zero, we obtain

$$1 - (R_B - R_E)\frac{2^{R_B}\ln 2}{\overline{\gamma}_B} = 0,$$

which results in

$$R_E = R_B - \frac{\overline{\gamma}_B}{2^{R_B}\ln 2}. \tag{7.26}$$

Likewise, by setting the first partial derivative of (7.20) with respect to R_E as zero, we obtain

$$\mathcal{F}(N_E, R_E, \overline{\gamma}_E) - (R_B - R_E)\mathcal{G}(N_E, R_E, \overline{\gamma}_E) = e^{\frac{2^{R_E}-1}{\overline{\gamma}_E}},$$

which results in

$$R_B = R_E + \frac{e^{\frac{2^{R_E}-1}{\overline{\gamma}_E}} - \mathcal{F}(N_E, R_E, \overline{\gamma}_E)}{\mathcal{G}(N_E, R_E, \overline{\gamma}_E)}. \tag{7.27}$$

Substituting (7.26) into (7.27), we obtain the fixed-point equation in (7.23) after some algebraic manipulations.

It is highlighted that Theorem 14 is of great significance since it is difficult to conduct numerical searching for R_B^* and R_E^* as per the constraint on (R_B, R_E) given by $0 < R_E < R_B < +\infty$. Instead, we can solve (7.23) iteratively by setting the initial value of R_E^* as zero. Substituting R_B^* and R_E^* into (7.20), we obtain the maximum value of $\Psi_f(R_B, R_E)$, which is denoted as Ψ_f^*. In the fixed-rate transmission scheme, the design task is to determine R_B^* and R_E^* jointly for given $\overline{\gamma}_B$ and $\overline{\gamma}_E$. We next conduct the asymptotic analysis with $N_E = 1$ in order to draw some insights on R_B^* and R_E^*.

***Corollary* 11** As $\overline{\gamma}_E \to 0$, R_B^* for a given $\overline{\gamma}_B$ can be obtained through solving the fixed-point equation given by

$$R_B^* = \frac{\overline{\gamma}_B}{2^{R_B^*} \ln 2}, \tag{7.28}$$

and the corresponding R_E^* approaches zero.

We provide the proof of Corollary 11 in the following. As $\overline{\gamma}_E \to 0$, we obtain $\mathcal{O}_{s,f}(R_E) \to 0$. Accordingly, (7.20) with $N_E = 1$ reduces to

$$\Psi_f(R_B, R_E) = (R_B - R_E)\, e^{-\frac{2^{R_B}-1}{\overline{\gamma}_B}}. \tag{7.29}$$

Setting the first derivative of (7.29) with respect to R_B as zero, we obtain the result in (7.28) after some algebraic manipulations.

From Corollary 11, we see that Eve can be ignored if she is far from Alice since $R_E^* \to 0$ as $\overline{\gamma}_E \to 0$. We also note that R_B^* is a function of $\overline{\gamma}_B$ only, which can be explained by the fact that R_B^* is determined through maximizing $R_B\left[1 - \mathcal{O}_{r,f}(R_B)\right]$. We also note that Ψ_f^* approaches a constant value determined by $\overline{\gamma}_B$ as $\overline{\gamma}_E \to 0$.

***Corollary* 12** As $\overline{\gamma}_E \to \infty$, R_B^* for a given $\overline{\gamma}_B$ can be obtained through solving the fixed-point equation given by

$$R_B^* = R_E^* + \frac{2^{R_E^*} - 1}{2^{R_E^*} \ln 2}, \tag{7.30}$$

where

$$R_E^* = R_B^* - \frac{\overline{\gamma}_B}{2^{R_B^*} \ln 2}, \tag{7.31}$$

and R_E^* can be obtained by substituting R_B^* into (7.31).

The proof of Corollary 12 is provided in the following. When $N_E = 1$, (7.20) reduces to

$$\Psi_f(R_B, R_E) = (R_B - R_E)\, e^{-\frac{2^{R_B}-1}{\overline{\gamma}_B}} \left(1 - e^{-\frac{2^{R_E}-1}{\overline{\gamma}_E}}\right). \tag{7.32}$$

Since R_E is still finite as $\overline{\gamma}_E \to \infty$, we apply $\lim_{x \to 0} e^{-x} \approx 1 - x$ into (7.32) and obtain

$$\lim_{\overline{\gamma}_E \to \infty} \Psi_f\left(R_B, R_E\right) \approx (R_B - R_E)\, e^{-\frac{2^{R_B}-1}{\overline{\gamma}_B}} \frac{2^{R_E} - 1}{\overline{\gamma}_E}. \tag{7.33}$$

We note $\frac{2^{R_E}-1}{\overline{\gamma}_E} > 0$ due to $R_E > 0$ as $\overline{\gamma}_E \to \infty$. Setting the first derivative of (7.33) with respect to R_B as zero, we obtain

$$(R_B - R_E)\,\frac{2^{R_B}\ln 2}{\overline{\gamma}_B} = 1. \tag{7.34}$$

Likewise, setting the first derivative of (7.33) with respect to R_E as zero, we obtain

$$-\frac{2^{R_E}-1}{\overline{\gamma}_E} + (R_B - R_E)\,\frac{2^{R_E}\ln 2}{\overline{\gamma}_E} = 0, \tag{7.35}$$

which results in (due to $\overline{\gamma}_E \neq 0$)

$$1 - 2^{R_E} + (R_B - R_E)\,2^{R_E}\ln 2 = 0. \tag{7.36}$$

Substituting (7.34) into (7.36), we obtain the fixed-point equation in (7.30) after some algebraic manipulations.

It is highlighted from Corollary 12 that (7.30) and (7.31) are independent of $\overline{\gamma}_E$, which indicates that R_B^* and R_E^* are not functions of $\overline{\gamma}_E$ as $\overline{\gamma}_E \to \infty$.

7.4.2 Numerical Results

In this subsection, we present numerical results to examine the impact of the number of antennas at Eve and the SNRs of the main channel and eavesdropper's channel, on R_B^* and R_E^*. We also conduct a thorough performance comparison between the adaptive transmission scheme and the fixed-rate transmission scheme in terms of the effective secrecy throughput.

In Fig. 7.3, we plot the effective secrecy throughput of the fixed-rate transmission scheme, $\Psi_f(R_B, R_E)$, versus R_B and R_E. The theoretic $\Psi_f(R_B, R_E)$ curve is generated via (7.20). In this figure, we first observe that the Monte Carlo simulation result precisely matches the theoretic curve. Moreover, we observe that there is indeed a unique pair of R_B and R_E which maximizes $\Psi_f(R_B, R_E)$. This demonstrates that we can determine the optimal (R_B, R_E) based on our proposed framework.

In Fig. 7.4, we plot the optimal wiretap code rates of the fixed-rate transmission scheme, R_B^* and R_E^*, versus $\overline{\gamma}_E$. The exact curves of R_B^* and R_E^* are obtained by

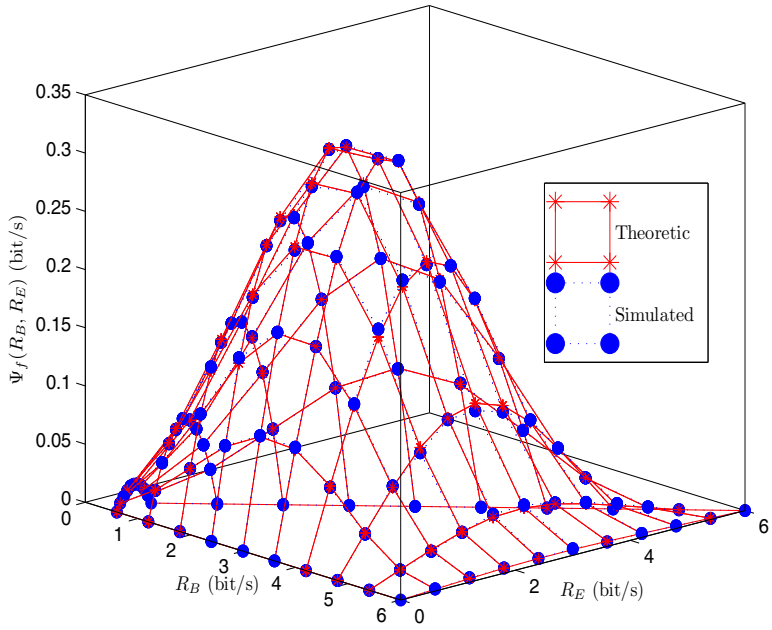

Figure 7.3: Effective secrecy throughput of the fixed-rate transmission scheme, $\Psi_f(R_B, R_E)$, versus R_B and R_E for $N_E = 1$, $\overline{\gamma}_B = 10$ dB, and $\overline{\gamma}_E = 5$ dB.

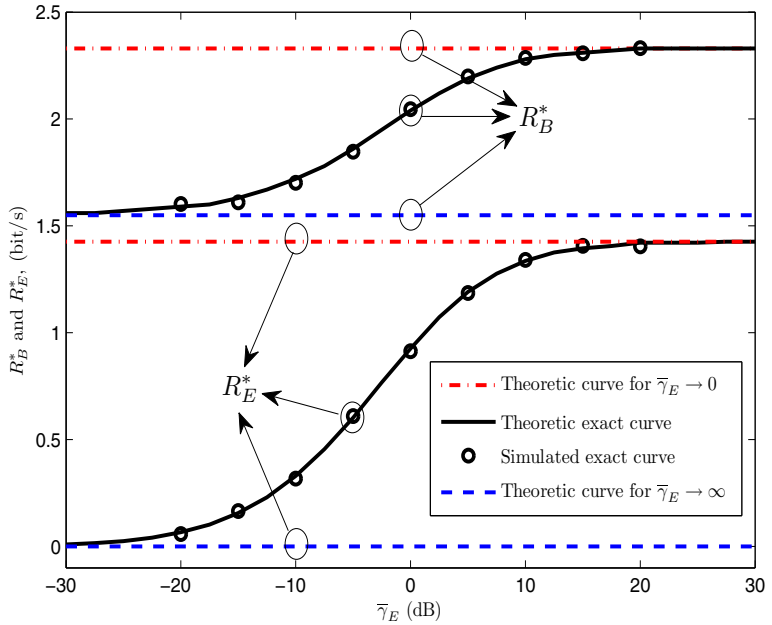

Figure 7.4: Optimal wiretap code rates of the fixed-rate transmission scheme, R_B^* and R_E^*, versus $\overline{\gamma}_E$ for $N_E = 1$ and $\overline{\gamma}_B = 5$ dB.

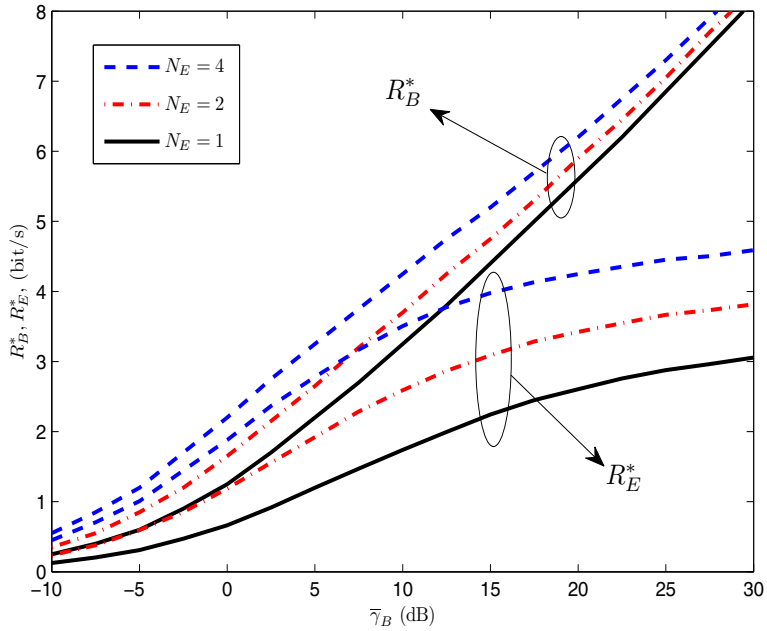

Figure 7.5: Optimal wiretap code rates of the fixed-rate transmission scheme, R_B^* and R_E^*, versus $\overline{\gamma}_B$ for $\overline{\gamma}_E = 5$ dB.

solving (7.23) and (7.24), respectively. The curve of R_B^* for $\overline{\gamma}_E \to 0$ is generated by solving (7.28), and R_E^* for $\overline{\gamma}_E \to 0$ is approximated as zero. The curves of R_B^* and R_E^* for $\overline{\gamma}_E \to \infty$ are achieved by solving (7.30) and (7.31), respectively. In this figure, we first observe that the Monte Carlo simulated R_B^* and R_E^* precisely match the theoretic R_B^* and R_E^*, respectively. We also observe that the exact curves of R_B^* and R_E^* approach the asymptotic curves of R_B^* and R_E^*, respectively, as $\overline{\gamma}_E \to 0$ and $\overline{\gamma}_E \to \infty$. This observation confirms the accuracy of our asymptotic analysis given in Corollary 11 and Corollary 12. Finally, we observe that both R_B^* and R_E^* increase as $\overline{\gamma}_E$ increases, but $(R_B^* - R_E^*)$ decreases as $\overline{\gamma}_E$ increases.

In Fig. 7.5, we plot R_B^* and R_E^* versus $\overline{\gamma}_B$ for different values of N_E. In this figure, we first observe that both R_B^* and R_E^* increase as $\overline{\gamma}_B$ increases, and $(R_B^* - R_E^*)$ increases as $\overline{\gamma}_B$ increases. We also observe that as $\overline{\gamma}_B \to 0$ both R_B^* and R_E^* approach zero, which indicates that the positive effective secrecy throughput cannot be achieved when Bob is very far from Alice. Furthermore, we observe that R_B^* is still a function of $\overline{\gamma}_B$ as $\overline{\gamma}_B \to \infty$, but R_E^* approaches a specific constant value. Finally, we observe

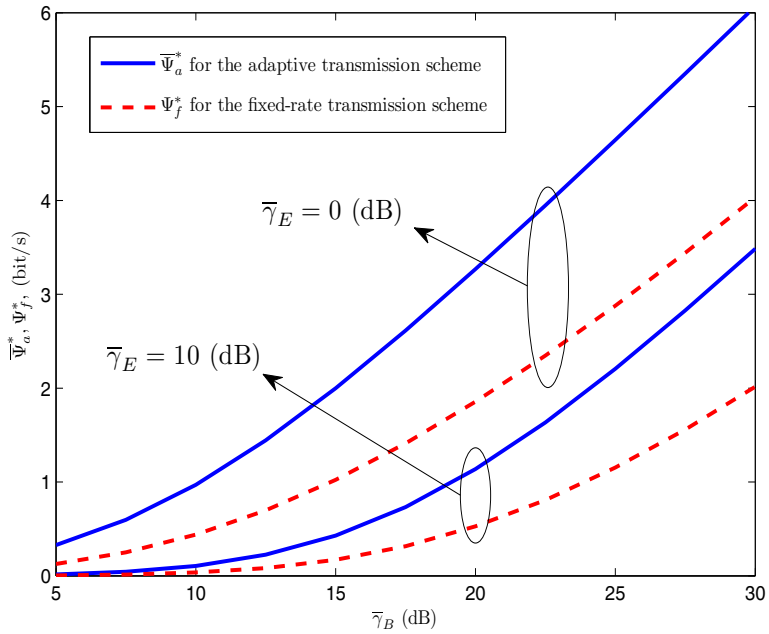

Figure 7.6: Average maximum effective secrecy throughput of the adaptive transmission scheme, $\overline{\Psi}_a^*$, and maximum effective secrecy throughput of fixed-rate transmission scheme, Ψ_f^*, versus $\overline{\gamma}_B$ for $N_A = 1$, $N_B = 1$, and $N_E = 2$.

that both R_B^* and R_E^* increase as N_E increases, but $(R_B^* - R_E^*)$ decreases as N_E increases.

Now, we conduct a thorough comparison between the adaptive transmission scheme and the fixed-rate transmission scheme. The results are presented in Fig. 7.6, where $\overline{\Psi}_a^*$ is the average maximum effective secrecy throughput of the adaptive transmission scheme, obtained by $\overline{\Psi}_a^* = \mathbb{E}_{\gamma_B}[\Psi_a^*]$. We first observe that both $\overline{\Psi}_a^*$ and Ψ_f^* increase as $\overline{\gamma}_B$ increases, but decrease as $\overline{\gamma}_E$ increases. This indicates that the geometric locations of Alice, Bob, and Eve are of significant importance in wiretap channels. As expected, we observe that the adaptive transmission scheme achieves higher effective secrecy throughput than the fixed-rate transmission scheme. In addition, we observe that the effective secrecy throughput gain of the adaptive transmission scheme over the fixed-rate transmission scheme is negligible in the regime of low $\overline{\gamma}_B$ (relative to $\overline{\gamma}_E$), but profound in the regime of high $\overline{\gamma}_B$. Of course, the effective secrecy through-

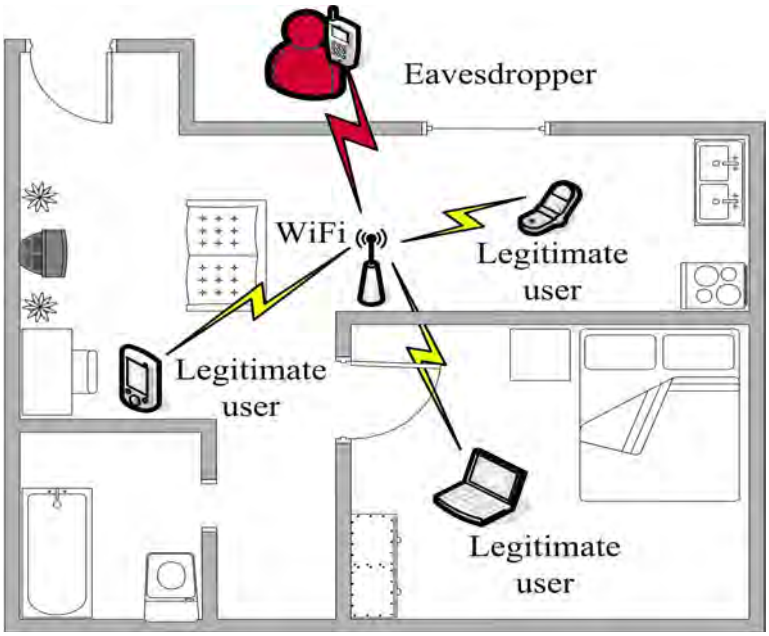

Figure 7.7: Illustration of a practical scenario based on which the annulus threat model proposed.

put is enhanced at the cost of feeding back C_B to Alice and adjusting R_B and R_E for each realization of the main channel.

7.5 Wiretap Code Rates Within A Passive Eavesdropping Scenario

In this section, we extend the optimization of the wiretap code rates for the adaptive and fixed-rate transmission schemes into an absolute passive eavesdropping scenario, where the average SNR of the eavesdropper's channel $\overline{\gamma}_E$ (in addition to C_E) is not known at Alice. To relax the assumption in the previous two sections that $\overline{\gamma}_E$ is known at Alice, we propose a new threat model, referred to as the annulus threat model. For this threat model, we derive closed-form expressions for the average effective secrecy throughput of the adaptive and fixed-rate transmission schemes, based on which the wiretap code rates are optimized.

7.5.1 Annulus Threat Model

Fig. 7.7 depicts a practical scenario where physical layer security may apply. In this scenario, the Wi-Fi point (Alice) and the legitimate user (Bob) are located inside a property (e.g., a house), but the eavesdropper (Eve) is bounded outside the property. In practice, Eve cannot be infinitely far from Alice. As such, in practical wiretap channels the distance between Alice and Eve should be larger than a specific value and less than another specific value. This motivates us to propose an annulus threat model. In the annulus threat model, we assume that Eve's location is uniformly distributed inside an annulus bounded by two concentric circles, where ρ_i and ρ_o are the radii of the inner circle and the outer circle, respectively, and Alice is at the center of the two concentric circles.

In the proposed annulus threat model, we denote the distance between Alice and Eve as ρ. Based on the path loss model, the average SNR of the eavesdropper's channel is a function of ρ, which can be expressed as [87]

$$\overline{\gamma}_E = c_0 \rho^{-\eta}, \tag{7.37}$$

where $c_0 = \overline{\gamma}_0 / \rho_r^{-\eta}$, $\overline{\gamma}_0$ is the reference average SNR of the eavesdropper's channel at the reference distance ρ_r, and η is the path loss exponent. In the previous sections, the effective secrecy throughput is derived as a function of $\overline{\gamma}_E$. In this section, we derive the average secrecy throughput over $\overline{\gamma}_E$ under the annulus threat model. To this end, we first present the pdf of ρ^2 in the following lemma.

***Lemma* 6** The square of the distance between Alice and Eve, ρ^2, follows a uniform distribution with ρ_i^2 and ρ_o^2 as the lower bound and upper bound, respectively, i.e., $\rho^2 \sim \mathbf{U}(\rho_i^2, \rho_o^2)$.

The proof of Lemma 6 is provided in the Appendix D.

7.5.2 Adaptive Transmission Scheme

It is highlighted that the adaptive transmission scheme represents a high complexity system where Bob feeds back C_B to Alice, and we only need to determine the value of R_E for this scheme since R_B is set as $R_B = C_B$. In order to optimize R_E, we first derive the average secrecy throughput of the adaptive transmission scheme for the annulus threat model in the following theorem.

***Theorem* 15** The average effective secrecy throughput of the adaptive transmission scheme for the annulus threat model is

$$\Psi_{a,t}(R_E, \rho_i, \rho_o) = (C_B - R_E) \times \left(1 - \sum_{j=0}^{N_E-1} \frac{2u^j}{j!} \frac{\gamma(v, u\rho_o^\eta) - \gamma(v, u\rho_i^\eta)}{(\rho_o^2 - \rho_i^2)\eta u^v}\right), \tag{7.38}$$

where $u = \left(2^{R_E} - 1\right)/c_0$, $v = j + 2/\eta$, and $\gamma(\cdot,\cdot)$ is the incomplete gamma function [124, Eq. (8.350.1)].

We present the proof of Theorem 15 in the following. Under the annulus threat model, the average effective secrecy throughput of the adaptive transmission scheme is

$$\Psi_{a,t}(R_E, \rho_i, \rho_o) = \mathbb{E}_\rho[\Psi_a(R_E)] = \int_{\rho_i^2}^{\rho_o^2} \frac{\Psi_a(R_E)}{\rho_o^2 - \rho_i^2} d\rho^2. \tag{7.39}$$

Substituting (7.10) and (7.37) into (7.39), we obtain

$$\begin{aligned}
\Psi_{a,t}(R_E, \rho_i, \rho_o) &= \int_{\rho_i^2}^{\rho_o^2} \frac{\Psi_a(R_E)}{\rho_o^2 - \rho_i^2} d\rho^2 \\
&= \frac{(C_B - R_E)}{\rho_o^2 - \rho_i^2} \int_{\rho_i^2}^{\rho_o^2} \left[1 - e^{-\frac{2^{R_E}-1}{c_0 \rho^{-\eta}}} \sum_{j=0}^{N_E-1} \frac{1}{j!} \left(\frac{2^{R_E}-1}{c_0 \rho^{-\eta}}\right)^j\right] d\rho^2 \\
&= (C_B - R_E) - \frac{(C_B - R_E)}{\rho_o^2 - \rho_i^2} \sum_{j=0}^{N_E-1} \frac{1}{j!} \left(\frac{2^{R_E}-1}{c_0}\right)^j \\
&\quad \times \left[\int_0^{\rho_o^2} \rho^{j\eta} e^{-\frac{2^{R_E}-1}{c_0}\rho^\eta} d\rho^2 - \int_0^{\rho_i^2} \rho^{j\eta} e^{-\frac{2^{R_E}-1}{c_0}\rho^\eta} d\rho^2\right].
\end{aligned} \tag{7.40}$$

We solve the integrals in (7.40) with the aid of [124, Eq. (3.381.8)], and obtain the desired result in (7.38) after some algebraic manipulations. This completes the proof of Theorem 15.

Using (7.38), the optimal value of R_E which maximizes the average effective secrecy throughput of the adaptive transmission scheme for the annulus threat model can be determined through

$$R_{E,t}^{\ddagger} = \underset{0<R_E<C_B}{\operatorname{argmax}} \Psi_{a,t}(R_E, \rho_i, \rho_o). \tag{7.41}$$

Substituting $R_{E,t}^{\ddagger}$ into (7.38), we obtain the maximum average effective secrecy throughput of the adaptive transmission scheme for the annulus threat model, denoted as $\Psi_{a,t}^{*}(\rho_i, \rho_o)$.

7.5.3 Fixed-Rate Transmission Scheme

We note that the fixed-rate transmission scheme represents a lower complexity system where Bob does not feed back C_B to Alice, and we have to jointly determine the values of R_B and R_E. In order to optimize (R_B, R_E), we first derive the average effective secrecy throughput of the fixed-rate transmission scheme for the annulus threat model in the following theorem.

***Theorem* 16** The average effective secrecy throughput of the fixed-rate transmission scheme for the annulus threat model is

$$\Psi_{f,t}(R_B, R_E, \rho_i, \rho_o) = (R_B - R_E) e^{-\frac{2^{R_B}-1}{\bar{\gamma}_B}} \left(1 - \sum_{j=0}^{N_E-1} \frac{2w^j}{j!} \frac{\gamma(v, w\rho_o^{\eta}) - \gamma(v, w\rho_i^{\eta})}{(\rho_o^2 - \rho_i^2)\eta w^v}\right), \tag{7.42}$$

where $w = \left(2^{R_E} - 1\right)/c_0$.

The proof of Theorem 16 is provided in the following. Under the annulus threat model, the average effective secrecy throughput of the fixed-rate transmission scheme is

$$\Psi_{f,t}(R_B, R_E, \rho_i, \rho_o) = \mathbb{E}_{\rho}[\Psi_f(R_B, R_E)] = \int_{\rho_i^2}^{\rho_o^2} \frac{\Psi_f(R_B, R_E)}{\rho_o^2 - \rho_i^2} d\rho^2. \tag{7.43}$$

Substituting (7.20) and (7.37) into (7.43), we obtain

$$\begin{aligned}\Psi_{f,t}(R_B,R_E,\rho_i,\rho_o) &= \int_{\rho_i^2}^{\rho_o^2} \frac{\Psi_f(R_B,R_E)}{\rho_o^2-\rho_i^2} d\rho^2 \\ &= \frac{(R_B-R_E)}{\rho_o^2-\rho_i^2} e^{-\frac{2^{R_B}-1}{\overline{\gamma}_B}} \int_{\rho_i^2}^{\rho_o^2} \left[1-e^{-\frac{2^{R_E}-1}{c_0\rho^{-\eta}}} \sum_{j=0}^{N_E-1} \frac{1}{j!} \left(\frac{2^{R_E}-1}{c_0\rho^{-\eta}}\right)^j\right] d\rho^2 \\ &= (R_B-R_E) e^{-\frac{2^{R_B}-1}{\overline{\gamma}_B}} \left[1-\frac{1}{\rho_o^2-\rho_i^2} \sum_{j=0}^{N_E-1} \frac{1}{j!} \left(\frac{2^{R_E}-1}{c_0}\right)^j \right. \\ &\quad \left. \times \left(\int_0^{\rho_o^2} \rho^{j\eta} e^{-\frac{2^{R_E}-1}{c_0}\rho^\eta} d\rho^2 - \int_0^{\rho_i^2} \rho^{j\eta} e^{-\frac{2^{R_E}-1}{c_0}\rho^\eta} d\rho^2\right)\right].\end{aligned} \tag{7.44}$$

We solve the integrals in (7.44) with the aid of [124, Eq. (3.381.8)], and obtain the result in (7.42) after some algebraic manipulations.

Using (7.42), the optimal (R_B, R_E) which maximizes the average effective secrecy throughput of the fixed-rate transmission scheme for the annulus threat model can be determined through

$$(R_B,R_E)_t^* = \underset{0<R_B,0<R_E<R_B}{\operatorname{argmax}} \Psi_{f,t}(R_B,R_E,\rho_i,\rho_o). \tag{7.45}$$

The values of R_B and R_E in $(R_B,R_E)_t^*$ are denoted as $R_{B,t}^*$ and $R_{E,t}^*$, respectively. Substituting $(R_B,R_E)_t^*$ into (7.42), we obtain the maximum average effective secrecy throughput of the fixed-rate transmission scheme for the annulus threat model, denoted as $\Psi_{f,t}^*(\rho_i,\rho_o)$.

7.5.4 Numerical Results

In this subsection, we present numerical results to examine the impact of ρ_i and ρ_o on the optimal wiretap code rates and the maximum average effective secrecy throughput of the adaptive and fixed-rate transmission schemes.

In Fig. 7.8, we plot the optimal redundancy rate, $R_{E,t}^\ddagger$, and the maximum average effective secrecy throughput, $\Psi_{a,t}^*(\rho_i,\rho_o)$, of the adaptive transmission scheme versus ρ_i and ρ_o. In this figure, we first observe that $R_{E,t}^\ddagger$ decreases as ρ_i increases, which

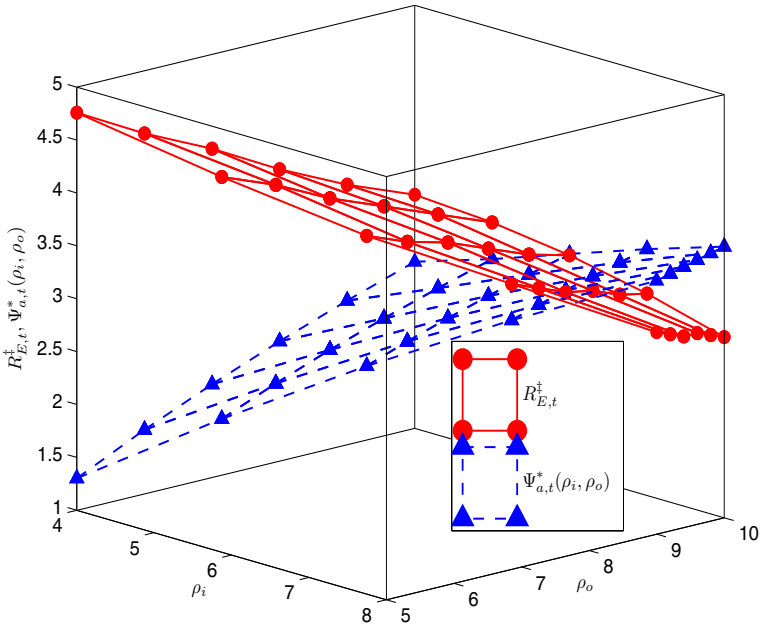

Figure 7.8: Optimal redundancy rate, $R^{\dagger}_{E,t}$, and the maximum average effective secrecy throughput, $\Psi^{*}_{a,t}(\rho_i,\rho_o)$, of the adaptive transmission scheme versus ρ_i and ρ_o for $N_E = 2$, $\gamma_B = 20$ dB, $\overline{\gamma}_0 = 30$ dB, $\rho_r = 1$, and $\eta = 3$.

reveals that the optimal redundancy rate used to confuse Eve can be reduced by increasing the inner boundary. We also observe that $R^{\ddagger}_{E,t}$ decreases as ρ_o increases. This can be explained by the fact that a larger outer boundary ρ_o means Eve is statistically further from Alice. Moreover, we observe $\Psi^{*}_{a,t}(\rho_i,\rho_o)$ increases as ρ_i increases, which indicates that the further the inner boundary is from Alice, the better secrecy performance the adaptive transmission scheme achieves. As such, a higher average effective secrecy throughput can be achieved through enlarging the inner boundary. We further observe that $\Psi^{*}_{a,t}(\rho_i,\rho_o)$ increases as ρ_o increases. This can be explained by the fact that $\Psi^{*}_{a,t}(\rho_i,\rho_o)$ is averaged over $\overline{\gamma}_E$ in the annulus threat model, and a larger ρ_o means that Eve is further from Alice on average since in the annulus threat model Eve's location is uniformly distributed in the annulus.

In Fig. 7.9, we plot the optimal wiretap code rates, $R^{*}_{B,t}$ and $R^{*}_{E,t}$, and the maximum average effective secrecy throughput, $\Psi^{*}_{f,t}(\rho_i,\rho_o)$, of the fixed-rate transmission scheme versus ρ_i and ρ_o. In this figure, we first observe that both $R^{*}_{B,t}$ and $R^{*}_{E,t}$

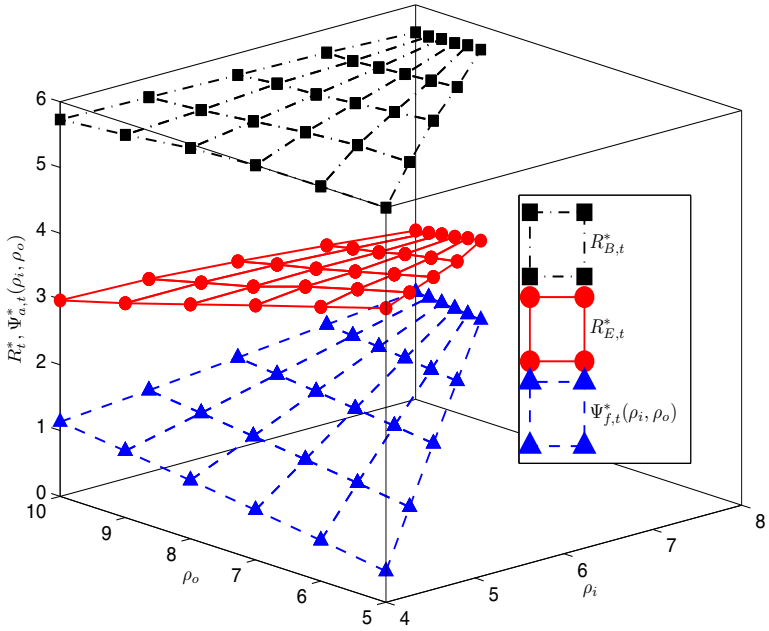

Figure 7.9: Optimal wiretap code rates, $R^*_{B,t}$ and $R^*_{E,t}$, and the maximum average effective secrecy throughput, $\Psi^*_{f,t}(\rho_i, \rho_o)$, of the fixed-rate transmission scheme versus ρ_i and ρ_o for $N_E = 2$, $\overline{\gamma}_B = 20$ dB, $\overline{\gamma}_0 = 30$ dB, $\rho_r = 1$, and $\eta = 3$.

decrease as ρ_i increases, and $R^*_{E,t}$ is more sensitive to ρ_i than $R^*_{B,t}$, which results in $\Psi^*_{f,t}(\rho_i, \rho_o)$ increasing as ρ_i increases. The above observation indicates that the further the inner boundary is from Alice, the better secrecy performance the fixed-rate transmission scheme achieves. We also observe that both $R^*_{B,t}$ and $R^*_{E,t}$ increase as ρ_o increases, and $R^*_{E,t}$ is more sensitive to ρ_o than $R^*_{B,t}$, which results in $\Psi^*_{f,t}(\rho_i, \rho_o)$ increasing as ρ_o increases. This is can be explained by the fact that $\Psi^*_{f,t}(\rho_i, \rho_o)$ is averaged over $\overline{\gamma}_E$, and a larger ρ_o means that Eve is statistically further from Alice.

7.6 Summary

In this chapter, we proposed a new framework in order to optimize the wiretap code rates for the SISOME wiretap channel. We considered the passive eavesdropping scenario in which even the average SNR of the eavesdropper's channel is unknown at the transmitter. The framework is based on a new performance metric, the effective

secrecy throughput, which captures explicitly the reliability constraint and secrecy constraint of wiretap channels. The framework does not require a determination of the secrecy outage probability *a priori* or subjectively, and therefore is very pragmatic.

Chapter 8

Conclusions and Future Works

We conclude this thesis by summarizing our contributions and discussing some potential future works.

8.1 Thesis Conclusions

In the first half of this thesis (Chapter 2, Chapter 3, and Chapter 4), new optimal LVSs were developed in order to verify claimed locations, leading to the following detailed contributions.

In Chapter 2, we developed an information-theoretic framework to optimize an LVS, in which the objective mutual information between the input and output data of the LVS is maximized. We also developed practical threat models for a non-colluding malicious user attack scenario, and investigated the performance of the LVS in terms of its input/output mutual information. The main results of Chapter 2 are summarized as follows.

- Our analysis revealed that the developed information-theoretic framework of an LVS is more robust to estimation errors in the *a prior* probabilities relative to tranditional Bayesian frameworks.

- We identified the threshold value which maximizes the input/output mutual

information, and then proved that the LRT is the decision rule that maximizes the input/output mutual information, and leads to the optimal information-theoretic LVS.

- Our analysis indicated that our LVS leads to an optimal solution for most realistic attack scenarios, where a malicious user outside a network region is attempting to spoof that he is within the network region. We further showed how optimality is approached as the malicious user moves further from the network region.

In Chapter 3, we analyzed the optimal detection performances of the RSS-based LVS and the DRSS-based LVS under the realistic setting of spatially correlated shadowing. To this end, we determined the optimal attack strategies of an attacker against the RSS-based and DRSS-based LVSs, in which the optimal transmit power and the best true location to launch an attack are provided. The main results of Chapter 3 are provided as follows.

- Our analysis demonstrated that the spatial correlation of the shadowing leads to a significant performance improvement for the RSS-based LVS and the DRSS-based LVS relative to the case with uncorrelated shadowing .

- The detection performance of the DRSS-based LVS was proved to be identical to that of the RSS-based LVS for all levels of correlated shadowing, as long as the attacker optimizes its transmit power. Only in the case where the attacker does not optimize its transmit power, did we find the performance of the RSS-based LVS to be better than the DRSS-based LVS.

In Chapter 4, we proposed and examined LVSs focusing on VANETs in the realistic setting of Rician fading channels. In these LVSs, a single authorized BS equipped with multiple antennas aims to detect an attacker that is spoofing its claimed location. The main results of Chapter 4 are listed as follows.

- We first determined the optimal attack strategy of an attacker, in which the optimal transmit power and the optimal beamformer for the attacker at an arbitrary location are derived, and then the optimal locations of the attacker were identified. Our analysis indicated that these optimal locations are determined solely by a single direction (due to the ability of the attacker to vary its transmit power and beamformer).

- Our analysis quantified the optimal LVSs performance as a function of the Rician K-factor of the legitimate channel and the tracking information of claimed locations, leading to the conclusion that the optimal LVSs performance increases significantly as the Rician K-factor increases or the tracking information accumulates.

- Our analysis revealed that the optimal LVSs performance limit is independent of the properties of the malicious channel, such as the Rician K-factor and noise levels, provided the malicious vehicle's antenna number is above a specified value.

In the second half of this thesis (Chapter 5, Chapter 6, and Chapter 7), robust transmission strategies, which utilized verified location information to enhance physical layer security, were developed, leading to the following additional detailed contributions.

In Chapter 5, we proposed and analyzed a new optimal LBB scheme for the Rician wiretap channel. In our LBB scheme the two key inputs are the locations of the legitimate receiver and the potential eavesdropper. Notably, the proposed scheme does not require the CSI of the main channel or the eavesdropper's channel, making it easy to deploy in a host of application settings. The main results of Chapter 5 are summarized as follows.

- We first derived the secrecy outage probability of the LBB scheme in a closed-form expression, which is valid for arbitrary values of Rician K-factors of the

main channel and the eavesdropper's channel. We then determined the optimal location-based beamformer and the minimum secrecy outage probability for the LBB scheme.

- In order to fully appreciate the gains of the LBB scheme, we also analyzed, for comparison, the secrecy performance of a NB scheme. The performance comparison between the LBB and NB schemes explored the value of the location information provided by the intended receiver and eavesdropper in enhancing wireless physical layer security.

In Chapter 6, new TAS schemes which examine the trade-off between feedback overhead and secrecy performance in MIMO wiretap channels were proposed and analyzed. To provide valuable insights into the proposed new schemes, we derived new closed-form expressions for their secrecy outage probabilities. The main results of Chapter 6 are presented as follows.

- Our formal analysis indicated that our TAS-Alamouti scheme achieves a lower secrecy outage probability than the traditional single TAS scheme conditioned on the SNR of the main channel being larger than a specific value. The performance enhancements are at the cost of negligible extra feedback relative to the single TAS and we showed how in some antenna configurations no additional feedback is required in order to realize such performance enhancements.

- We optimized power allocation across the selected antennas in the TAS-Alamouti scheme, leading to the TAS-Alamouti-OPA scheme. Our conducted analysis revealed that the TAS-Alamouti-OPA outperforms the single TAS unconditionally.

In Chapter 7, we developed a new framework for optimizing wiretap code rates for SISOME wiretap channels when the capacity of the eavesdropper's channel was not available at the transmitter. Our framework was based on a new metric, referred to

as the effective secrecy throughput, which explicitly captured both the reliability constraint and the secrecy constraint of wiretap channels. The main results of Chapter 7 are summarized as follows.

- Utilizing our new framework, we optimized wiretap code rates for adaptive and fixed-rate transmission schemes when the capacity of the main channel was available and unavailable at the transmitter, respectively.
- The above optimizations were further extended into an absolute passive eavesdropping scenario where even the eavesdropper's location is not available at the transmitter. For this scenario, we derived closed-form expressions for the average effective secrecy throughput of the adaptive and the fixed-rate transmission schemes.

8.2 Future Works

Finally we present some thoughts on what we believe to be the major issues in relation to future works in location verification and physical layer security for wireless communications.

This thesis has focussed on theoretical investigations of optimal LVSs. It would be useful if some future work could focus on experimental implementations of our developed location verification algorithms in real networks (e.g., VANETs). Some potential challenges and research directions in such deployments are detailed as follows. (i) Future research effort should focus on the prediction of channel conditions based on limited resources. Such wireless channel identification is a major issue since *a priori* experiments may not be attainable to determine channel parameters (e.g., Rician K-factors, path loss exponent) in some real networks. (ii) The processing time delay is a key aspect for incorporating LVSs in real networks and will be of practical concern in the immediate future. For example, in VANETs the frequency of updated claimed locations by a vehicle is expected to be 10 Hz, and thus the processing time

delay of a specific LVS, which is embedded in such VANETs, should be less than 0.1 second. It would be useful to determine the network limitations imposed on real networks (e.g., number of vehicles per base station, server processing capabilities) in order to guarantee such tight delay requirements. (iii) Strategies of fusing local (distributed) LVS decisions into a final decision in large scale networks also requires future research effort. In such fusing strategies, the trade-off between the detection performance and processing time delay of an LVS embedded in a real network should be be carefully investigated.

Physical layer security in wireless communication has received considerable theoretical research effort. However, very few experimental deployments have been conducted in order to test and verify transmission schemes developed in the context of physical layer security. Our developed transmission schemes (e.g., LBB and TAS-Alamouti schemes) are candidates for such deployments since they are of low complexity and do not require high feedback overhead. However, some challenges remain in experimental implementations of our transmission schemes. A major challenge is how to achieve accurate channel parameters required by the transmission schemes. For example, in mobile networks the average SNR of a wireless channel is dynamic and thus is hard to measure or predict. Another challenge is to examine the impact of real world limitations imposed on our transmission schemes in real large scale networks. For example, deployment of an optimal location-based beamformer for multiple intended receivers and potential eavesdroppers again raises issues of processing capabilities and limitations.

As a final thought we note that location verification in the context of quantum communication systems has previously been considered (e.g., [135–139]), and it has been argued that such systems are able to securely verify a location under all known threat models [138]. Use of such quantum systems are of particular interest since, as stated in earlier this thesis, in a purely classical system any defensive strategy for an LVS is ultimately doomed if the colluding adversary is in a formal sense afforded unlimited resources (e.g., an unlimited number of attackers with no constraints imposed

on their locations). However, the implementation of quantum location verification in the context of wireless networks faces many unsolved challenges, such as the development of long-term quantum memory and the integration quantum information transfer between devices (most likely in the form of weak laser beams). Nevertheless real quantum information networks are already deployed over large scales for the purposes of quantum cryptography applications, and their integration into all forms of classical communication systems is only a matter of time. Of particular interest to the work outlined in this thesis would be a study of how to optimally integrate quantum information into the LVS and its associated communication infrastructure structure. Since quantum information is likely to remain the most valuable resource in such combined classical/quantum networks, discovering how to minimize the use of such quantum resources whilst still obtaining unconditional location verification would likely be a worthwhile endeavor.

Appendix A

Proof of Theorem 4

We provide here the proof of Theorem 4 presented in Chapter 3 on page 70. Based on (3.26), (3.27), (3.48), and (3.49), we can see that $\alpha_R^o(\mathbf{x}_t)$, $\beta_R^o(\mathbf{x}_t)$, $\alpha_D(\mathbf{x}_t)$, and $\beta_D(\mathbf{x}_t)$ are all in the form of a $\mathcal{Q}$ function. We denote $\alpha_R^o(\mathbf{x}_t) = \mathcal{Q}(\zeta_R^o)$, $\beta_R^o(\mathbf{x}_t) = \mathcal{Q}(\eta_R^o)$, $\alpha_D(\mathbf{x}_t) = \mathcal{Q}(\zeta_D)$, and $\beta_D(\mathbf{x}_t) = \mathcal{Q}(\eta_D)$. In order to prove $\alpha_R^o(\mathbf{x}_t) = \alpha_D(\mathbf{x}_t)$ and $\beta_R^o(\mathbf{x}_t) = \beta_D(\mathbf{x}_t)$ for $\lambda_R = \lambda_D$, we only need to prove $\zeta_R^o - \eta_R^o = \zeta_D - \eta_D$. As per (3.26), (3.27), (3.48), and (3.49), in order to prove $\zeta_R^o - \eta_R^o = \zeta_D - \eta_D$ (such as to prove Theorem 4) we have to prove the following equation

$$(\mathbf{w}–\mathbf{u})^T \mathbf{R}^{-1} (\mathbf{w}–\mathbf{u}) = (\mathbf{\Delta v}–\mathbf{\Delta u})^T \mathbf{D}^{-1} (\mathbf{\Delta v}–\mathbf{\Delta u}) . \tag{A.1}$$

Based on the SVD of $\mathbf{R}$, we can transform the RSS observation vector $\mathbf{y}$ into another observation vector $\mathbf{y}'$ by rotating and scaling[1]. We can then obtain the DRSS observations from $\mathbf{y}'$ instead of $\mathbf{y}$. The transformation from $\mathbf{y}$ to $\mathbf{y}'$ is unique since the singular values of $\mathbf{R}$ are unique. In addition, $\mathbf{y}$ follows a multivariate normal distribution. As such, the transformation from $\mathbf{y}$ to $\mathbf{y}'$ keeps all the properties of $\mathbf{y}$ in $\mathbf{y}'$, which means the performance of an LVS based on $\mathbf{y}$ is identical to the performance of an LVS based on $\mathbf{y}'$ [140, 141]. Therefore, in order to prove Theorem 4 we only have

[1]The covariance matrix $\mathbf{R}$ is a real positive-definite symmetric matrix, and thus the SVD of $\mathbf{R}$ can be written as $\mathbf{R} = \mathbf{S}\mathbf{R}'\mathbf{S}^T$. As such, $\mathbf{y}'$ is given by $\mathbf{y}' = \mathbf{R}'^{\frac{1}{2}}\mathbf{S}\mathbf{y}$ and the covariance matrix of $\mathbf{y}'$ will be $\mathbf{I}_N$.

to prove (A.1) for $\mathbf{R} = \mathbf{I}_N$. Denoting $\mathbf{g} = \mathbf{v} - \mathbf{u}$, we have $\Delta v_m - \Delta u_m = g_m - g_N$. Substituting $\mathbf{R} = \mathbf{I}_N$ into $\mathbf{w}$ given in (3.16), we obtain

$$\mathbf{w} - \mathbf{u} = \mathbf{g} - \frac{\mathbf{g}^T \mathbf{R}^{-1} \mathbf{1}_N}{\mathbf{1}_N^T \mathbf{R}^{-1} \mathbf{1}_N} \mathbf{1}_N = \mathbf{g} - \left(\frac{1}{N} \sum_{j=1}^{N} g_j \right) \mathbf{1}_N. \tag{A.2}$$

With regard to the left side of (A.1), for $\mathbf{R} = \mathbf{I}_N$ we have

$$\begin{aligned}
(\mathbf{w}–\mathbf{u})^T \mathbf{R}^{-1} (\mathbf{w}–\mathbf{u}) &= \sum_{i=1}^{N} \left(g_i - \frac{1}{N} \sum_{j=1}^{N} g_j \right)^2 \\
&= \sum_{i=1}^{N} \left[g_i^2 - \frac{2}{N} g_i \sum_{j=1}^{N} g_j + \frac{1}{N^2} \left(\sum_{j=1}^{N} g_j \right)^2 \right] \\
&= \left[\sum_{i=1}^{N} g_i^2 - \frac{2}{N} \left(\sum_{i=1}^{N} g_i \right) \left(\sum_{j=1}^{N} g_j \right) + \frac{1}{N} \left(\sum_{j=1}^{N} g_j \right)^2 \right] \\
&= \left[\sum_{i=1}^{N} g_i^2 - \frac{1}{N} \left(\sum_{i=1}^{N} g_i \right)^2 \right].
\end{aligned} \tag{A.3}$$

As per the definition of $\mathbf{D}$ given in (3.36), for $\mathbf{R} = \mathbf{I}_N$ we have

$$\mathbf{D} = \mathbf{I}_{N-1} + \mathbf{1}_{(N-1)\times(N-1)}, \tag{A.4}$$

where $\mathbf{1}_{(N-1)\times(N-1)})$ is the $(N-1) \times (N-1)$ matrix with all elements set to unity. Then, based on the Sherman-Morrison formula [142], we have

$$\begin{aligned}
\mathbf{D}^{-1} &= \left[\mathbf{I}_{N-1} + \mathbf{1}_{(N-1)\times(N-1)} \right]^{-1} \\
&= \left[\mathbf{I}_{N-1} + \mathbf{1}_{(N-1)} \times \mathbf{1}_{(N-1)}^T \right]^{-1} \\
&= \left[\mathbf{I}_{N-1}^{-1} - \frac{\mathbf{I}_{N-1}^{-1} \mathbf{1}_{(N-1)\times(N-1)} \mathbf{I}_{N-1}^{-1}}{1 + \mathbf{1}_{(N-1)}^T \mathbf{I}_{N-1}^{-1} \mathbf{1}_{(N-1)}} \right] \\
&= \left[\mathbf{I}_{N-1} - \frac{\mathbf{1}_{(N-1)\times(N-1)}}{N} \right].
\end{aligned} \tag{A.5}$$

Substituting (A.5) into the right side of (A.1), we have

$$\begin{aligned}
(\boldsymbol{\Delta}\mathbf{v}-\boldsymbol{\Delta}\mathbf{u})^T\,\mathbf{D}^{-1}\,(\boldsymbol{\Delta}\mathbf{v}-\boldsymbol{\Delta}\mathbf{u}) &= (\boldsymbol{\Delta}\mathbf{v}-\boldsymbol{\Delta}\mathbf{u})^T\left[\mathbf{I}_{N-1}-\frac{\mathbf{1}_{(N-1)\times(N-1)}}{N}\right](\boldsymbol{\Delta}\mathbf{v}-\boldsymbol{\Delta}\mathbf{u}) \\
&= (\boldsymbol{\Delta}\mathbf{v}-\boldsymbol{\Delta}\mathbf{u})^T\,\mathbf{I}_{N-1}\,(\boldsymbol{\Delta}\mathbf{v}-\boldsymbol{\Delta}\mathbf{u}) \\
&\quad -\frac{1}{N}\,(\boldsymbol{\Delta}\mathbf{v}-\boldsymbol{\Delta}\mathbf{u})^T\,\mathbf{1}_{(N-1)}\times\mathbf{1}_{(N-1)}^T\,(\boldsymbol{\Delta}\mathbf{v}-\boldsymbol{\Delta}\mathbf{u}) \\
&= \sum_{i=1}^{N-1}(g_i-g_N)^2-\frac{1}{N}\left[\sum_{i=1}^{N-1}(g_i-g_N)\right]^2 \\
&= \sum_{i=1}^{N}(g_i-g_N)^2-\frac{1}{N}\left[\sum_{i=1}^{N}(g_i-g_N)\right]^2 \\
&= \sum_{i=1}^{N}(g_i-g_N)^2-\frac{1}{N}\sum_{i=1}^{N}(g_i-g_N)\left[\sum_{j=1}^{N}(g_j-g_N)\right] \\
&= \left[\sum_{i=1}^{N}g_i^2-\frac{1}{N}\left(\sum_{i=1}^{N}g_i\right)^2\right]. \qquad \text{(A.6)}
\end{aligned}$$

Comparing (A.3) with (A.6), we can see that we have proved (A.1) for $\mathbf{R}=\mathbf{I}_N$. This completes the proof of Theorem 4.

Appendix B

Proof of Theorem 5

We provide here the proof of Theorem 5 presented in Chapter 4 on page 89. Substituting (4.5) into (4.10), we have

$$D_{KL}\left(f\left(\mathbf{y}|p_1,\mathbf{b}_1,\mathbf{x}_1,\mathcal{H}_1\right)||f\left(\mathbf{y}|\mathcal{H}_0\right)\right) = \underbrace{\mathrm{tr}(\mathbf{R}_0^{-1}\mathbf{R}_1) - N_B - \ln\left(\frac{\det\mathbf{R}_1}{\det\mathbf{R}_0}\right)}_{h_1(p_1)} + \underbrace{(\mathbf{m}_0-\mathbf{m}_1)^\dagger\mathbf{R}_0^{-1}(\mathbf{m}_0-\mathbf{m}_1)}_{h_2(p_1,\mathbf{b}_1)}. \tag{B.1}$$

Based on (B.1), we know that only the term $h_2\left(p_1,\mathbf{b}_1\right)$ is a function of $\mathbf{b}_1$. As such, we first derive the optimal $\mathbf{b}_1$ that minimizes $h_2\left(p_1,\mathbf{b}_1\right)$ for a given p_1. Given the format of $\mathbf{R}_0$ presented in (4.7), we can see that $h_2\left(p_1,\mathbf{b}_1\right)$ is minimized when $\|\mathbf{m}_0-\mathbf{m}_1\|^2$ is minimized. Defining $\mathbf{G} = \sqrt{p_1\mathrm{g}(d_1)K_1/(1+K_1)}\,\overline{\mathbf{H}}_1$, we have

$$\begin{aligned} h_3\left(\mathbf{b}_1\right) &\triangleq \|\mathbf{m}_0-\mathbf{m}_1\|^2 \\ &= \mathbf{b}_1^\dagger\mathbf{G}^\dagger\mathbf{G}\mathbf{b}_1 - \mathbf{m}_0^\dagger\mathbf{G}\mathbf{b}_1 - \mathbf{b}_1^\dagger\mathbf{G}^\dagger\mathbf{m}_0 + \mathbf{m}_0^\dagger\mathbf{m}_0. \end{aligned} \tag{B.2}$$

Performing the SVD for the symmetric positive semidefinite matrix $\mathbf{Q} \triangleq \mathbf{G}^\dagger\mathbf{G}$, we have

$$\mathbf{U}\mathbf{V}\mathbf{U}^\dagger = \mathbf{Q}. \tag{B.3}$$

We note that $\mathbf{Q}$ is a rank-1 matrix and we denote the unique eigenvalue of $\mathbf{Q}$ as η. Then, we have

$$\eta = \|\mathbf{Q}\| = \frac{p_1 g(d_1) K_1 N_B N_1}{1+K_1}. \tag{B.4}$$

Denoting $\mathbf{b}_1 = \mathbf{U}\mathbf{p}$ (i.e., $\mathbf{p} = \mathbf{U}^\dagger \mathbf{b}_1$), following (B.2) and (B.3) we have

$$h_3(\mathbf{b}_1) = \mathbf{p}^\dagger \mathbf{V}\mathbf{p} - \mathbf{m}_0^\dagger \mathbf{G}\mathbf{U}\mathbf{p} - \mathbf{p}^\dagger \mathbf{U}^\dagger \mathbf{G}^\dagger \mathbf{m}_0 + \mathbf{m}_0^\dagger \mathbf{m}_0. \tag{B.5}$$

We note that $\mathbf{U}^\dagger \mathbf{G}^\dagger \mathbf{m}_0$ is a complex $N_1 \times 1$ vector and we denote the i-th complex element of $\mathbf{U}^\dagger \mathbf{G}^\dagger \mathbf{m}_0$ as $c_{Ri} + j c_{Ii}$. Since $\mathbf{Q}$ is a rank-1 matrix, we have $\mathbf{U}^\dagger \mathbf{G}^\dagger \mathbf{m}_0[i] = 0$ for $i = 2, 3, \cdots, N_1$. Denoting the i-th complex element of $\mathbf{p}$ as $p_{Ri} + j p_{Ii}$, following (B.5) we have

$$h_3(\mathbf{b}_1) = \eta(p_{R1}^2 + p_{I1}^2) - 2(c_{R1} p_{R1} + c_{I1} p_{I1}) + \mathbf{m}_0^\dagger \mathbf{m}_0. \tag{B.6}$$

Using (B.6), we have $p_{R1} = c_{R1}\eta$ and $p_{I1} = c_{I1}\eta$ in order to minimize $h_3(\mathbf{b}_1)$ without any constraints, which results in

$$\mathbf{p}^o[1] = \mathbf{U}^\dagger \mathbf{G}^\dagger \mathbf{m}_0[1]/\eta, \tag{B.7}$$

where $\mathbf{p}^o$ denotes the optimal $\mathbf{p}$ that minimizes $h_3(\mathbf{p})$ for a given p_1. We note that there is a constraint for the minimization of $h_3(\mathbf{b}_1)$, which is $\|\mathbf{b}_1\| = 1$ (i.e., $\|\mathbf{p}\| = 1$ since $\mathbf{U}$ is a unitary matrix). As such, we have to guarantee $c_{R1}^2 + c_{I1}^2 \leq \eta$, which means that we have to guarantee $\|\mathbf{U}^\dagger \mathbf{G}^\dagger \mathbf{m}_0\|/\eta \leq 1$. Based on the definitions of $\mathbf{G}$ and $\mathbf{m}_0$, and noting $\mathbf{t}_1 \mathbf{t}_1^\dagger = N_1$ we have

$$\begin{aligned}
\|\mathbf{U}^\dagger \mathbf{G}^\dagger \mathbf{m}_0\|^2 &= \|\mathbf{G}^\dagger \mathbf{m}_0\|^2 \\
&= \frac{p_0 \mathrm{g}(d_0) K_0 N_0}{1+K_0} \frac{p_1 \mathrm{g}(d_1) K_1}{1+K_1} \mathbf{r}_0^\dagger \mathbf{r}_1 \mathbf{t}_1 \mathbf{t}_1^\dagger \mathbf{r}_1^\dagger \mathbf{r}_0 \\
&= \frac{p_0 \mathrm{g}(d_0) K_0 N_0}{1+K_0} \frac{p_1 \mathrm{g}(d_1) K_1 N_1}{1+K_1} |\mathbf{r}_1^\dagger \mathbf{r}_0|^2.
\end{aligned} \tag{B.8}$$

We also note that the maximum value of $|\mathbf{r}_1^\dagger \mathbf{r}_0|^2$ is N_B^2, which is achieved when $\mathbf{r}_1 = \mathbf{r}_0$. Then, as per (B.4) we have

$$\frac{\|\mathbf{U}^\dagger \mathbf{G}^\dagger \mathbf{m}_0\|}{\eta} \leq \underbrace{\sqrt{\frac{p_0 \mathrm{g}(d_0) K_0}{1+K_0}} \sqrt{\frac{1+K_1}{p_1 \mathrm{g}(d_1) K_1}} \sqrt{\frac{N_0}{N_1}}}_{\mathcal{L}(N_1)}. \tag{B.9}$$

In order to guarantee $\mathcal{L}(N_1) \leq 1$, the malicious vehicle has to guarantee $N_1 \geq N_1^*$, where N_1^* is obtained by setting $\mathcal{L}(N_1) = 1$ and is given by

$$N_1^* = \left\lceil \max\left\{2, \frac{p_0 g(d_0) K_0 N_0}{K_1[p_0 g(d_0) + (1+K_0)(\sigma_0^2 - \sigma_1^2)]}\right\}\right\rceil. \tag{B.10}$$

The reason for $N_1^* \geq 2$ is that the minimum dimension of $\mathbf{p}$ must be 2 if $\mathbf{r}_1$ is to remain a function of θ_1. We assume the malicious vehicle can guarantee $N_1 \geq N_1^*$, and therefore guarantee $\|\mathbf{U}^\dagger \mathbf{G}^\dagger \mathbf{m}_0\|/\eta \leq 1$. As such, the optimal solution $\mathbf{p}^o[1] = \mathbf{U}^\dagger \mathbf{G}^\dagger \mathbf{m}_0[1]/\eta$ can always be achieved. This optimal solution indicates that $\mathbf{p}^o[i]$, for $i \geq 2$, can take any values in order to realize $\|\mathbf{p}^o\| = 1$.

We next derive the optimal value of p_1. Substituting $\mathbf{p}^o[1] = \mathbf{U}^\dagger \mathbf{G}^\dagger \mathbf{m}_0[1]/\eta$ into (B.5), we have

$$h_3(\mathbf{b}_1^o) = \mathbf{m}_0^\dagger \mathbf{m}_0 - \frac{\|\mathbf{U}^\dagger \mathbf{G}^\dagger \mathbf{m}_0\|^2}{\eta} = \frac{p_0 g(d_0) K_0 N_0}{1+K_0}\left(N_B - \frac{|\mathbf{r}_1^\dagger \mathbf{r}_0|^2}{N_B}\right), \tag{B.11}$$

where $\mathbf{b}_1^o = \mathbf{U}\mathbf{p}^o$. We note that $|\mathbf{r}_1^\dagger \mathbf{r}_0|^2$ is a function of only N_B, θ_0, and θ_1. Thus, $h_3(\mathbf{b}_1^o)$ is not a function of p_1 anymore. Based on (B.1), we know that $h_1(p_1)$ is a function of only p_1. This indicates that the optimal p_1 is the one that minimizes $h_1(p_1)$. After some algebra, we can show that that $h_1(p_1)$ is minimized when $\mathbf{R}_0 = \mathbf{R}_1$, which results in the desirable result in (4.12). We note that to achieve (4.12) we require $\sigma_1^2 < p_0 g(d_0)/(1+K_0) + \sigma_0^2$. This is reasonable as the channel noise variance will be lower than the useful signal power. Finally, substituting $p_1^*(\mathbf{x}_1)$ into (B.7) we obtain the desirable result in (4.13).

We note that if the condition $N_1 \geq N_1^*$ cannot be guaranteed, the minimum KL divergence for any given $\mathbf{x}_1$ will be larger than that for $N_1 \geq N_1^*$. To prove this statement, we have to prove the following equation

$$\begin{aligned} &D_{KL}\left(f\left(\mathbf{y}|p_1'(\mathbf{x}_1), \mathbf{b}_1'(\mathbf{x}_1), \mathbf{x}_1, \mathcal{H}_1\right) || f\left(\mathbf{y}|\mathcal{H}_0\right)\right) \\ &\qquad \geq D_{KL}\left(f\left(\mathbf{y}|p_1^*(\mathbf{x}_1), \mathbf{b}_1^*(\mathbf{x}_1), \mathbf{x}_1, \mathcal{H}_1\right) || f\left(\mathbf{y}|\mathcal{H}_0\right)\right), \end{aligned} \tag{B.12}$$

where $p_1'(\mathbf{x}_1)$ and $\mathbf{b}_1'(\mathbf{x}_1)$ denote the optimal values of p_1 and $\mathbf{b}_1$ under the condition $N_1 < N_1^*$ for any given $\mathbf{x}_1$. Following (B.6), we have $h_3(\mathbf{b}_1'(\mathbf{x}_1)) \geq h_3(\mathbf{b}_1^*(\mathbf{x}_1))$. This is

due to the fact that $\mathbf{b}'_1(\mathbf{x}_1)$ minimizes $h_3(\mathbf{b}_1)$ under the constraint $p_{R1}^2+p_{I1}^2 \leq 1$, but $\mathbf{b}^*_1(\mathbf{x}_1)$ minimizes $h_3(\mathbf{b}_1)$ without any constraints. Noting $h_1(p^*_1(\mathbf{x}_1)) = 0$, we have $h_1(p'_1(\mathbf{x}_1)) \geq h_1(p^*_1(\mathbf{x}_1))$. This is due to $h_1(p_1) \geq 0$ for any values of p_1 since the KL divergence is not negative. Then, we have

$$h_1(p'_1(\mathbf{x}_1))+h_3(\mathbf{b}'_1(\mathbf{x}_1)) \geq h_1(p^*_1(\mathbf{x}_1))+h_3(\mathbf{b}^*_1(\mathbf{x}_1)). \tag{B.13}$$

Since $\mathbf{R}_0$ is independent of N_1, following (B.1) we can see (B.13) proves (B.12).

Appendix C

Proof of Theorem 9

We provide here the proof of Theorem 9 presented in Chapter 5 on page 116. Substituting (5.16) into (5.23), $P_{out}\left(R_s\right)$ is derived as

$$P_{out}\left(R_s\right)=\int_0^{\infty} f_{\gamma_E}(\gamma_E)\frac{\gamma\left(\widetilde{m}_B,\frac{2^{R_s}(1+\gamma_E)-1}{\widetilde{m}_B^{-1}\widetilde{\gamma}_B}\right)}{\Gamma(\widetilde{m}_B)}d\gamma_E, \tag{C.1}$$

where $\gamma\left(\alpha,\mu\right)=\int_0^{\mu}e^{-t}t^{\alpha-1}dt$, $\mathrm{Re}\{\alpha\}>0$, is the lower incomplete gamma function. In order to obtain the result in (C.1), we have utilized the following identity [124, Eq. (3.381.1)]

$$\int_0^u t^{\nu-1}e^{-\mu t}dt=\mu^{-\nu}\gamma(\nu,\mu u). \tag{C.2}$$

To make progress, we adopt the following identity to expand $\gamma\left(\alpha,\mu\right)$ [124, Eq. (8.354.1)]

$$\gamma\left(\alpha,\mu\right)=\sum_{n=0}^{+\infty}\frac{\Gamma(\alpha)\mu^{\alpha+n}e^{-\mu}}{\Gamma(\alpha+n+1)}. \tag{C.3}$$

As per (C.3), we have

$$\begin{aligned}\gamma\left(\widetilde{m}_B, \frac{2^{R_s}(1+\gamma_E)-1}{\widetilde{m}_B^{-1}\widetilde{\overline{\gamma}}_B}\right) &= \sum_{n=0}^{+\infty} \frac{\Gamma(\widetilde{m}_B)\left(\frac{2^{R_s}(1+\gamma_E)-1}{\widetilde{m}_B^{-1}\widetilde{\overline{\gamma}}_B}\right)^{\widetilde{m}_B+n} \exp\left(-\frac{2^{R_s}(1+\gamma_E)-1}{\widetilde{m}_B^{-1}\widetilde{\overline{\gamma}}_B}\right)}{\Gamma\left(\widetilde{m}_B+n+1\right)} \\ &= \sum_{n=0}^{+\infty} \frac{\Gamma(\widetilde{m}_B)(2^{R_s}\gamma_E)^{\widetilde{m}_B+n}\left(1+\frac{2^{R_s}-1}{2^{R_s}\gamma_E}\right)^{\widetilde{m}_B+n}}{\left(\frac{\widetilde{\overline{\gamma}}_B}{\widetilde{m}_B}\right)^{\widetilde{m}_B+n} \exp\left(\frac{2^{R_s}(1+\gamma_E)-1}{\widetilde{m}_B^{-1}\widetilde{\overline{\gamma}}_B}\right)\Gamma(\widetilde{m}_B+n+1)} \\ &= \sum_{n=0}^{+\infty} \frac{\Gamma(\widetilde{m}_B)\exp\left(-\frac{2^{R_s}(1+\gamma_E)-1}{\widetilde{m}_B^{-1}\widetilde{\overline{\gamma}}_B}\right)(2^{R_s}\gamma_E)^{\widetilde{m}_B+n}}{\left(\frac{\widetilde{\overline{\gamma}}_B}{\widetilde{m}_B}\right)^{\widetilde{m}_B+n}\Gamma(\widetilde{m}_B+n+1)} \\ &\quad \times \sum_{l=0}^{+\infty}\binom{\widetilde{m}_B+n}{l}\left(\frac{2^{R_s}-1}{2^{R_s}\gamma_E}\right)^l, \end{aligned} \tag{C.4}$$

in which the identity [124, Eq. (1.110)]

$$(1+\mu)^\alpha = \sum_{l=0}^{+\infty}\binom{\alpha}{l}\mu^l \tag{C.5}$$

is employed. Substituting (5.22) and (C.4) into (C.1), we have

$$\begin{aligned} P_{out}\left(R_s\right) = \int_0^\infty &\left(\frac{\widetilde{m}_E}{\widetilde{\overline{\gamma}}_E}\right)^{N_E\widetilde{m}_E} \frac{\gamma_E^{N_E\widetilde{m}_E-1}}{\Gamma(N_E\widetilde{m}_E)}\exp\left(\frac{-\widetilde{m}_E\gamma_E}{\widetilde{\overline{\gamma}}_E}\right)\times \\ &\sum_{n=0}^{+\infty}\frac{\exp\left(-\frac{2^{R_s}(1+\gamma_E)-1}{\widetilde{m}_B^{-1}\widetilde{\overline{\gamma}}_B}\right)(2^{R_s}\gamma_E)^{\widetilde{m}_B+n}}{\left(\frac{\widetilde{\overline{\gamma}}_B}{\widetilde{m}_B}\right)^{\widetilde{m}_B+n}\Gamma(\widetilde{m}_B+n+1)}\times \\ &\sum_{l=0}^{+\infty}\binom{\widetilde{m}_B+n}{l}\left(\frac{2^{R_s}-1}{2^{R_s}\gamma_E}\right)^l d\gamma_E \\ = \frac{\widetilde{m}_B^{\widetilde{m}_B}\widetilde{m}_E^{N_E\widetilde{m}_E}2^{\widetilde{m}_B R_s}}{\Gamma(N_E\widetilde{m}_E)\widetilde{\overline{\gamma}}_B^{\widetilde{m}_B}\widetilde{\overline{\gamma}}_E^{N_E\widetilde{m}_E}} &\sum_{n=0}^{+\infty}\frac{\widetilde{m}_B^n 2^{nR_s}\exp\left(-\frac{\widetilde{m}_B\left(2^{R_s}-1\right)}{\widetilde{\overline{\gamma}}_B}\right)}{\widetilde{\overline{\gamma}}_B^n\Gamma(\widetilde{m}_B+n+1)}\times \\ &\sum_{l=0}^{+\infty}\frac{\binom{\widetilde{m}_B+n}{l}\left(2^{R_s}-1\right)^l}{2^{lR_s}}\int_0^\infty \frac{\gamma_E^{\widetilde{m}_B+N_E\widetilde{m}_E+n-l-1}}{\exp\left(\frac{\left(2^{R_s}\widetilde{m}_B\widetilde{\overline{\gamma}}_E+\widetilde{m}_E\widetilde{\overline{\gamma}}_B\right)\gamma_E}{\widetilde{\overline{\gamma}}_B\widetilde{\overline{\gamma}}_E}\right)}d\gamma_E. \end{aligned} \tag{C.6}$$

We then obtain the desirable result in (5.23) by solving the integral in (C.6) as per the following identity [124, Eq. (3.381.4)]

$$\int_0^\infty t^{\nu-1}e^{-\mu t}dt = \frac{1}{\mu^\nu}\Gamma_G(\nu). \tag{C.7}$$

Appendix D

Proof of Lemma 6

We provide here the proof of Lemma 6 presented in Chapter 7 on page 179. In the Cartesian coordinate system, we denote the location of Eve by (u, v). In the annulus threat model, the joint pdf of u and v is

$$f_{U,V}(u,v) = \begin{cases} \frac{1}{\pi(\rho_o^2-\rho_i^2)}, & \rho_i^2 \leq u^2+v^2 \leq \rho_o^2, \\ 0, & \text{otherwise.} \end{cases} \tag{D.1}$$

In the polar coordinate system, we denote the location of Eve by (ρ, θ). As such, we obtain $u = \rho\cos\theta$ and $v = \rho\sin\theta$. The Jacobian matrix for this coordinate change is given by

$$J(\rho,\theta) = \frac{\partial(u,v)}{\partial(\rho,\theta)} = \begin{bmatrix} \cos\theta & -\rho\sin\theta \\ \sin\theta & \rho\cos\theta \end{bmatrix}. \tag{D.2}$$

Using (D.2), the determinant of $J(\rho, \theta)$ is calculated as $|J(\rho,\theta)| = \rho$. Based on Jacobian techniques for the transformation of random variables [143], the joint pdf of ρ and θ is given by

$$f_{\mathrm{P},\Theta}(\rho,\theta) = f_{U,V}(u,v)|J(\rho,\theta)| = \begin{cases} \frac{\rho}{\pi(\rho_o^2-\rho_i^2)}, & 0\leq\theta\leq 2\pi,\ \rho_i\leq\rho\leq\rho_o, \\ 0, & \text{otherwise.} \end{cases} \tag{D.3}$$

Using (D.3), the marginal pdf of ρ is derived as

$$f_{\mathrm{P}}(\rho) = \int_0^{2\pi} f_{\mathrm{P},\Theta}(\rho,\theta)d\theta = \begin{cases} \frac{2\rho}{\rho_o^2-\rho_i^2}, & \rho_i\leq\rho\leq\rho_o, \\ 0, & \text{otherwise.} \end{cases}$$

In order to derive the pdf of ρ^2, we denote $\lambda = \rho^2$. As per the rules on the transformation of random variables, the pdf of ρ^2 is given by

$$f_{\mathrm{P}^2}(\rho^2) = \left|\frac{d\rho}{d\lambda}\right| f_{\mathrm{P}}(\rho) = \begin{cases} \frac{1}{\rho_o^2 - \rho_i^2}, & \rho_i^2 \leq \rho^2 \leq \rho_o^2, \\ 0, & \text{otherwise.} \end{cases} \tag{D.4}$$

This completes the proof of Lemma 6.

Bibliography

[1] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Commun. Mag.*, vol. 18, no. 5, pp. 66–74, Apr. 2011.

[2] H. V. Poor, "Information and inference in the wireless physical layer," *IEEE Commun. Mag.*, vol. 19, no. 1, pp. 40–47, Feb. 2012.

[3] R. A. Malaney, "A location enabled wireless security system," in *Proc. IEEE GlobeCOM*, Nov. 2004, pp. 2196–2200.

[4] A. Vora and M. Nesterenko, "Secure location verification using radio broadcast," *IEEE Trans. on Dependable and Secure Computing*, vol. 3, no. 4, pp. 377–385, Oct. 2006.

[5] R. A. Malaney, "Securing Wi-Fi networks with position verification: Extended version," *International J. Security Netw.*, vol. 2, no. 1, pp. 27–36, Mar. 2007.

[6] S. *Č*apkun, K. B. Rasmussen, M. *Č*agalj, and M. Srivastava, "Secure location verification with hidden and mobile base station," *IEEE Trans. Mobile Comput.*, vol. 7, no. 4, pp. 470–483, Apr. 2008.

[7] Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, "Detecting 802.11 MAC-layer spoofing using received signal strength," in *Proc. IEEE INFOCOM*, Apr. 2008, pp. 1768–1776.

[8] Y. Chen, J. Yang, W. Trappe, and R. P. Martin, "Detecting and localizing identity-based attacks in wireless and sensor networks," *IEEE Trans. Veh. Technol.*, vol. 59, no. 5, pp. 2418–2434, Jun. 2010.

[9] R. Zekavat and R. Buehrer, *Handbook of position location: Theory, practice and advances*, John Wiley & Sons, 2012.

[10] J. Chiang, J. Haas, J. Choi, and Y. Hu, "Secure location verification using simultaneous multilateration," *IEEE Trans. Wireless Commun.*, vol. 11, no. 2, pp. 584–591, Feb. 2012.

[11] J. Yang, Y. Chen, and W. Trappe, and J. Cheng, "Detection and localization of multiple spoofing attackers in wireless networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 1, pp. 44–58, Jan. 2013.

[12] B. M. Ledvina, M. L. Psiaki, S. P. Powell, and P. M. Kintner, "Bitwise parallel algorithms for efficient software correlation applied to a GPS software receiver," *IEEE Trans. Wirel. Commun.*, vol. 3, no. 5, pp. 1469–1473, Sep. 2004.

[13] N. O. Tippenhauer, K. B. Rasmussen, C. Popper, and S. Capkun, "IPhone and iPod location spoofing: Attacks on public WLAN-based positioning systems," SysSec Technical Report. ETH Zurich, Apr. 2008.

[14] B. Hofmann-Wellenhof, H. Lichtenegger, and J. Collins, *Global positioning system: Theory and practice*, 4th ed., Springer Verlag, 1997.

[15] N. Bulusu, J. Heidemann, and D. Estrin, "GPS-less low cost outdoor localization for very small devices," *IEEE Pers. Commun.*, vol. 7, no. 5, pp. 28–34, Oct. 2000.

[16] T. Leinmüller, E. Schoch, F. Kargl, and C. Maihöfer, "Influence of falsified position data on geographic ad-hoc routing," in *Proceedings of the second European Workshop on Security and Privacy in Ad hoc and Sensor Networks (ESAS)*, Jul. 2005, pp. 102–112.

[17] T. Leinmüller and E. Schoch, "Greedy routing in highway scenarios: The impact of position faking nodes," in *Proc. WIT*, 2006.

[18] M. Al-Rabayah and R. Malaney, "A new scalable hybrid routing protocol for VANETs," *IEEE Trans. Veh. Technol.*, vol. 61, no. 6, pp. 2625–2635, Jul. 2012.

[19] S. Chen, Y. Zhang, and W. Trappe, "Inverting sensor networks and actuating the environment for spatio-temporal access control" in *Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks*, Oct. 2006, pp. 1–12.

[20] S. Capkun, M. Cagalj, G. Karame, and N. O. Tippenhauer, "Integrity regions: Authentication through presence in wireless networks", *IEEE Trans. Mob. Comput.*, vol. 9, no. 11, pp. 1608–1621, Nov. 2010.

[21] F. Liu and X. Cheng, "LKE: A self-configuring scheme for location-aware key establishment in wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 1, pp. 224–232, Jan. 2008.

[22] M. Mauve, A. Widmer, and H. Hartenstein, "A survey on position-based routing in mobile ad hoc networks," *IEEE Network*, vol. 15, no. 6, pp. 30–39, Nov. 2001.

[23] Q. Yang, A. Lim, and P. Agrawal, "Connectivity aware routing in vehicular networks," in *Proc. IEEE WCNC*, Mar. 2008, pp. 2218–2223.

[24] E. Bertino, B. Catania, M. L. Damiani, and P. Perlasca, "GEO-RBAC: A spatially aware RBAC," in *Proceedings of the 10th ACM Symposium on Access Control Models and Technologies*, Jun. 2005, pp. 29–37.

[25] R. A. Malaney, "A secure and energy efficient scheme for wireless VoIP emergency service," in *Proc. IEEE GlobeCOM*, Nov. 2006, pp. 1–6.

[26] M. Raya and J.-P. Hubaux, "The security of vehicular ad hoc networks," in *Proceedings of SASN'05*, Nov. 2005, pp. 11–21.

[27] P. Papadimitratos, V. Gligor, and J.-P. Hubaux, "Securing vehicular communications–assumptions, requirements and principles," in *Proc. ESCAR*, Nov. 2006, pp. 5–14.

[28] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Secur.*, vol. 15, no. 1, pp. 39–68, Jan. 2007.

[29] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, "Secure vehicular communication systems: Design and architecture," *IEEE Commun. Mag.*, vol. 46, no. 11, pp. 100–109, Nov. 2008.

[30] A. Jaeger, N. Biβmeyer, H. Stubing, and S. A. Huss, "A novel framework for efficient mobility data verification in vehicular ad-hoc networks," *International Journal of ITS Research*, vol. 10, no. 1, pp. 11–21, Jan. 2012.

[31] B. Yu, C. Xu, and B. Xiao, "Detecting Sybil attacks in VANETs", *J. Parallel Distrib. Comput.*, vol. 73, no. 6, pp. 746–756, Jun. 2013.

[32] R. A. Malaney, "Wireless intrusion detection using tracking verification," in *Proc. IEEE ICC*, Jun. 2007, pp. 1558–1563.

[33] S. Yan, R. Malaney, I. Nevat, and G. Peters, "Optimal information-theoretic wireless location verification," *IEEE Trans. Veh. Technol.*, vol. 63, no. 7, pp. 3410–3422, Sep. 2014.

[34] M. Barkat, *Signal detection and estimation*, Boston, MA: Artech House, 2005.

[35] D. B. Faria and D. R. Cheriton, "Detecting identity-based attacks in wireless networks using singalprints," in *Proceedings of ACM WiSe*, Sep. 2006, pp. 43–52.

[36] N. Sastry, U. Shankar, and D. Wagner, "Secure verification of location claims," in *Proc. ACM WiSe*, Sep. 2003, pp. 1–10.

[37] Z. Yu, L. Zang, and W. Trappe, "Evaluation of localization attacks on power-modulated challenge-response systems," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 2, pp. 259–272, Jun. 2008.

[38] E. Ekici, S. Vural, J. McNair, and D. Al-Abri, "Secure probabilistic location verification in randomly deployed wireless sensor networks," *Ad Hoc Net.*, vol. 6, no. 2, pp. 195–209, Apr. 2008.

[39] Y. Wei and Y. Guan, "Lightweight location verification algorithms for wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 5, pp. 938–950, May 2013.

[40] T. Leinmüller, E. Schoch, and F. Kargl, "Position verification approaches for vehicular ad hoc networks," *IEEE Wireless Commun.*, vol. 13, no. 5, pp. 16–21, Oct. 2006.

[41] N. Alsharif, A. Wasef and X. Shen, "Mitigating the effects of position-based routing attacks in vehicular ad hoc networks", in *Proc. IEEE ICC*, Jun. 2011, pp. 1–5.

[42] O. Abumansoor and A. Boukerche, "A secure cooperative approach for nonline-of-sight location verification in VANET," *IEEE Trans. Veh. Technol.*, vol. 61, pp. 275–285, Jan. 2012.

[43] Z. Ren, W. Li, and Q. Yang, "Location verification for VANETs routing," in *Proc. IEEE WIMOB*, Oct. 2009, pp. 141–146.

[44] M. Abu-Elkheir, S. A. Hamid, H. S. Hassanein, I. M. Elhenawy, and S. Elmougy, "Position verification for vehicular networks via analyzing two-hop neighbors information," in *Proceedings of IEEE Conference on Local Computer Networks (LCN)*, Oct. 2011, pp. 805–812.

[45] M. Abu-Elkheir, H. S. Hassanein, I. M. Elhenawy, and S. Elmougy, "Map-guided trajectory-based position verification for vehicular networks," in *Proceedings of IEEE Wireless Communications and Networking Conference (WCNC)*, Apr. 2012, pp. 2538–2542.

[46] P. Zhang, Z. Zhang, and A. Boukerche, "Cooperative location verification for vehicular ad-hoc networks", in *Proc. IEEE ICC*, Jun. 2012, pp. 37–41.

[47] Y. Chen and Y. Wei, "A beacon-based trust management system for enhancing user centric location privacy in VANETs,", *J. Commun. Netw.*, vol. 15, no. 2, pp. 153–163, Apr. 2013.

[48] G. Yan, S. Olariu, and M. C. Weigle, "Providing VANET security through active position detection," *Computer Communications*, Vol. 31, no. 12, pp. 2883–2897, Jul. 2008.

[49] T. M. Chen and V. Venkataramanan, "Dempster-Shafer theory for intrusion detection in ad hoc networks," *IEEE Internet Comput.*, vol. 9, no. 6, pp. 35–41, Nov. 2005.

[50] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Techn. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[51] A. Wyner, "The wire-tap channel," *Bell Syst. Techn. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[52] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[53] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas–Part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[54] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[55] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[56] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.

[57] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for secrecy in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.

[58] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," *IEEE Signal Process. Lett.*, vol. 19, no. 6, pp. 372–375, Jun. 2012.

[59] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Secure transmission via transmit antenna selection in MIMO wiretap channels," in *Proc. IEEE GlobeCOM*, Dec. 2012, pp. 807–812.

[60] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels," *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 144–154, Jan. 2013.

[61] S. Yan, N. Yang, R. Malaney, and J. Yuan, "Transmit antenna selection with Alamouti coding and power allocation in MIMO wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 13, no. 3, pp. 1656–1667, Mar. 2014.

[62] T. Gucluoglu and T. M. Duman, "Performance analysis of transmit and receive antenna selection over flat fading channels," *IEEE Trans. Wirelss Commun.*, vol. 7, no. 8, pp. 3056–3065, Aug. 2008.

[63] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[64] G. Gu, P. Fogla, D. Dagon, W. Lee, and B. Skoric, "An information-theoretic measure of intrusion detection capability," College of Computing, Georgia Tech, Tech. Rep. GIT-CC-05-10, 2005.

[65] G. Gu, P. Fogla, D. Dagon, W. Lee, and B. Skoric, "Measuring intrusion detection capability: An information-theoretic approach," in *Proc. ASIACCS*, Mar. 2006, pp. 90–101.

[66] M. Gudmundson, "Correlation model for shadow fading in mobile radio systems," *Electron. Lett.*, vol. 27, no. 23, pp. 2145–2146, Aug. 1991.

[67] J. C. Liberti and T. S. Rappaport, "Statistics of shadowing in indoor radio channels at 900 and 1900 MHz," in *Proc. IEEE MILCOM*, Oct. 1992, pp. 1066–1070.

[68] K. Zayana and B. Guisnet, "Measurements and modelisation of shadowing cross-correlations between two base-stations," in *Proc. IEEE ICUPC*, Oct. 1998, pp. 101–105.

[69] J. Weitzen and T. Lowe, "Measurement of angular and distance correlation properties of log-normal shadowing at 1900 MHz and its application to design of PCS systems," *IEEE Trans. Veh. Technol.*, vol. 51, no. 2, pp. 265–273, Mar. 2002.

[70] S. S. Szyszkowicz, H. Yanikomeroglu, and J. S. Thompson, "On the feasibility of wireless shadowing correlation models," *IEEE Trans. Veh. Technol.*, vol. 59, no. 9, pp. 4222–4236, Nov. 2010.

[71] N. Patwari and P. Agrawal, "Effects of correlated shadowing: Connectivity, localization, and RF tomography," in *Proc. IEEE IPSN*, Apr. 2008, pp. 82–93.

[72] K.-J. Yang and Y.-R. Tsai, "Location tracking in mobile networks under correlated shadowing effects," in *Proc. IEEE WCNC*, Apr. 2009, pp. 1–5.

[73] J. Wang, Q. Gao, Y. Yu, P. Cheng, L. Wu, and H. Wang, "Robust device-free wireless localization based on differential RSS measurements,", *IEEE Trans. Ind. Electron.*, vol. 60, no. 12, pp. 5943–5952, Dec. 2013.

[74] T. Zhang and L. Delgrossi, *Vehicle safety communications: Protocols, security, and privacy*, Wiley, 2012.

[75] G. Yan, S. Olariu, and M. Weigle, "Providing location security in vehicular ad hoc networks," *IEEE Wireless Commun.*, vol. 16, no. 6, pp. 48–55, Dec. 2009.

[76] Y. Hao, J. Tang, and Y. Cheng, "Cooperative Sybil attack detection for position based applications in privacy preserved VANETs," in *Proc. IEEE GlobeCOM*, Dec. 2011, pp. 1–5.

[77] M. Fogue, F. Martinez, P. Garrido, M. Fiore, C. Chiasserini, C. Casetti, J. Cano, C. Calafate, and P. Manzoni, "Securing warning message dissemination in VANETs using cooperative neighbor position verification," *IEEE Trans. Veh. Technol.*, DOI: 10.1109/TVT.2014.2344633.

[78] F. Rusek, D. Persson, B. K. Lau, E. G. Larsson, T. L. Marzetta, O. Edfors, and F. Tufvesson, "Scaling up MIMO: Opportunities and challenges with very large arrays," *IEEE Signal Proces. Mag.*, vol. 30, no. 1, pp. 40–46, Jan. 2013.

[79] E. G. Larsson, F. Tufvesson, O. Edfors, and T. L. Marzetta, "Massive MIMO for next generation wireless systems," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 186–195, Feb. 2014.

[80] T. L. Marzetta, "Noncooperative cellular wireless with unlimited numbers of base station antennas," *IEEE Trans. Wireless Commun.*, vol. 9, no. 11, pp. 3590–3600, Nov. 2010.

[81] H. Yin, D. Gesbert, M. Filippou, and Y. Liu, "A coordinated approach to channel estimation in large-scale multipleantenna systems," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 2, pp. 264–273, Feb. 2013.

[82] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.

[83] D. Klinc, J. Ha, S. W. McLaughlin, J. Barros, and B.-J. Kwak, "LDPC codes for the Gaussian wiretap channel," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 532–540, Sep. 2011.

[84] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *Proc. IEEE ISIT*, Sep. 2005, pp. 2152–2155.

[85] S. Yan, R. Malaney, I. Nevat, and G. Peters, "An information theoretic location verification system for wireless networks," in *Proc. IEEE GlobeCOM*, Dec. 2012, pp. 5415–5420.

[86] J. Neyman and E. Pearson, "On the problem of the most efficient tests of statistical hypotheses," *Phil. Trans. R. Soc. A*, vol. 231, pp. 289–337, Jan. 1933.

[87] A. Goldsmith, *Wireless communications*, Cambridge, U.K.: Cambridge Univ. Press, 2005.

[88] T. Cover and J. Thomas, *Elements of information theory*, Wiley interscience, 2006.

[89] R. Kass and A. Raftery, "Bayes factors," *Journal of the American statistical association*, vol. 90, pp. 773–795, Jun. 1995.

[90] I. Nevat, G. Peters, and I. Collings, "Distributed detection in sensor networks over fading channels with multiple antennas at the fusion centre," *IEEE Trans. Signal Process.*, vol. 62, no. 3, pp. 671–683, Feb. 2014.

[91] B. Xiao, B. Yu, and C. Gao, "Detection and localization of Sybil nodes in VANETs," in *Proc. Workshop DIWANS*, Sep. 2006, pp. 1–8.

[92] J.-H. Song, V. W. S. Wong, and V. C. M. Leung, "Secure location verification for vehicular ad-hoc networks," in *Proc. IEEE GlobeCOM*, Dec. 2008, pp. 1–5.

[93] G. Yan, S. Olariu, and M. Weigle, "Cross-layer location verification enhancement in vehicular networks," in *Proc. IEEE Intelligent Vehicles Symposium (IV)*, Jun. 2010, pp. 95–100.

[94] L. Dawei, L. Moon-Chuen, and W. Dan, "A node-to-node location verification method," *IEEE Trans. Ind. Electron*, vol. 57, pp. 1526–1537, May 2010.

[95] J. Yang, Y. Chen, S. Macwan, C. Serban, S. Chen, and W. Trappe, "Securing mobile location-based services through position verification leveraging key distribution," in *Proc. IEEE WCNC*, Apr. 2012, pp. 2694–2699.

[96] M. Feder, N. Merhav, and M. Gutman, "Universal prediction of individual sequences," *IEEE Trans. Information Theory*, vol. 38, pp. 1258–1270, Jul. 1992.

[97] R. Linsker, "Self-organization in a perceptual network," *IEEE Computer*, vol. 21, pp. 105–117, Mar. 1988.

[98] R. Malaney, "Nuisance parameters and location accuracy in log-normal fading models," *IEEE Trans. Wireless Commun.*, vol. 6, no. 3, pp. 937–947, Mar. 2007.

[99] J. Wang, J. Chen, and D. Cabric, "Cramer-rao bounds for joint RSS/DOA-based primary-user localization in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 12, no. 3, pp. 1363–1375, Mar. 2013.

[100] C. F. Mecklenbräuker, A. F. Molisch, J. Karedal, F. Tufvesson, A. Paier, L. Bernadó T. Zemen, O. Klemp, and N. Czink, "Vehicular channel characterization and its implications for wireless system design and performance," *Proc. IEEE*, vol. 99, no. 7, pp. 1189–1212, Jul. 2011.

[101] P. Alexander, D. Haley, and A. Grant, "Cooperative intelligent transport systems: 5.9-GHz field trials, *Proc. IEEE*, vol. 99, no. 7, pp. 1213–1235, Jul. 2011.

[102] P. Agrawal and N. Patwari, "Correlated link shadow fading in multihop wireless networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 8, pp. 4024–4036, Aug. 2009.

[103] R. M. Vaghefi and R. M. Buehrer, "Received signal strength-based sensor localization in spatially correlated shadowing," in *Proc. IEEE ICASSP*, May 2013, pp. 4076–4080.

[104] S. Kullback and R. A. Leibler, "On information and sufficiency," *Annals of Mathematical Statistics*, vol. 22, no. 1, pp. 79–86, 1951.

[105] R. Meireles, M. Boban, P. Steenkiste, O. Tonguz, and J. Barros, "Experimental study on the impact of vehicular obstructions in VANETs," in *Proc. IEEE Vehic. Net. Conf.*, Dec. 2010, pp. 338–345.

[106] J. Gozalves, M. Sepulcre, and R. Bauza, "IEEE 802.11p vehicle to infrastructure communications in urban environments, *IEEE Commun. Mag.*, vol. 50, no. 5, pp. 176–183, May 2012.

[107] G. Taricco and E. Riegler, "On the ergodic capacity of correlated Rician fading MIMO channels with interference," *IEEE Trans. Inf. Theory*, vol. 57, no. 7, pp. 4123–4137, Jul. 2011.

[108] R. Prasad and A. Kegel, "Effects of Rician faded and lognormal shadowed signals on spectrum efficiency in microcellular radio," *IEEE Trans. Veh. Technol.*, vol. 42, no. 3, pp. 274–281, Aug. 1993.

[109] S. Eguchi and J. Copas, "Interpreting Kullback-Leibler divergence with the Neyman-Pearson lemma," *J. Multivar. Anal.*, vol. 97, no. 9, pp. 2034–2040, Oct. 2006.

[110] P. Ioannides and C. Balanis, "Uniform circular arrays for smart antennas," *IEEE Antennas Propag. Mag.*, vol. 47, pp. 192–206, Aug. 2005.

[111] J. Li and A. P. Petropulu, "Ergodic secrecy rate for multiple-antenna wiretap channels with Rician fading," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 861–867, Sep. 2011.

[112] N. S. Ferdinand, D. Benevides da Costa, and M. Latva-aho, "Physical layer security in MIMO OSTBC line-of-sight wiretap channels with arbitrary transmit/receive antenna correlation," *IEEE Wireless Comm. Lett.*, vol. 2, no. 5, pp. 467–470, Oct. 2013.

[113] J.-A. Tsai, R. Buehrer, and B. D. Woerner, "BER performance of a uniform circular array versus a uniform linear array in a mobile radio environment," *IEEE Trans.Wireless Comm.*, vol. 3, no. 3, pp. 695–700, May 2004.

[114] X. Zhou, M. R. McKay, B. Maham, and A. Hjørungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Commun. Lett.*, vol. 15, no. 3, pp. 302–304, Mar. 2011.

[115] S. Yan, G. Geraci, N. Yang, R. Malaney, and J. Yuan, "On the target secrecy rate for SISOME wiretap channels," in *Proc. IEEE ICC*, Jun. 2014, pp. 987–992.

[116] B. Fisher and A. K*ılı*çman, "Some results on the Gamma function for negative integers", *Appl. Math. Inf. Sci.*, vol. 6, No. 2, pp. 173-176, May 2012.

[117] E. Telatar, "Capacity of multi-antenna gaussian channels," *Eur. Trans. Telecommun.*, vol. 10, no. 6, pp. 585–596, Nov. 1999.

[118] V. Annapureddy, D. Marathe, T. Ramya, and S. Bhashyam, "Outage probability of multiple-input single-output (MISO) systems with delayed feedback," *IEEE Trans. Commun.*, vol. 57, no. 2, pp. 319–326, Feb. 2009.

[119] M. Kang and M.-S. Alouini, "Largest eigenvalue of complex Wishart matrices and performance analysis of MIMO MRC systems, *IEEE J. Selec. Areas Commun.*, vol. 21, no. 3, pp.418–426, Apr. 2003.

[120] T. Taniguchi, S. Sha, Y. Karasawa, and M. Tsuruta, "Approximation of largest eigenvalue distribution in Rician MIMO channels," in *Proc. IEEE PIMRC*, Sep. 2007, pp. 1–5.

[121] S. Yan, N. Yang, R. Malaney, and J. Yuan, "Transmit antenna selection with Alamouti scheme in MIMO wiretap channels," in *Proc. IEEE GlobeCOM*, Dec. 2013, pp. 687–692.

[122] S. Alamouti, "A simple transmit diversity technique for wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 16, no. 8, pp. 1451–1458, Oct. 1998.

[123] Z. Chen, J. Yuan, B. Vucetic, and Z. Zhou, "Performance of Alamouti scheme with transmit antenna selection," in *Proc. IEEE PIMRC*, Sep. 2004, pp. 1135–1141.

[124] I. S. Gradshteyn and I. M. Ryzhik, *Table of integrals, series and products*, 7th ed., Academic, San Diego, CA, 2007.

[125] J. G. Proakis. *Digital communicarions*, 3rd ed, McGraw-Hill. 1995.

[126] H. A. David, *Order statistics*, John Wiley & Sons, 1970.

[127] V. Tarokh, H. Jafarkhani, and A. R. Calderbank, "Space-time block coding for wireless communications: Performance results," *IEEE J. Sel. Areas Commun.*, vol. 17, no. 3, pp. 451–460, Mar. 1999.

[128] V. Tarokh, H. Jafarkhani, and A. R. Calderbank, "Space-time block codes from orthogonal designs," *IEEE Trans. Inf. Theory*, vol. 45, no. 5, pp. 1456–1467, Jul. 1999.

[129] W. K. Harrison, J. Almeida, M. R. Bloch, S. W. McLaughlin, and J. Barros, "Coding for secrecy: An overview of error-control coding techniques for physical-layer security," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 41–50, Sep. 2013.

[130] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[131] S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 Channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 4033–4039, Sep. 2009.

[132] A. Shah and A.M. Haimovich, "Performance analysis of maximal ratio combining and comparison with optimum combining for mobile radio communications with cochannel interference," *IEEE Trans. Veh. Technol.*, vol. 49, no. 4, pp. 1454–1463, Jul. 2000.

[133] Z. Chen, J. Yuan, and B. Vucetic, "Analysis of transmit antenna selection/maximal-ratio combining in Rayleigh fading channels," *IEEE Trans. Veh. Technol.*, vol. 54, no. 4, pp. 1312–1321, Jul. 2005.

[134] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "Interference-assisted secrect communication," in *Proc. IEEE Inform. Theory Workshop (ITW)*, May 2008, pp. 164–168.

[135] A. Kent, R. Beausoleil, W. Munro, and T. Spiller, "Tagging Systems," U.S. Patent US2006/0022832, 2006.

[136] R. A. Malaney, "Location-dependent communications using quantum entanglement," *Phys. Rev. A*, vol. 81, no. 4, pp. 042319-1–042319-4, Apr. 2010.

[137] R. A. Malaney, "Quantum location verification in noisy channels," in *Proc. IEEE GlobeCOM*, Dec. 2010, pp. 1–6.

[138] R. A. Malaney, "Location verification in quantum communications," WIPO Patent WO/2011/044629, 2011.

[139] H. Buhrman, N. Chandran, S. Fehr, R. Gelles, V. Goyal, R. Ostrovsky and C. Schaffner, "Position-based quantum cryptography: Impossibility and constructions," in *Advances in Cryptology*, vol. 6841 of Lecture Notes in Computer Science, pp. 429–446, Springer-Verlag, 2011.

[140] L. L. Scharf and B. Friedlander, "Matched subspace detectors," *IEEE Trans. Signal Process.*, vol. 42, no. 8, pp. 2146–2157, Aug. 1994.

[141] S. M. Kay and J. R. Gabriel, "An Invariance property of the generalized likelihood ratio test," *IEEE Signal Process. Lett.*, vol. 10, no. 12, pp. 352–355, Dec. 2003.

[142] J. Sherman and W. J. Morrison, "Adjustment of an inverse matrix corresponding to a change in one element of a given matrix," *Ann. Math. Statist.*, vol. 21, no. 1, pp. 124–127, Mar. 1950.

[143] A. Leon-Garcia, *Probability and random processes for electrical engineering*, 2nd ed. Cambridge, MA: Addison-Wesley, 1994.