# Physical layer security in RIS-assisted V2V communication

Capstone Project Final Report

Altynbek Serikov

Nazarbayev University
Department of Electrical and Computer Engineering
School of Engineering and Digital Sciences

This project report was created on TexStudio editing platform using LaTeX. All the figures were drawn using draw.io online software tool.

NAZARBAYEV UNIVERSITY

**Electrical and Computer Engineering**
Nazarbayev University
http://www.nu.edu.kz

**Title:**
Physical layer security in RIS-assisted V2V communication

**Theme:**
Capstone Project Final Report

**Project Period:**
Spring 2024

**Project Group:**
Laboratory for Wireless Innovation

**Participant(s):**
Altynbek Serikov

**Supervisor(s):**
Galymzhan Nauryzbayev

**Copies:** 1

**Page Numbers:** 27

**Date of Completion:**
April 22, 2024

**Abstract:**

Physical layer security (PLS) aims to ensure the confidentiality and authenticity of transmitted data by capitalizing on the inherent randomness of wireless channels. Owing to the popularity of intelligent transportation systems (ITS), PLS research has sparked renewed interest in the wireless research community. This paper investigates the performance of secure communication in a vehicle-to-vehicle (V2V) communication scenario using a reconfigurable intelligent surface (RIS). Additionally, we introduce the concept of non-orthogonal multiple access (NOMA) to enhance communication efficiency in V2V networks. This study aims to comprehensively analyze secrecy performance, including parameters such as secrecy outage probability (SOP) and probability of non-zero secrecy capacity (PNZSC). Our research aims to demonstrate the effectiveness of RIS in providing secure and reliable communication within V2V NOMA networks. Ultimately, our study contributes to advancing secure communication protocols in ITS.
*Keywords*— Vehicular communication, physical layer security, eavesdropper, RIS, secrecy outage

# Contents

# Preface

Effective control policies can win time and let scientists discover ways of conquering the virus or at least transitioning the spread to the endemic stage. The results of this project can be further used to build the foundation for optimal control policies in case of any possible future out-breaks. This project also plays a significant role in meeting the national healthcare and economic priorities. COVID-19 pandemic is spreading worldwide. Saving the lives and health of its citizens is the primary priority of every country. Therefore, modeling and predicting the spread of diseases and selecting the optimal intervention strategies is beneficial to the government. Further research on this topic can lead to more key findings, which to model other diseases and create flexible intervention policies that include vaccination. In general, small epiphanies and insights that accompanied the project might become a central point for other deep-learning research and projects in other areas such as computer vision, neurolinguistic programming, and artificial intelligence.The aim of my Capstone Project is to study and implement a physical layer security (PLS) approach for securing V2V (vehicle-to-vehicle) communication in autonomous vehicles. V2V communication enables autonomous vehicles to share information such as location, speed, and trajectory, which is crucial for safe and efficient driving. However, this communication is vulnerable to security threats such as eavesdropping and tampering, which can cause accidents and put lives at risk. To address this problem, I will investigate the use of PLS techniques such as artificial noise, beamforming, and power control to secure V2V communication. These techniques exploit the characteristics of the wireless channel between the sender and receiver to ensure secure communication without the need for encryption. The goal of this project is to develop a practical and effective PLS scheme for V2V communication in autonomous vehicles. In the initial phase of the project, I will conduct a comprehensive literature review of PLS techniques for wireless communication and their application in V2V communication. Based on the review, I will propose a novel PLS scheme for V2V communication that takes into account the unique characteristics of the autonomous vehicle environment. In the second phase of the project, I will implement and evaluate the proposed scheme using simulation and experimental tests. The simulation will be conducted using a

MATLAB, while the experimental tests will be performed using a testbed consisting of multiple autonomous vehicles equipped with V2V communication devices. The ultimate goal of this project is to demonstrate the effectiveness and practicality of the proposed PLS scheme for V2V communication in autonomous vehicles. The research results will be disseminated through publications in high-quality journals and conference proceedings, and the prototype-driven design specification will be developed for further hardware realization. Overall, the successful completion of this project will contribute to the development of secure and safe autonomous vehicle technology

I would like to extend my heartfelt gratitude to my dedicated supervisors, Professors Galymzhan Nauryzbayev and Mohd Hamza Naim Shaikh. Their unwavering support and guidance throughout my research journey have been invaluable. It is worth noting that we are fortunate to reside in the same city, which eliminated any time zone challenges. I deeply appreciate their commitment to my success, readily providing their expertise, resources, and mentorship. Their presence and accessibility have been instrumental in ensuring the quality and timely completion of my research. I am truly fortunate to have had the opportunity to work with such dedicated mentors.

I would also like to express my gratitude to NU Library for generously offering students free access to an extensive collection of research papers and articles, which greatly facilitated my research endeavors.

Nazarbayev University, April 22, 2024

Altynbek Serikov
<altynbek.serikov@nu.edu.kz>

# Chapter 1

# Introduction

## 1.1 Background

The transportation industry's future depends on several factors, including autonomous driving, passenger and driver safety, traffic management, and entertainment. Efficient and secure intelligent transportation systems (ITSs) require the integration of sixth-generation (6G) technology in vehicular communications since the implementation of ITS is entirely dependent on the exchange of massive information with ultra-wide bandwidth, low latency, and high reliability. Vehicular communication, a critical component of ITS, involves various wireless technologies such as vehicle-to-pedestrian (V2P), vehicle-to-infrastructure (V2I), and vehicle-to-vehicle (V2V) communication. Furthermore, with the advancement of 6G technology, vehicles will access highly precise safety information, smart traffic management support, and advanced entertainment features. Therefore, 6G services will lead to a wireless vehicular network that is fully automated, self-driving, and safe [1, 2, 3]. Lately, emerging vehicular technologies like autonomous driving, cooperative vehicular networks, Internet of Vehicles (IoV), vehicular ad-hoc networks (VANETs), air-to-ground (A2G) networks, and space–air-ground integrated networks (SAGINs) have garnered significant interest from scholars and professionals in both the academic and industrial sectors [4, 5, 6].

In vehicular communications, two prevalent secure transmission methods are recognized [7]: cryptographic techniques based on keys and physical layer security (PLS) approaches [8, 9, 10]. PLS employs the wireless channel's randomness to ensure confidentiality and authentication [11, 12]. PLS offers several advantages over cryptographic technologies based on upper layers [13, 14]. Notably, it can be easily implemented without necessitating substantial communication resources to share secret keys among authorized users [7]. Moreover, PLS eliminates the need to consider specific security protocol executions or implement additional security measures beyond the physical layer in higher layers of communication technology. It

can rapidly authenticate legitimate nodes even before demodulation and decoding, preventing wasteful signal processing for unintended transmissions. Extensive research has analyzed wireless communication between vehicles and infrastructure, both with and without PLS [3].

PLS utilizes intrinsic propagation channel characteristics, such as fading, interference, and noise, to enable secure transmission without keys. The reconfigurable intelligent surface (RIS)-aided communication systems show significant potential for PLS applications [15]. RIS technology facilitates the reflection of electromagnetic waves, creating alternative paths for wireless communication. This capability enhances signal strength and bypasses obstructions, making it valuable for improving vehicular communication systems. Importantly, RIS technology achieves this without necessitating adjustments to the transceiver or infrastructure, making it a cost-effective and energy-efficient solution for indirect line-of-sight (LoS) links. Compared to conventional communication systems, RIS introduces a novel design parameter that can enhance wireless networks by expanding coverage, minimizing interference, and increasing secrecy capacity and outage resilience [16, 17].

Non-orthogonal multiple access (NOMA) can serve multiple vehicles at the same time and frequency domain simultaneously, providing multiplexing in the power domain and thus exhibiting significant improvements in spectral efficiency (SE), low latency, and higher data rate compared to other techniques [18, 19]. Moreover, with the growing demand for ITS applications and vehicle-to-everything (V2X) communication and the huge number of devices accessing the dynamic wireless channel, providing broadband connectivity for vehicular communications is challenging. It is a well-established fact that placing multiple antennas on terminals and RIS can significantly improve transmission reliability and, hence, system performance. Therefore, NOMA combined with RIS can be a potential solution to effectively address the problems of reduced access collisions, massive connectivity, high reliability, and low latency for V2V communication [20, 21].

## 1.2 Related Works

Inspired by the combined advantages of RIS and NOMA, [22] introduced RIS-supported NOMA networks to improve the system's SE and energy efficiency (EE). In [23], the researchers examined perfect and imperfect RIS scenarios. They adjusted the active beamforming at the base station (BS) and the passive beamforming at RIS to enhance the total data transfer rate. In [24], the authors highlighted the enhanced performance of secure communication using RIS in both V2V and V2I communications. They explored two scenarios: RIS acts as a relay for V2V communication, and RIS serves as the receiver in V2I communication. Similarly, in [25], the authors conducted a comparative analysis of RIS and relay-assisted average secrecy capacity in the V2X communication context. Their findings suggested that

RIS outperforms conventional relay-assisted V2X communication systems. Moreover, in [26] and[27], the authors proposed the implementation of artificial noise to improve the performance of PLS for wireless networks. Artificial noise, including white, pink, and Gaussian, is intentionally generated to disrupt or mask unwanted signals, enhancing secure communication performance.

In [28], a secure communication setup was detailed where a multi-antenna access point (AP) communicates with a single-antenna user in the vicinity of a single-antenna eavesdropper (Eve), with RIS at the same distance from the user and the eavesdropper. It was demonstrated that by modifying the phase shifts of RIS's reflecting elements (REs), the signal reflected by RIS can amplify the received signal power at the user by aligning constructively with the direct signal. Conversely, this reflected signal is designed to interfere destructively with the signal at the eavesdropper, thus diminishing its received power and enhancing the user's secrecy rate. Furthermore, AP's transmit beamforming can be adjusted to find an equilibrium between directing the signal power toward RIS and the user/eavesdropper for the purpose of enhancing or canceling the signal, respectively. Consequently, when the active transmit beamforming at AP and the passive reflect beamforming at RIS are optimized, the user's secrecy rate can be maximized.

In the study documented in [29], the authors employed Wyner's wiretap model, a classical secure communication model. They considered V2V communication, where a sender vehicle transmits confidential information to a receiver vehicle, while Eve may attempt to intercept the information. The authors assumed that V2V transmission channels are influenced by independent double-Rayleigh fading, a standard statistical model for wireless channels. Additionally, the security of confidential messages was significantly compromised when the channel state information (CSI) was imperfect, particularly during vehicle movement. In a different scenario presented in [30], a fixed transmitter communicated a secret message to a mobile receiver with multiple antennas and passive Eve nearby. The security of confidential messages faced substantial risks due to imperfect CSI, particularly during vehicle movement. In [31], the authors considered a vehicular communication scenario in which a source vehicle, with RIS-based AP, sends confidential information to a destination vehicle while an eavesdropper vehicle attempts to receive and decrypt the information. In their system, they considered an intelligent AP in which RIS knows CSI so that the phases induced by RIS can be adjusted to maximize the resulting signal-to-noise ratio (SNR) through appropriate phase compensations and proper alignment of the reflected signals from REs. It should be noted that while the researchers in [32] explored the PLS aspects of RIS-assisted NOMA networks, their focus was solely on Rayleigh fading. Nevertheless, given the central limit theorem-based CSI of the reflected links, there is a discrepancy between the analytical outcomes and the simulation findings, especially when the count of RIS elements is low. In [33], the secure downlink of a RIS-supported

NOMA network is examined, wherein BS is engaged in communication with two legitimate users amidst the presence of Eve. It is noted that these legitimate users utilize an orthogonal resource block in the power-domain NOMA. The configuration assumes that BS, both NOMA users, and Eve each possess a single antenna. RIS is strategically positioned. Specifically, the first user, identified as a standard user, has the capability to engage with BS without RIS's intervention. In contrast, the second, recognized as the cell-edge user, requires RIS's assistance communicating with BS. Concurrently, RIS presents an eavesdropping opportunity for Eve, who would otherwise be unable to intercept messages from BS. Moreover, the communication links between RIS and the first user and between BS catering to the second user and Eve are obstructed, attributed to their spatial separation and physical barriers. The authors in [34] investigated the efficacy of vehicular communication networks, specifically focusing on the V2V networks. These networks are enhanced by both RIS and simultaneous transmitting and reflecting intelligent omni-surface (STAR-IOS). The performance of these networks is examined under the frameworks of both non-orthogonal multiple access (NOMA) and orthogonal multiple access (OMA) schemes. The study positions RIS near the transmitting vehicle and STAR-IOS close to the receiving vehicles. It is also highlighted that STAR-IOS harnesses an energy-splitting (ES) protocol for its communication processes. Furthermore, the fading channels existing between RIS and STAR-IOS are characterized by a composite Fisher-Snedecor F distribution, according to the research findings. Their numerical findings underscored the substantial benefits of RIS/STAR-IOS in vehicular communications, particularly highlighting the superiority of the NOMA scheme over OMA in reducing the outage probability (OP) and augmenting ergodic capacity (EC) and energy efficiency (EE). In [33, 35] PLS aspects of downlink communication in RIS-aided NOMA networks, focusing on scenarios where an eavesdropper is present was investigated. There, RIS is deployed to enhance the signal quality, aiding cell-edge users in communicating with the base station (BS). The research derived the expected value of new channel statistics for reflected links under Nakagami-$m$ fading to characterize network performance. Both secrecy outage probability (SOP) and ASC are evaluated, with closed-form expressions derived for these metrics. Additionally, the study investigates the influence of various network parameters on overall performance, particularly focusing on the secrecy performance of RIS-aided NOMA networks, where BS communicates with a pair of NOMA users in the presence of an eavesdropper. In [36], the performance of cooperative vehicular comunications utilizing NOMA at intersections in the presence of interference was examined. Closed-form expressions for the outage probability and quasi-closed-form expressions for the average achievable rate were derived using stochastic geometry tools. Two scenarios were considered: V2V communications with destination nodes situated on the roads, and V2I communications with destination nodes located outside the roads. It was

**Table 1.1:** Related Works

| Reference | Direct Link | Channels | RIS | NOMA |
|---|---|---|---|---|
| Ref. [24] | No | Rayleigh | Yes | No |
| Ref. [25] | No | Nakagami-*m* | Yes | No |
| Ref. [26] | Yes | Rayleigh | Relay | Yes |
| Ref. [28] | Yes | Rayleigh | RIS | Yes |
| Ref. [29] | Yes | Double-Rayleigh | No | No |
| Ref. [30] | Yes | Nakagami-*m* | No | No |
| Ref. [31] | Yes | Double-Rayleigh | RIS as AP | No |

observed that the outage probability increased while the average achievable rate decreased at intersections. Additionally, it was found that employing cooperative NOMA led to enhancements in both outage probability and average achievable rate compared to OMA at intersections. Specifically, cooperative NOMA demonstrated superior performance over cooperative OMA, particularly for higher data rates. Nonetheless, inadequate selection of system parameters, such as power allocation coefficient and data rates, resulted in a significant decline in the performance of cooperative NOMA. To mitigate this, the impact of relay position was investigated. A summary of related works is also provided in Table 1.1

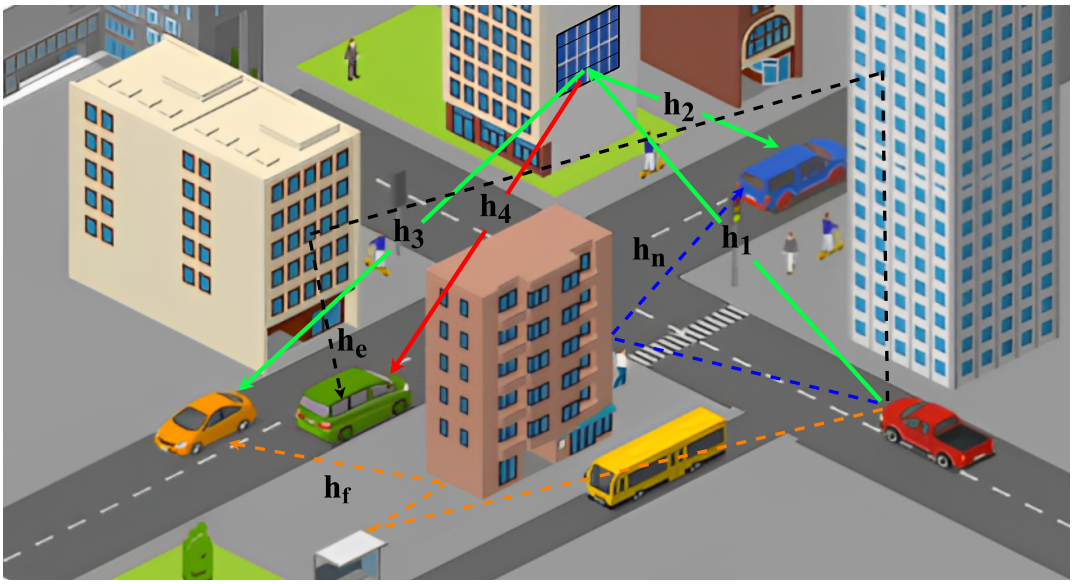


**Figure 1.1:** Schematic depicting the considered RIS-aided V2V NOMA in the presence of Eavesdropper.

# Chapter 2

# System Model

Fig. 1 depicts a common scenario of a road intersection in an urban environment where the direct link between vehicles may not be available due to obstacles. Specifically, we consider a V2V communication scenario where the source vehicle ($V_s$) wants to securely transmit information to a set of desired vehicles in the presence of an unintended vehicle ($V_e$) that is overhearing the confidential transmission. As shown in Figure 1, the source vehicle ($V_s$) communicates (green-colored links) with a pair of vehicles, namely, a near vehicle ($V_n$) and a far vehicle ($V_f$), in the presence of an unintended vehicle ($V_e$) acting as an eavesdropper (red-colored link). To improve the link qualities of $V_n$ and $V_f$, we employ a reconfigurable intelligent surface (RIS) consisting of $M$ ($M > 1$) reflecting elements (REs). The RIS is configured to beamform the signal from $V_s$ towards $V_n$ and $V_f$ through $M_1 = \eta M$ and $M_2 = (1 - \eta)M$ REs, where $M_1 + M_2 = M$ and $\eta \in (0, 1)$. Similarly, $V_e$ will receive random reflections from all $M$ REs of the RIS. Note that while there can be multiple desired vehicles, for complexity requirements, we limit ourselves to a 2-vehicle scenario in this study.

### Channel Model

Since the direct link between the source and destination vehicles is subject to scattering at both ends, they are characterized using a double Rayleigh fading model. Similarly, the channel between the source vehicle to the RIS and the RIS to destination vehicles can be modeled using Nakagami-$m$ fading. It is assumed that all channels experience frequency-flat fading, and the channel state information (CSI) is available at the source. Additionally, it is assumed that the power of the second and further reflections of the RIS is negligible.

**NOMA Protocol**

The superimposed signal is transmitted from the $V_s$ to the pair of desired NOMA vehicles, $V_n$ and $V_f$ can be expressed as

$$x_s = \zeta_n x_n + \zeta_f x_f, \tag{2.1}$$

here $x_n$ and $x_f$ define the message signal of $V_n$ and $V_f$, respectively. Further, $\zeta_n$ and $\zeta_f$ are the power allocation coefficients for $V_n$ and $V_f$ which satisfies the power domain NOMA constraint, i.e., $\zeta_n^2 + \zeta_f^2 = 1$. For justice between the NOMA paired vehicles, we employ $\zeta_n < \zeta_f$.

**Received Signal Model**

The received signal, $y_n$, at $V_n$ for the considered scenario can be expressed as

$$y_n = [h_n + \mathbf{h_1}\mathbf{\Theta}\mathbf{h_2}](\zeta_n x_n + \zeta_f x_f)\sqrt{P_s} + N_o, \tag{2.2}$$

where $P_s$ is transmitted power and $N_o$ is additive white Gaussian noise (AWGN) with $N_o \sim \mathcal{CN}\left(0, \sigma^2\right)$. Further, $h_n$ is the direct link between $V_s$ and $V_n$ which is characterized through double-Rayleigh fading, with the scale factor of $\sigma_n^2$. Likewise, the elements of $\mathbf{h_1}$ and $\mathbf{h_2}$ follow Nakagami-$m$ fading with the shape and scale factor of $m_1$, $m_2$ and $\Omega$, $\Omega_n$, respectively. Here, it is assumed that all channel coefficients are independent of each other. Further, the variable $\mathbf{\Theta}$ represents the matrix of reflection coefficients for the RIS.

Likewise, the received signal, $y_f$, at $V_f$ can be written as

$$y_f = [h_f + \mathbf{h_1}\mathbf{\Theta}\mathbf{h_3}](\zeta_n x_n + \zeta_f x_f)\sqrt{P_s} + N_o,$$

where $h_f$ is the direct link between the $V_s$ and $V_f$ and it is characterized by double-Rayleigh fading, with a scale factor of $\sigma_f^2$. Here, the elements of $\mathbf{h_3}$ are Nakagami-$m$ faded with shape and scale factor of $m_3$ and $\Omega_f$, respectively.

Likewise, we can express the received signal $V_e$ as

$$y_e = [h_e + \mathbf{h_1}\mathbf{\Theta}\mathbf{h_4}](\zeta_n x_n + \zeta_f x_f)\sqrt{P_s} + N_o, \tag{2.3}$$

where $h_e$ is the direct link between $V_s$ and $V_e$ and it is a double Rayleigh faded channel with a scale factor of $\sigma_e^2$. While the elements of $h_4$ are Nakagami-$m$ faded with shape and scale factor of $m_4$ and $\Omega_e$, respectively.

# Chapter 3

# Methodology

## 3.1 Methods and Procedure of Data Collection

I. Literature Review: A thorough examination of existing literature related to physical layer security (PLS) techniques for wireless communication and their application in vehicle-to-vehicle (V2V) communication. This extensive review will serve as the foundation for the proposed PLS scheme.

II. Mathematical Model Development: The creation of mathematical models and equations pertaining to the PLS techniques under consideration, including artificial noise, beamforming, and power control. These models will be fundamental in understanding and implementing the PLS scheme. As the project primarily involves simulations and experimental tests, this section will provide detailed insights into the methods and procedures for data collection:

III. Simulation Setup: A comprehensive explanation of the MATLAB-based simulation environment, including specific parameters, scenarios, and data collection techniques employed during the simulations.

IV. Experimental Testbed: A description of the testbed setup, encompassing the autonomous vehicles equipped with V2V communication devices and outlining the procedures for data collection during real-world experiments.

## 3.2 Methods and Procedure of Data Analysis

I. Data Processing: Detailed elucidation of how the collected data will be processed, organized, and prepared for analysis to ensure accuracy and relevance.

II. Mathematical Analysis: Explanation of the mathematical methods, calculations, and algorithms employed for data analysis, including any statistical techniques used to derive meaningful insights from the collected data.

## 3.3 Ethical Issues

I. Privacy and Security: I will discuss potential privacy concerns related to data collected during experiments and outline measures to ensure the security and confidentiality of V2V communication data.

II. Compliance: Ensuring full compliance with ethical guidelines and standards relevant to research involving autonomous vehicles and wireless communication, demonstrating a commitment to ethical research practices.

# Chapter 4

# Results and Discussions

## 4.1 Performance Analysis

### 4.1.1 Secrecy Outage Probability

The SOP can be defined as the probability of achieving the non-negative target level of secure communication. Thus, the SOP for $V_n$ and $V_f$ can be formulated as

$$P_{out}^{n} = \Pr\left\{C_n < R_s^n\right\} \tag{4.1}$$

and

$$P_{out}^{f} = \Pr\left\{C_f < R_s^f\right\}, \tag{4.2}$$

with $R_s^n$ and $R_s^f$ being the targeted secrecy rate thresholds at $V_n$ and $V_f$, respectively. Equation can be rewritten as

$$P_{out}^{n} = \Pr\left\{R_n - R_{en} < R_s^n\right\}. \tag{4.3}$$

Then we get following expression

$$P_{out}^{n} = \Pr\left\{\log_2(1+|\mathcal{H}_n|^2\zeta_n^2\Upsilon) - \log_2(1+|\mathcal{H}_e|^2\zeta_n^2\Upsilon) < R_s^n\right\}, \tag{4.4}$$

equivalently

$$P_{out}^{n} = \Pr\left\{\frac{1+|\mathcal{H}_n|^2\zeta_n^2\Upsilon}{1+|\mathcal{H}_e|^2\zeta_n^2\Upsilon} < \lambda_n\right\}, \tag{4.5}$$

here $\lambda_n = 2^{R_s^n}$ is the secrecy threshold for $V_n$. After rearranging and mathematical manipulations (4.5) can be expressed as

$$P_{out}^{n} = \Pr\left\{|\mathcal{H}_n|^2\zeta_n^2\Upsilon < \lambda^n\left(|\mathcal{H}_e|^2\zeta_n^2\Upsilon + 1\right) - 1\right\}. \tag{4.6}$$

Further, dividing both sides of the inequality by $\zeta_n^2\Upsilon$, then taking square root we get the following expression

$$P_{out}^n = \Pr\left\{|\mathcal{H}_n^2| < \frac{\lambda^n\left(|\mathcal{H}_e|^2\zeta_n^2\Upsilon+1\right)-1}{\zeta_n^2\Upsilon}\right\}, \tag{4.7}$$

which is CDF of $|\mathcal{H}_n|^2$ and can be formulated mathematically as

$$P_{out}^n = F_{|\mathcal{H}_n|^2}\left(\frac{\lambda^n\left(|\mathcal{H}_e|^2\zeta_n^2\Upsilon+1\right)-1}{\zeta_n^2\Upsilon}\right). \tag{4.8}$$

Since we have another random variable inside the equation, (4.8) can be modeled as

$$P_{out}^n = \int_0^\infty F_{|\mathcal{H}_n|^2}\left(\frac{\lambda^n\left(x\zeta_n^2\Upsilon+1\right)-1}{\zeta_n^2\Upsilon}\right) f_{|\mathcal{H}_e|^2}(x)dx, \tag{4.9}$$

here $f_{|\mathcal{H}_e|^2}(x)$ is PDF of $|\mathcal{H}_e|^2$ gain. To solve this integral we then utilize Taylor series expansion for CDF of gamma distribution.

$$\begin{aligned} P_{out}^n = 1 - \int_0^\infty \sum_{k=0}^{\alpha_n-1}\frac{\beta_n^k}{k!}\left\{\frac{\lambda^n\left(x\zeta_n^2\Upsilon+1\right)-1}{\zeta_n^2\Upsilon}\right\}^k \\ \times\exp\left(-\beta_n\frac{\lambda^n\left(x\zeta_n^2\Upsilon+1\right)-1}{\zeta_n^2\Upsilon}\right) f_{|\mathcal{H}_e|^2}(x)dx. \end{aligned} \tag{4.10}$$

After mathematical manipulations and using a PDF of the eavesdropper's channel gain, we get

$$P_{out}^n = 1 - \sum_{k=0}^{\alpha_n-1} t_1 t_2 I_1, \tag{4.11}$$

where

$$\begin{aligned} t_1 &= \frac{\beta_n^k\beta_e^{\alpha_e}}{k!(\zeta_n^2\Upsilon)^k\Gamma(\alpha_e)} \quad t_2 = \frac{\exp\left(\frac{\beta_n}{\zeta_n^2\Upsilon}\right)}{\exp\left(\frac{\lambda_n\beta_n}{\zeta_n^2\Upsilon}\right)}, \\ I_1 &= \int_0^\infty \exp(-(\beta_n\lambda_n+\beta_e)x)x^{\alpha_e-1}[\lambda_n(x\zeta_n^2\Upsilon+1)-1]^k dx. \end{aligned} \tag{4.12}$$

The integral part can be solved using the confluent hypergeometric function.

$$U(a,b,z) = \Gamma(a)\int_0^\infty \exp(-zt)t^{a-1}(1+t)^{b-a-1}dt, \tag{4.13}$$

further changing variables and mathematical manipulations $I_1$ can be expressed as

$$I_1 = \frac{(\lambda_n - 1)^k}{t_3^{\alpha_e - 1}} U\left(\alpha_e, k + \alpha_e + 1, \frac{\beta_n \lambda_n + \beta_e}{t_3}\right) \Gamma(\alpha_e), \tag{4.14}$$

where $t_3$ is equal to

$$t_3 = \frac{\lambda_n \zeta_n^2 \mathrm{Y}}{\lambda_n - 1}. \tag{4.15}$$

Similarly, as for the far vehicle

$$\begin{aligned} P_{out}^f &= \Pr\left\{R_f - R_{ef} < R_s^f\right\} \\ &= \Pr\left\{\frac{1 + \frac{|\mathcal{H}_f|^2 \zeta_f^2 \mathrm{Y}}{|\mathcal{H}_f|^2 \zeta_n^2 \mathrm{Y} + 1}}{1 + \frac{|\mathcal{H}_e|^2 \zeta_f^2 \mathrm{Y}}{|\mathcal{H}_e|^2 \zeta_n^2 \mathrm{Y} + 1}} < \lambda_f\right\}, \end{aligned} \tag{4.16}$$

after mathematical manipulations we get

$$P_{out}^f = \Pr\left\{|\mathcal{H}_f|^2 < \frac{|\mathcal{H}_e|^2 \mathrm{Y}(\lambda_f - \zeta_n^2) + \lambda_f - 1}{|\mathcal{H}_e|^2 \zeta_n^2 \mathrm{Y}(\mathrm{Y} - \lambda_f) + \mathrm{Y}(1 - \zeta_n^2 \lambda_f)}\right\}, \tag{4.17}$$

here $\lambda_f = 2^{R_s^f}$. By utilizing Tailor series expansion on (4.17) we get

$$\begin{aligned} P_{out}^f = 1 - \int_0^\infty \sum_{k=0}^{\alpha_f - 1} \frac{\beta_f^k}{k!} \left\{\frac{x\mathrm{Y}(\lambda_f - \zeta_n^2) + \lambda_f - 1}{x\zeta_n^2 \mathrm{Y}(\mathrm{Y} - \lambda_f) + \mathrm{Y}(1 - \zeta_n^2 \lambda_f)}\right\}^k \\ \times \exp\left(-\beta_f \frac{x\mathrm{Y}(\lambda_f - \zeta_n^2) + \lambda_f - 1}{x\zeta_n^2 \mathrm{Y}(\mathrm{Y} - \lambda_f) + \mathrm{Y}(1 - \zeta_n^2 \lambda_f)}\right) f_{|\mathcal{H}_e|^2}(x) dx. \end{aligned} \tag{4.18}$$

However, SOP for the Far user cannot be integrated due to the complexity and the large number of components. Thus asymptotic SOP and probabability of non-zero secrecy capacity can be evaluated.

### 4.1.2 Asymptotic Secrecy Outage Probability

Thus, asymptotic SOP can be evaluated, when Y goes to $\infty$ (4.5) can be approximated as

$$P_{out}^n \approx \Pr\left\{\frac{|\mathcal{H}_n|^2 \zeta_n^2 \mathrm{Y}}{|\mathcal{H}_e|^2 \zeta_n^2 \mathrm{Y}} < \lambda_n\right\}. \tag{4.19}$$

Further, the expression can be simplified as

$$\begin{aligned} P_{out}^n &= \Pr\left\{|\mathcal{H}_n|^2 < |\mathcal{H}_e|^2 \lambda_n\right\} \\ &= \int_0^\infty F_{|\mathcal{H}_n|^2}(x\lambda_n) f_{|\mathcal{H}_e|^2}(x) dx, \end{aligned} \tag{4.20}$$

then using series expansion of CDF of gamma distribution we get the following equation

$$P_{out}^{n} = 1 - \int_{0}^{\infty} \sum_{k=0}^{\alpha_n - 1} \frac{\beta_n^k}{k!} x^k \lambda_n^{\frac{k}{2}} \exp(-\beta_n x \sqrt{\lambda_n}) \frac{\beta_e^{\alpha_e} x^{\alpha_e - 1}}{\Gamma(\alpha_e)} \exp(-\beta_e x) dx. \tag{4.21}$$

After collecting like terms and using equations from book, a closed-form equation for SOP can be formulated as

$$P_{out}^{n} = 1 - \sum_{k=0}^{\alpha_n - 1} \frac{K_1 \Gamma(k + \alpha_e)}{(\beta_n \lambda_n + \beta_e)^{\alpha_e + k}}, \tag{4.22}$$

here $K_1 = \frac{\beta_e^{\alpha_e} \beta_n^k \lambda^k}{\Gamma(\alpha_e) k!}$. Likewise, asymptotic $P_{out}^{f}$ can be evaluated.

$$P_{out}^{f} \approx \Pr \left\{ \frac{1 + \frac{\zeta_f^2}{\zeta_n^2}}{1 + \frac{\zeta_f^2}{\zeta_n^2}} < \lambda_f \right\} = \Pr \left\{ 1 < \lambda_f \right\} = 1 \ \ (\text{if } R_s^f > 0). \tag{4.23}$$

### 4.1.3 Probability of Non-Zero Secrecy Capacity

$$\begin{aligned} P_{nzc}^{n} &= \Pr \left\{ R_n - R_{en} > 0 \right\} = \Pr \left\{ \frac{1 + |\mathcal{H}_n|^2 \zeta_n^2 \Upsilon}{1 + |\mathcal{H}_e|^2 \zeta_n^2 \Upsilon} > 1 \right\} \\ &= \Pr \left\{ |\mathcal{H}_n|^2 > |\mathcal{H}_e|^2 \right\} = 1 - \Pr \left\{ |\mathcal{H}_n|^2 <= |\mathcal{H}_e|^2 \right\}, \end{aligned} \tag{4.24}$$

which can be expressed as

$$P_{nzc}^{n} = \int_{0}^{\infty} \frac{\gamma(\alpha_e, \beta_e x)}{\Gamma(\alpha_e)} \frac{\beta_n^{\alpha_n}}{\Gamma(\alpha_n)} x^{\alpha_n - 1} \exp -\beta_e x dx. \tag{4.25}$$

(4.25) can be solved using equation (6.455) Similarly, for the far vehicle, non-zero secrecy probability can be evaluated as

$$\begin{aligned} P_{nzc}^{n} = &\frac{\beta_n^{\alpha_n}}{\Gamma(\alpha_e)\Gamma(\alpha_n)} \frac{\beta_e^{\alpha_e} \Gamma(\alpha_n + \alpha_e)}{\alpha_e (\beta_e + \beta_n)^{\alpha_e + \alpha_n}} \\ &\times {}_1F_1 \left( 1, \alpha_n + \alpha_e; \alpha_e + 1; \frac{\beta_e}{\beta_e + \beta_n} \right), \end{aligned} \tag{4.26}$$

$$P_{nzc}^{f} = \Pr \left\{ R_f - R_{ef} > 0 \right\} = \Pr \left\{ \frac{1 + \frac{|\mathcal{H}_f|^2 \zeta_f^2 \Upsilon}{|\mathcal{H}_f|^2 \zeta_n^2 \Upsilon + 1}}{1 + \frac{|\mathcal{H}_e|^2 \zeta_f^2 \Upsilon}{|\mathcal{H}_e|^2 \zeta_n^2 \Upsilon + 1}} \right\}, \tag{4.27}$$

bringing to a common denominator and collecting like terms, (4.28) can be written as

$$P_{nzc}^{f} = \Pr\left\{|\mathcal{H}_f|^2 > |\mathcal{H}_e|^2\right\}. \tag{4.28}$$

Utilizing similar steps as for near vehicle (4.28) can be evaluated as

$$P_{nzc}^{f} = \frac{\beta_f^{\alpha_f}}{\Gamma(\alpha_e)\Gamma(\alpha_f)} \frac{\beta_e^{\alpha_e}\Gamma(\alpha_f+\alpha_e)}{\alpha_e(\beta_f+\beta_e)^{\alpha_e+\alpha_f}} \times {}_1F_1\left(1, \alpha_f+\alpha_e; \alpha_e+1; \frac{\beta_e}{\beta_e+\beta_f}\right). \tag{4.29}$$

This completes the analytical evaluation of the proposed secure RIS-aided V2V NOMA communication systems.

## 4.2 Results

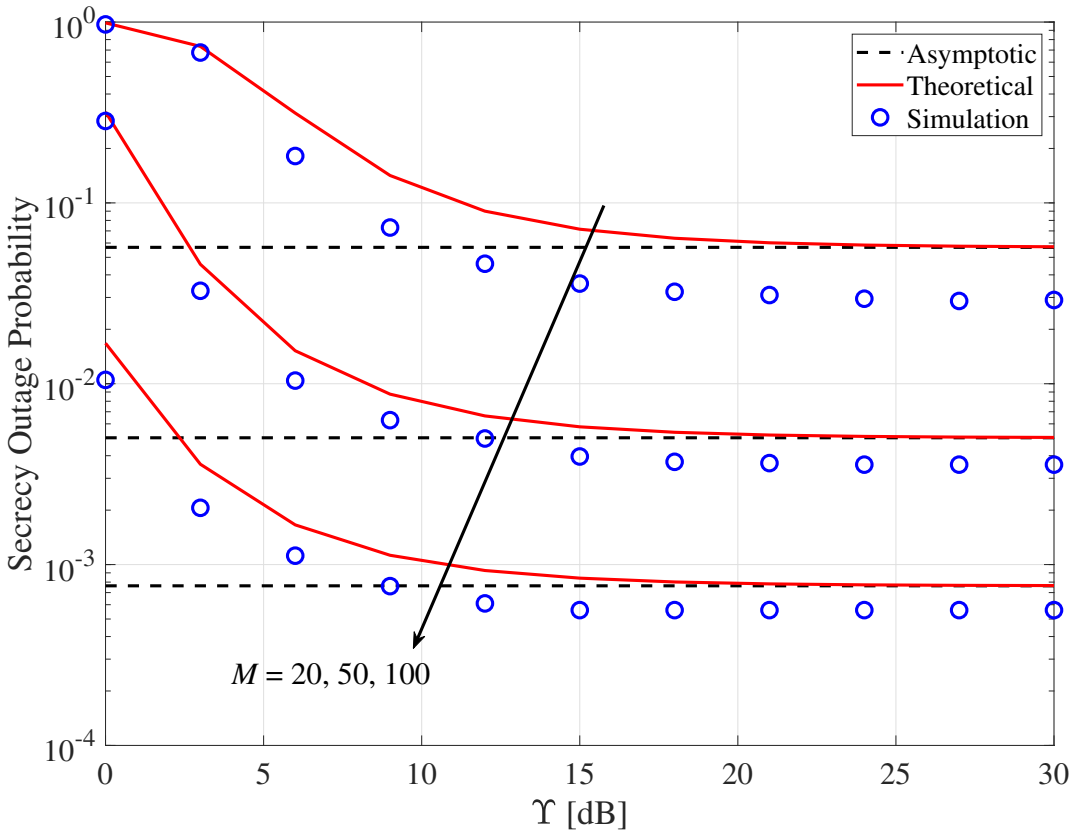


**Figure 4.1:** Secrecy outage probability for the $V_n$.

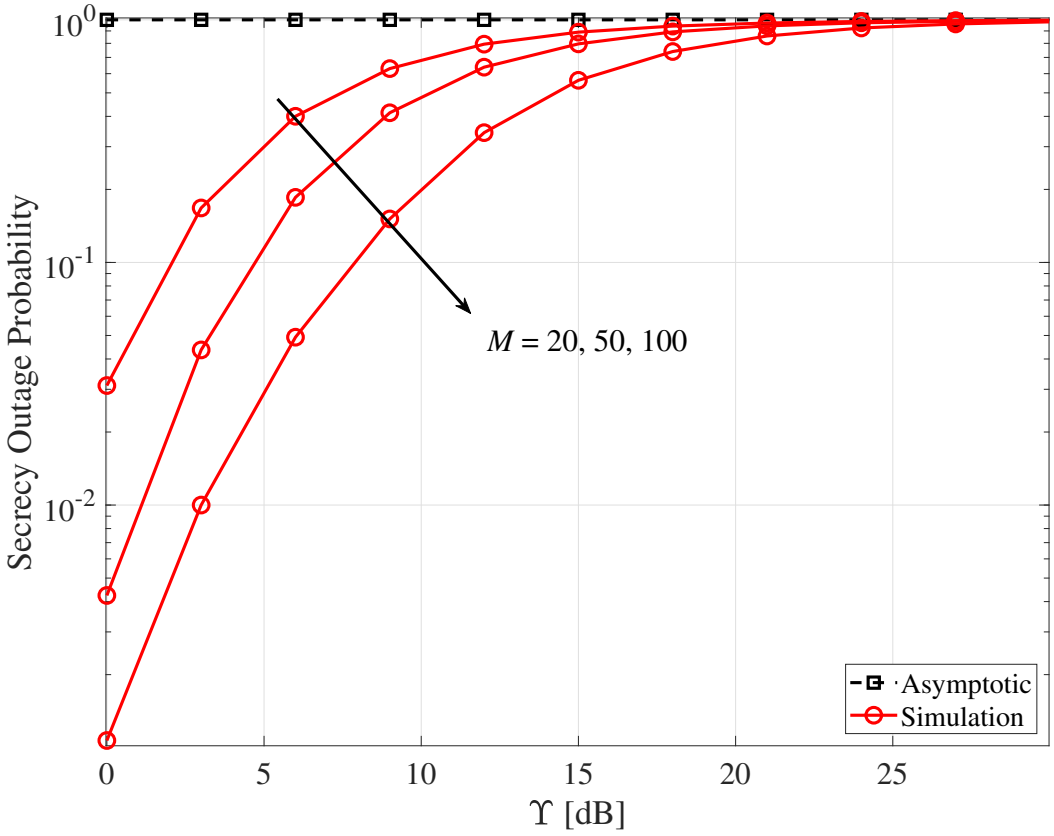


**Figure 4.2:** Secrecy outage probability for the $V_f$.

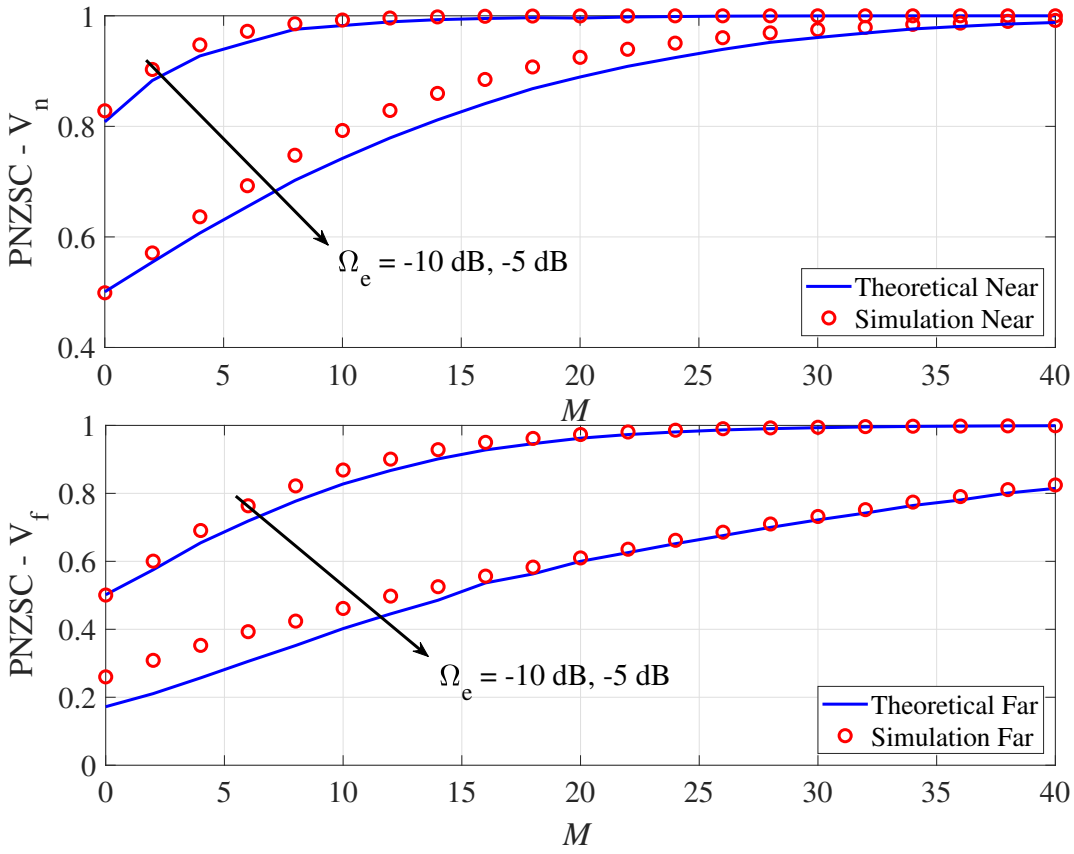


**Figure 4.3:** Probability of non-zero secrecy capacity for both vehicles

**Table 4.1:** Simulation Parameters

| Parameter | Simulation Values |
|---|---|
| Shape Parameter | $\{m_1, m_2, m_3, m_4\}$ = {5, 5, 5, 5}[37] |
| Spread Parameter | $\{\Omega_s, \Omega_n, \Omega_f, \Omega_e\} = \{-5, -5, -10, -15\}$ [38] |
| Scale Parameter | $\{\sigma_n^2, \sigma_f^2, \sigma_e^2\} = \{0, -5, -10\}$[39] |
| Power Allocation | $\{\zeta_n^2, \zeta_f^2\} = \{0.3, 0.7\}$ [40, 41] |
| REs Allocation | $\eta = 0.5$ |
| Target Secrecy Rate | $\{R_s^n, R_s^f\} = \{5, 0.5\}$ [42, 43] |
| Variance of Noise | $\sigma^2 = -120$[42] |

## 4.3 Discussions

In this section, the correctness of the derived closed-form expressions of SOP, ASOP, and PNZSC is verified through Monte Carlo simulations. The system parameters used for the simulation are listed in Table 4.1, unless specified differently.

Fig. 4.1 illustrates the SOP performance of $V_n$ in the presence of $V_e$. Notably, all the curves in this plot demonstrate a saturation effect as SNR increases, with the saturation level varying with respect to $M$. The increase in $M$ corresponds to an enhancement in outage performance. However, it is essential to recognize that a disparity exists between the simulation values and the other two curves. This discrepancy can be attributed to employing an approximation method, specifically the Taylor series expansion for the Gamma distribution.

Fig. 4.2 demonstrates SOP for $V_f$. It is worth noting that, in all three scenarios, SOP converges to a saturation point at one value. This phenomenon is attributed to its correlation with Y, wherein an increase in Y leads to the saturation of capacities of both $V_f$ and $V_e$, consequently causing SOP to approach 1 naturally. Furthermore, it is imperative to emphasize the paradoxical observation that an increase in $M$ results in a degradation of the secrecy performance of $V_f$. This observation is intriguing, as it suggests that, for larger values of $M$, both $V_f$ and $V_e$ reach the capacity saturation at an earlier stage. Fig. 4.3 depicts PNZSC for both $V_n$ and $V_f$. The simulation explores two distinct scenarios by varying the parameter $\Omega_e$ of $V_e$. When $\Omega_e$ is low (which means $V_e$ is located far), the secrecy performance is better. In both cases, PNZSC consistently converges toward 1. Notably, the PNZSC performance of $V_n$ surpasses that of $V_e$. This superior performance can be attributed to utilizing NOMA and the effects of path loss.

# Chapter 5

# Conclusion

In this paper, we studied physical layer security in RIS-aided NOMA-enabled wireless vehicular communication. We investigated the average secrecy capacity and secrecy outage probability for NOMA-paired vehicles. The results show that by selecting appropriate power allocation constants and transmitting SNR secrecy performance can be improved.

# Bibliography


[1] Yurui Cao et al. "Toward Smart and Secure V2X Communication in 5G and Beyond: A UAV-Enabled Aerial Intelligent Reflecting Surface Solution". In: *IEEE Vehicular Technology Magazine* 17.1 (2022), pp. 66–73. DOI: 10.1109/MVT.2021.3136832.

[2] Mohd Hamza Naim Shaikh et al. "On the Performance of Dual RIS-assisted V2I Communication under Nakagami-m Fading". In: *2022 IEEE 96th Vehicular Technology Conference (VTC2022-Fall)*. 2022, pp. 1–5. DOI: 10.1109/VTC2022-Fall57202.2022.10012862.

[3] Chen Chen, Baoji Wang, and Rongqing Zhang. "Interference Hypergraph-Based Resource Allocation (IHG-RA) for NOMA-Integrated V2X Networks". In: *IEEE Internet of Things Journal* 6.1 (2019), pp. 161–170. DOI: 10.1109/JIOT.2018.2875670.

[4] Fangchun Yang et al. "An overview of Internet of Vehicles". In: *China Communications* 11.10 (2014), pp. 1–15. DOI: 10.1109/CC.2014.6969789.

[5] Timothy Brown et al. "Ad hoc UAV ground network (AUGNet)". In: *AIAA 3rd" Unmanned Unlimited" Technical Conference, Workshop and Exhibit*. 2004, p. 6321.

[6] Jiadai Wang, Jiajia Liu, and Nei Kato. "Networking and Communications in Autonomous Driving: A Survey". In: *IEEE Communications Surveys & Tutorials* 21.2 (2019), pp. 1243–1274. DOI: 10.1109/COMST.2018.2888904.

[7] Yiliang Liu, Hsiao-Hwa Chen, and Liangmin Wang. "Physical Layer Security for Next Generation Wireless Networks: Theories, Technologies, and Challenges". In: *IEEE Communications Surveys Tutorials* 19.1 (2017), pp. 347–376. DOI: 10.1109/COMST.2016.2598968.

[8] Haji M Furqan et al. "Intelligent physical layer security approach for V2X communication". In: *arXiv preprint arXiv:1905.05075* (2019).

[9] Chao Wang et al. “Physical Layer Security Enhancement Using Artificial Noise in Cellular Vehicle-to-Everything (C-V2X) Networks”. In: *IEEE Transactions on Vehicular Technology* 69.12 (2020), pp. 15253–15268. DOI: 10.1109/TVT.2020.3037899.

[10] Xuewen Luo et al. “Physical Layer Security in Intelligently Connected Vehicle Networks”. In: *IEEE Network* 34.5 (2020), pp. 232–239. DOI: 10.1109/MNET.011.1900628.

[11] Haji M Furqan, Jehad Hamamreh, Huseyin Arslan, et al. “Physical layer security for NOMA: Requirements, merits, challenges, and recommendations”. In: *arXiv preprint arXiv:1905.05064* (2019).

[12] Xianbin Wang, Peng Hao, and Lajos Hanzo. “Physical-layer authentication for wireless security enhancement: current challenges and future developments”. In: *IEEE Communications Magazine* 54.6 (2016), pp. 152–158. DOI: 10.1109/MCOM.2016.7498103.

[13] Bruce Schneier. “Description of a new variable-length key, 64-bit block cipher (Blowfish)”. In: *Fast Software Encryption: Cambridge Security Workshop Cambridge, UK, December 9–11, 1993 Proceedings*. Springer. 2005, pp. 191–204.

[14] Matthieu Bloch and Joao Barros. *Physical-layer security: from information theory to security engineering*. Cambridge University Press, 2011.

[15] Ertugrul Basar. “Transmission Through Large Intelligent Surfaces: A New Frontier in Wireless Communications”. In: *2019 European Conference on Networks and Communications (EuCNC)*. 2019, pp. 112–117. DOI: 10.1109/EuCNC.2019.8801961.

[16] Yuanwei Liu et al. “Reconfigurable Intelligent Surfaces: Principles and Opportunities”. In: *IEEE Communications Surveys & Tutorials* 23.3 (2021), pp. 1546–1577. DOI: 10.1109/COMST.2021.3077737.

[17] Xiaojun Yuan et al. “Reconfigurable-Intelligent-Surface Empowered Wireless Communications: Challenges and Opportunities”. In: *IEEE Wireless Communications* 28.2 (2021), pp. 136–143. DOI: 10.1109/MWC.001.2000256.

[18] Yuya Saito et al. “System-level performance evaluation of downlink non-orthogonal multiple access (NOMA)”. In: *2013 IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*. 2013, pp. 611–615. DOI: 10.1109/PIMRC.2013.6666209.

[19] Zhiguo Ding et al. “Application of Non-Orthogonal Multiple Access in LTE and 5G Networks”. In: *IEEE Communications Magazine* 55.2 (2017), pp. 185–191. DOI: 10.1109/MCOM.2017.1500657CM.

[20] Boya Di et al. “Non-Orthogonal Multiple Access for High-Reliable and Low-Latency V2X Communications in 5G Systems”. In: *IEEE Journal on Selected Areas in Communications* 35.10 (2017), pp. 2383–2397. DOI: 10.1109/JSAC.2017.2726018.

[21] Abbas Ahmed et al. “Cooperative Non-Orthogonal Multiple Access for Beyond 5G Networks”. In: *IEEE Open Journal of the Communications Society* 2 (2021), pp. 990–999. DOI: 10.1109/OJCOMS.2021.3075081.

[22] Tianwei Hou et al. “Reconfigurable Intelligent Surface Aided NOMA Networks”. In: *IEEE Journal on Selected Areas in Communications* 38.11 (2020), pp. 2575–2588. DOI: 10.1109/JSAC.2020.3007039.

[23] Xidong Mu et al. “Exploiting Intelligent Reflecting Surfaces in NOMA Networks: Joint Beamforming Optimization”. In: *IEEE Transactions on Wireless Communications* 19.10 (2020), pp. 6884–6898. DOI: 10.1109/TWC.2020.3006915.

[24] Yun Ai et al. “Secure Vehicular Communications Through Reconfigurable Intelligent Surfaces”. In: *IEEE Transactions on Vehicular Technology* 70.7 (2021), pp. 7272–7276. DOI: 10.1109/TVT.2021.3088441.

[25] Neji Mensi, Danda B. Rawat, and Elyes Balti. “Physical Layer Security for V2I Communications: Reflecting Surfaces Vs. Relaying”. In: *2021 IEEE Global Communications Conference (GLOBECOM)*. 2021, pp. 01–06. DOI: 10.1109/GLOBECOM46510.2021.9685258.

[26] Beixiong Zheng et al. “Secure NOMA Based Two-Way Relay Networks Using Artificial Noise and Full Duplex”. In: *IEEE Journal on Selected Areas in Communications* 36.7 (2018), pp. 1426–1440. DOI: 10.1109/JSAC.2018.2824624.

[27] Xinrong Guan, Qingqing Wu, and Rui Zhang. “Intelligent reflecting surface assisted secrecy communication: Is artificial noise helpful or not?” In: *IEEE Wireless Communications Letters* 9.6 (2020), pp. 778–782.

[28] Miao Cui, Guangchi Zhang, and Rui Zhang. “Secure Wireless Communication via Intelligent Reflecting Surface”. In: *IEEE Wireless Communications Letters* 8.5 (2019), pp. 1410–1414. DOI: 10.1109/LWC.2019.2919685.

[29] Yun Ai et al. “On Physical Layer Security of Double Rayleigh Fading Channels for Vehicular Communications”. In: *IEEE Wireless Communications Letters* 7.6 (2018), pp. 1038–1041. DOI: 10.1109/LWC.2018.2852765.

[30] Sagar Kavaiya et al. “Physical Layer Security in Cognitive Vehicular Networks”. In: *IEEE Transactions on Communications* 69.4 (2021), pp. 2557–2569. DOI: 10.1109/TCOMM.2020.3038904.

[31] Abubakar U. Makarfi et al. "Physical Layer Security in Vehicular Networks with Reconfigurable Intelligent Surfaces". In: *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*. 2020, pp. 1–6. DOI: 10.1109/VTC2020-Spring48590.2020.9128438.

[32] Liang Yang and Yongjie Yuan. "Secrecy outage probability analysis for RIS-assisted NOMA systems". In: *Electronics Letters* 56.23 (2020), pp. 1254–1256.

[33] Zhiqing Tang et al. "Physical Layer Security of Intelligent Reflective Surface Aided NOMA Networks". In: *IEEE Transactions on Vehicular Technology* 71.7 (2022), pp. 7821–7834. DOI: 10.1109/TVT.2022.3168392.

[34] Farshad Rostami Ghadi, Masoud Kaveh, and Diego Martín. "Performance Analysis of RIS/STAR-IOS-aided V2V NOMA/OMA Communications over Composite Fading Channels". In: *IEEE Transactions on Intelligent Vehicles* (2023), pp. 1–9. DOI: 10.1109/TIV.2023.3337898.

[35] Ishan Budhiraja et al. "A Systematic Review on NOMA Variants for 5G and Beyond". In: *IEEE Access* 9 (2021), pp. 85573–85644. DOI: 10.1109/ACCESS.2021.3081601.

[36] Baha Eddine Youcef Belmekki, Abdelkrim Hamza, and Benoît Escrig. "Performance analysis of cooperative NOMA at intersections for vehicular communications in the presence of interference". In: *Ad Hoc Networks* 98 (2020), p. 102036.

[37] Ferkan Yilmaz, Mazen Omar Hasna, and Khalid Qaraqe. "Alternative expressions of the PDF and CDF for Gamma, $\eta$- $\mu$ and $\kappa$- $\mu$ shadowed distributions with applications in wireless communications". In: *Physical Communication* 56 (2023), p. 101935.

[38] Neha Jaiswal et al. "Physical Layer Security Performance of NOMA-Aided Vehicular Communications Over Nakagami-$m$ Time-Selective Fading Channels With Channel Estimation Errors". In: *IEEE Open Journal of Vehicular Technology* 4 (2023), pp. 72–100. DOI: 10.1109/OJVT.2022.3222187.

[39] Majid H. Khoshafa, Telex M. N. Ngatched, and Mohamed H. Ahmed. "RIS-Aided Physical Layer Security Improvement in Underlay Cognitive Radio Networks". In: *IEEE Systems Journal* (2023), pp. 1–12. DOI: 10.1109/JSYST.2023.3296012.

[40] Boqun Zhao et al. "Ergodic Rate Analysis of STAR-RIS Aided NOMA Systems". In: *IEEE Communications Letters* 26.10 (2022), pp. 2297–2301. DOI: 10.1109/LCOMM.2022.3194363.

[41] Dulaj Gunasinghe and Gayan Amarasuriya. "Performance Analysis of STAR-RIS for Wireless Communication". In: *IEEE International Conference on Communications*. 2022, pp. 3275–3280. DOI: 10.1109/ICC45855.2022.9838939.

[42] Mohd Hamza Naim Shaikh et al. "A Downlink RIS-Aided NOMA System With Hardware Impairments: Performance Characterization and Analysis". In: *IEEE Open Journal of Signal Processing* 3 (2022), pp. 288–305. DOI: 10.1109/OJSP.2022.3194416.

[43] Mohamed G. Abd El Ghafour et al. "Secrecy Outage Probability of Full-Duplex Relaying Vehicular Networks". In: *2022 10th International Japan-Africa Conference on Electronics, Communications, and Computations (JAC-ECC)*. 2022, pp. 98–103. DOI: 10.1109/JAC-ECC56395.2022.10044034.

# Appendix A

# Appendix A

Shape and rate parameters of gamma distribution can be derived as

$$\alpha_n = \frac{\mathbb{E}\left[|\mathcal{H}_n|^2\right]^2}{\mathbb{V}\left[|\mathcal{H}_n|^2\right]} \text{ and } \beta_n = \frac{\mathbb{E}\left[|\mathcal{H}_n|^2\right]}{\mathbb{V}\left[|\mathcal{H}_n|^2\right]}. \tag{A.1}$$

Further $\mathbb{E}\left[|\mathcal{H}_n|^2\right]$ can be expressed as

$$\begin{aligned}\mathbb{E}\left[|\mathcal{H}_n|^2\right] &= \mathbb{E}\left[|h_n + \mathbf{h_1}\Theta\mathbf{h_2}|^2\right] \\ &= \mathbb{V}[\mathcal{H}_n] + \mathbb{E}[\mathcal{H}_n]^2. \end{aligned}\tag{A.2}$$

Since $h_n$ is double Rayleigh fading $\mathbb{E}[h_n] = \sigma_n^2 \frac{\pi}{2}$. Second component can be written as

$$\mathbb{E}[\mathbf{h_1}\Theta\mathbf{h_2}] = \mathbb{E}\left[\sum_{i=1}^{M_1} \left|{h_1}^i\right| \left|{h_2}^i\right|\right], \tag{A.3}$$

here $h_1$ and $h_2$ are Nakagami-$m$ fading components their expected values are equal to

$$\mathbb{E}\left[h_1\right] = \frac{\Gamma(m_1 + \frac{1}{2})}{\Gamma(m_1)} \sqrt{\frac{\Omega}{m_1}}, \tag{A.4}$$

$$\mathbb{E}\left[h_2\right] = \frac{\Gamma(m_2 + \frac{1}{2})}{\Gamma(m_2)} \sqrt{\frac{\Omega_n}{m_2}}. \tag{A.5}$$

Further equation can be mathematically evaluated as

$$\mathbb{E}\left[\sum_{i=1}^{M_1} \left|{h_1}^i\right| \left|{h_2}^i\right|\right] = \frac{\Gamma(m_1+\frac{1}{2})}{\Gamma(m_1)} \sqrt{\frac{\Omega}{m_1}} \frac{\Gamma(m_2+\frac{1}{2})}{\Gamma(m_2)} \sqrt{\frac{\Omega_n}{m_2}} M_1. \tag{A.6}$$

Then $\mathbb{E}[\mathcal{H}_n]$ can be expressed as

$$\mathbb{E}[\mathcal{H}_n] = \frac{\Gamma(m_1+\frac{1}{2})}{\Gamma(m_1)}\sqrt{\frac{\Omega}{m_1}}\frac{\Gamma(m_2+\frac{1}{2})}{\Gamma(m_2)}\sqrt{\frac{\Omega_n}{m_2}}M_1 + \sigma_n^2\frac{\pi}{2}. \tag{A.7}$$

Further since the components of $\mathcal{H}_n$ are independent $\mathbb{V}[\mathcal{H}_n]$ can be expressed as

$$\mathbb{V}[\mathcal{H}_n] = \mathbb{V}[h_n] + \mathbb{V}\left[\sum_{i=1}^{M_1}\left|{h_1}^i\right|\left|{h_2}^i\right|\right], \tag{A.8}$$

then

$$\mathbb{V}[h_n] = \frac{16-\pi^2}{4}\sigma_n^4. \tag{A.9}$$

Further variance for nakagami-$m$ fading coefficients can be expressed as

$$\mathbb{V}[h_1] = \Omega\left(1 - \frac{1}{m_1}\left(\frac{\Gamma(m_1+\frac{1}{2})}{\Gamma(m_1)}\right)^2\right), \tag{A.10}$$

$$\mathbb{V}[h_2] = \Omega_n\left(1 - \frac{1}{m_2}\left(\frac{\Gamma(m_2+\frac{1}{2})}{\Gamma(m_2)}\right)^2\right), \tag{A.11}$$

then

$$\begin{aligned}\mathbb{V}\left[\sum_{i=1}^{M_1}\left|{h_1}^i\right|\left|{h_2}^i\right|\right] &= \Omega\Omega_n \\ &\times\left[1 - \frac{1}{m_1m_2}\left(\frac{\Gamma(m_1+\frac{1}{2})}{\Gamma(m_1)}\right)^2\left(\frac{\Gamma(m_2+\frac{1}{2})}{\Gamma(m_2)}\right)^2\right]M_1.\end{aligned} \tag{A.12}$$

Further $\mathbb{V}[\mathcal{H}_n]$ can be evaluated as

$$\begin{aligned}\mathbb{V}[\mathcal{H}_n] &= \frac{16-\pi^2}{4}\sigma_n^4 + \Omega\Omega_nM_1 \\ &\times\left[1 - \frac{1}{m_1m_2}\left(\frac{\Gamma(m_1+\frac{1}{2})}{\Gamma(m_1)}\right)^2\left(\frac{\Gamma(m_2+\frac{1}{2})}{\Gamma(m_2)}\right)^2\right].\end{aligned} \tag{A.13}$$

Then

$$\begin{aligned}\mathbb{E}\left[|\mathcal{H}_n|^2\right] &= \frac{16-\pi^2}{4}\sigma_n^4 + \Omega\Omega_nM_1 \\ &\times\left[1 - \frac{1}{m_1m_2}\left(\frac{\Gamma(m_1+\frac{1}{2})}{\Gamma(m_1)}\right)^2\left(\frac{\Gamma(m_2+\frac{1}{2})}{\Gamma(m_2)}\right)^2\right] \\ &+\left(\frac{\Gamma(m_1+\frac{1}{2})}{\Gamma(m_1)}\sqrt{\frac{\Omega}{m_1}}\frac{\Gamma(m_2+\frac{1}{2})}{\Gamma(m_2)}\sqrt{\frac{\Omega_n}{m_2}}M_1 + \sigma_n^2\frac{\pi}{2}.\right)^2\end{aligned} \tag{A.14}$$

Further $\mathbb{V}\left[|\mathcal{H}_n|^2\right]$ can be expressed as

$$\mathbb{V}\left[|\mathcal{H}_n|^2\right] = \mathbb{E}\left[|\mathcal{H}_n|^4\right] - \mathbb{E}\left[|\mathcal{H}_n|^2\right]^2. \tag{A.15}$$

Since our channel is approximated through Gamma. 4th moment of expected value can be calculated as

$$\mathbb{E}\left[|\mathcal{H}_n|^4\right] = \frac{\theta^4\Gamma(4+k)}{\Gamma(k)}, \tag{A.16}$$

here

$$k = \frac{\mathbb{E}\left[|\mathcal{H}_n|\right]^2}{\mathbb{V}\left[|\mathcal{H}_n|\right]} \text{ and } \theta = \frac{\mathbb{V}\left[|\mathcal{H}_n|\right]}{\mathbb{E}\left[|\mathcal{H}_n|\right]}. \tag{A.17}$$

Then (A.14) and (A.16) is substituted to (A.15) Next, (A.15) and (A.14) is substituted to (A.1) to get $\alpha_n$ and $\beta_n$. Similar steps are performed to get $\alpha_f$ and $\beta_f$. However, for $V_e$ we need a different approach because of the presence of random phases. Thus

$$\alpha_e = \frac{\mathbb{E}[\mathcal{H}_e]^2}{\mathbb{V}[\mathcal{H}_e]} \text{ and } \beta_e = \frac{\mathbb{E}[\mathcal{H}_e]}{\mathbb{V}[\mathcal{H}_e]}. \tag{A.18}$$

Further $\mathbb{E}[\mathcal{H}_e]$ and $\mathbb{V}[\mathcal{H}_e]$ can be calculated as

$$\begin{aligned}\mathbb{E}[\mathcal{H}_e] &= \mathbb{E}\left[h_e + \sum_{i=1}^{M} {h_1}^i {h_4}^i \exp(\theta_i)\right] \\ &= \mathbb{E}\left[h_e + \sum_{i=1}^{M} G^i \exp(\theta_i)\right].\end{aligned} \tag{A.19}$$

Since all paths have random and equally distributed phases, they will have imaginary and real parts. Both of them are Gaussian random distributions with parameters $\mu = 0$ and $\sigma$. Here $\sigma$ is the square root of its variance. And their envelope will be Rayleigh distribution. Further $G^i \exp(\theta_i)$ can be expressed as

$$G^i \exp(\theta_i) = X + jY \quad G^2 = X^2 + Y^2, \tag{A.20}$$

since $X$ and $Y$ are independent but identical distributions (A.20) can be written as

$$\begin{aligned}&G^2 = 2X^2 \\ &\mathbb{V}[X] = \mathbb{E}[X^2] - \mathbb{E}[X]^2 = \mathbb{E}[X^2] = \mathbb{E}\left[\frac{G^2}{2}\right] = \frac{\mathbb{V}[G] + \mathbb{E}[G]^2}{2}.\end{aligned} \tag{A.21}$$

In addition, the variance of components of $h_e$ is $2\sigma_e^2$ Finally, the variance of the overall real part will be

$$\mathbb{V}[\mathcal{H}_e^r] = \frac{\left(\mathbb{V}[h_1 h_4] + \mathbb{E}[h_1 h_4]^2\right) M}{2} + \frac{\mathbb{V}[h_e] + \mathbb{E}[h_e]^2}{2}, \tag{A.22}$$

here $\mathbb{E}[h_e] = \sigma_e^2 \frac{pi}{2}$ and $\mathbb{V}[h_e] = \frac{16-\pi^2}{4}\sigma_e^4$.

$$\mathbb{V}[h_4] = \Omega_e \left(1 - \frac{1}{m_4}\left(\frac{\Gamma(m_4+\frac{1}{2})}{\Gamma(m_4)}\right)^2\right), \tag{A.23}$$

further

$$\mathbb{V}[h_1 h_4] = \Omega\Omega_e \left[1 - \frac{1}{m_1 m_2}\left(\frac{\Gamma(m_1+\frac{1}{2})}{\Gamma(m_1)}\right)^2 \left(\frac{\Gamma(m_4+\frac{1}{2})}{\Gamma(m_4)}\right)^2\right], \tag{A.24}$$

then

$$\mathbb{E}\left[h_4\right] = \frac{\Gamma(m_4+\frac{1}{2})}{\Gamma(m_4)}\sqrt{\frac{\Omega_e}{m_4}}. \tag{A.25}$$

$$\mathbb{E}\left[h_1 h_4\right] = \frac{\Gamma(m_1+\frac{1}{2})}{\Gamma(m_1)}\sqrt{\frac{\Omega}{m_1}}\frac{\Gamma(m_4+\frac{1}{2})}{\Gamma(m_4)}\sqrt{\frac{\Omega_e}{m_4}}. \tag{A.26}$$

After, substituting values into (A.22) we get

$$\mathbb{V}[\mathcal{H}_e^r] = \frac{\Omega\Omega_e M + 4\sigma_e^4}{2}. \tag{A.27}$$

The variance of the Imaginary part will be the same so their envelope will result in Rayleigh with mean and variance as

$$\mathbb{E}[\mathcal{H}_e] = \sqrt{\frac{\Omega\Omega_e M + 4\sigma_e^4}{2}\frac{\pi}{2}}. \tag{A.28}$$

$$\mathbb{V}[\mathcal{H}_e] = \frac{\Omega\Omega_e M + 4\sigma_e^4}{2}\frac{4-\pi}{2}. \tag{A.29}$$

Further to calculate $\mathbb{E}[|\mathcal{H}_e|^2]$

$$\mathbb{E}\left[|\mathcal{H}_e|^2\right] = \mathbb{V}[\mathcal{H}_e] + \mathbb{E}[\mathcal{H}_e]^2 = \Omega\Omega_e M + 4\sigma_e^4, \tag{A.30}$$

$$\mathbb{V}\left[|\mathcal{H}_e|^2\right] = \mathbb{E}\left[|\mathcal{H}_e|^4\right] - \mathbb{E}\left[|\mathcal{H}_e|^2\right]^2. \tag{A.31}$$

Here we need to calculate the fourth moment of Rayleigh distribution which is $\sigma^4$

$$\begin{aligned}\mathbb{V}\left[|\mathcal{H}_e|^2\right] &= 8\mathbb{V}\left[\mathcal{H}_e^r\right]^2 - \mathbb{E}\left[|\mathcal{H}_e|^2\right]^2 \\ &= \Omega^2\Omega_e^2 M^2 + 8\sigma_e^4\Omega\Omega_e M + 16\sigma_e^8,\end{aligned} \tag{A.32}$$

after getting shape and rate constants for the gamma approximation method we substitute (A.32) and (A.30) to (A.18)