Physical Layer Security in Wireless Cooperative Networks using Jamming and Beamforming

Author: Jeevan Jutla
Supervisor: Prof. Mohammad Shikh-Bahaei
Student ID: 20027901

April 2023

Abstract

Physical Layer Security is an emerging concept used in wireless communications alongside cryptography to prevent unauthorized devices from eavesdropping on a legitimate transmission. It offers low computational cost and overhead by injecting an interfering signal in the wiretap channels of potential eavesdroppers. This dissertation investigates the problem of effectively improving the security of wireless communication networks. The study focuses on the integration of jamming and beamforming techniques to achieve enhanced security, particularly in Vehicle-to-Everything (V2X) networks.

The research provides a comprehensive analysis of three distinct cooperative jamming schemes, examining their effectiveness in maintaining secure communication channels. Subsequently, the integration of cooperative jamming with beamforming is explored to assess its impact on overall security performance.

The novel contribution of this dissertation is the implementation of a two-phase cooperative jamming scheme combined with relay selection and beamforming in a V2X network scenario. By comparing the performance of this approach to traditional cooperative jamming methods using metrics such as secrecy rates and secrecy outage probability, the proposed two phase cooperative jamming scheme demonstrates significant improvements in physical layer security for V2X networks.

Originality Avowal

I verify that I am the sole author of this report, except where explicitly stated to the contrary. I grant the right to King's College London to make paper and electronic copies of the submitted work for purposes of marking, plagiarism detection and archival, and to upload a copy of the work to Turnitin or another trusted plagiarism detection service. I confirm this report does not exceed 25,000 words.

Jeevan Jutla
April 2023

Acknowledgements

I extend my sincerest thanks to my supervisor, Prof. Mohammad Shikh-Bahaei, for their unwavering support and guidance throughout my dissertation journey. Their insightful comments, constructive feedback, and boundless patience have had a profound impact on shaping my research and writing. I am also deeply grateful to my secondary supervisor, Yinchao Yang, for their valuable contributions and feedback, which have helped me refine my research questions and methods. I am thankful to the Engineering department Kings College London for their continual support and provision of the necessary resources that have enabled me to successfully complete this research.

Contents

Chapter 1

Introduction

Wireless communication systems have experienced rapid growth and widespread adoption, fundamentally transforming our daily lives, work, and social interactions. Among the various advancements in this field, cooperative networks have gained prominence as they address challenges related to reliability, capacity and coverage across different communication scenarios. With the increasing reliance on cooperative networks, safeguarding transmitted information at the physical layer has become a matter of utmost importance. As the landscape of cybersecurity threats evolves, new techniques for enhancing physical layer security must be developed to combat increasingly sophisticated attacks such as eavesdropping and jamming.

This dissertation investigates the problem of effectively improving physical layer security in cooperative wireless networks, focusing on the integration of jamming and beamforming techniques to achieve enhanced security, particularly on the applications in Vehicle-to-Everything (V2X) networks. The research provides a comprehensive analysis of existing cooperative jamming schemes, assessing their effectiveness in maintaining secure communication channels and their uses in V2X networks. It also explores the integration of cooperative jamming with beamforming and its security performance in cooperative networks.

The novel contribution of this dissertation is the evaluation and implementation of a two-phase cooperative jamming scheme combined with beamforming in a V2X network scenario. The performance of this scheme is compared to traditional cooperative jamming methods using metrics such as secrecy rates and secrecy outage probability. The analysis demonstrate that the novel two-phase cooperative jamming scheme, when combined with beamforming, offers substantial improvements in physical layer security for V2X networks.

Chapter 2

Literature Evaluation

2.1 Physical Layer Security

Wireless communication has become essential in modern life, transmitting various data types, including sensitive and personally identifiable information. As of January 2022, the UN's International Telecommunication Union reported 5.3 billion internet users worldwide [36] accounting for 65% of the global population. However, the increase in wireless devices has also led to a rise in cybercrime. The World Economic Forum estimates that cybercrime will cost $5 trillion by 2024 and $10.5 trillion by 2025 [10]. Therefore, enhancing the security of wireless networks to combat these malicious activities is crucial.

Cooperative wireless networks, first introduced by Cover and Gamal [4], represent a significant advancement in wireless communication technology. These networks involve multiple nodes collaborating to transmit and relay information, improving network performance and security. Cooperative networks have contributed to the development of distributed antenna systems used in 4G and 5G networks [11] and cooperative multiple access protocols implemented in wireless communication standards including the IEEE 802.11n and 802.11ac [23]. As wireless devices become more prevalent and secure communication becomes increasingly important, cooperative networks offer a promising solution to address the growing demand for cutting-edge network technologies.

Traditionally, data transmission security is handled at the software levels of the Open System Interconnection (OSI) model, which addresses confidentiality, integrity and availability using cryptographic algorithms. These methods are considered secure, assuming eavesdroppers have limited computing power. However, quantum computing threatens the security of these cryptographic schemes due to its immense computational capacity, enabling unauthorized users to intercept data transmissions and access and modify the data, as shown by Shor's [28] and Grover's Algorithm [12]. Although powerful enough quantum computers are still 20-30 years away [6], cybercriminals and threat actors are already taking advantage of this by engaging in Harvest Now Decrypt Later (HNDL) attacks, where encrypted data is intercepted and stored with the belief that future access to quantum computers will enable decryption. They believe that intercepting and storing sensitive data now will still hold value in the future and upon the breakthrough of powerful enough quantum computers they will be able to decrypt this data [3]. These eavesdropping attacks can be conducted passively or actively. Passive attacks involve silently listening to transmissions and stealing information, while active attacks use aggressive techniques like denial of service and routing attacks to degrade signal quality.

Attackers can also combine passive and active eavesdropping attacks to form an attack such as the man in the middle (MITM) attack. In these attacks, cybercriminals can intercept the communication between two parties and

can potentially modify, relay or jam the data being transmitted. While cryptographic measures can sometimes protect against these attacks, they may not be sufficient to prevent tampering or modification of data. Security researchers Xia et al. [38] demonstrated a MITM attack to break the security of OpenSSL, a widely used cryptographic library for network communications. Furthermore, cryptographic algorithms cannot identify if these types of attacks are occurring, resulting in the need for complex network security and intrusion detection systems to ensure security, as concluded by both Hoang et al. [16] and Kapetanovic et al. [19].

Side channel attacks represent another class of weaknesses that exploit vulnerabilities in cryptographic algorithms. These attacks were first publicised by Paul Kocher in 1996 [30], who demonstrated that power consumption measurements and electromagnetic radiation emissions of a microcontroller executing RSA encryption could reveal the secret key, enabling an attacker to break the encryption. Instead of targeting the mathematical foundations of cryptographic schemes, side-channel attacks exploit unintentional information leakage during their implementation. Side channel information including power consumption, electromagnetic radiation or execution time, can be analyzed by attackers to infer sensitive data, including encryption keys. Gathering and analyzing this unintentional information leakage allows adversaries to bypass cryptographic algorithm security mechanisms and gain unauthorized access to protected data. Examples include the 2005 vulnerability discovery in widely used smart cards by Mangard et al. [25] and demonstrations in 2014 and 2015 by security researcher Colin O'Flynn, who used electromagnetic side channel analysis to extract secret keys from various IoT devices.

Traditional security methods used in wireless communication is becoming more at risk due to the open and overlapping design of wireless transmission, which allows attackers to passively or actively eavesdrop on the channel, raising concerns about confidentiality and security. To mitigate these risks, wireless networks must possess certain capabilities beyond cryptography. The concept of Physical Layer Security differs from traditional cryptographic technologies by providing security without encryption in the upper layers. PLS uses wireless channel characteristics such as channel fading, noise and interference to provide security even against attackers with significant computational resources. Sánchez et al. [33] review of PLS approaches to secure 5G networks concludes that the "*level of secrecy will not be affected even if the eavesdropper has powerful computing.*" Furthermore, PLS can detect when an attack is occurring, as demonstrated by Kapetanovic et al. [18] work on beamforming to detect eavesdropping attacks.

The majority of research in the area of PLS is focused on discovering different methods to supplement current security protocols in wireless networks, which typically rely on cryptographic algorithms and to ensure long-term security that supports the advancements of 5G and 6G wireless networks and improvements in computational power.

Information theoretic security, also known as unconditional security or perfect secrecy, is a robust security model for cryptographic systems. It guarantees security not by computational complexity but by the underlying information theory. A cryptosystem with information-theoretic security is considered unbreakable, even by an attacker with unlimited computational power [22]. This level of security is particularly relevant for PLS, which focuses on ensuring the confidentiality and integrity of data transmitted over a communication channel. Within the scope of Physical Layer Security, information-theoretic security is achieved when an eavesdropper is unable to extract any meaningful information from the transmitted data, despite having access to the communication channel and possessing infinite computational capabilities. To achieve this level of security, it is necessary to optimise the architecture of the communication system in order to maximise the difference between the mutual knowledge between the reciever and the eavesdropper [31].

Shannon's wiretap channel model [27] is a foundational concept in PLS and information-theoretic security. A sender communicates with a legitimate receiver in a noisy channel, while an eavesdropper listens in. The objective is to maximize the information exchange between sender and receiver while minimizing the information exchange between the sender and eavesdropper. By achieving this, perfect secrecy can be maintained, preventing the eavesdropper from acquiring any useful information about the transmitted data. Shannon introduced the concept of channel capacity [1], which represents the maximum information transmission rate achievable over a communication channel while reducing the probability of error. In the context of an Additive White Gaussian Noise (AWGN) channel the channel capacity is expressed as follows:

$$C = B\log_2(1 + SNR) \tag{2.1}$$

$$SNR = \frac{P}{\sigma^2} \tag{2.2}$$

where B is the channel's bandwidth, P is the power of the signal, σ^2 is the noise power and SNR is the signal-to-noise ratio.

Secrecy capacity is essential in PLS, as it defines the secure signal transmission rate to a legitimate receiver without eavesdropper intrusion. In Shannon's wiretap model, Alice sends confidential information (A) to Bob (B) while avoiding eavesdropper Eve (E). Shannon introduced perfect secrecy but deemed it impractical in some networks due to key management issues.

Wyner proposed weak secrecy as an alternative [37], with transmission rate $R = \frac{k}{n}$ (bits/channel) and equivocation rate $\Delta = \frac{1}{k}H(A_k|E_n)$. In practical situations, weak secrecy can be attained even when the eavesdropper's channel state remains unknown, but weak secrecy can sometimes be insufficient due to its reliance on maintaining a non-zero rate of uncertainty at the eavesdropper's end. This non-zero rate of uncertainty means that while the eavesdropper may not have complete access to the transmitted information, they may still gain partial knowledge of it.

Information theoretic security metrics have been crucial for developing secrecy coding but can be hard to evaluate. Alternative metrics are used to assess PLS performance, such as secrecy rate, which calculates the reliable transmission rate without eavesdropper decoding. In a Gaussian channel, secrecy rate (R_s) is determined by the difference between the sender (A) and receiver (B) and the sender (A) and eavesdropper (E) :

$$R_s = R_B - R_E = \log_2\left(1 + \frac{P_{TH} * B}{\sigma_B^2}\right) - \log_2\left(1 + \frac{P_{TH} * E}{\sigma_E^2}\right),$$

Another essential metric is secrecy outage probability (SOP), which defines the likelihood that a specified secrecy rate cannot be reached for a given system. SOP is especially beneficial when Alice knows limited channel state information (CSI) on both Bob and Eve. SOP is utilised in various situations when the transmitter is aware of the eavesdroppers CSI. [17].

Secrecy ergodic capacity is another crucial metric in evaluating PLS performance. It represents the average secrecy capacity over all possible channel realizations, taking into account the variability and randomness of wireless communication channels. Similar to secrecy outage probability (SOP), secrecy ergodic capacity focuses on the achievable secrecy rates under varying channel conditions. However, unlike SOP, which quantifies the probability of failing to achieve a specific secrecy rate, secrecy ergodic capacity provides an overall measure of the expected secrecy rate that can be maintained over time [32]. This metric enables the assessment of the long-term secrecy

performance of a communication system, accounting for the inherent uncertainties in the wireless environment.

2.2 PLS Techniques

To increase the PLS in cooperative networks, many relaying technologies are utilised [43], with amplify and forward (AF) and decode and forward (DF) being the most prevalent options.

AF relays function by receiving a signal, amplifying it and forwarding the amplified signal to the destination. This method preserves the signal's structure, making it less vulnerable to eavesdropping. However, AF relays may also amplify noise, which can degrade the signal quality at the legitimate receiver as shown by Yu and Li [40]. DF relays decode the signal, recover the original information, and then re-encode and transmit the signal to the destination. This process can improve the overall signal quality, as the relay does not forward noise. However, successful DF operation relies on the relay's ability to decode the source signal correctly, which has been proven in noisy environments [21].

Cooperative networks using AF or DF relays have proven capability of enhancing communication security through jamming and beamforming [7]. Jamming introduces intentional interference to degrade the eavesdropper's received signal quality, while beamforming focuses the message in the desired direction of the legitimate receiver, making it harder for eavesdroppers to intercept the signal. By employing AF or DF relays along with jamming and beamforming techniques, cooperative networks can achieve higher levels of physical layer security, protecting confidential information from potential eavesdroppers.

Beamforming

Beamforming is a popular PLS technique that directs signals efficiently toward specific directions, maximizing the signal difference between intended and unintended receivers. By focusing the beam on the target, beamforming increases the signal-to-noise power ratio [18] and suppresses reception or transmission toward the unintended user. This technique enhances the system's energy efficiency by concentrating energy in a specific direction instead of spreading it out.

In physical layer security, beamforming aims to direct the transmitted signal toward the intended user while considering the eavesdropper attempting to decode the transmitted information. Many studies have explored beamforming optimization problems in PLS to develop algorithms that minimize interference and maximize transmission secrecy, using techniques like semi-definite relaxation [15] and Taylor expansion [24]. These methods have proven to provide computational efficiency and accuracy in solving non-convex optimization problems, leading to enhanced security performance while maintaining a reasonable computational cost.

Artificial Noise

Artificial noise (AN) is a technique that degrades the eavesdropper's channel quality by generating an interference signal. The transmitter divides its power between sending information to the destination and transmitting noise to the eavesdropper. The generation of artificial noise relies on the transmitter's awareness of the eavesdroppers' CSI [41]. By leveraging this knowledge, the transmitter can strategically allocate power to produce AN that specifically disrupts the eavesdroppers' channels, while minimizing its effect on the legitimate user's channel. This targeted interference enables the transmitter to boost the overall security of the communication system without substantially degrading the communication quality between the transmitter and the intended receiver.

Cooperative Jamming

Cooperative jamming the most common PLS technique proposed to enhance security and prevent eavesdropping in wireless networks [8]. It involves a source to transmit its message to the legitimate receiver and uses a relay to transmit a jamming signal to create interference and degrade the eavesdropper's channel improving the secrecy rate. Current research in cooperative jamming focuses on integrating this technique with 5G and 6G technologies. However, the literature still lacks a comprehensive understanding of cooperative jamming's performance in various dynamic network topologies and deployment scenarios.

Energy Harvesting

Energy harvesting (EH) is a promising technology for wireless networks, enabling devices to collect energy from external sources including solar power, wind or radio frequency. In the context of PLS, energy harvesting provides an opportunity to enhance security by powering cooperative nodes or jammers, reducing energy consumption and enabling more effective countermeasures against eavesdropping.

Integrating EH into PLS schemes can improve the overall network performance by reducing the energy cost [35]. For example, EH-powered cooperative jammers can create interference for eavesdroppers, degrading their channel quality while preserving the legitimate receiver's signal integrity. Moreover, energy harvesting can enable energy-constrained devices, such as embedded or IoT devices [9], to participate in cooperative jamming or relaying, contributing to improved network security.

Recent studies have explored the combination of EH and PLS, focusing on the power allocation between EH transmission and AN generation. These studies aim to maximize secrecy rates and ensure secure communication under various channel conditions and energy constraints. Integrating energy harvesting into PLS schemes is expected to be a vital research area in the design of future secure wireless networks. However, the literature still lacks an in-depth investigation into the impact of different EH techniques and energy source availability on PLS performance.

Two-Phase Cooperative Jamming

Two-phase cooperative jamming is a recent technique first published by Hatami et al. [14] that divides the transmission process into two distinct phases. This approach leverages cooperative jammers to confuse the eavesdropper while employing beamforming to prevent interference at the desired relays. During the first phase, the source node sends a signal to the relays, while the relay nodes provide jamming signals to confound the listening eavesdroppers. During this phase, the beamforming method is used to decrease interference at friendly nodes that will receive the delivered message. The message is beamformed to the destination by two chosen relays in the second step. As a result, the receiver may decode the provided information without being influenced by the jamming signals, but the eavesdropper's capacity to intercept the transmission is severely reduced.

Two-phase cooperative jamming, a relatively new physical layer security technique, has not been studied as extensively as other methods, such as beamforming and cooperative jamming. The complexity introduced by its two distinct transmission phases and the involvement of multiple nodes, coupled with the difficulty of obtaining accurate CSI for both legitimate receivers and eavesdroppers, has contributed to the scarcity of research in this area. Additionally, the limited applicability of this technique in scenarios with strict resource constraints or a small number of nodes has led researchers to focus more on established techniques with proven results.

Current research shows no application of two-phase cooperative jamming in V2X networks thus far. Therefore, this dissertation aims to explore the potential of this technique in enhancing physical layer security in the dynamic and challenging environment of V2X networks through a novel simulation. By investigating the effectiveness of two-phase cooperative jamming in V2X networks, this research seeks to contribute to the understanding and development of robust and scalable security solutions for these critical communication systems.

2.3 Vehicle to Everything (V2X) Networks

Vehicle-to-Everything (V2X) networks have become a vital technology for facilitating intelligent transportation systems, enabling communication among vehicles, infrastructure, devices, and other vehicles. These networks accommodate real-time and safety-critical applications, such as collision detection and prevention, traffic management, and emergency service response coordination. Ensuring secure communication is vital for the proper functioning of these applications, as security breaches could lead to catastrophic consequences. Physical layer security techniques can help to improve the security of V2X networks and reduce eavesdropping attacks [13].

V2X networks pose unique challenges that make securing them a complex task. The constantly changing network topology, resulting from node mobility, makes it difficult to maintain consistent levels of secrecy in the communication. V2X networks often operate under resource constraints [39], including limited bandwidth, power, and computational resources. As V2X networks continue to grow in size and complexity, scalable security solutions are essential. Several physical layer security techniques can be employed to improve the security of V2X networks. Beamforming can be utilized in V2X networks [2] to direct the transmitted signal toward the intended vehicle or infrastructure while minimizing the signal strength in the direction of potential eavesdroppers. This technique can improve the secrecy rate and energy efficiency in V2X communications, even in the presence of highly dynamic network topologies. Researchers have proposed adaptive beamforming algorithms [29] that adjust to the rapidly changing positions of vehicles in V2X networks to maintain a high level of security.

In V2X (Vehicle-to-Everything) networks, the physical layer security techniques explored above can be utilized to diminish the eavesdropper's channel quality by producing interference signals. da Silva et al. [5] proved these strategies to be especially effective in situations where vehicles are in close proximity and eavesdroppers are more likely to be present. Energy harvesting can be integrated into V2X networks to power cooperative nodes or jammers, reducing energy consumption and enabling more effective countermeasures against eavesdropping. Vehicles equipped with energy harvesting capabilities can participate in cooperative jamming or relaying, contributing to improved network security. Zhu et al. [42] explored the combination of energy harvesting and artificial noise in V2X networks, focusing on power allocation between EH and AN generation. The study concluded that the optimal allocation strategy led to a significant improvement in network security while maintaining energy efficiency, demonstrating the potential of combining energy harvesting and artificial noise in V2X networks to create a more secure and sustainable communication environment. AF and DF relays can be employed in V2X networks [26] to improve communication security through jamming and beamforming.

While various PLS techniques have shown promise in enhancing the security of V2X networks, several research gaps remain specifically the development of adaptive and robust PLS techniques that can handle the highly dynamic nature of V2X networks. To contribute to the research in this area, this dissertation presents a novel simulation, which compares the performance of the promising two-phase cooperative jamming scheme against a conventional cooperative jamming scheme. The findings of this comparison will provide valuable insights into the effectiveness of these techniques and their potential for further development and application within V2X network security.

Chapter 3

Cooperative Jamming

This chapter examines the effectiveness of three cooperative jamming schemes: traditional cooperative jamming, optimal relay selection and energy harvesting. Section 3.1 discusses a basic cooperative jamming scheme as a foundation for further analysis. Section 3.2 extends the basic scheme by combining jamming and optimal relay selection, evaluating the performance of three popular algorithms. In Section 3.3, a technique that combines jamming and energy harvesting is introduced, comparing the secrecy rate performance of various relaying modes to understand their implications. Lastly, Section 3.4 explores Optimal Relay Selection (ORS), a sub-scheme determining the most effective primary relaying mode between AF and DF to be utilized in Chapter 4.

3.1 Traditional Cooperative Jamming

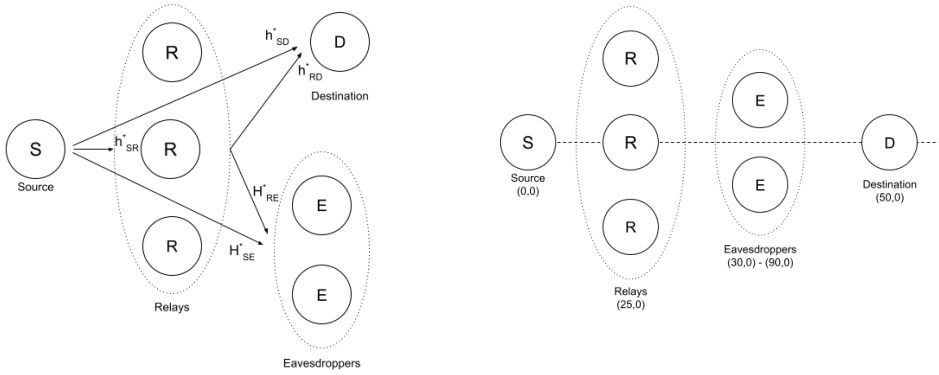
The cooperative jamming scheme explored in this system is modelled on the research by Dong et al. [7]. This section focuses on improving security between a source and a destination, facilitated by cooperating relays while being passively eavesdropped by at least one attacker. A conventional cooperative jamming scheme is examined, where the relay sends a jamming signal aimed at eavesdroppers, while a direct transmission serves as a reference to gauge the effectiveness of this technique.

3.1.1 System Model

A wireless network model is simulated where the source sends an encoded signal symbol $\sqrt{P_s}x$ directly to the destination and the relays transmit a separate jamming signal z with the aim of causing interference at the eavesdroppers node. The attackers are passive and aim to intercept the transmitted information without attempting to modify it. For simplicity, a one dimensional model is used, as depicted in Figure 3.1(b) where the source, relays and destination are positioned along a line. The network has a single source, three relays, one eavesdropper and one destination. The source, located at (0, 0), transmits a symbol to the destination at (50, 0) via three relays situated halfway at (25, 0), while the eavesdropper moves from (30, 0) to (90, 0). The number of relays can be adjusted without significantly impacting the model.

3.1.2 Analytical Results

The following notation is used. Bold uppercase letters ($\mathbf{R}$, etc) represent matrices and bold lowercase letters ($\mathbf{w}$,$\mathbf{h}$ etc) represent column vectors (nx1). $\| \boldsymbol{h} \|$ denotes the 2-norm of vector h and $|h|$ denotes the magnitude of complex number h. Conjugate, transpose and conjugate transpose are represented by $(\cdot)^*$, $(\cdot)^T$ and $(\cdot)^\dagger$ respectively.



(a) Two-Dimensional system model (b) One-Dimensional system model

Figure 3.1: System Model

The message at the destination and the eavesdropper is modelled as:

$$y_d = \sqrt{P_s} h_{SD}^* x + \mathbf{h}_{RD}^\dagger \mathbf{w} z + n_d \qquad (3.1) \qquad\qquad y_e = \sqrt{P_s} h_{SE}^* x + \mathbf{h}_{RE}^\dagger \mathbf{w} z + n_e \qquad (3.2)$$

where vector $\mathbf{w}$ [3x1] is a weight vector of all relays, n_d and n_e are complex Gaussian white noise at the destination and the eavesdropper, h_{SD}^* and h_{SE}^* are source destination and the source eavesdropper channels and $\mathbf{h}_{RD}^\dagger$ and $\mathbf{h}_{RE}^\dagger$ are channel vectors.

To evaluate the level of secrecy, it is necessary to define the channel capacity, which represent the highest achieveable communication rate with minimal probability of errors. In this context, the transmission rate is defined as:

$$R = \log_2(1 + \text{SNR}) \quad \text{(bits/s/Hz)} \qquad (3.3)$$

where $\text{SNR} = \frac{P}{N}$ with P being the power of transmitting a signal and N being the noise power.

From equations (3.1) and (3.2) the inference power for the relays can be deduced as, representing the power of the jamming signal in each of these channels:

$$n_{RD} = \mathbf{w}^\dagger \mathbf{R}_{RD} \mathbf{w} \qquad (3.4) \qquad\qquad n_{RE} = \mathbf{w}^\dagger \mathbf{R}_{RE} \mathbf{w} \qquad (3.5)$$

where $\mathbf{R}_{RD} = \mathbf{h}_{RD} \mathbf{h}_{RD}^\dagger$ and $\mathbf{R}_{RE} = \mathbf{h}_{RE} \mathbf{h}_{RE}^\dagger$.

The secrecy rate can be expressed as:

$$R_d = \log_2 \left(1 + \frac{P_s \left| h_{SD} \right|^2}{n_{RD} + \sigma^2} \right) \text{(bits/s/Hz)} \qquad (3.6) \qquad R_e = \log_2 \left(1 + \frac{P_s \left| h_{SE} \right|^2}{n_{RE} + \sigma^2} \right) \text{(bits/s/Hz)} \qquad (3.7)$$

Finally from (3.6) and (3.7) the secrecy rate of the whole connection is:

$$R_S(\mathbf{w}, P_s) = \max\{R_d - R_e, 0\} = \log_2 \left(1 + \frac{P_s \left\| h_{SD} \right\|^2}{n_{RD} + \sigma^2} \right) - \log_2 \left(1 + \frac{P_s \left\| h_{SE} \right\|^2}{n_{RE} + \sigma^2} \right) \qquad (3.8)$$

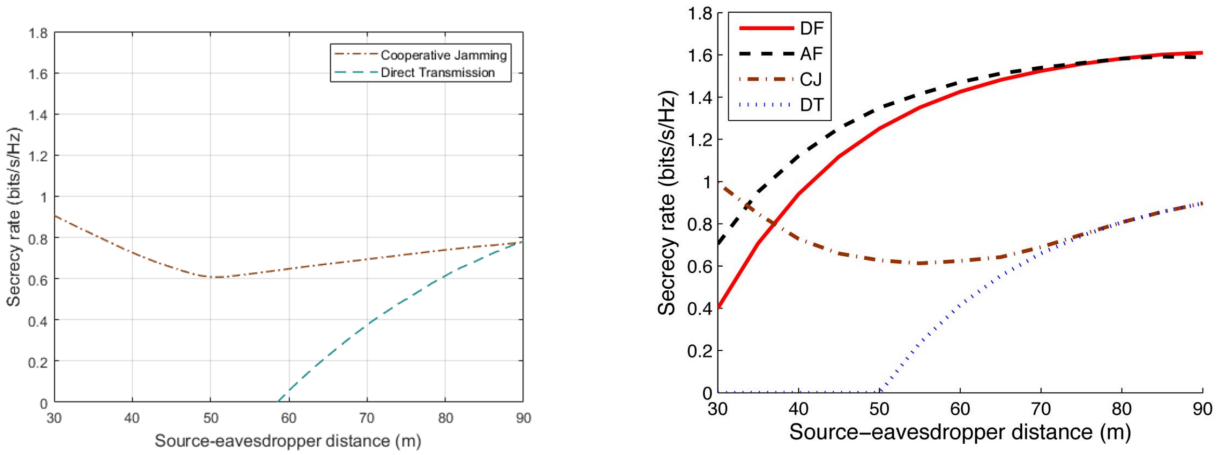
where $\mathbf{w} = \mu \parallel \mathbf{h}_{RD} \parallel^2 \mathbf{h}_{RE} - \mu \mathbf{h}_{RD}^{\dagger} \mathbf{h}_{RE} \mathbf{h}_{RD}$ and the scalar coefficient $\mu = \sqrt{\frac{P_0 - P_S}{\|\mathbf{h}_{RD}\|^4 \|\mathbf{h}_{RE}\|^2 - \|\mathbf{h}_{RD}\|^2 |\mathbf{h}_{RD}^{\dagger} \mathbf{h}_{RE}|^2}}$

The channels between the relays and the eavesdropper are given as:

$$\mathbf{h}_{RE} = (d_{RE})^{-c/2} e \tag{3.9}$$

$$\mathbf{e} = \begin{pmatrix} a_1 + b_1 i \\ a_2 + b_2 i \\ a_3 + b_3 i \end{pmatrix} \tag{3.10}$$

The complex number $\mathbf{e}$ is equal to the number of relays in use where a_n and b_n are normally distributed random numbers, $c = 3.5$ is the path loss exponents and d_{RE} is the from the relays to the eavesdropper. Similarly, other channels are defined based on the distance between their respective transmitters and receivers. The noise power $\sigma^2 = -60$dBm, the source power $P_s = -1$ and the total transmit power constraint $P_0 = 0$dBm. In the simulation the program calculates the secrecy rate at each position from 30 to 90 metres, 1 meter each step, for 100,000 times and takes the average results.



(a) Reproduced Results

(b) Published Results

Figure 3.2: Simulated results comparing Secrecy Rate vs Source Eavesdropper Distance

3.1.3 Analysis

Figure 3.2 illustrates the secrecy rate for the simulation in comparison to the published results from paper [7]. The figure can be divided into two sections, each with distinct characteristics.

The eavesdropper moves away from the source and towards the destination in the first stage (30-50 metres). This necessitates an increase in jamming power to create larger interference, while simultaneously reducing the power allocated to the message signal. As a result, the channel capacity between the source and destination reduces while increasing between the source and eavesdropper. This results in a decline in the secrecy rate.

As the eavesdropper moves into the second section (50-90 meters), the source can allocate more power to the transmitted message and less power to the jamming signal, given that the eavesdropper is now farther from the source than the destination. This results in an improved secrecy rate as the channel capacity between the source and destination increases compared to the capacity of the source-eavesdropper channel. However, the rate of growth in this section is not as rapid as in the first, which aligns with the published results. This can be attributed to the fact that the source must still allocate power for interference, even when the eavesdropper is outside the source-destination range.

Ultimately, when the eavesdropper is positioned distant from the source and relays, using a lot of power to broadcast jamming signals is not advantageous. In such cases, even in the absence of jamming, the received strength of the transmitted message at the eavesdropper remains low due to significant route loss. Therefore, in these circumstances, the secrecy rate might still rise. The findings show that cooperative jamming can increase physical layer security by creating a noise level that makes it difficult for eavesdroppers to interpret transmitted messages. Optimizing power distribution among the relays is still essential, though. Overall, the results of this cooperative jamming technique are consistent with the research and provide a good basis for continued development and improvement in later chapters.

3.2 Relay Selection and Jamming

This section presents the combination technique of jamming and relay selecting based off the system model in paper [20]. The primary goal is to determine the optimal relay selection policy from among three possible algorithms, based on their respective secrecy rates.

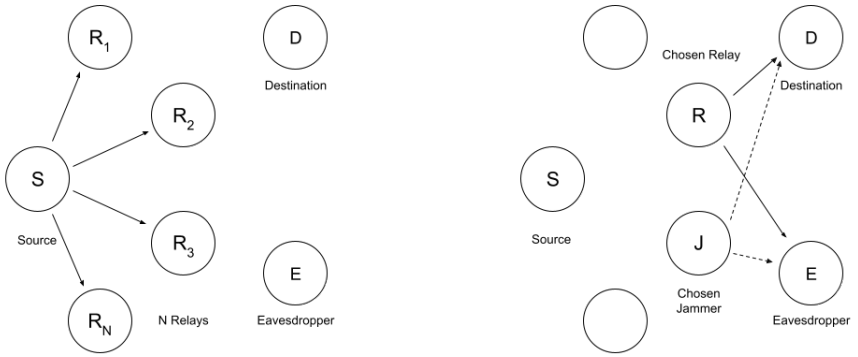
3.2.1 System Model

The proposed scheme builds on the previous cooperative jamming technique and allows for strategic selection of two relay nodes. The first relay functions conventionally, aiding the source in transmitting a message to the destination using the DF approach while the second relay acts as a jammer and creates deliberate interference in the eavesdroppers channel. Employing this method ensures that the eavesdropper's reception is effectively jammed while avoiding interference at the destination. This approach avoids the decrease in secrecy rate that was observed in traditional cooperative jamming.

This model will operate in the DF mode in a Rayleigh fading environment and is separated into two phases. During the first phase the source transmits a signal to four or more intermediate relays and in the second phase, two relays are chosen based on formulas: one relay acts normally and relays the signal to the destination while the other relay acts as a jammer and broadcasts interference signal to protect the transmission. Additionally, to simplify the model and take use of the DF technique, it is assumed that all of the relays can properly decode the message. The main objective is to increase system secrecy by choosing the appropriate relay and jammer based on predetermined parameters. It is assumed that the direct links between the source and eavesdropper and the source and destination, are either unavailable or not secure enough to make the influence of the chosen relay and jammer more obvious. Therefore, all transfers have to go through the relays. This assumption allows us to demonstrate how the relay and jammer selections impact the system's secrecy rate better. By routing all transfers through the relays, the system can maintain a better level of control over the flow of information and enhance its overall security.

It is assumed that both the source to the destination and source to the eavesdropper channels are severely impacted by deep fading.This is due to obstacles blocking the signal path between the source, destination, and eavesdropper, causing interference. However, the relays can function effectively because they are situated at the corners of these obstacles and have a clear path to the destination and source.

The cooperative protocol functions by utilizing two separate orthogonal channels, such as in frequencies or time slots. The eavesdropper can only intercept on the cooperative channel, which includes relay-destination communication, but not on the broadcast channel, which includes source-relay communication. Additionally, there is a crucial assumption outlined in reference [2]: the destination node is unable to counteract jamming signals that may



(a) Phase One (b) Phase Two

Figure 3.3: System Model

be present, preventing the eavesdropper from tracing the jamming signal. Furthermore, the destination node must also have the capability to mitigate interference as the source does.

For this simulation, the same setup is utilized as in the previous case however, the number of relays is allowed to vary. Although the paper sets it to 4 testing with different numbers does not impact the results. The simulation employs a one-dimensional model, featuring a single source, N relays, one eavesdropper, and one destination point. The source is placed at coordinate (0, 0) and will transmit symbol x to N relays, which are randomly installed between coordinates (1, 0) and (49, 0). Two of these relays are chosen as the jammer and broadcaster, respectively, responsible for continuing the signal transfer to the destination at coordinate (50, 0). The eavesdropper is positioned halfway between the source and destination at coordinate (25, 0). Another assumption is that the destination node lacks the ability to counteract jamming signals that may be present, preventing the eavesdropper from tracing the jamming signal. Moreover, the destination node must possess the capability to mitigate interference, similar to the source.

3.2.2 Analytical Results

The secrecy rate at the destination node and the eavesdropper node respectively is calculated using:

$$R_d = \frac{1}{2}\log_2\left(1 + \frac{P^*|h_{RD}|^2}{1 + P^*|h_{JD}|^2}\right) \qquad (3.11) \qquad R_d = \frac{1}{2}\log_2\left(1 + \frac{P^*|h_{RE}|^2}{1 + P^*|h_{JE}|^2}\right) \qquad (3.12)$$

where P is the transmitted or jamming power at the chosen relay or jammer, h_{RD},h_{JD}, h_{RE} and h_{JE} are the channel coefficients for the relay-destination, jammer-destination, relay-eavesdropper and jammer-eavesdropper respectively.

Therefore it is assumed that all the relays decode the source signal successfully and thus the secrecy rate of the whole connection can be calculated as:

$$R_s = R_d - R_e = \frac{1}{2}\log_2\left(1 + \frac{P^*|h_{RD}|^2}{1 + P^*|h_{JD}|^2}\right) - \frac{1}{2}\log_2\left(1 + \frac{P^*|h_{RE}|^2}{1 + P^*|h_{JE}|^2}\right) \qquad (3.13)$$

In order to choose the appropriate relay and jammer to maximise the secrecy rate of the different techniques the following relay and jammer selection techniques are analyzed:

Optimal Selection with Jamming (OSJ)

The selection policy in this technique is simple and involves choosing the best relay and jammer in the relays set in order to get the maximum secrecy rate:

$$(R, J) = \underset{R \neq J}{\operatorname{argmax}} \{R_s(R, J)\} = \underset{R \neq J}{\operatorname{argmax}} \left\{ \frac{1 + \frac{P^*|h_{RD}|^2}{1+P^*|h_{JD}|^2}}{1 + \frac{P^*|h_{RE}|^2}{1+P^*|h_{JE}|^2}} \right\} \tag{3.14}$$

However, this policy requires many comparisons which can increase the calculated time significantly if the quantity of relays increases. For that reason, the selection policy is proposed with a simpler approximation form as below:

$$\begin{cases} R = \arg\max \left\{ \frac{P^*|h_{RD}|^2}{P^*|h_{RE}|^2} \right\} \\ J = \underset{J \neq R}{\arg\min} \left\{ \frac{P^*|h_{JD}|^2}{P^*|h_{JE}|^2} \right\} \end{cases} \tag{3.15}$$

Optimal Switching (OS)

Constantly broadcasting it may not always be advantageous for the system since, as the system model states, the destination cannot erase the jamming signal. In some cases, such as when the jammer is close to the target, persistent interference can be damaging to the system and reduce the secrecy rate. This was demonstrated by the findings of Chapter 3.1. An intelligent switching approach for optimal selection that may be utilised with or without jamming is suggested by [20] as a solution to this problem. When comparing the secrecy rates with and without the jamming signal, the intelligent switching theory may be written as an inequality:

$$R_S(R, J) > R_S(R) \tag{3.16}$$

Using the simplified of the OSJ case we have:

$$\frac{|h_{JD}|^2}{|h_{JE}|^2} < 1 \tag{3.17}$$

This condition guarantees that the jamming signal interference at the destination is less than the eavesdropper so that it is not negatively impacted

Optimal Selection with Controlled Jamming (OSCJ)

In this situation, we assume that the jamming signal can be read at the intended destination but not at the eavesdropper. Based on this assumption, we may alter the calculation for the secrecy rate at the start as follows:

$$R_s = R_d - R_e = \frac{1}{2}\log_2\left(1 + P^*|h_{RD}|^2\right) - \frac{1}{2}\log_2\left(1 + \frac{P^*|h_{RE}|^2}{1 + P^*|h_{JE}|^2}\right) \tag{3.18}$$

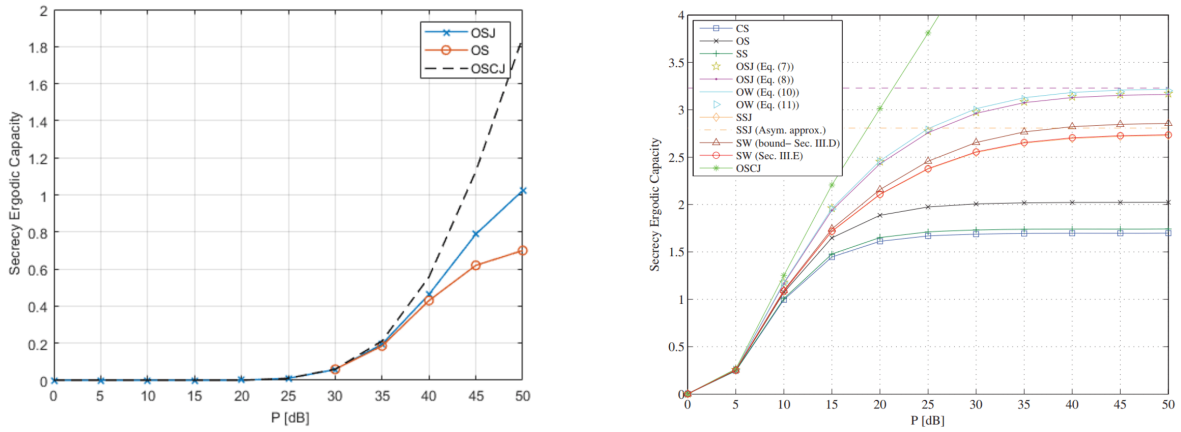
The choice of conditions for the jammer and relays is expressed as:

$$\begin{cases} R = \arg\max \left\{ \frac{P^*|h_{RD}|^2}{P^*|h_{RE}|^2} \right\} \\ J = \arg\min_{J \neq R} \left\{ P^*|h_{JE}|^2 \right\} \end{cases} \tag{3.19}$$

The channel coefficients are the same as the previous section: $h_{RE} = (d_{RE})^{-c/2}e$, where d is the distance between the two nodes, e is a uniformly distributed random complex number and c is the path loss exponent. The goal of this simulation is to demonstrate the relationship between secrecy rate and transmitted power P. For the simulation $c = 3.5$ and= the transmitted power runs from 0 to 50 dBm.

The first simulation examines the link between secrecy rate and transmitted power, while the second, run independently, studies the relation between secrecy rate and eavesdropper position. Understanding the link between the eavesdropper and the secrecy rate is critical, especially when applying these findings to dynamic systems with varying distances between nodes, such as vehicle networks (V2X), which we investigate in Chapter 5.

Due to the randomization of relay positions in the simulation, significant instability occurs. To address this, the simulation is manually tested, and a satisfactory result is selected, with the set of relays fixed accordingly. After identifying an appropriate set of relays, the test is conducted 10,000 times, and the average secrecy rate is calculated. A suitable set of relays (3, 30, 35, 37) is identified, resulting in a sufficiently high secrecy rate. The choice of jammer and relay depends on the chosen policy.



(a) Reproduced Results

(b) Published Results

Figure 3.4: Simulated results comparing Secrecy Ergodic Capacity vs P(dB) for the different selection schemes

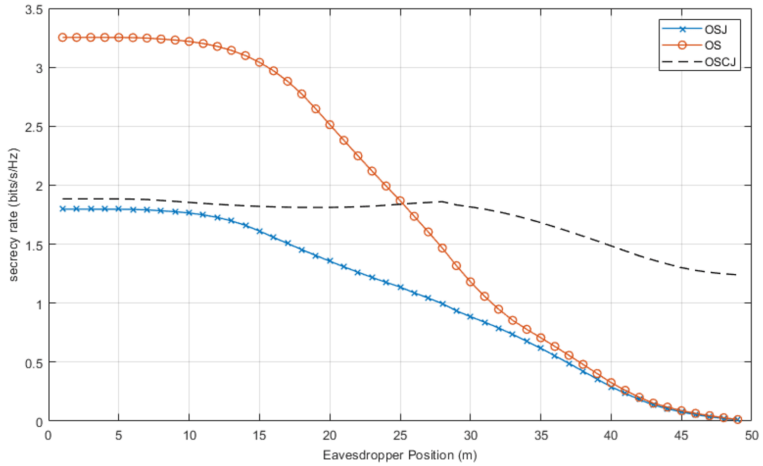


Figure 3.5: Novel comparison of Average Secrecy Rate Vs Eavesdropper Position

3.2.3 Analysis

Figure 3.4 is annotated with three colored lines: orange, blue and black, representing the secrecy rates of OS, OSJ, and OSCJ, respectively. The choice of jammer and relay depends on the selection policy.

The first simulation investigates the correlation between the average secrecy rate (RS) and transmitted power (P). The chosen jammer in the OS case is (3, 0), while in the OSJ and OSCJ cases, the chosen jammers are the same (30, 0). The selected relays for all policies are (37, 0). The results reveal that as transmission power increases, so do the secrecy rates. Notably, after P=25 dBm, the secrecy rates exhibit a significant increase. The three cases have similar results until P=35 dBm, after which the secrecy rate of OSCJ increases dramatically compared to the increase in the OSJ secrecy rate.

The second simulation investigates the correlation between the average secrecy rate (RS) and the eavesdropper position is examined. In this test, the chosen jammers for all policies are (37, 0), while the selected relays differ for each policy: (30, 0) for OSJ, (33, 0) for OS, and (35, 0) for OSCJ. It is crucial to remember the assumption that the eavesdropper cannot receive signals directly from the source in phase 1 but must wait until phase 2 when the chosen relay broadcasts the decoded message to the destination. As the selected relays for all policies are located in the middle from (30, 0) to (35, 0), the secrecy rates are high when the eavesdropper is near the source (from (0, 0) to (15, 0)) and decrease as the eavesdropper moves towards the chosen relay. In the range around the selected relay, the secrecy rates for all policies remain stable before dropping significantly when the eavesdropper approaches the chosen jammer and destination.

In dynamic systems like V2X networks the constantly changing network topology, resulting from node mobility makes it difficult to maintain consistent levels of secrecy. We can see that OSCJ offers a more stable and predictable result compared to OS, where it is higher in the shorter distances but drops to a low rate in the larger distances. For applications where secure communication is crucial at closer distances, such as collision avoidance and platooning, a higher secrecy rate at lower distances (0 to 15m) might be more favorable. In these scenarios, vehicles need to exchange sensitive information at close range, and a higher secrecy rate can help protect against eavesdropping attacks.

On the other hand, if the primary concern is maintaining a consistent level of security across all nodes in the network, regardless of their distance, a constant secrecy rate of 2 for all distances up to 50m might be more suitable. This would ensure that all nodes can communicate securely with each other, even if they are located farther apart. This could be particularly beneficial for applications like traffic management and emergency response coordination, where communication between nodes at varying distances is necessary.

3.3 Energy Harvesting in Single Hop Relay with Jamming

This chapter introduces the technique that combines jamming and energy harvesting. This model is based off the research carried out by Rupali Sinha and Poonam Jindal in [34].

3.3.1 System Model

This simulation focuses on examining a single-hop network that utilizes relaying and energy harvesting techniques in conjunction with jamming signals. The aim is to enhance the system's secrecy rate while also promoting energy efficiency.

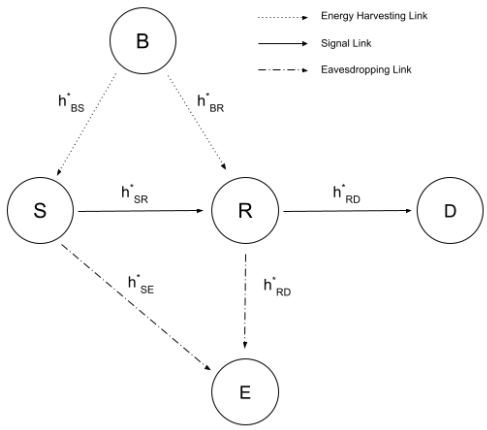


Figure 3.6: System Model Utilizing the Energy Harvesting Scheme

As depicted in Figure 3.3, the system comprises of standard nodes, however this particular case includes a power beacon that supplies energy to the friendly nodes. At each node complex additive white Gaussian noise (AWGN) is randomly generated, which introduces noise to the system. Two commonly employed schemes, DF and AF are investigated in this system to facilitate a comparison for determining the primary scheme for analysis in Chapter 3. It is important to clarify that the system's relay operates in both full and half duplex, depending on the time slot it is in.

3.3.2 Analytical Results

Energy Harvesting

Energy harvesting, also known as power harvesting or ambient power, is the process of capturing and storing energy from an external source, such as a power beacon in this system. The EH scheme used in this model is the time switching based EH protocol. In Figure 3.4, T represents the time duration needed to send a specific signal from the source node to the destination node, where $0 < \alpha < 1$ is the time coefficient of T. The period of time T is separated into three different time slots: the first time slot, during which the source and relay harvest energy from the power beacon, lasts for αT seconds. The last two time slots are for sending the signal from the source to the relay and from the relay to the destination, and they each last for $(1-\alpha)T/2$.

The energy harvesting at the source and the relay is given as:

$$E_S = \eta P_B \alpha T |h_{BS}^*|^2 \qquad (3.20) \qquad\qquad E_R = \eta P_B \alpha T |h_{BR}^*|^2 \qquad (3.21)$$

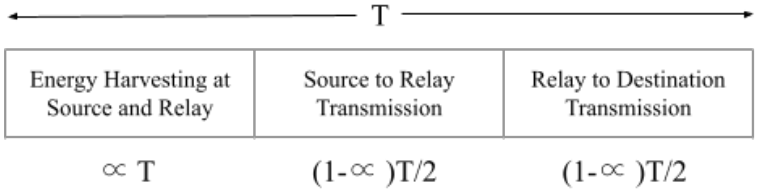
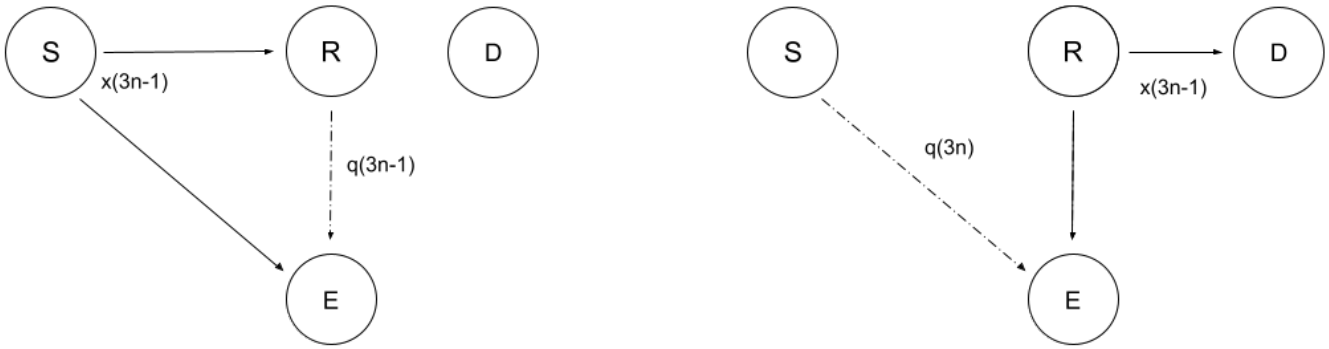


Figure 3.7: Time switching based EH protocol



(a) Transmission in (3n-1)th time slot

(b) Transmission in (3n)th time slot

Figure 3.8: Illustration of the signals transmitted in the time slots

where $0 < \eta < 1$ is the energy conversion efficiency, P_B is the power provided by the beacon, $|h^*_{BS}|$ and $|h^*_{BR}|$ are channel coefficients of the beacon-source and beacon-relay links.

The power transmitted by the source and relay are:

$$P_S = \frac{2\eta P_B \alpha |h^*_{BS}|^2}{1-\alpha} \tag{3.22}$$

$$P_R = \frac{2\eta P_B \alpha |h^*_{BR}|^2}{1-\alpha} \tag{3.23}$$

Decode and Forward

The scheme has two phases illustrated in figure 3.8a and 3.8b that should be followed in order. There are two types of time slots shown in the figures: (3n-1)th and (3n)th time slots. The (3n-1)th time slot refers to the 2nd, 5th, 8th, 11th, etc time slots, which correspond to the Source to Relay Transmission time slot in figure 3.7. The (3n)th time slot refers to the 3rd, 6th, 9th, 12th, etc time slots, which correspond to the Relay to Destination Transmission time slot.

The source node transmits the signal x(3n-1) to both the eavesdropper and the relay during the first phase, which happens in the (3n-1)th time slot as illustrated in 3.8(a). During this time, the relay transmits the eavesdropper a jamming signal q(3n-1). The received signals at the relay and eavesdropper during this period are stated as follows:

$$y_R(3n-1) = \sqrt{P_S} h^*_{SR} x(3n-1) + n_R(3n-1) \tag{3.24}$$

$$y_E(3n-1) = \sqrt{P_S} h^*_{SE} x(3n-1) + \sqrt{P_J} h^*_{RE} q(3n-1) n_E(3n-1) \tag{3.25}$$

where the power of the jamming signal is denoted by P_J and the AWGN at the relay and eavesdropper is $n_R(3n-1)$ and $n_E(3n-1)$ respectively.

The relay correctly decodes the signal from the destination and sends it to both the destination and the eavesdropper during the second phase, which occurs in the (3n)th time slot, as illustrated in figure 3.8(b). Simultaneously, the source emits a jamming signal to disrupt the eavesdropper. During the (3n)th time slot, the signal received by the eavesdropper and destination is represented as:

$$y_E(3n) = \sqrt{P_R} h^*_{RE} x_1(3n-1) + \sqrt{P_J} h^*_{SE} q(3n) + (3n) \tag{3.26}$$

$$y_D(3n) = \sqrt{P_R} h^*_{RD} x_1(3n-1) + n_D(3n) \tag{3.27}$$

where $n_D(3n)$ denotes the AWGN at the destination. From these formulas we can evaluate the secrecy rate as:

$$R_d = \frac{1}{2}\log_2\left(1 + P_R\alpha_{RD}\right) \tag{3.28}$$

$$R_e = \frac{1}{2}\log_2\left(1 + \frac{P_S\alpha_{SE}}{1+P_J\alpha_{RE}} + \frac{P_S\alpha_{RE}}{1+P_J\alpha_{SE}}\right) \tag{3.29}$$

where $\alpha_{RE} = \frac{|h_{RE}|^2}{\sigma^2}$, $\alpha_{RD} = \frac{|h_{RD}|^2}{\sigma^2}$ and $\alpha_{SE} = \frac{|h_{SE}|^2}{\sigma^2}$
The secrecy rate of the whole system is given as:

$$R_s = \max\left(R_d - R_e, 0\right) = \max\left(\frac{1}{2}\log_2\left(\frac{1+P_R\alpha_{RD}}{1+\frac{P_S\alpha_{SE}}{1+P_J\alpha_{RE}} + \frac{P_S\alpha_{RE}}{1+P_J\alpha_{SE}}}\right), 0\right) \tag{3.30}$$

Amplify and Forward

The AF system is divided into two stages. The theory and formulae employed in the first phase are identical to those used in the DF approach, as illustrated in Figure 3.8(a). The idea in the second phase is identical to that of the DF approach, but with a little modification. Instead of deciphering the signal, the relay amplifies it and sends it to its destination. As a result, in the (3n) time slot, the formulae for the received signal at both the eavesdropper and the destination are updated to:

$$y_E(3n) = G\sqrt{P_S} h^*_{RE} y_R(3n-1) + \sqrt{P_J} h^*_{SE} q(3n) + n_E(3n) \tag{3.31}$$

$$y_D(3n) = G\sqrt{P_S} h^*_{RD} y_R(3n-1) + n_D(3n) \tag{3.32}$$

where G is the scaling factor of amplification and given by $G = \frac{1}{\sqrt{P_S|h_{SR}|^2+N}}$ and N is the variance of noise. From equations (3.31) and (3.32) the formulas for secrecy rates at the destination and eavesdropper of the AF scheme can be evaluated as:

$$R_d = \frac{1}{2}\log_2\left(1 + G^2 P_S\alpha_{RD}\right) \tag{3.33}$$

$$R_e = \frac{1}{2}\log_2\left(1 + \frac{P_S\alpha_{SE}}{1+P_J\alpha_{RE}} + \frac{G^2P_S\alpha_{RE}}{1+P_J\alpha_{SE}}\right) \tag{3.34}$$

Therefore the secrecy rate of the whole system is given as:

$$R_S = \max\left\{R_d - R_e, 0\right\} = \max\left\{\frac{1}{2}\log_2\left(\frac{1+G^2P_S\alpha_{RD}}{1+\frac{P_S\alpha_{SE}}{1+P_J\alpha_{RE}} + \frac{G^2P_S\alpha_{RE}}{1+P_J\alpha_{SE}}}\right)\right\} \tag{3.35}$$

In this energy harvesting and jamming scenario, three simulations were conducted, similar to those presented in the paper. The purpose of these simulations was to examine the impact of relay-eavesdropper distance (d_RE), relay-destination distance (d_RD), and path loss exponent (c) on the secrecy rate (RS) of two promising, namely AF and DF. Although there were slight differences in the data setup between the three tests, the overall approach was identical.

The channel coefficients are set the same as in the previous simulations: $h = d^{-c/2}e$, where d is the distance between the two nodes, e is a uniformly distributed random complex number and c is the path loss exponent.

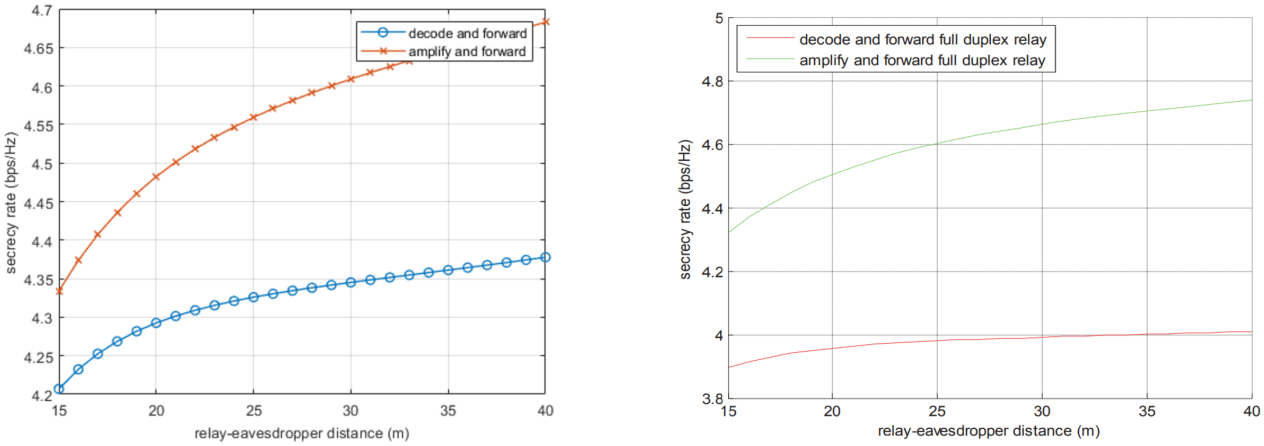
For the first test, the distance between the relay and eavesdropper was varied in the range of $[15, 40]$ meters,

while keeping other parameters fixed. The following parameters were set: $d_{BS} = d_{BR} = 7$ (m), $d_{SR} = 10$ (m), $d_{RD} = 15$ (m), noise power $\sigma^2 = -60$ dBm, beacon power $P_B = 30$ dBm, $\alpha = 0.99$, $\eta = 0.9$, $c = 3.5$ and the jamming power of relay and source to be equal at $P_J = 10$ dBm.

For the second test comparing the secrecy rate versus the path loss exponent, the following parameters were set: $d_{BS} = d_{BR} = 7$ (m), $d_{SR} = 10$ (m), $d_{RE} = 15$ (m), noise power $\sigma^2 = -60$ dBm, beacon power $P_B = 30$ dBm, $\alpha = 0.99$, $\eta = 0.9$, $c = 3.5$ and the jamming power of relay and source to be equal at $P_J = 10$ dBm.

For the last test comparing the secrecy rate versus path loss exponent the following parameters were set: $d_{BS} = d_{BR} = 7$ (m), $d_{SR} = 10$ (m), $d_{RD} = d_{RE} = 15$ (m), noise power $\sigma^2 = -60$ dBm, beacon power $P_B = 30$ dBm, $\alpha = 0.99$, $\eta = 0.9$, $c = 3.5$ and the jamming power of relay and source to be equal at $P_J = 10$ dBm.

The path loss exponent was increased 0.2 each step from 2 to 4. The simulation is performed 10,000 times, with a uniformly distributed random complex number being changed each time, and the final result is obtained by taking the average.



(a) Reproduced Results

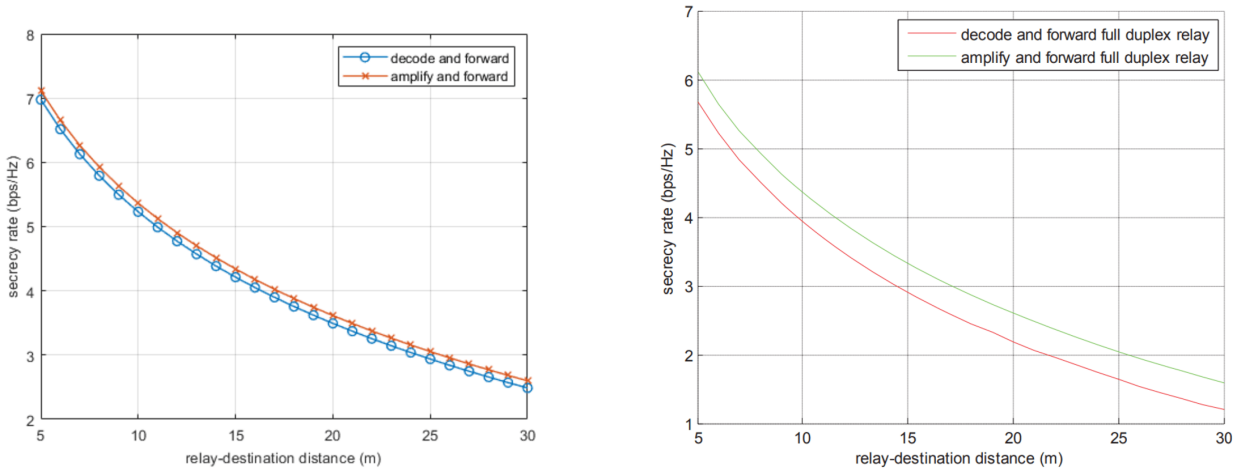
(b) Published Results

Figure 3.9: Simulated results comparing Secrecy Rate versus Relay Eavesdropper Distance

3.3.3 Analysis

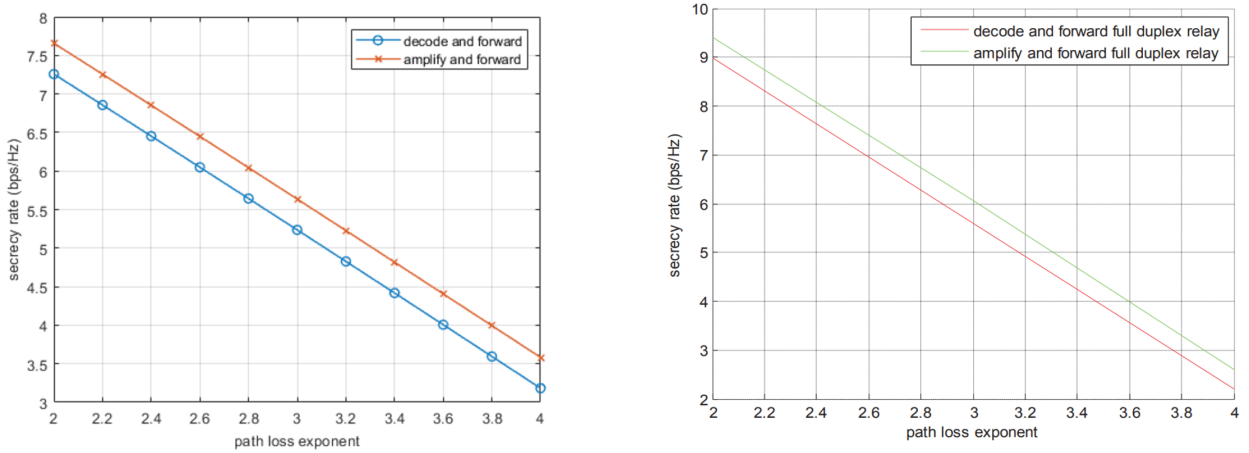
Figure 3.8 represents the relationship between the average secrecy rate and the distance between the relay and the eavesdropper. Both the AF and DF procedures indicate a rise in secrecy rates as the distance between the two entities grows. The trends observed in the plot align closely with the results reported in prior research and are notably stable, consistently exceeding a value of 4. This represents a significant stride in the enhancement of secrecy rates, particularly in comparison to cooperative jamming (RS<<1) and relay selection with cooperative jamming (0<RS<2). Additionally, it is noteworthy that throughout the experiment, the AF method consistently outperformed the DF approach, achieving a higher secrecy rate by a margin of at least 0.15 and up to 0.7 in the tests conducted.

Figure 3.10 illustrates the average secrecy rate plotted against the distance between the relay and destination. The results obtained reveal an inverse correlation between the distance separating the two entities and the secrecy rates achieved using both the AF and DF techniques, consistent with prior research conducted by the author. Im-



(a) Reproduced Results (b) Published Results

Figure 3.10: Simulated results comparing of Secrecy Rate versus Relay Destination Distance



(a) Reproduced Results (b) Published Results

Figure 3.11: Simulated results comparing Secrecy Rate versus Path Loss Exponent

pressively, the secrecy rates for both AF and DF approaches can reach a maximum of 7, surpassing any previously reported values in this study, while no result fell below 2. Remarkably, throughout the experiment, the AF method consistently yielded superior outcomes relative to the DF approach, although the difference between the two is not overly significant.

A plot of secrecy rate vs path loss exponent is shown in Figure 3.11. The DF method shows a fall in secrecy rates from around 7.25 to 3.2 when the route loss exponent grows from 2 to 4. Likewise, the AF method is reduced from 7.6 to 3.5. Despite being slightly lower, these findings are consistent with earlier study findings and the conclusions provided in the publication. While the secrecy rates of both approaches are significantly reduced, the findings remain favorable, with final values more than 3 at a route loss exponent of 4.

The integration of energy harvesting and cooperative jamming techniques has emerged as a valuable approach for enhancing the security of V2X networks, addressing the unique challenges posed by these dynamic and resource-constrained systems. By effectively combining these two techniques, the network can simultaneously benefit from increased secrecy rates and the efficient use of energy resources, offering a practical and robust solution for real-

world applications.

Energy harvesting enables the network to convert ambient energy sources, such as solar, thermal, or radio frequency energy, into usable electrical power, providing a sustainable and continuous power supply for V2X network nodes. This not only alleviates the reliance on conventional battery-powered systems but also allows for extended network lifetime and reduced operational costs. Moreover, energy harvesting enables the network to adapt to varying environmental conditions, enhancing the overall resilience and reliability of the system.

Through the analysis of three simulations, it has been demonstrated that the proposed technique of combining energy harvesting and cooperative jamming outperforms cooperative jamming alone, as well as relay selection combined with cooperative jamming, comparing both secrecy rate results and energy usage. Specifically, for the same amount of total power for the source and relay, such as P=30 dBm, the lowest secrecy rate achieved using energy harvesting is higher than 2, while the maximum secrecy rate achieved using cooperative jamming and relay selection cannot exceed 2. Additionally, the findings reveal that the AF scheme generally outperforms the DF approach in enhancing channel security. However, to determine the optimal choice between AF and DF for the beamforming and jamming combination technique, the analysis of paper [43] will be conducted before proceeding to Chapter 4.

3.4 Relaying Mode Selection for Chapter 4

Dong et al. [7] shows that the AF scheme outperforms the DF system, although the difference is not statistically significant. In the simulations performed in Section 3.3, the advantage of the AF scheme over the DF system is more apparent, even though the difference is not substantial in the second simulation. This chapter will compare the two schemes and make the final selection for the main scheme that will be covered in Chapter 4 to determine whether relaying mode is ideal.

3.4.1 System Model

The cooperative wireless network suggested in [43] has several relays and takes AF and DF protocols into account. The simulation will focus solely on the standard AF and DF optimal relay selection schemes, abbreviated as P-AFbORS and P-DFbORS. Although the paper evaluates a variety of schemes in conventional and traditional approaches, including MRC and ORS, this study will only look at these two. It is vital to remember that the simulation results are displayed in terms of intercept probability, which represents the occurrence of the event when the channel capacity is negative. In other words, it occurs when the channel capacity of the wiretap link (relay-eavesdropper) is less than the channel capacity of the main link (source-relay-destination).
The connections of the cooperative wireless network system are all described as Rayleigh fading channels and any noise at any node is modelled as a complex Gaussian random variable with zero mean and variance. Furthermore, the study's AF and DF systems are presumed to be without eavesdropper and direct links between source and destination. This happens when there is no direct line of sight between the source and the eavesdropper, or when the source is too far away from both the destination and the eavesdropper for the broadcast signal to reach them.

3.4.2 Analytical Results

Direct Transmission

To demonstrate the impact of the AF and DF protocols, a direct transmission (DT) approach is also taken into account. It is assumed that the source sends a signal s with power P, and the eavesdropper receives a replica of the signal, which is given as:

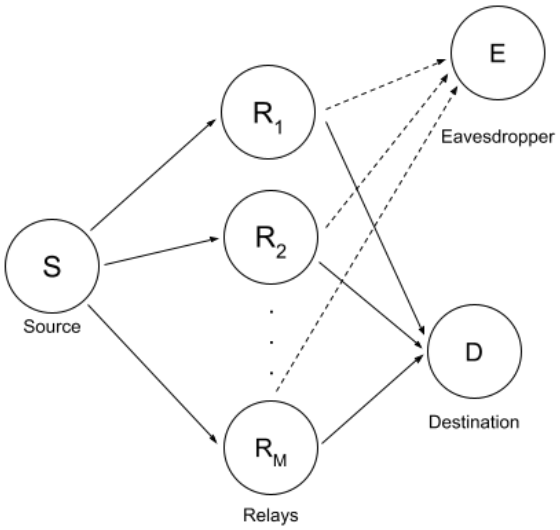


Figure 3.12: System Model of the Optimal Relay Selection Case

$$r_d = \sqrt{P} h_{sd} s + n_d \tag{3.36}$$

$$r_e = \sqrt{P} h_{se} s + n_e \tag{3.37}$$

where h_{sd} and h_{se} represents a fading coefficient of the channel from the source to destination and source to the eavesdropper respectively and n_d and n_e is the AWGN at the destination and eavesdropper.

The direct transmission channel capacity is expressed as:

$$C_{sd}^{\text{direct}} = \log_2 \left(1 + \frac{|h_{sd}|^2 P}{\sigma_n^2} \right) \tag{3.38}$$

$$C_{se}^{\text{direct}} = \log_2 \left(1 + \frac{|h_{se}|^2 P}{\sigma_n^2} \right) \tag{3.39}$$

where σ_n^2 is the noise variance. As previously stated, the direct transmission system's channel capacity is determined by computing the difference between the main channel and the wiretap channel:

$$C^{\text{direct}} = C_{sd}^{\text{direct}} - C_{se}^{\text{direct}} = \log_2 \left(1 + \frac{|h_{sd}|^2 P}{\sigma_n^2} \right) - \log_2 \left(1 + \frac{|h_{se}|^2 P}{\sigma_n^2} \right) \tag{3.40}$$

The probability of intercept can be deduced from the definition provided in the system model section as follows:

$$P_{\text{intercept}}^{\text{direct}} = \Pr \left(\left(1 + \frac{|h_{sd}|^2 P}{\sigma_n^2} \right) < \left(1 + \frac{|h_{se}|^2 P}{\sigma_n^2} \right) \right) = \Pr(|h_{sd}|^2 < |h_{se}|^2) \tag{3.41}$$

Since the Rayleigh fading model is considered, $|h_{sd}|^2$ and $|h_{se}|^2$ can be recognised to follow exponential distributions. Therefore an expression for the direct transmission intercept probability can be derived as:

$$P_{\text{intercept}}^{\text{direct}} = \frac{\sigma_{se}^2}{\sigma_{se}^2 + \sigma_{sd}^2} \tag{3.42}$$

where $\sigma_{se}^2 = E(|h_{se}|^2)$ and $\sigma_{sd}^2 = E(|h_{sd}|^2)$.

The formula demonstrates that the probability of intercept for direct transmission is independent of the transmit power P. Therefore, increasing the transmit power P does not enhance the security performance of the system.

Amplify and Forward Protocol (P-AFbORS)

In the AF system, the transmission operation is divided into two parts. In the initial step, the source delivers the signal s to all M relays. In the second stage, the signal is amplified and conveyed to the destination, which also includes selecting the optimal relay node. To ensure a fair comparison with direct transmission, the transmitted power at each stage must be decreased in half to $P/2$. As a consequence, the signal received at relay r_i may be expressed as follows:

$$r_i = \sqrt{\frac{P}{2}} h_{si} s + n_i \tag{3.43}$$

where h_{si} denotes the fading coefficient from the source to destination and n_i is the AWGN at relay r_i. The received signal at the destination poses some complexity as it involves the optimal selection of relay r_i, which amplifies the signal r_i by a factor of $\frac{h_{si}^*}{|h_{si}|^2\sqrt{\frac{P}{2}}}$.

$$r_d = \sqrt{\frac{P}{2}} h_{id} s + \frac{h_{id} h_{si}^*}{|h_{si}|^2} n_i + n_d \tag{3.44}$$

Using this we can infer the channel capacity of the AF protocol from R_i to the destination by:

$$C_{id}^{\mathrm{AF}} = \log_2 \left(1 + \frac{|h_{si}|^2 |h_{id}|^2 \frac{P}{2}}{(|h_{si}|^2 + |h_{id}|^2)\sigma^2} \right) \tag{3.45}$$

The signal received by the eavesdropper from R_i, is expressed in the same form as the received signal at the destination:

$$r_e = \sqrt{\frac{P}{2}} h_{ie} s + \frac{h_{ie} h_{si}^*}{|h_{si}|^2} n_i + n_e \tag{3.46}$$

The channel capacity of the link between R_i, and the eavesdropper, using the AF protocol, is determined by:

$$C_{ie}^{\mathrm{AF}} = \log_2 \left(1 + \frac{|h_{si}|^2 |h_{ie}|^2 \frac{P}{2}}{(|h_{si}|^2 + |h_{ie}|^2)\sigma^2} \right) \tag{3.47}$$

The channel capacity of the entire AF protocol system with R_i can be expressed as:

$$C_i^{\mathrm{AF}} = C_{id}^{\mathrm{AF}} - C_{ie}^{\mathrm{AF}} = \log_2 \left(\frac{1 + \frac{|h_{si}|^2 |h_{id}|^2 P}{2(|h_{si}|^2 + |h_{id}|^2)\sigma_n^2}}{1 + \frac{|h_{si}|^2 |h_{ie}|^2 P}{2(|h_{si}|^2 + |h_{ie}|^2)\sigma_n^2}} \right)$$

We have to address the critical question of determining the condition that governs the selection of the optimal relay R_i. As highlighted in section 3.2 the optimal relay maximizes the channel capacity of the AF system. This selection criterion can be expressed as follows:

$$R_i = \arg\max_{i \in R} C_i^{\mathrm{AF}} = \arg\max_{i \in R} \left(\frac{1 + \frac{|h_{si}|^2 |h_{id}|^2 P}{2(|h_{si}|^2 + |h_{id}|^2)\sigma_n^2}}{1 + \frac{|h_{si}|^2 |h_{ie}|^2 P}{2(|h_{si}|^2 + |h_{ie}|^2)\sigma_n^2}} \right)$$

where R serves as a set of M relays. The intercept probability of the P-AFbORS scheme can be expressed as:

$$P_{\text{intercept}}^{(\text{P-AFbORS})} = \Pr\left(\max_{i \in R} C_i^{\mathrm{AF}} < 0 \right) = \prod_{i=1}^{M} \Pr\left(|h_{id}|^2 < |h_{ie}|^2 \right) \tag{3.48}$$

Assuming that $|h_{ie}|^2$ and $|h_{id}|^2$ are independent exponentially distributed random variables, we can formulate this as:

$$P_{\text{intercept}}^{(\text{P-AFbORS})} = \prod_{i=1}^{M} \frac{\sigma_{ie}^2}{\sigma_{ie}^2 + \sigma_{id}^2} \tag{3.49}$$

where $\sigma_{ie}^2 = \mathbb{E}(|h_{ie}|^2)$ and $\sigma_{id}^2 = \mathbb{E}(|h_{id}|^2)$.

Decode and Forward Protocol (P-DFbORS)

The DF relaying protocol system runs in two independent phases, much like the P-AFbORS instance. The source sends an encoded signal to all M relays in the first stage. The ideal relay is chosen in the second step in order to decode the signal and send it to the intended location. This two-step method reduces the transmit power consumption for each stage to $P/2$ making it easier to compare with the direct transmission.

Because the encoded signal from the source to the relays and the decoded signal from the selected relay to the destination are two unique signals, we may consider the two steps to be separate operations. The main channel's channel capacity may therefore be calculated as the minimum of the two stages' channel capacities:

$$C_{sid}^{\text{DF}} = \min(C_{si}, C_{id}) \tag{3.50}$$

where C_{si} and C_{id} represent the channel capacities of the source-relay links and the selected relay-destination link, respectively. This can be expressed as:

$$C_{si} = \log_2\left(1 + \frac{|h_{si}|^2 P}{2\sigma_n^2}\right) \tag{3.51}$$

$$C_{id} = \log_2\left(1 + \frac{|h_{id}|^2 P}{2\sigma_n^2}\right) \tag{3.52}$$

Since the eavesdropper can wiretap the transmission of R_i, we can deduce the channel capacity of R_i-eavesdropper link as:

$$C_{ie}^{\text{DF}} = \log_2\left(1 + \frac{|h_{ie}|^2 P}{2\sigma_n^2}\right) \tag{3.53}$$

From (3.50), (3.51), (3.52), and (3.53), the capacity channel of the DF protocol system with R_i is given by:

$$C_i^{\text{DF}} = \log_2\left(1 + \frac{\min(|h_{si}|^2, |h_{id}|^2)P + 2\sigma_n^2}{|h_{ie}|^2 P + 2\sigma_n^2}\right) \tag{3.54}$$

Therefore, from the formula of channel capacity shown above, the criteria for selecting the optimal relay R_i can be expressed as:

$$R_i = \arg\max_{i \in R} C_i^{\text{DF}} = \arg\max_{i \in R}\left(\frac{\min(|h_{si}|^2, |h_{id}|^2)P + 2\sigma_n^2}{|h_{ie}|^2 P + 2\sigma_n^2}\right) \tag{3.55}$$

We can determine the probability of intercept for the P-DFbORS scheme by utilizing the intercept event definition and the formula provided above. This probability can be expressed as follows:

$$P_{\text{intercept}}^{(\text{P-DFbORS})} = \Pr\left(\max_{i \in R} C_i^{\text{DF}} < 0\right) = \prod_{i=1}^{M} \Pr\left(\min(|h_{si}|^2, |h_{id}|^2) < |h_{ie}|^2\right) \tag{3.56}$$

As the random exponent distributions of $|h_{si}|^2$, $|h_{id}|^2$, and $|h_{ie}|^2$ have mean values of σ_{si}^2, σ_{id}^2, and σ_{ie}^2 respectively, we can express the minimum value of X as $X = \min(|h_{si}|^2, |h_{id}|^2)$, where [43] represents the cumulative density function as:

$$P_X(X < x) = 1 - \exp\left(-\frac{x}{\sigma_{si}^2} - \frac{x}{\sigma_{id}^2}\right) \tag{3.57}$$

where $x \geq 0$. From (3.56) and (3.57) we can deduce

$$\Pr\left(\min(|h_{si}|^2, |h_{id}|^2) < |h_{ie}|^2\right) = \frac{\sigma_{id}^2\sigma_{ie}^2 + \sigma_{si}^2\sigma_{ie}^2}{\sigma_{id}^2\sigma_{ie}^2 + \sigma_{si}^2\sigma_{ie}^2 + \sigma_{si}^2\sigma_{id}^2} \tag{3.58}$$

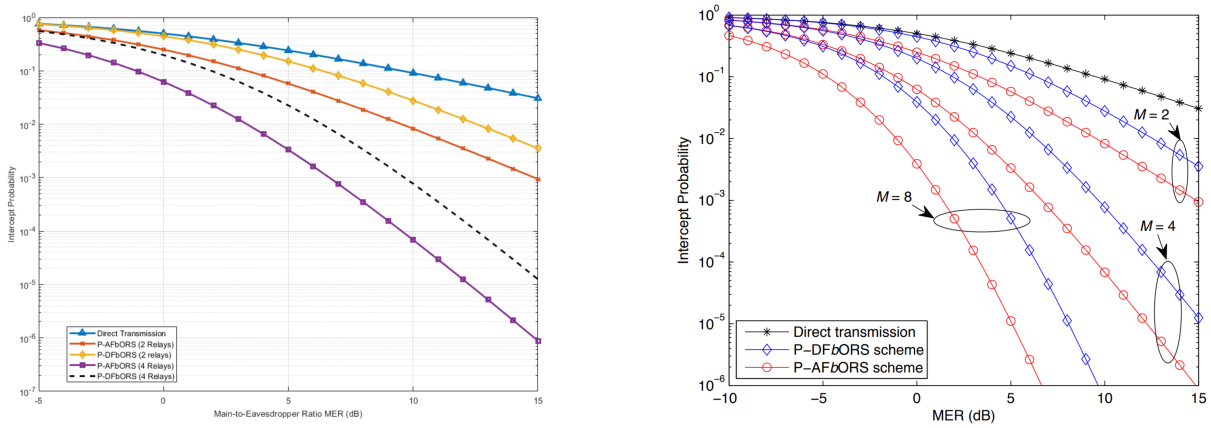
Substituting (3.58) into (3.57) we have:

$$P_{\text{intercept}}^{(\text{P-DFbORS})} = \prod_{i=1}^{M} \frac{\sigma_{id}^2\sigma_{ie}^2 + \sigma_{si}^2\sigma_{ie}^2}{\sigma_{id}^2\sigma_{ie}^2 + \sigma_{si}^2\sigma_{ie}^2 + \sigma_{si}^2\sigma_{id}^2} \tag{3.59}$$

When comparing the intercept probabilities of AF and DF protocols with the following conditions: $\frac{\sigma_{id}^2\sigma_{ie}^2+\sigma_{si}^2\sigma_{ie}^2}{\sigma_{id}^2\sigma_{ie}^2+\sigma_{si}^2\sigma_{ie}^2+\sigma_{si}^2\sigma_{id}^2} > 0$ and $\frac{\sigma_{ie}^2}{\sigma_{ie}^2+\sigma_{id}^2} > 0$, [43] states that we can prove that $\frac{\sigma_{ie}^2}{\sigma_{ie}^2+\sigma_{id}^2} < \frac{\sigma_{id}^2\sigma_{ie}^2+\sigma_{si}^2\sigma_{ie}^2}{\sigma_{id}^2\sigma_{ie}^2+\sigma_{si}^2\sigma_{ie}^2+\sigma_{si}^2\sigma_{id}^2}$ which leads to:

$$\prod_{i=1}^{M} \frac{\sigma_{ie}^2}{\sigma_{ie}^2 + \sigma_{id}^2} < \prod_{i=1}^{M} \frac{\sigma_{id}^2\sigma_{ie}^2 + \sigma_{si}^2\sigma_{ie}^2}{\sigma_{id}^2\sigma_{ie}^2 + \sigma_{si}^2\sigma_{ie}^2 + \sigma_{si}^2\sigma_{id}^2} \tag{3.60}$$

Therefore, it can be concluded that the intercept probability of P-AFbORS is lower than P-DFbORS. Therefore, it can be mathematically concluded that the AF scheme has an advantage over the DF scheme.



(a) Reproduced Results

(b) Published Results

Figure 3.13: Simulated results comparing Intercept Probability vs Main to Eavesdropper Ratio (dB)

3.4.3 Analysis

The graph clearly illustrates that the intercept probability of the P-AFbORS technique is consistently lower (indicating higher performance) compared to the P-DFbORS system for the same number of relays (M=2 or M=4). Furthermore, P-AFbORS and P-DFbORS also outperform direct transmission. The intercept probability for both AF and DF systems decreases when the number of relays is raised from 2 to 4, indicating an improvement in network physical security. This section's major purpose was to compare the AF and DF procedures in order to select which one to focus on in Chapter 4. Based on the mathematical proof, simulations in this section, the results of the 3.1 simulation, and the results of the 3.3 simulation, the final conclusion is that the AF protocol is the better choice, as it demonstrates superior performance overall compared to the DF protocol.

Chapter 4

Cooperative Jamming & Beamforming

Building on the findings of Chapter 3, this chapter explores the integration of cooperative jamming and beamforming techniques. A two-phase cooperative jamming algorithm is presented, laying the foundation for developing novel and secure V2X communication systems in Chapter 5.

4.1 Two-Phase Cooperative Jamming and Beamforming

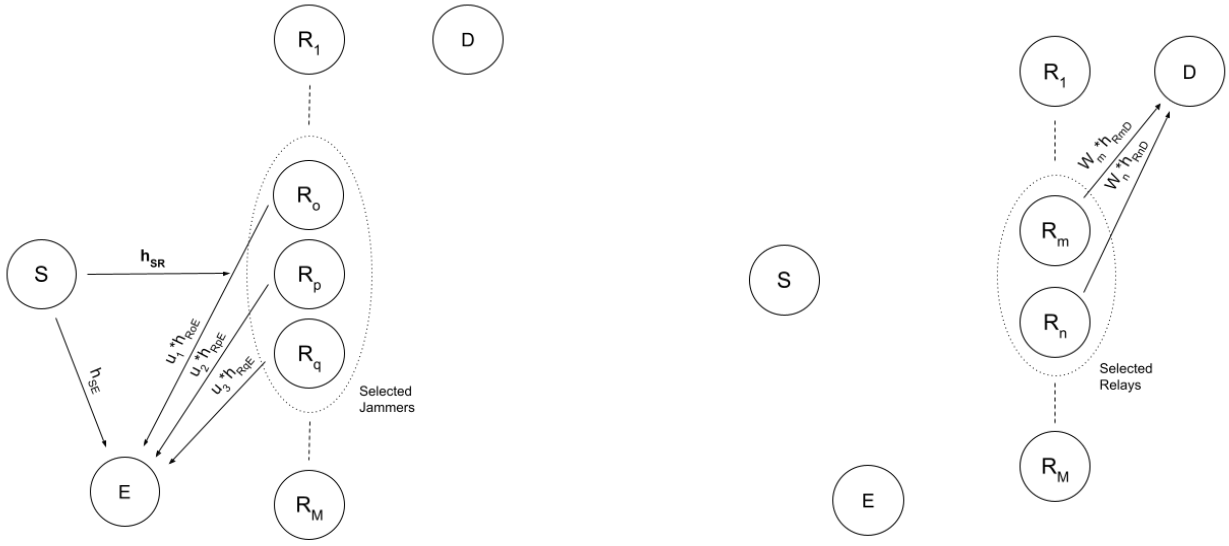
In this chapter, we expand upon the cooperative jamming techniques explored in Chapter 3 by incorporating beamforming and jamming techniques, as well as a selection policy for multiple relays and jammers. We model a two-phase cooperative jamming technique following the research in [14], which consists of selecting relays based on their links to the destination and subsequently choosing jammers based on their links to the source and relays. We demonstrate that the combination technique outperforms traditional cooperative jamming schemes.

4.1.1 System Model

A two-phase wireless cooperative network featuring cooperative jamming, beamforming and relay selection is considered. The system model, illustrated in Figure 4.1, is similar to the models discussed in previous sections, with one source, one eavesdropper, one destination and eight relays. The eavesdropper is passive, receiving and decoding the signal without interfering or modifying the transmission. This scheme emphasizes the significance of AF cooperative networks (or the importance of multiple relays); as a result, the source-destination channel is assumed to be unavailable, and all transmissions are routed through the network. However, a direct link from the source to the eavesdropper is added to simulate a genuine scenario in which an eavesdropper can intercept the signal directly.

One distinctive feature of this scheme is the selection of more than one jammer and relay. Specifically, three relays, denoted as jammers, and two relays, designated as forwarding relays, are selected. Figure 3.4 provides the notation and illustrates the system's operation. As with other AF relaying network systems, the operation is divided into two phases:

The source sends a message to five free relays in the first phase, and three relays are then chosen to broadcast jamming signals to interfere with the eavesdroppers' channel. The second step selects two forwarding relays to employ beamforming to send the message to the destination node.



(a) Phase 1 (b) Phase 2

Figure 4.1: Two-Phase Cooperative Jamming System Model

4.1.2 Analytical Results

The paper prioritizes the selection of relays before the selection of jammers, as the primary goal is to increase the quality of the source-destination channel, so we begin with discussing the selection of relays first. Assuming that R_m, R_n are the chosen relays for phase two, the received signals are given as:

$$y_D^{(2)} = \sqrt{P_R}\mathbf{w}^T\mathbf{h}_{RD,(m,n)}x + n_D^{(2)} \qquad (4.1) \qquad\qquad y_E^{(2)} = \sqrt{P_R}\mathbf{w}^T\mathbf{h}_{RE,(m,n)}x + n_E^{(2)} \qquad (4.2)$$

where P_R is the transmit power of relays, x is the transmitted signal, $\mathbf{w} = [w_m \quad w_n]^T$, $\mathbf{h}_{RD,(m,n)} = [h_{RD,(m)} \quad h_{RD,(n)}]$ and $\mathbf{h}_{RE,(m,n)} = [h_{RE,(m)} \quad h_{RE,(n)}]$ are complex channel coefficient vectors of chosen relays to the destination and eavesdropper respectively n_D and n_E are the AWGN at the destination node and the eavesdropper node.

The SNR equations at the destination and the eavesdropper can be deduced from (4.1) and (4.2) to be expressed as:

$$\gamma_D^{(2)} = \frac{P_R|\mathbf{w}^T\mathbf{h}_{RD,(m,n)}|}{\sigma_n^2} \qquad (4.3) \qquad\qquad \gamma_E^{(2)} = \frac{P_R|\mathbf{w}^T\mathbf{h}_{RE,(m,n)}|}{\sigma_n^2} \qquad (4.4)$$

where σ_n^2 is the noise power.

Similarly to previous sections, the achievable secrecy rate formulas at the destination eavesdropper and the whole system are given as:

$$R_D = \frac{1}{2}\log_2(1+\gamma_D) \qquad (4.5) \qquad\qquad R_E = \frac{1}{2}\log_2(1+\gamma_E) \qquad (4.6)$$

$$R_S = \max(R_D - R_E, 0) \qquad (4.7)$$

The selected relays utilize a beamforming vector that is designed to prevent leakage of information to the eavesdropper:

$$[w_{mn}] \begin{bmatrix} h_{RE,(m)} \\ h_{RE,(n)} \end{bmatrix} = 0 \quad \text{s.t.} \quad \mathbf{w}^\dagger \mathbf{w} = 1 \tag{4.8}$$

From the expression, we can deduce the components of vector W as:

$$w_m = \alpha h_{RE,(n)} \tag{4.9}$$

$$w_n = -\alpha h_{RE,(m)} \tag{4.10}$$

where $\alpha = \frac{1}{|h_{RE,(m)}|^2 + |h_{RE,(n)}|^2}$.

By substituting (4.9) and (4.10) into SNR at the destination (4.3), we have the following formula:

$$\gamma_D^{(2)} = \frac{\alpha^2 P_R}{\sigma_n^2} |h_{RE,(n)} h_{RD,(m)} - h_{RE,(m)} h_{RD,(n)}|^2 \tag{4.11}$$

The next consideration is the relay selection rule. The principle behind this rule is similar to the selection rules presented in 3.2, as the objective is to select the two relays that maximize the SNR at the destination. The rule can be expressed as follows:

$$(m, n) = \arg \max_{m,n \in 1,\ldots,8 \;\; m \neq n} \gamma_{D,(m,n)}^{(2)} \tag{4.12}$$

Returning to phase 1, where the jammers are selected, we assume that the chosen jammers are R_o, R_P, R_q as previously mentioned, and beamforming vector for jammers is given by $u = [u_1 \quad u_2 \quad u_3]^T$. Although five relays receive the signal from the source, we are only concerned with the signal received at the two selected relays, R_m, R_n, which can be expressed as:

$$y_{R_m}^{(1)} = \sqrt{P_S} h_{SR_m} x + \sqrt{P_J} \mathbf{u}^T \mathbf{h}_{JR_m} z + n_{R_m}^{(1)} \tag{4.13}$$

$$y_{R_n}^{(1)} = \sqrt{P_S} h_{SR_n} x + \sqrt{P_J} \mathbf{u}^T \mathbf{h}_{JR_n} z + n_{R_n}^{(1)} \tag{4.14}$$

where x denotes the transmitted signal, z is the jamming signal, $\mathbf{h}_{JR_m} = [h_{R_O R_m} \quad h_{R_p R_m} \quad h_{R_q R_m}]^T$ and $\mathbf{h}_{JR_n} = [h_{R_O R_n} \quad h_{R_p R_n} \quad h_{R_q R_n}]^T$ are channel coefficient vectors between the selected jammers R_o, R_P, R_q and the corresponding selected relays R_m, R_n. The channel coefficients between the source and the two selected relays R_m, R_n are denoted by h_{SR_m} and h_{SR_n}. Additionally, $n_{R_m}^{(1)}$ and $n_{R_n}^{(1)}$ represent the AWGN at R_m, R_n respectively.

The received signal by the eavesdropper in phase 1 is given as:

$$y_E = \sqrt{P_S} h_{SE} x + \sqrt{P_J} u^T h_{JE} z + n_E \tag{4.15}$$

where $\mathbf{h}_{JE} = [h_{R_O E} \quad h_{R_p E} \quad h_{R_q E}]^T$ is the channel coefficient vector between the three selected jammers and the eavesdropper.

In order for the selected relays to transmit a high-quality version of the received signal from the source to the destination, the artificial noise effect from the jammers must be eliminated. This leads to a triple-condition design, which can be expressed as follows:

$$\begin{pmatrix} h_{R_O R_m} & h_{R_p R_m} & h_{R_q R_m} \\ h_{R_O R_n} & h_{R_p R_n} & h_{R_q R_n} \\ u_1^* & u_2^* & u_3^* \end{pmatrix} \begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \tag{4.16}$$

Calculating the matrix multiplication above will lead to three equations of beamforming vector components in phase

1 as below:

$$u_1 = \frac{h_{R_pR_m}h_{R_qR_n} - h_{R_pR_n}h_{R_qR_m}}{\sqrt{(h_{R_pR_m}h_{R_qR_n} - h_{R_pR_n}h_{R_qR_m})^2 + (h_{R_oR_n}h_{R_qR_m} - h_{R_oR_m}h_{R_qR_n})^2 + (h_{R_oR_m}h_{R_pR_n} - h_{R_pR_m}h_{R_oR_n})^2}} \tag{4.17}$$

$$u_2 = \frac{h_{R_oR_n}h_{R_qR_m} - h_{R_oR_m}h_{R_qR_n}}{\sqrt{(h_{R_pR_m}h_{R_qR_n} - h_{R_pR_n}h_{R_qR_m})^2 + (h_{R_oR_n}h_{R_qR_m} - h_{R_oR_m}h_{R_qR_n})^2 + (h_{R_oR_m}h_{R_pR_n} - h_{R_pR_m}h_{R_oR_n})^2}} \tag{4.18}$$

$$u_3 = \frac{h_{R_oR_m}h_{R_pR_n} - h_{R_pR_m}h_{R_oR_n}}{\sqrt{(h_{R_pR_m}h_{R_qR_n} - h_{R_pR_n}h_{R_qR_m})^2 + (h_{R_oR_n}h_{R_qR_m} - h_{R_oR_m}h_{R_qR_n})^2 + (h_{R_oR_m}h_{R_pR_n} - h_{R_pR_m}h_{R_oR_n})^2}} \tag{4.19}$$

From equation (4.15) we can deduce the SNR at the eavesdropper in phase 1 as:

$$\gamma_E = \frac{P_S|h_{SE}|^2}{\sigma_n^2 + P_J|u^T h_{JE}|^2} \tag{4.20}$$

In contrast to the relay selection policy the jammer selection policy aims to minimize γ_E to decrease the quality of the eavesdroppers channel, which translates to maximizing $|u^T h_{JE}|^2$ because it is the only component in the equation that is related to the jammer. Therefore, the jammer selection policy can be expressed as:

$$(o, p, q) = \arg \max_{o,p,q \in \{1,\dots,8\}\ o,p,q \neq m,n} \left|\mathbf{u}^T \mathbf{h}_{JE}\right|^2 \tag{4.21}$$

Combining the results from the two phases leads to the following formula for achievable secrecy rate:

$$R_S = \max\left\{\frac{1}{2}\log_2\left(\frac{1+\gamma_D^{(2)}}{1+\gamma_E^{(1)}+\gamma_E^{(2)}}\right), 0\right\} \tag{4.22}$$

The destination is situated 50 meters away from the source at (50, 0), and the eavesdropper is positioned at the midpoint of this distance at (25, 0). The group of eight relays will be generated randomly within the range of (1, 0) and (49, 0). The channel coefficient is set as $h = d^{-\frac{c}{2}}e$, where d is the distance between two nodes, e is a uniformly distributed random complex number $(a + bi)$ and $c = 3.5$ is the path loss exponent.

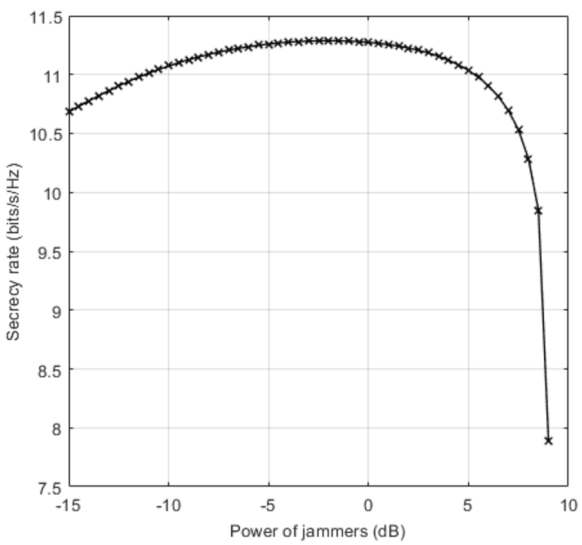
In the simulation comparing secrecy rate versus power of jammers the source power $P_S = 3$dBm and the power of relays as $P_R = P_T - P_S - P_J$. The power of jammer is set shifting in range $[-15; 10]$ dBm with the length of each step being 0.5dBm.

In the simulation comparing secrecy rate versus eavesdropper's position, the total power of the system $P_T = 10$dBm, source power $P_S = 3$dBm, power of jammer $P_J = 3$dBm and the power of relays $P_R = P_T - P_S - P_J$. The eavesdropper's position is changed from 5 meters to 49 meters away from the source.

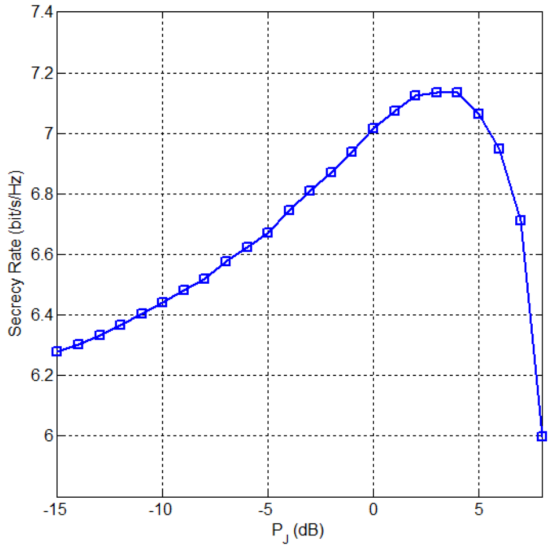
4.1.3 Analysis

The first simulation result, depicted in Figure 4.2, demonstrates a clear trend in the secrecy in line with the published results. Initially the secrecy rate increases from approximately 10.7 to a maximum of 11.3. However, as the jammer power reaches approximately 7dB the secrecy rate drops sharply. This trend can be attributed to the increased jammer power, which initially enhances the transmission channel but eventually drains the power from the source and relays, leading to a dramatic decline in the secrecy rate.

In the second simulation, show in in Figure 4.3, the relationship between the eavesdropper position, the selected relay positions and the jammer positions as well as the correlation between the eavesdroppers positions and secrecy

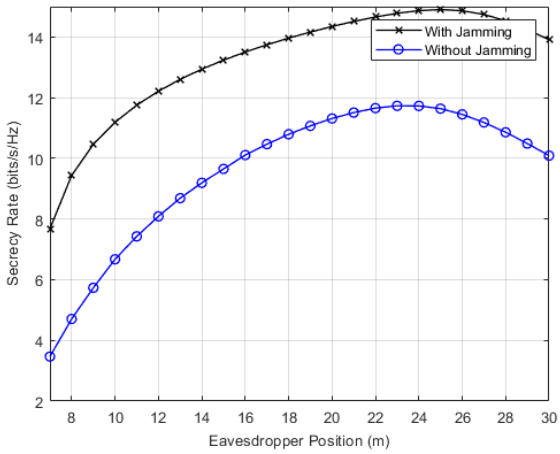


(a) Reproduced Results

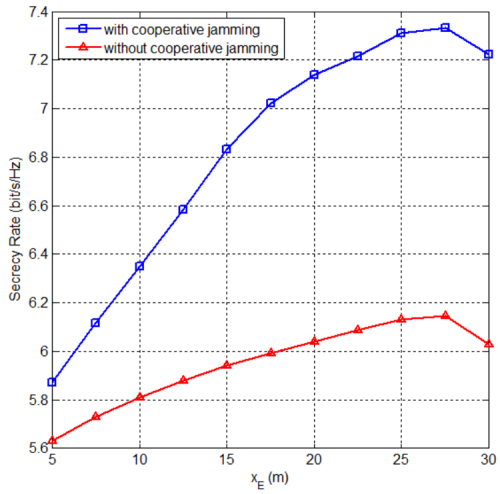


(b) Published Results

Figure 4.2: Simulated results Secrecy Rate vs Power of Jammers (dB)



(a) Reproduced Results



(b) Published Results

Figure 4.3: Simulated results comparing Secrecy Rate vs Eavesdropper Position (m)

rate is observed. The results indicate that the secrecy rate increases rapidly when the eavesdropper is within the range of the first two jammer and the first relay. However, the secrecy rate declines when the eavesdropper moves farther from the selected relays, despite the presence of another jammer.

Comparing this two phase cooperative jamming with beamforming selection technique to the best secrecy rate obtained in the energy harvesting and jamming case (which reached just above 7 and below 8), the combination technique demonstrates superior performance with secrecy rates nearing 15 in the second simulation and almost 11.5 in the first simulation. Consequently, this combination scheme is the preferred choice for further development, given its dominant performance in increasing the secrecy rate compared to other schemes.

Chapter 5

Cooperative Jamming and Beamforming in V2X Networks

This chapter integrates the PLS techniques explored in Chapters 3 and 4 to develop a novel Vehicle-to-Everything (V2X) system. The primary objective of this system is to securely transmit confidential information between vehicles, infrastructure and users, with the aid of two relays: the data node and the helping node. We compare the effectiveness of two techniques, a two-phase cooperative jamming scheme that was explored in Chapter 4.1 and a simple cooperative jamming scheme similar to that of Chapter 3.1. As of the time of this research there has been no published work implementing this scheme into a V2X network.

The model results prove that the two-phase cooperative jamming technique significantly surpasses the simple cooperative jamming scheme in preserving the confidentiality and security of the transmitted information within V2X network. This outcome highlights the potential of two-phase cooperative jamming as a superior approach for enhancing physical layer security in V2X communication systems.

5.1 System Model

We consider a vehicle-to-everything (V2X) system, in which a vehicle aims to transmit confidential information to other vehicles, users and infrastructure under Rayleigh fading channels. We employ two cooperative jamming strategies namely the two-phase cooperative jamming technique explored in Chapter 4.1 and simple cooperative jamming. We implement the two-phase scheme in the same order as the previous section and likewise assume that the global CSI is available for the system design.

The V2X system consists of a data node that transmits information to a vehicle, user and infrastructure while multiple eavesdroppers attempt to intercept the communication. The channels between the data node and legitimate receivers (vehicle, user and infrastructure) are represented by $\boldsymbol{h}_v \in \mathbb{C}^{N\times 1}$, $\boldsymbol{h}_u \in \mathbb{C}^{N\times 1}$, and $\boldsymbol{h}_i \in \mathbb{C}^{N\times 1}$, respectively. The helper node, which aids in secure communication, has channels $\boldsymbol{E}_{e1} \in \mathbb{C}^{N\times 1}$, $\boldsymbol{E}_{e2} \in \mathbb{C}^{N\times 1}$ and $\boldsymbol{E}_{ek} \in \mathbb{C}^{N\times 1}$ to the eavesdroppers, while the channels from the source node to the eavesdroppers are represented by $\boldsymbol{g}_{e1} \in \mathbb{C}^{N\times 1}$, $\boldsymbol{g}_{e2} \in \mathbb{C}^{N\times 1}$ and $\boldsymbol{g}_{ek} \in \mathbb{C}^{N\times 1}$.

The channels are generated as Rayleigh fading channels, and the noise is modeled as additive white Gaussian noise (AWGN) with power N_o.

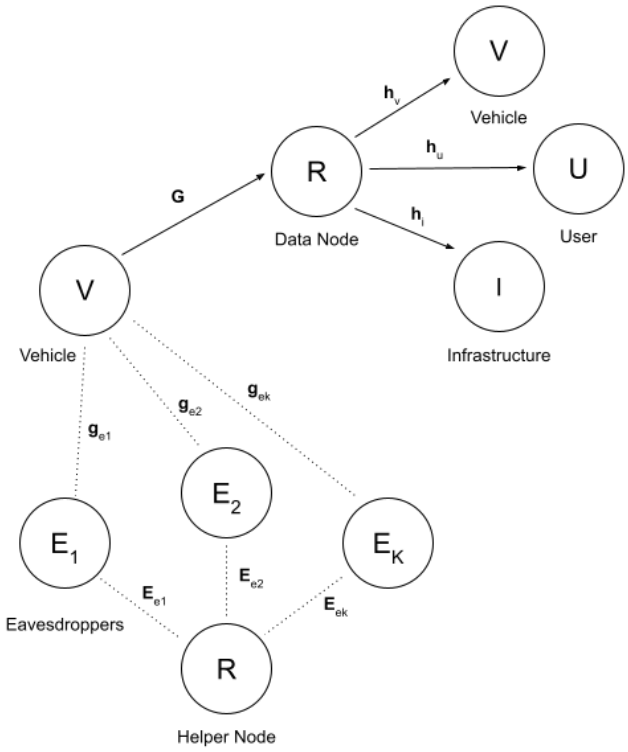


Figure 5.1: Illustration of V2X System Model

5.2 Analytical Results

For both the jamming strategies, the SNR at the legitimate receivers (vehicle, user and infrastructure) are calculated as:

$$SNR = \frac{|\boldsymbol{h}|^2}{No} \tag{5.1}$$

The SNR at the eavesdroppers is computed differently for the two jamming strategies. For two-phase cooperative jamming we used equation (5.2) and for simple cooperative jamming we use (5.3).

$$SNR_E = \frac{|\boldsymbol{h}_E \cdot \phi|^2}{No + J_1 + J_2} \tag{5.2}$$

$$SNR_{E_s} = \frac{|\boldsymbol{h}_E \cdot \phi_s|^2}{No + J_s} \tag{5.3}$$

Here, $\boldsymbol{h}_E$ represents the channels between the source and eavesdroppers, ϕ and ϕ_s are the phase shifts for the two-phase and simple jamming, respectively and J_1, J_2, and J_s represent the jamming signal powers from data and helper nodes. The secrecy rate is the difference between the logarithm of (1+SNR) for the legitimate receiver and eavesdropper and for the vehicle, user and infrastructure under both jamming strategies is calculated as:

$$C_s = \log_2\left(\frac{1+SNR}{1+SNR_E}\right) \tag{5.4}$$

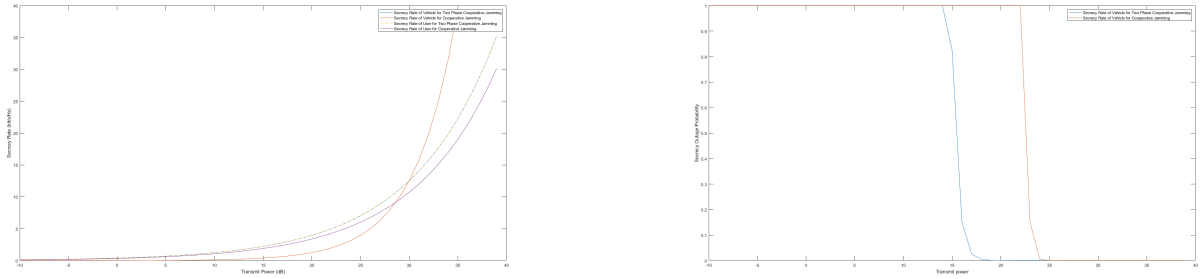
$$C_{s_s} = \log_2\left(\frac{1+SNR}{1+SNR_{E_s}}\right) \tag{5.5}$$

The secrecy outage probability is the probability that the secrecy rate of the legitimate receiver falls below a predefined threshold. In this analysis, the threshold is set at 2.35. The secrecy outage probability is calculated for the vehicle under both jamming strategies using:

$$P_{out} = \frac{1}{mc}\sum_{i=1}^{mc} \mathbb{1}\left(C_s < 2.35\right) \tag{5.6}$$

$$P_{out_s} = \frac{1}{mc}\sum_{i=1}^{mc} \mathbb{1}\left(C_{s_s} < 2.35\right) \tag{5.7}$$

Here, mc is the number of Monte Carlo simulations, and $\mathbb{1}(\cdot)$ is an indicator function that is equal to 1 if the condition inside the parentheses is true and 0 otherwise. Monte Carlo simulations are employed to calculate the average performance of the system over a large number of random channel realizations. In this analysis, the number of Monte Carlo simulations is set to 100,000.



(a) Secrecy Rate of Vehicle and User

(b) Secrecy Outage Probability of Vehicle

Figure 5.2: Simulated Results of Vehicle and User under Simple Jamming and Two Phase Jamming

5.3 Analysis

Figure 5.2(a) presents a comparison of the secrecy rates for vehicles and users under both cooperative and two-phase cooperative jamming. The results demonstrate that two-phase cooperative jamming yields superior secrecy rates at lower transmit power levels. As transmit power increases, the secrecy rates for both vehicles and users improve. However, the implementation of two-phase cooperative jamming leads to a more significant increase in secrecy rates, indicating its greater effectiveness compared to simple cooperative jamming.

Figure 5.2(b) depicts the secrecy outage probability for vehicles under cooperative and two-phase cooperative jamming, given a target rate of 2 bps/Hz. The system performance is notably enhanced when utilizing two-phase jamming. In this scenario, both the data node and helper node contribute to generating the jamming signal directed at the eavesdropper, resulting in an increased secrecy rate. Conversely, in simple cooperative jamming only the helper node generates the jamming signal towards the eavesdropper leading to a less effective outcome.

V2X technology enables numerous safety and efficiency applications in the context of vehicular communications, such as collision avoidance, intersection safety, emergency vehicle warnings and traffic flow optimization. Ensuring the security and privacy of V2X communications is paramount, as unauthorized access to sensitive data can lead to severe consequences. Two-phase cooperative jamming has emerged as a promising technique for enhancing the security of V2X communication systems.

The results of our analysis demonstrate that two-phase cooperative jamming outperforms simple cooperative jamming in terms of secrecy rate and secrecy outage probability for legitimate receivers, including vehicles and users. These findings suggest that two-phase cooperative jamming provides better protection against eavesdroppers, particularly at lower transmit power levels, which are more common in practical scenarios. This improvement can be attributed to the additional phase shift introduced in the two-phase cooperative jamming, which enhances the security of the communication against eavesdroppers. Furthermore, two-phase cooperative jamming increases the difficulty for eavesdroppers to locate and disable the jamming signals due to the use of two transmitters located at different positions.

In summary, the analytical and system model of the V2X system employing cooperative jamming strategies demonstrates the effectiveness of two-phase cooperative jamming in providing secure communication in vehicular networks. By analyzing the secrecy rate and secrecy outage probability, we can gain insights into the performance of these strategies and their suitability for secure communication in V2X systems.

Despite the fact that simple jamming can be easier to implement and may exhibit improved performance at higher power levels, two-phase cooperative jamming remains a more effective and secure solution for practical scenarios with limited transmit power. Moreover, two-phase cooperative jamming can be readily integrated into existing wireless devices, facilitating swift deployment without the need for specialized hardware.

Overall, the adoption of two-phase cooperative jamming in V2X communication systems can significantly enhance the security and privacy of these networks, ensuring the safe and reliable operation of applications such as collision avoidance, intersection safety, and emergency vehicle warnings. As V2X technology continues to evolve and be integrated into modern transportation systems, the implementation of robust security measures, such as two-phase cooperative jamming, will be crucial for the protection of sensitive data and the safety of road users.

Chapter 6

Conclusion Further Developments

In conclusion this dissertation present a comprehensive analysis of various techniques used for enhancing the security of wireless communication systems, specifically V2X systems, focusing on cooperative jamming and two-phase cooperative jamming. Results indicate that two-phase cooperative jamming outperforms simple cooperative jamming and other methods in terms of secrecy for legitimate receivers, such as vehicles and users. This approach provides enhanced protection against eavesdroppers, particularly at lower transmit power levels typically found in real-world situations and makes it more difficult for eavesdroppers to locate and disable jamming signals. The integration of beamforming into the two-phase scheme further benefits V2X networks by reducing interference for legitimate receivers.

The integration of energy harvesting and cooperative jamming has emerged as a favourable approach to increase network security, particularly for V2X systems that face unique challenges due to their dynamic and resource-constrained nature. In general, the AF scheme outperforms the DF method in boosting channel security, making AF the recommended choice for further development.

The impact of this research extends to various safety and efficiency applications in the context of vehicular communications, such as collision avoidance, intersection safety, emergency vehicle warnings, and traffic flow optimization. Ensuring the security and privacy of V2X communications is paramount, as unauthorized access to sensitive data can lead to severe consequences.

Future research in this domain could investigate modeling V2X systems in dynamic environments using stochastic geometry, which would involve randomly generating streets and nodes through Poisson processes, similar to the method employed by da Silva et al. [5]. This approach would yield more accurate results that align with the inherent randomness and varying node distances found in V2X systems. However, it has been demonstrated in [] that the differences between dynamic and static modeling are

Chapter 7

Legal, Social, Ethical and Professional Issues

The integration of secure V2X communication systems is vital for ensuring the security and privacy of sensitive data transmitted between vehicles and infrastructure. Unauthorized access to this information can result in severe consequences, such as traffic accidents or misuse of personal data. Cybersecurity measures must be in place to protect against potential threats including cyber-attacks, data breaches and eavesdropping. The development of cooperative jamming and energy harvesting techniques can play a significant role in enhancing the overall security and resilience of V2X communication systems.

One of the key benefits of enhancing V2X communication systems security is the potential to promote electric vehicles and reduce dependence on fossil fuels. Secure and reliable V2X communication can facilitate smart charging infrastructure and optimize energy consumption, which can ultimately contribute to a more sustainable transportation system. The development of energy harvesting techniques can further improve the energy efficiency of these communication systems, reducing their damage on the environmental.

The implementation of secure V2X communication systems must comply with global standards to ensure interoperability and seamless communication between different manufacturers and countries. Organizations such as the International Organization for Standardization (ISO), the Institute of Electrical and Electronics Engineers (IEEE), and the Society of Automotive Engineers (SAE) have developed various standards for V2X communications. Compliance with these standards is critical for the successful deployment of V2X systems on a large scale. The widespread adoption of secure V2X communication systems can lead to significant legal, social, and ethical implications. From a legal perspective, data protection and privacy laws must be considered when handling sensitive information transmitted through V2X systems. Additionally, liability issues may arise in the event of accidents or malfunctions involving autonomous vehicles.

Socially, the adoption of V2X communication systems can lead to a transformation of transportation infrastructure with potential benefits such as reduced traffic congestion, lower emissions and improved road safety. However, it may also raise concerns about job displacement, particularly for drivers in industries like trucking and taxi services.

Ethically, the development and implementation of V2X communication systems must consider the potential for misuse, biases in algorithms, and equitable access to technology. It is essential to identify and mitigate any unintended consequences or vulnerabilities that could be exploited for malicious purposes. To counteract misuse,

developers and engineers must ensure that these systems are designed and deployed responsibly and inclusively, minimizing potential negative impacts on society.

Equitable access to technology is another vital consideration. Efforts should be made to ensure that V2X communication systems are accessible and affordable for all members of society, regardless of their socio-economic status. This may involve public-private partnerships and government initiatives aimed at promoting the widespread adoption of V2X technology. Engineers and professionals involved in the development and implementation of V2X communication systems must adhere to ethical principles and professional codes of conduct. This includes ensuring the safety, reliability, and security of these systems while protecting users' privacy and considering the potential social and environmental impacts of their work.

In conclusion, the development and implementation of secure V2X communication systems encompass various legal, social, ethical, and professional aspects. Addressing these issues is essential for the successful deployment and adoption of V2X systems, ultimately contributing to a safer, more efficient, and sustainable transportation system.

References

[1] Joao Barros and Miguel RD Rodrigues. Secrecy capacity of wireless channels. In *2006 IEEE international symposium on information theory*, pages 356–360. IEEE, 2006.

[2] Ibtissem Brahmi, Monia Hamdi, Fadoua Mhiri, and Faouzi Zarai. Semidefinite relaxation of a joint beamforming and power control for downlink v2x communications. In *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*, pages 1355–1360. IEEE, 2019.

[3] Walter Brattain and John Bardeen. Quantum and the cybersecurity imperative. *Dig tal Debates*, page 15, 2022.

[4] Thomas Cover and Abbas El Gamal. Capacity theorems for the relay channel. *IEEE Transactions on information theory*, 25(5):572–584, 1979.

[5] Leonardo Barbosa da Silva, Evelio Martín Garcia Fernández, and Ândrei Camponogara. Physical layer security techniques applied to vehicle-to-everything networks. *arXiv preprint arXiv:2301.05123*, 2023.

[6] Ronald De Wolf. The potential impact of quantum computers on society. *Ethics and Information Technology*, 19:271–276, 2017.

[7] Lun Dong, Zhu Han, Athina P Petropulu, and H Vincent Poor. Improving wireless physical layer security via cooperating relays. *IEEE transactions on signal processing*, 58(3):1875–1888, 2009.

[8] Lun Dong, Zhu Han, Athina P Petropulu, and H Vincent Poor. Cooperative jamming for wireless physical layer security. In *2009 IEEE/SP 15th Workshop on Statistical Signal Processing*, pages 417–420. IEEE, 2009.

[9] Xiaolin Fang, Ming Yang, and Wenjia Wu. Security cost aware data communication in low-power iot sensors with energy harvesting. *Sensors*, 18(12):4400, 2018.

[10] World Economic Forum. The global risks report 2023. 18(1):98, 2023. URL `https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf`.

[11] Hongyuan Gao, Waleed Ejaz, and Minho Jo. Cooperative wireless energy harvesting and spectrum sharing in 5g networks. *IEEE Access*, 4:3647–3658, 2016.

[12] Liang Hao, JunLin Li, and GuiLu Long. Eavesdropping in a quantum secret sharing protocol based on grover algorithm and its solution. *Science China Physics, Mechanics and Astronomy*, 53:491–495, 2010.

[13] Monowar Hasan, Sibin Mohan, Takayuki Shimizu, and Hongsheng Lu. Securing vehicle-to-everything (v2x) communication platforms. *IEEE Transactions on Intelligent Vehicles*, 5(4):693–713, 2020.

[14] Mohammad Hatami, Mojtaba Jahandideh, and Hamid Behroozi. Two-phase cooperative jamming and beamforming for physical layer secrecy. In *2015 23rd Iranian Conference on Electrical Engineering*, pages 456–461. IEEE, 2015.

[15] Veria Havary-Nassab, Shahram Shahbazpanahi, Ali Grami, and Zhi-Quan Luo. Network beamforming based on second order statistics of the channel state information. In *2008 IEEE International Conference on Acoustics, Speech and Signal Processing*, pages 2605–2608. IEEE, 2008.

[16] Tiep M Hoang, Trung Q Duong, Hoang Duong Tuan, Sangarapillai Lambotharan, and Lajos Hanzo. Physical layer security: Detection of active eavesdropping attacks by support vector machines. *IEEE Access*, 9:31595–31607, 2021.

[17] Furqan Jameel, Shurjeel Wyne, and Ioannis Krikidis. Secrecy outage for wireless sensor networks. *IEEE Communications Letters*, 21(7):1565–1568, 2017.

[18] Dzevdan Kapetanovic, Gan Zheng, and Fredrik Rusek. Physical layer security for massive mimo: An overview on passive eavesdropping and active attacks. *IEEE Communications Magazine*, 53(6):21–27, 2015.

[19] Dzevdan Kapetanovic, Gan Zheng, and Fredrik Rusek. Physical layer security for massive mimo: An overview on passive eavesdropping and active attacks. *IEEE Communications Magazine*, 53(6):21–27, 2015.

[20] Ioannis Krikidis, John S Thompson, and Steve McLaughlin. Relay selection for secure cooperative networks with jamming. *IEEE Transactions on Wireless Communications*, 8(10):5003–5011, 2009.

[21] Xuesong Liang, Shi Jin, Xiqi Gao, and Kai-Kit Wong. Outage performance for decode-and-forward two-way relay network with multiple interferers and noisy relay. *IEEE Transactions on Communications*, 61(2):521–531, 2013.

[22] Yingbin Liang, H Vincent Poor, Shlomo Shamai, et al. Information theoretic security. *Foundations and Trends® in Communications and Information Theory*, 5(4–5):355–580, 2009.

[23] Pei Liu, Zhifeng Tao, Zinan Lin, Elza Erkip, and Shivendra Panwar. Cooperative wireless communications: A cross-layer approach. *IEEE Wireless communications*, 13(4):84–92, 2006.

[24] Weixin Lu, Kang An, and Tao Liang. Robust beamforming design for sum secrecy rate maximization in multibeam satellite systems. *IEEE Transactions on Aerospace and Electronic Systems*, 55(3):1568–1572, 2019.

[25] Stefan Mangard, Elisabeth Oswald, and Thomas Popp. *Power analysis attacks: Revealing the secrets of smart cards*, volume 31. Springer Science & Business Media, 2008.

[26] 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)*, pages 01–06. IEEE, 2021.

[27] Neri Merhav. Shannon's secrecy system with informed receivers and its application to systematic coding for wiretapped channels. *IEEE Transactions on Information Theory*, 54(6):2723–2734, 2008.

[28] Robbe Motmans. *Analysis and simulations of Shor's algorithm.* PhD thesis, KU Leuven, 2018.

[29] Iftikhar Rasheed, Fei Hu, Yang-Ki Hong, and Bharat Balasubramanian. Intelligent vehicle network routing with adaptive 3d beam alignment for mmwave 5g-based v2x communications. *IEEE Transactions on Intelligent Transportation Systems*, 22(5):2706–2718, 2020.

[30] Srivaths Ravi, Anand Raghunathan, Paul Kocher, and Sunil Hattangady. Security in embedded systems: Design challenges. *ACM Transactions on Embedded Computing Systems (TECS)*, 3(3):461–491, 2004.

[31] Phillip A Regalia, Ashish Khisti, Yingbin Liang, and Stefano Tomasin. Secure communications via physical-layer and information-theoretic techniques. *Proc. IEEE*, 103(10):1698–1701, 2015.

[32] Zouheir Rezki, Ashish Khisti, and Mohamed-Slim Alouini. On the ergodic secrecy capacity of the wiretap channel under imperfect main channel estimation. In *2011 Conference Record of the Forty Fifth Asilomar Conference on Signals, Systems and Computers (ASILOMAR)*, pages 952–957. IEEE, 2011.

[33] José David Vega Sánchez, Luis Urquiza-Aguiar, and Martha Cecilia Paredes Paredes. Physical layer security for 5g wireless networks: A comprehensive survey. In *2019 3rd cyber security in networking conference (CSNet)*, pages 122–129. IEEE, 2019.

[34] Rupali Sinha and Poonam Jindal. A study of physical layer security with energy harvesting in single hop relaying environment. In *2017 4th international conference on signal processing and integrated networks (SPIN)*, pages 530–533. IEEE, 2017.

[35] Pietro Tedeschi, Savio Sciancalepore, and Roberto Di Pietro. Security in energy harvesting networks: A survey of current solutions and research challenges. *IEEE Communications Surveys & Tutorials*, 22(4):2658–2693, 2020.

[36] International Telecommunication Union. International telecommunication union statistics. 2022. URL `https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx`.

[37] Aaron D Wyner. The wire-tap channel. *Bell system technical journal*, 54(8):1355–1387, 1975.

[38] Hong Xia, Qianqian Pei, and Yajuan Xi. The analysis and research of freak attack based on openssl. In *6th International Conference on Information Engineering for Mechanics and Materials*, pages 15–19. Atlantis Press, 2016.

[39] Rui Xiong, Chunxi Zhang, Huasong Zeng, Xiaosu Yi, Lijing Li, and Peng Wang. Reducing power consumption for autonomous ground vehicles via resource allocation based on road segmentation in v2x-mec with resource constraints. *IEEE Transactions on Vehicular Technology*, 71(6):6397–6409, 2022.

[40] Meng Yu and Jing Li. Is amplify-and-forward practically better than decode-and-forward or vice versa? In *Proceedings.(ICASSP'05). IEEE International Conference on Acoustics, Speech, and Signal Processing, 2005.*, volume 3, pages iii–365. IEEE, 2005.

[41] Tong-Xing Zheng and Hui-Ming Wang. Optimal power allocation for artificial noise under imperfect csi against spatially random eavesdroppers. *IEEE Transactions on Vehicular Technology*, 65(10):8812–8817, 2015.

[42] Zhengyu Zhu, Zhongyong Wang, Zheng Chu, Di Zhang, and Byonghyo Shim. Robust energy harvest balancing optimization with v2x-swipt over miso secrecy channel. *Computer Networks*, 137:61–68, 2018.

[43] Yulong Zou, Xianbin Wang, and Weiming Shen. Optimal relay selection for physical-layer security in cooperative wireless networks. *IEEE journal on selected areas in communications*, 31(10):2099–2111, 2013.

Appendix A

Source Code

The source code utilized throughout this dissertation, which includes the implementation of various techniques and simulations discussed in the text, can be accessed via the following link :https://github.com/jjjutla/Physical-Layer-Security-Simulations. This online repository contains all the necessary files and documentation, allowing interested readers and researchers to reproduce the results, as well as to further explore and expand upon the topics and concepts presented in this work. Sharing the source code in this manner not only fosters transparency but also encourages collaboration and knowledge exchange within the scientific community.