Physical Layer Security Solutions Against Passive and Colluding Eavesdroppers in Large Wireless Networks and Impulsive Noise Environments

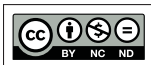
by

Michael ATALLAH

MANUSCRIPT-BASED THESIS PRESENTED TO ÉCOLE DE TECHNOLOGIE SUPÉRIEURE
IN PARTIAL FULFILLMENT FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY
Ph.D.

MONTREAL, AUGUST 8, 2019

ÉCOLE DE TECHNOLOGIE SUPÉRIEURE
UNIVERSITÉ DU QUÉBEC



BOARD OF EXAMINERS

THIS THESIS HAS BEEN EVALUATED

BY THE FOLLOWING BOARD OF EXAMINERS

M. Georges Kaddoum, Thesis Supervisor
Department of Electrical Engineering, École de Technologie Supérieure

M. Julien Gascon-Samson , President of the Board of Examiners
Department of Software Engineering and Information Technologies, École de Technologie Supérieure

M. Chamseddine Talhi, Member of the jury
Department of Software Engineering and Information Technologies, École de Technologie Supérieure

M. Yousef R. Shayan, External Independent Examiner
Department of Electrical and Computer Engineering, Concordia University

THIS THESIS WAS PRESENTED AND DEFENDED

IN THE PRESENCE OF A BOARD OF EXAMINERS AND THE PUBLIC

ON JULY 17, 2019

AT ÉCOLE DE TECHNOLOGIE SUPÉRIEURE

ACKNOWLEDGEMENTS

Firstly, I would like to express my sincere gratitude to my advisor professor Dr. Georges Kaddoum, for the continuous support of my Ph.D study and related research, for his patience, motivation, and immense knowledge. His guidance helped me in all the time of research and writing of this thesis.

I thank my labmates for the stimulating discussions, for the sleepless nights we were working together before deadlines, and for all the fun we have had in the last four years.

Last but not the least, I would like to thank my parents, my brothers and my best friend Michèlle, for supporting me spiritually throughout writing this thesis and in my life in general.

Solutions de Sécurité de Couche Physique Contre les Récepteurs Indistincts Passifs et Complexes dans les Grands Réseaux sans Fil et les Environnements à Bruit Impulsif

Michael ATALLAH

RÉSUMÉ

Les réseaux sans fil ont connu des évolutions rapides vers la durabilité, l'évolutivité et l'interopérabilité. Les sociétés en réseau futures conduisent l'économie numérique à une communauté plus globale d'infrastructures intelligentes et de services connectés pour une société plus durable et plus intelligente. En outre, une énorme quantité d'informations sensibles et confidentielles, telles que les dossiers médicaux, les supports électroniques, les données financières et les fichiers des clients, est transmise via des canaux sans fil. La mise en œuvre de la distribution et de la gestion des clés de couche supérieure a été mise au défi par l'émergence de ces nouveaux systèmes avancés. Afin de résister à divers abus malveillants et attaques de sécurité, la sécurité de couche physique (PLS) est devenue une alternative attrayante. Le concept de base derrière PLS est d'exploiter les caractéristiques des canaux sans fil pour la confidentialité. Son objectif est d'aveugler les oreilles indiscrètes de sorte qu'ils ne puissent en extraire aucune informations confidentielles des signaux reçus. Cette thèse présente des solutions et des analyses pour améliorer le PLS dans les réseaux sans fil.

Dans le deuxième chapitre, nous examinons les performances de capacité de confidentialité d'un réseau à double saut amplifier et transférer (AF) pour les techniques de formation de faisceau réparti (DBF) et de relais opportuniste (OR). Nous calculons la capacité de mise à l'échelle pour deux grands ensembles; des relais fiables et des relais agressifs peu fiables coopérant avec un dépisteur visant à intercepter le message. Nous montrons que l'échelle de capacité dans le DBF est délimitée par une valeur qui dépend du rapport entre le nombre de relais agressifs dignes de confiance et ceux qui ne le sont pas, alors que la mise à l'échelle de la capacité de OU est limitée dans le haut par une valeur qui dépend du nombre de relais ainsi que du rapport signal sur bruit (SNR).

Dans le troisième chapitre, nous proposons une nouvelle technique de multidiffusion par localisation, destinée aux grands réseaux AF bi-phase, qui vise à améliorer la sécurité en présence d'écoutes indiscrètes passives non-collupères. Nous démontrons analytiquement que la technique proposée augmente la sécurité en réduisant la probabilité de re-choisir un secteur qui a des oreilles indiscrètes, pour chaque temps de transmission. De plus, nous montrons également que la capacité de confidentialité de notre technique est la même que pour la radiodiffusion. Ci-après, les limites inférieure et supérieure de la probabilité de défaillance du secret sont calculées et il est montré que les performances de sécurité sont remarquablement améliorées par rapport à la technique de multidiffusion classique.

Dans le quatrième chapitre, nous proposons un nouveau protocole de coopération pour les réseaux de capteurs sans fil à amplification et transmission doubles à phase double, visant à améliorer la sécurité de la transmission tout en tenant compte des capacités limitées des nœuds de capteurs. Dans un tel réseau, une partie des K relais peut être de potentiels oreilles indis-

crètes passives. Pour réduire l'impact de ces relais non fiables sur la sécurité du réseau, nous proposons un nouveau protocole de transmission, dans lequel la source accepte de partager avec la destination une information CSI (Channel State Information) donnée de source sécurisée lien relais-destination pour encoder le message. Ensuite, la source utilisera à nouveau cette CSI pour mapper le bon message sur un certain secteur tout en transmettant de faux messages aux autres secteurs. L'adoption d'un tel protocole de sécurité est prometteuse en raison de la disponibilité d'un grand nombre de capteurs électroniques bon marché dotés de capacités de calcul limitées. Pour le schéma proposé, nous avons dérivé la probabilité de coupure du secret (SOP) et démontré que la probabilité de recevoir les informations codées à droite par un relais peu fiable sont inversement proportionnelles au nombre de secteurs. Nous montrons également que le comportement agressif des relais non fiables coopérants n'est pas efficace par rapport au cas où chaque relais non sécurisé tente d'intercepter individuellement le message transmis.

Enfin, nous examinons les performances de sécurité de la couche physique sur les canaux à évanouissements de Rayleigh en présence de bruit impulsif, telles que rencontrées par exemple dans les environnements de électrique intelligent. Pour ce schéma, les métriques de performance de confidentialité ont été prises en compte avec et sans brouillage assisté par destination du côté de l'espionneur. D'après les résultats obtenus, il est vérifié que la POS, sans brouillage assisté par destination, est un revêtement de sol avec un rapport signal sur bruit élevé valeurs et qu'il peut être considérablement amélioré avec l'utilisation du brouillage.

Mots-clés: Couche physique, brouillage, transmission sectorielle, bruit impulsif.

Physical Layer Security Solutions Against Passive and Colluding Eavesdroppers in Large Wireless Networks and Impulsive Noise Environments

Michael ATALLAH

ABSTRACT

Wireless networks have experienced rapid evolutions toward sustainability, scalability and interoperability. The digital economy is driven by future networked societies to a more holistic community of intelligent infrastructures and connected services for a more sustainable and smarter society. Furthermore, an enormous amount of sensitive and confidential information, e.g., medical records, electronic media, financial data, and customer files, is transmitted via wireless channels. The implementation of higher layer key distribution and management was challenged by the emergence of these new advanced systems. In order to resist various malicious abuses and security attacks, physical layer security (PLS) has become an appealing alternative. The basic concept behind PLS is to exploit the characteristics of wireless channels for the confidentiality. Its target is to blind the eavesdroppers such that they cannot extract any confidential information from the received signals. This thesis presents solutions and analyses to improve the PLS in wireless networks.

In the second chapter, we investigate the secrecy capacity performance of an amplify-and-forward (AF) dual-hop network for both distributed beamforming (DBF) and opportunistic relaying (OR) techniques. We derive the capacity scaling for two large sets; trustworthy relays and untrustworthy aggressive relays cooperating together with a wire-tapper aiming to intercept the message. We show that the capacity scaling in the DBF is lower bounded by a value which depends on the ratio between the number of the trustworthy and the untrustworthy aggressive relays, whereas the capacity scaling of OR is upper bounded by a value depending on the number of relays as well as the signal to noise ratio (SNR).

In the third chapter, we propose a new location-based multicasting technique, for dual phase AF large networks, aiming to improve the security in the presence of non-colluding passive eavesdroppers. We analytically demonstrate that the proposed technique increases the security by decreasing the probability of re-choosing a sector that has eavesdroppers, for each transmission time. Moreover, we also show that the secrecy capacity scaling of our technique is the same as for broadcasting. Hereafter, the lower and upper bounds of the secrecy outage probability are calculated, and it is shown that the security performance is remarkably enhanced, compared to the conventional multicasting technique.

In the fourth chapter, we propose a new cooperative protocol, for dual phase amplify-and-forward large wireless sensor networks, aiming to improve the transmission security while taking into account the limited capabilities of the sensor nodes. In such a network, a portion of the K relays can be potential passive eavesdroppers. To reduce the impact of these untrustworthy relays on the network security, we propose a new transmission protocol, where the source agrees to share with the destination a given channel state information (CSI) of source-trusted relay-destination link to encode the message. Then, the source will use this CSI again to map

the right message to a certain sector while transmitting fake messages to the other sectors. Adopting such a security protocol is promising because of the availability of a high number of cheap electronic sensors with limited computational capabilities. For the proposed scheme, we derived the secrecy outage probability (SOP) and demonstrated that the probability of receiving the right encoded information by an untrustworthy relay is inversely proportional to the number of sectors. We also show that the aggressive behavior of cooperating untrusted relays is not effective compared to the case where each untrusted relay is trying to intercept the transmitted message individually.

Fifth and last, we investigate the physical layer security performance over Rayleigh fading channels in the presence of impulsive noise, as encountered, for instance, in smart grid environments. For this scheme, secrecy performance metrics were considered with and without destination assisted jamming at the eavesdropper's side. From the obtained results, it is verified that the SOP, without destination assisted jamming, is flooring at high signal-to-noise-ratio values and that it can be significantly improved with the use of jamming.

Keywords: Physical Layer, Jamming, Sectoral Transmission, Impulsive Noise.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABREVIATIONS

AWGN	Additive White Gaussian Noise
AF	Amplify-and-Forward
CB	Cooperative Beamforming
CDF	Cumulative Distribution Function
CJ	Cooperative Jamming
CRN	Cognitive Radio Network
CSI	Channel State Information
D2D	Device-to-Device
DBF	Distributed Beamforming
ESR	Ergodic Secrecy Rate
FDJ	Full Duplex Jammer
HDJ	Half Duplex Jammer
IJ	Intended Jamming
IoBT	Internet-of-Battlefield-Things
MC-DCSK	Multi-Carrier Differential Chaos Shift Keying
MIMO	Multiple-Input Multiple-Output
MISO	Multiple-Input Single-Output
NOMA	Non-Orthogonal Multiple Access
OR	Opportunistic Relaying

PDF	Probability Density Function
PLS	Physical Layer Security
PU	Primary User
RSS	Received Signal Strength
SINR	Signal-to-Interference-plus-Noise Ratio
SNR	Signal-to-Noise Ratio
SOP	Secrecy Outage Probability
SPCA	Sequential Parametric Convex Approximation
SU	Secondary User

INTRODUCTION

Wireless communication is an integral part of our lives; it also has significant social repercussions. Privacy and confidentiality with respect to the transmitted information over the wireless medium is vital, especially for applications concerning medical information, e-banking, and e-commerce. However, wireless communications are often vulnerable to eavesdropping and signal interception Mavoungou *et al.* (2016); Neshenko *et al.* (2019); Hong *et al.* (2013). Many security requirements are considered in the design of wireless networks, like integrity, confidentiality checks, authentication and spectrum access control Lou & Ren (2009); Shiu *et al.* (2011). Integrity ensures that the information that has been transmitted is utilized and modified by the legitimate user. Confidentiality refers to the prevention of unauthorized information disclosure. Authentication refers to the individuality of different terminals' confirmations. Spectrum access control refers to the prevention of denial-of-service type attacks. Usually, these security tasks are mostly undertaken in the protocol stack of the network's upper layers with the usage of cryptographic encryption and decryption methods. When employing symmetric-key cryptosystems, the two users have to share a common private key that is encrypting and decrypting the private message Hong *et al.* (2013). However, this requires a secure channel or protocol for the secret keys sharing. The secret key management and distribution has its own difficulties Schneier (1998); they lead to security vulnerabilities in wireless systems. As a substitute, the cryptosystems of the public key allow the use of two different keys; a public one for encryption and a separate private one for decryption. The first one is also available to all users since the private key is only known by the receiver. Therefore, cryptographic methods rely on the hardness of the computation to decrypt the message to achieve security when there is no availability of the secret key. As the computation power increases, e.g., with the development of quantum computers, the computational hardness of some mathematical problems, which is the basis of the decryption and encryption, will not hold, resulting in many cryptosystems' break down Hong *et al.* (2013). Moreover, in future networks, more devices will

be connected to nodes with different power and computational capabilities. Furthermore, due to the decentralized nature of the networks, devices join or leave the network in random time instants, which renders the management and distribution of cryptographic keys a challenging task. Therefore, many signal and coding processing techniques have been developed in the physical layer to enhance and to support security in wireless systems. Many contributions have been made to find alternative security solutions to fit the requirements of current and emerging wireless networks Goel & Negi (2008); Gopala *et al.* (2008); Shannon (1949); Bloch & Barros (2011). Therefore, the security of the physical layer can facilitate the cryptographic keys' distribution to enhance the security. Even though the fast variations of the channel and the broadcast nature of the wireless medium may cause additional challenges to their design, the physical layer security techniques also exploit the wireless transmissions' properties to better protect the communication channel Hong *et al.* (2013).

Contributions and Outline

The first chapter is the literature review that browses briefly the applied security techniques in the physical layer. The contributions of our thesis are summerized as follows:

In Chapter 2, the secrecy capacity scaling was investigated in the presence of untrustworthy aggressive relays that are cooperating between each other to intercept the message. Moreover, destination assisted jamming was applied. Two transmission strategies were studied: opportunistic relaying and distributed beamforming techniques. The secrecy scaling bounds were calculated for both DBF and OR. For DBF, it is shown that its secrecy scaling is lower bounded by a value related to the number of the trustworthy and the untrustworthy relays in the network, and that intended jamming, when applied, remarkably enhances the security. Moreover, the DBF showed better security performance compared to OR, which gives DBF the priority to be applied in large wireless networks when the security is demanded.

In Chapter 3, to reduce the probability that an eavesdropper would have a continuous access to the transmitted message, the legitimate transmitter decided to change its transmission from broadcasting to a location-based multicasting technique, in the presence of destination assisted jamming. In this way, if it is not in the covered sector, the eavesdropper cannot access the transmitted message. The secrecy capacity scaling was calculated and showed that this location-based multicasting technique scales similar to the broadcasting one. Moreover, analytical expressions of the lower and upper bounds of the secrecy outage probability were also provided. The proposed protocol was shown to be secure and confusing to the eavesdropper since the later cannot have access to the transmitted information all the time.

Chapter 4 proposes a novel protocol that implements the location-based multicasting protocol, to transmit the useful information in one sector and fake information towards the other sectors. The main advantage of this technique is its immunity towards the presence of aggressive relays when they plan to cooperate between each other to intercept the message. The results showed that this aggressive cooperation by the eavesdroppers will hardly increase the amount of the stolen information. Also, it is proved that by increasing the number of multicasted sectors, the security performance is enhanced. No jamming was applied in this scenario; however, the performance of the proposed protocol overcomes the secrecy performance of the conventional jamming technique.

In Chapter 5, new secrecy capacity expressions in the presence of impulsive noise and destination assisted jamming are proposed. This new alternative approach in reformulating the secrecy capacity expressions allows the other researchers to analyse their proposed system models easily in the presence of impulsive noise. Analytical expressions for the secrecy outage probability, with and without jamming, were provided. From the obtained results, it was shown that the SOP without destination assisted jamming is flooring at high SNR values, and that it could be enhanced remarkably by adding destination assisted jamming techniques.

Author's Publications

Here, we list the published and submitted journals and conference papers denoted by J and C respectively.

- J1: **M. Atallah** and G. Kaddoum, "Secrecy Analysis in Wireless Network with Passive Eavesdroppers by Using Partial Cooperation," in IEEE Transactions on Vehicular Technology, Apr. 2019. DOI: 10.1109/TVT.2019.2913934

- J2: **M. Atallah** and G. Kaddoum, "Secrecy Capacity Scaling With Untrustworthy Aggressive Relays Cooperating With a Wire-Tapper," in IEEE Wireless Communications Letters, vol. 5, no. 4, pp. 376-379, Aug. 2016. DOI: 10.1109/LWC.2016.2561285

- J3: **M. Atallah** and G. Kaddoum, "Design and Performance Analysis of Secure Multicasting Cooperative Protocol for Wireless Sensor Network Applications," submitted to IEEE Wireless Communications Letters March. 2019

- J4: **M. Atallah**; M. S. Alam; and G. Kaddoum: 'Secrecy Analysis of Wireless Sensor Network in Smart Grid with Destination Assisted Jamming', IET Communications, 2019, DOI: 10.1049/iet-com.2018.5344 IET Digital Library, https://urnals/digital-library.theiet.org/content/jo 10.1049/iet-com.2018.5344

- J5: G. Kaddoum, H. Tran, L. Kong and **M. Atallah**, "Design of Simultaneous Wireless Information and Power Transfer Scheme for Short Reference DCSK Communication Systems," in IEEE Transactions on Communications, vol. 65, no. 1, pp. 431-443, Jan. 2017. DOI: 10.1109/TCOMM.2016.2619707

- C1: **M. Atallah** and G. Kaddoum, "Secrecy Analysis of Cooperative Network with Untrustworthy Relays Using Location-Based Multicasting Technique," 2017 5th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), Prague, 2017, pp. 206-210. DOI: 10.1109/FiCloudW.2017.74

- C2: **M. Atallah**, G. Kaddoum and L. Kong, "A Survey on Cooperative Jamming Applied to Physical Layer Security," 2015 IEEE International Conference on Ubiquitous Wireless Broadband (ICUWB), Montreal, QC, 2015, pp. 1-5. DOI: 10.1109/ICUWB.2015.7324413

CHAPTER 1

LITERATURE REVIEW

1.1 Physical Layer Security Concept

As shown in Fig. 1.1, a generic wireless communication network model consisting of three nodes, namely a legitimate transmitter (Alice), an intended receiver (Bob) and an eavesdropper (Eve), is taken into consideration. We call the link between Alice and Bob the main channel, while the link between Alice and Eve is called the wiretap channel. This model exemplifies the specific features of most multi-user secure communication systems. The vital concept of the secrecy capacity relies on goal of maximizing the legitimate channel capacity or minimizing the capacity of the illegitimate channels, which is attainable via the usage of the dynamic nature of the wireless channels, otherwise it is equal to zero Gopala *et al.* (2008). In Bloch *et al.* (2008), the secrecy capacity over an additive white Gaussian noise (AWGN) channel $C_{s,A}$ and Rayleigh fading channel $C_{s,R}$ are respectively given by

$$C_{s,A} = \left[\frac{1}{2}\log_2\left(1+\frac{P}{\sigma_m^2}\right) - \frac{1}{2}\log_2\left(1+\frac{P}{\sigma_w^2}\right)\right]^+, \tag{1.1}$$

$$C_{s,R} = \left[\log_2\left(1+\frac{P|h_m|^2}{\sigma_m^2}\right) - \log_2\left(1+\frac{P|h_w|^2}{\sigma_w^2}\right)\right]^+, \tag{1.2}$$

where $[x]^+ = \max\{0,x\}$, P represents the transmitted power, σ_m^2 and σ_w^2 are the noise power of the main channel and wiretap channel, respectively. Moreover, h_m and h_w are the instantaneous channel coefficients of the main channel and wiretap channel, respectively. Also, the received signal-to-noise ratios (SNRs) at Bob and Eve are defined as $\gamma_m = \frac{P|h_m|^2}{\sigma_m^2}$ and $\gamma_w = \frac{P|h_w|^2}{\sigma_w^2}$, respectively. To achieve security, our aim is to keep the secrecy capacity C_s strictly positive, i.e. $C_s > 0$. In Fig. 1.2, the average secrecy capacity of a Rayleigh fading channel (1.2) is compared with that of a Gaussian wiretap channel (1.1). Strikingly, one can observe that the secrecy capacity over Rayleigh fading channels is higher than over AWGN channels. In other words, we can use the fading property of the physical layer to decrease the SNR of the wiretap channel.

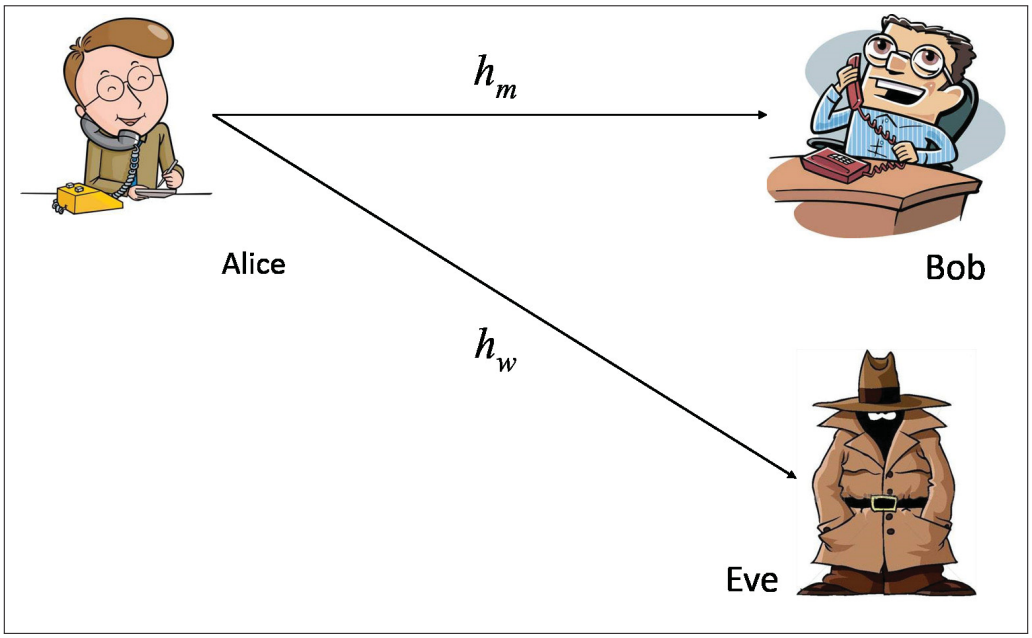


Figure 1.1 Wireless wiretap system model

Besides using the fading characteristics of the wireless channel, many other methods to improve the secrecy performance of the wireless communication systems have been suggested. In Shiu *et al.* (2011), physical layer security methods are classified into five major approaches: multiple-input-multiple-output (MIMO) channel, theoretical secrecy capacity, coding schemes (channel coding and network coding), power allocation, and signal design (artificial noise). Additionally, cooperative relay Han *et al.* (2015); Wang *et al.* (2013a); Chen *et al.* (2013), cooperative jamming Atallah *et al.* (2015); Ibrahim *et al.* (2015); Jameel *et al.* (2018), interleaving and spreading in frequency and time to secure Multi-Carrier Differential Chaos Shift Keying (MC-DCSK) Kaddoum *et al.* (2012) and energy harvesting Xing *et al.* (2014) are other useful methods. In the following section, we will describe the widely used methods in physical layer security.

1.2 Physical Layer Security Techniques

In this section, we will explore the most commonly used techniques to enhance the security in the physical layer.

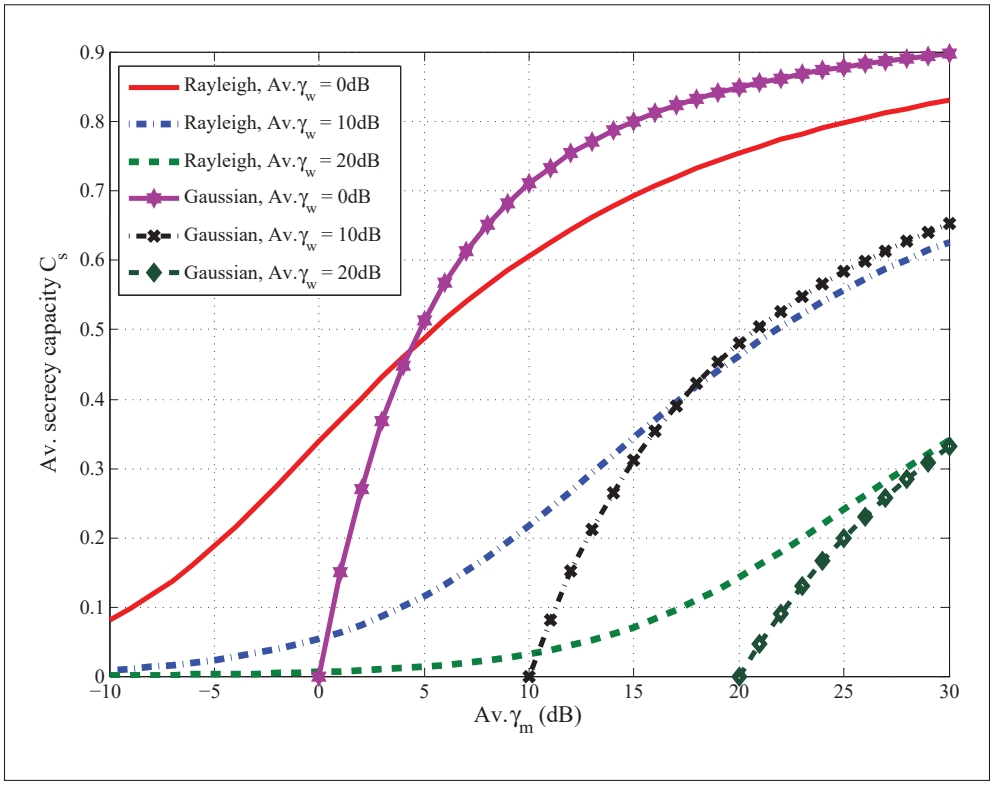


Figure 1.2 Normalized average secrecy capacity versus $\overline{\gamma}_m$, for chosen values of $\overline{\gamma}_w$, in Rayleigh and Gaussian wiretap channels

1.2.1 Artificial Noise and Artificial Fading

A. Artificial Noise

In multi-antenna systems, Artificial noise is one of the most popular techniques to guarantee security at the physical layer Goel & Negi (2008); Khisti & Wornell (2010). The basic idea behind artificial noise technique is that the channel state information (CSI) of the main channel is unknown by the eavesdroppers. Thus, they will be distracted and unable to decode the

transmitted information-bearing symbols. In Fig. 1.1, the source sends its signal

$$x = u + v, \tag{1.3}$$

where u is the message and v is the added artificial noise. v is chosen such that $h_m v = 0$. Then, the signal received by the legitimate receiver Bob is

$$\begin{aligned} y_b &= h_m x + n_b = h_m(u+v) + n_b \\ y_b &= h_m u + n_b, \end{aligned} \tag{1.4}$$

whereas the signal received by the eavesdropper Eve is

$$\begin{aligned} y_e &= h_w x + n_e = h_w u + h_w v + n_e \\ y_e &= h_w u + h_w v + n_e, \end{aligned} \tag{1.5}$$

hence, the secrecy capacity is obtained as

$$C_s = \left[\log_2 \left(1 + \frac{P_u |h_m|^2}{\sigma_b^2} \right) - \log_2 \left(1 + \frac{P_u |h_w|^2}{P_v |h_w|^2 + \sigma_e^2} \right) \right]^+, \tag{1.6}$$

where P_u and P_v are the transmitted power of u and v respectively, σ_b^2 and σ_e^2 are the noise power at the legitimate receiver and the eavesdropper, respectively. h_m and h_w are the channel coefficients of the main and wiretap links, respectively. We can see from (1.6) that the secrecy capacity is improved by adding the artificial noise compared to (1.2). The authors in Lin *et al.* (2013b) proposed a generalized scheme for injecting artificial noise to a legitimate channel. Their scheme was shown to be efficient under various channel conditions. Their simulation results showed that their algorithm outperforms other previous algorithms in enhancing the secrecy capacity. In Zhang *et al.* (2016b), an efficient algorithm was proposed to study the optimal resource allocation for maximizing the weighted sum secrecy rate with a new frequency domain artificial noise aided transmission strategy. Also, in Zeng *et al.* (2019), the authors proposed a strategy to secure the confidential information of massive MIMO-NOMA networks,

where the base station, based on the estimated CSI, precodes the confidential information and injects artificial noise.

B. Artificial Fading

Different from the artificial noise, the main idea of artificial fading is to weight the transmitted information symbol s randomly by a weighting coefficient k. The transmitted signal could be written as

$$x = ks, \tag{1.7}$$

with a constraint that $h_m k = 1$, where h_m is the channel coefficient between the transmitter and the legitimate receiver. Therefore, the received signal at the legitimate receiver becomes

$$y_m = h_m ks + n_m = s + n_m, \tag{1.8}$$

where n_m is the AWGN at the receiver. Therefore, the receiver will be able to decode its received signal directly without any channel coefficient h_m, whereas the signal received at the eavesdropper becomes

$$y_w = h_w ks + n_w, \tag{1.9}$$

where h_w is the channel coefficient between the transmitter and the eavesdropper, and n_w is the AWGN at the eavesdropper. The authors in Wang *et al.* (2015c) compared between artificial noise and artificial time-varying multiplicative noise that they named it artificial fast fading scheme since this scheme results in an equivalent fast fading channel for the eavesdropper. They concluded that the artificial noise scheme achieves a larger secrecy rate when the transmitter has more antennas than the eavesdropper. Otherwise the artificial fast fading is superior. Motivated by their results, they proposed a hybrid artificial noise-artificial fast fading scheme to achieve a better secrecy performance than either schemes. As mentioned in Wang & Yang (2012), the unwanted wireless communication links can deliberately be corrupted by double beam switching of the smart antenna array as a novel concept of artificial fading. In Wang *et al.* (2014a), artificial fast fading was applied by randomly weighting the information sym-

bols at different transmitting antennas in a special way so that the eavesdropper's channel is a fast fading channel while that of the intended receiver is an additive white Gaussian noise channel. In Song (2018), the researchers proposed a novel cross layer design by combining artificial fast fading with secret-keys in the upper layer crypto-system to nullify the information leakage for any number of antennas at the eavesdropper. For both artificial noise and artificial fading, it is assumed that the transmitter and the receiver are acquainted of the main channel. Subsequently, the legitimate channel's security performance becomes easily assailable by the eavesdropper. Moreover, the mobility of the legitimate nodes, with the artificial noise and artificial fading techniques, which adds complexity due to the rapid changes in the characteristics of the legitimate channels, has not yet been investigated.

1.2.2 Spoofing

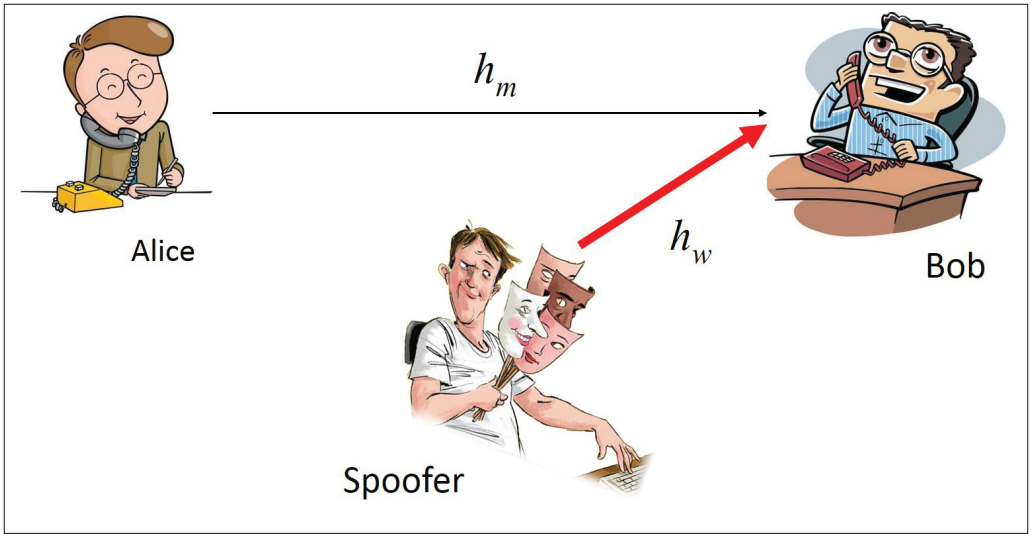


Figure 1.3 The spoofer is transmitting a deceiving signal to a legitimate receiver

In wireless networks, a spoofing attack, depicted in Fig.1.3, is a situation in which a node transmits deceiving signals to a legitimate receiver by acting as if it is a legitimate transmitter. Spoofing attacks studies have investigated the detection of the spoofers' location, which can be done by measuring the received signal strength (RSS) transmitted by the attacker. Mathemati-

cally, RSS is given by

$$RSS(dB) = P_{tx} + \rho - PL, \tag{1.10}$$

where P_{tx} is the transmitted power, PL is the path loss and ρ is the gain of the transmitting antenna. To locate the spoofer, many receivers should work collaboratively to measure the RSSs Wang & Yang (2013). Another way to estimate the spoofer's location is by measuring the angle of the arrived signal Chen *et al.* (2012), this method is more accurate than the former one Wang & Yang (2013). In Liu *et al.* (2019), the authors proposed a new pilot spoofing attack detection scheme by employing another node as a trusted user, which also cooperates in the uplink training process and helps to detect pilot spoofing in multiple-input single-output (MISO) systems. Also, to prevent spoofing attacks, finger prints or link signatures are used as useful methods Zhang *et al.* (2008). Link signature is extracted from the channel impulse response as a function of time delay and the magnitude of the impulse response. By applying the latter, the legitimate nodes are able to distinguish each other since the channels between them are identified and are well known between them. Therefore, being in a different location, a spoofer could be easily detected from the link signature of its channel. The weakness of the link signature method lies in the complexity of the key signature calculation at the legitimate nodes when they are changing their locations. Essentially, the available work in this particular field has mainly focused on locating the spoofers. Therefore, to establish a protocol on how to protect the legitimate nodes or even attack the spoofers, further work needs to be done. Very few works studied the mobility of the legitimate nodes in the context of spoofing attacks. Consequently, an investigation is needed in this field to provide a certain level of security when nodes are moving or for fast varying channel conditions.

1.2.3 Multi Antenna and Beamforming Based Techniques

To enhance the security in the physical layer, multiple antenna techniques are widely applied Yang *et al.* (2013); Zhang *et al.* (2015); Li *et al.* (2014a); Wang *et al.* (2014b); Banawan & Ulukus (2014); Xing *et al.* (2014); Vishwakarma & Chockalingam (2014); Oggier & Hassibi (2011). Fig 1.4 shows a general MIMO wiretap channel, where the source,

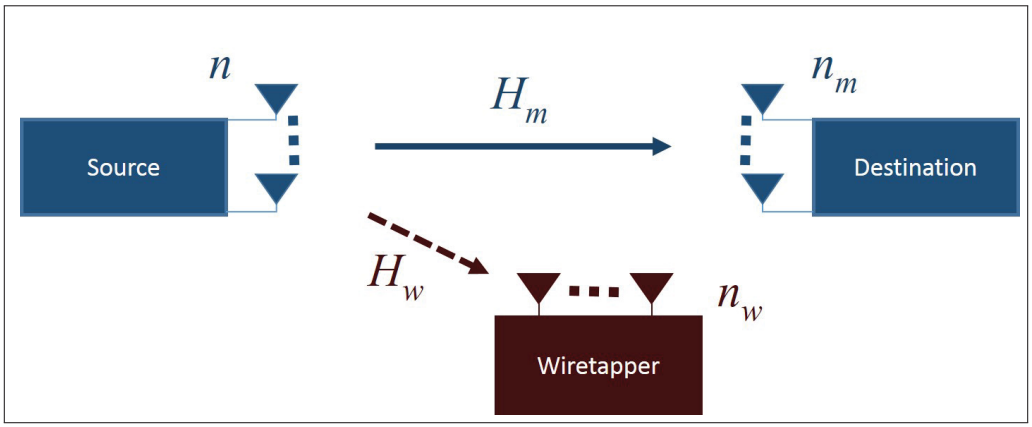


Figure 1.4 Representation of a general MIMO wiretap channel

destination, and wiretapper are equipped with n, n_m and n_w antennas, respectively. The source transmits an $n \times 1$ complex transmitted signal $\mathbf{X}$ with covariance matrix $\mathbf{K}_x = E\{\mathbf{X}\mathbf{X}^H\}$, satisfying the power constraint $Tr(\mathbf{K}_x) \leq P$. Therefore, the signals received by the destination and the wiretapper are

$$\mathbf{Y}_m = \mathbf{H}_m \mathbf{X} + \mathbf{N}_m, \tag{1.11}$$

and

$$\mathbf{Y}_w = \mathbf{H}_w \mathbf{X} + \mathbf{N}_w, \tag{1.12}$$

respectively, where $\mathbf{N}_m$ and $\mathbf{N}_w$ are respectively $n_m \times 1$ and $n_w \times 1$ complex white Gaussian additive noise vectors. Therefore, the secrecy capacity of MIMO wiretap channels is given in Oggier & Hassibi (2011) by

$$C_S = \max_{K_x \geq 0, Tr(K_x)=P} \log\det(\mathbf{I} + \mathbf{H}_m \mathbf{K}_x \mathbf{H}_m^H) - \log\det(\mathbf{I} + \mathbf{H}_w \mathbf{K}_x \mathbf{H}_w^H) \tag{1.13}$$

where $\mathbf{H}_m$ and $\mathbf{H}_w$ are respectively $n_m \times n$ and $n_w \times n$ fixed channel matrices. Moreover, $(.)^H$ is the Hermitian and $\mathbf{I}$ denotes the identity matrix. It is clear from (1.13) that the secrecy capacity is enhanced by increasing the numbers of antennas at the destination. The secrecy performance of MIMO wiretap channels was analysed in Kong *et al.* (2016) and Kong *et al.* (2018a). The authors in Yang *et al.* (2013) assumed a scenario where multiple legitimate users

are receiving multiple independent data streams from a base station; during the transmission, many eavesdroppers with multiple antennas are interested in the transmission stream of the base station. Colluding or not, the eavesdroppers may also use receiving beamforming method to maximize the signal-to-interference-plus-noise ratio (SINR) of the streams they are wiretapping. To guarantee a confidential transmission between the legitimate users and the base station, the cooperative jammer will work on keeping the SINR at the eavesdroppers below a certain threshold level. Another scenario in Li *et al.* (2014a) studied the Gaussian wiretap channel's secrecy capacity aided by an external jammer. While the jammer and the eavesdropper are equipped with multiple antennas, each of the receiver and the transmitter have a single one. The authors in Wang *et al.* (2014b) revealed a scenario for secure transmission within a two-hop amplify-and-forward relay network scheme, such that for a large number of antennas, the ergodic secrecy capacity (ESC) is independent of the number of antennas at the source and dependent on the number of antennas at the destination. In Kong *et al.* (2018b), the analysis of the secrecy performance in MIMO wireless networks was provided for two schemes: the nearest user and the best user based on its SNR. The researchers in Tran *et al.* (2019) proposed two transmit antenna selection solutions in MIMO NOMA networks. Their study showed that increasing the number of antennas at the legitimate nodes only has an impact on low and medium range of transmitted SNR values. Beamforming, a technique used to direct the signal transmission or reception, is also an efficient method and it is applied in many works with the cooperative jamming technique Wang *et al.* (2013a); Tran & Kong (2014); Wang *et al.* (2013b); Han *et al.* (2015); Vishwakarma & Chockalingam (2014). In Wang *et al.* (2013a), a scheme with joint cooperative jamming and beamforming was proposed to raise the security level of a cooperative relay network, where part of the nodes use a distributed beamforming mechanism while the others are simultaneously jamming the eavesdropper. In Tran & Kong (2014), another beamforming scheme was proposed; by preventing the eavesdroppers from using the beamformers to suppress the jamming signals. It also uses two orthogonal dimensions for transmitting and receiving signals. Moreover, a hybrid cooperative jamming and beamforming scheme was proposed in Wang *et al.* (2013b) also; the idea behind this work is that in both hops of a cooperative transmission, some intermediate nodes relay the signals to the legit-

imate receivers by adopting the beamforming distribution, while the other nodes are jamming the eavesdropper, which eventually leads in protection of the transmitted data. The authors in Han *et al.* (2015) developed an optimal relay assignment algorithm to solve a problem to maximize secrecy capacity, and an algorithm on smart jamming was also proposed to increase the system's secrecy capacity. In Alsaba *et al.* (2019), the authors studied a null-steering beamforming technique to enhance the security in NOMA systems by injecting a jamming signal and directing it toward the malicious node while being suppressed in the direction of the legitimate users. Also, the researchers in Akhlaghpasand *et al.* (2019) proposed a framework to protect the uplink transmission from jamming attacks in massive MIMO systems by suppressing the jamming interference during the detection of the useful information sent by the legitimate users. However, one of the challenges in beamforming is when the nodes are moving, which makes it difficult to track and direct the beams towards these nodes, besides that when working in high frequencies, these beams could be easily blocked, even by hand.

1.2.4 Relay and Cooperative Methods

In the context of relay networks, we can divide the security issues in two broad categories, namely trusted relays and untrusted relays.

A. Trusted Relays:

The eavesdropper and the relays are two separated network entities. Fig. 1.5 shows one of the most frequently used relay-based wiretap scenarios. To counteract external eavesdroppers, the relays can play various roles. They may be acting as traditional relays or both jamming partners as well as relaying components in order to strengthen the secure transmission. The concept of trusted relays was used in Arafa *et al.* (2018) to secure downlink NOMA systems. In Atallah & Kaddoum (2019), the source and the destination share the CSI of source-trusted relay-destination link to encode the messages and to map the transmission. The authors in Dahmane *et al.* (2017) introduced a weighted probabilistic and trust-aware strategy to provide high security and integrity level with less relays. In addition, in Waqas *et al.* (2018), secret key

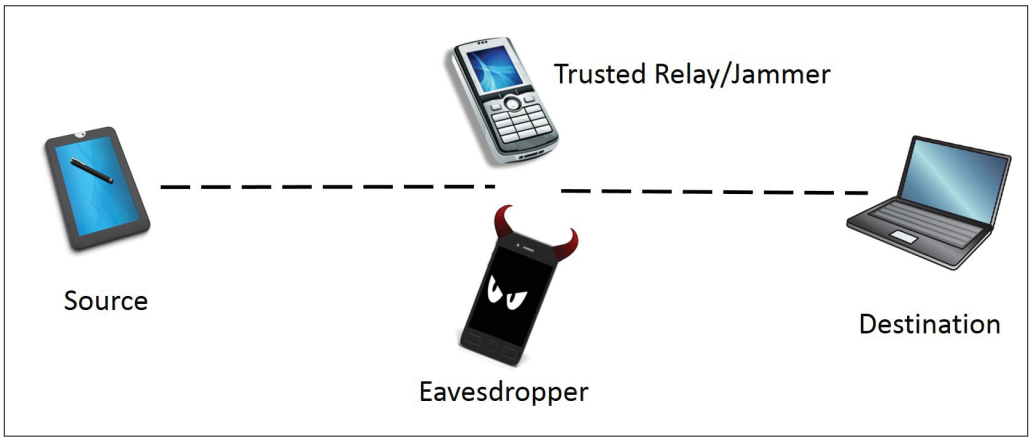


Figure 1.5 Representation of trusted (distinct relay and eavesdropper) relay network

generation was investigated in D2D communications in the presence of trusted and untrusted relays. Another novel noise-forwarding strategy called deaf helper phenomenon was also proposed in Lai & El Gamal (2008); to confuse the eavesdropper, dummy codewords independent of the secret message are sent by the full-duplex relays. This strategy was also investigated in Bassily & Ulukus (2013, 2012). In Li *et al.* (2013), a security-oriented transmission scheme was proposed in cognitive radio network CRN with the aid of multiple relays. To maximize the secondary user (SU) link secrecy capacity, both cooperative jamming techniques and beamforming are used to improve the performance of the SU while providing a good protection to the primary users (PUs). The proposed scheme contributes in securing the SU's transmission while the SNR attenuation at the PU receiver is kept acceptable. Another interesting security scheme, in a centralized cognitive radio network (CRN), was proposed in Wen *et al.* (2019), where the base station is communicating with a PU in the presence of an eavesdropper, while the SU acts as a friendly jammer. This jammer could be fully trusted or untrusted when it does not send jamming signals all the time for selfish reasons. Therefore, a selection criterion was adopted to evaluate the trust degree of this jammer and its effect on the secrecy performance.

B. Untrusted Relays:

Unlike the aforementioned case, the relay itself is sometimes considered an untrusted user; it

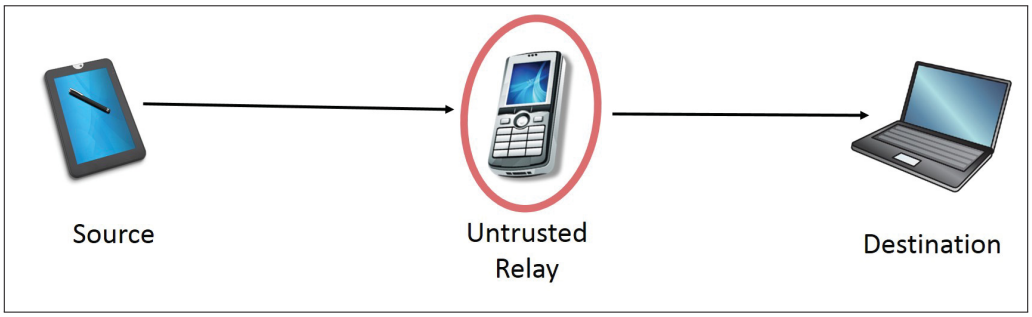


Figure 1.6 Representation of untrusted (co-located relay and eavesdropper) relay network

acts both as an eavesdropper and a traditional relay, i.e., as shown in Fig. 1.6 the relay node and the eavesdropper are co-locating. First studied in Oohama (2007) for general relay channels, this type of model implies that the source desires to use the relay to communicate with the destination while it intends to shield the relay of the message. Under the assumption that some of the messages that have been transmitted are confidential to the relay, coding problems associated with the relay-wiretap channel are studied. In Shrestha *et al.* (2019), the authors studied the secrecy performance of a multi-hop ad-hoc wireless network in the presence of untrusted and trusted relays in each hop. To perform the transmission, the most secure relay will be chosen in each hop to deliver the message. The researchers in El Shafie *et al.* (2017) proposed a new scheme to secure a wireless network in the presence of untrusted relays. The destination and another cooperative jammer inject artificial noise to jam these relays for two reasons; to prevent them from intercepting their received messages and to help them harvest energy to charge their batteries. In Atallah & Kaddoum (2017) and Atallah & Kaddoum (2019), new location-based multicasting techniques were proposed to reduce the possibility of an untrustworthy relay intercepting the whole transmitted message. As an interesting result, the use of an untrustworthy relay can still be beneficial in increasing the secrecy capacity Yener & He (2010); Jeong *et al.* (2012); Sun *et al.* (2012); Kuhestani *et al.* (2016). In the following section, we will explore a very important cooperating method in physical layer security; the cooperative jamming technique, which is a promising method and has attracted significant attention. This method was proposed originally for a multiple access wiretap channel, where multiple legiti-

mate users wish to establish secure communications with an intended receiver in the presence of an eavesdropper. Since an eavesdropper could be part of a wireless network as an untrusted relay, we will explore here some major types of the eavesdroppers' behaviors.

Active behavior:

Here, as an example, the eavesdropper could attack the wireless system by sending jamming signals. In this case, it is possible to locate this active eavesdropper and change the current strategies to avoid this type of attacks.

Passive behavior:

In this type, each eavesdropper will work individually to intercept the message, without doing

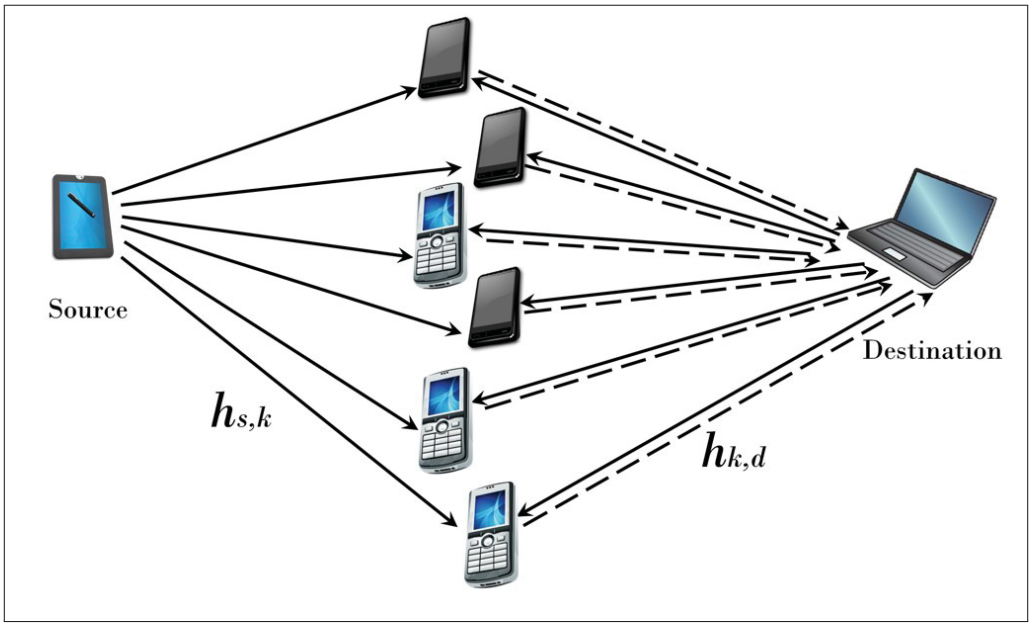


Figure 1.7 Eavesdroppers' passive behavior

any action that could lead to detect its real identity or its place. Therefore, it's hard to locate this kind of eavesdroppers compared to the active one, Fig.1.7.

Colluding behavior:

For this type of behavior, the eavesdroppers will collude together to intercept the message, by sending all their received signals towards another wiretapper. In the literature, this behavior was called the colluding, cooperating or aggressive behavior, Fig1.8.

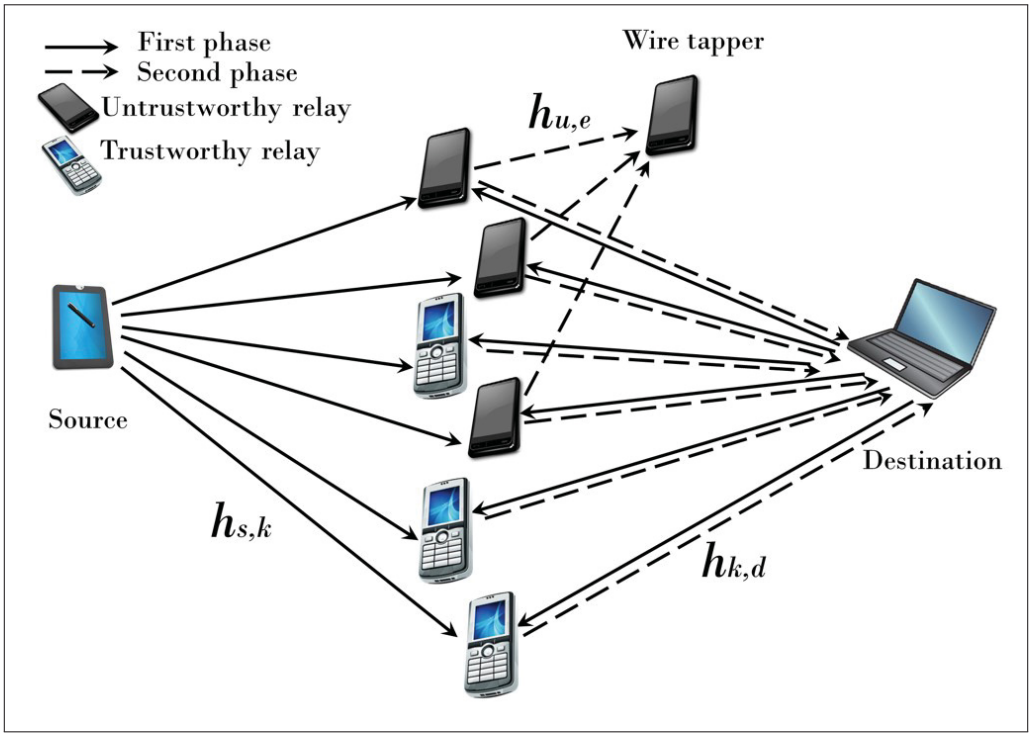


Figure 1.8 Eavesdroppers' colluding behavior

1.2.4.1 Cooperative Jamming

To confuse the eavesdropper, a special technique called cooperative jamming can be used where an artificial noise is introduced by a helpful interferer. The secrecy performance analysis with cooperative jamming was studied in the presence of the impulsive noise Atallah *et al.* (2019), aggressive relays Atallah & Kaddoum (2016), mixture Gamma distribution Kong & Kaddoum (2019), $\alpha\mu$ fading channels Kong & Kaddoum (2019), Hybrid Millimeter Wave Networks Vuppala *et al.* (2018) , and device-to-device (D2D)-enabled cellular networks Tolossa *et al.* (2018). In the following section, we will introduce the cooperative jamming techniques which are used to increase the physical layer security. To improve the secrecy capacity, we should either increase the legitimate receiver's SNR or decrease the eavesdropper's SNR. A natural approach to achieve the latter is to introduce interferers into the system, Fig. 1.9.

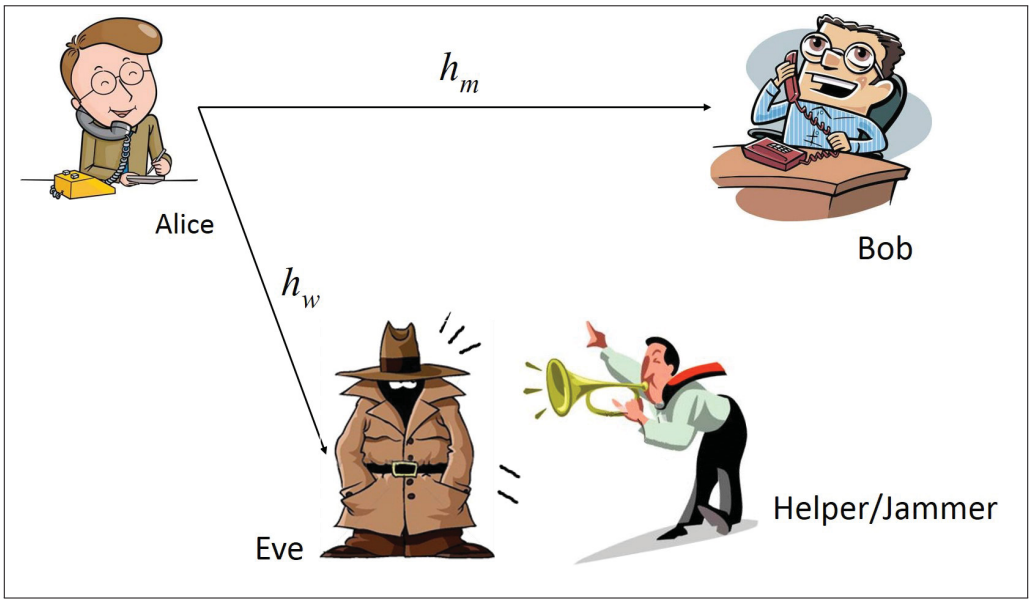


Figure 1.9 Representation of a network with a jammer

1.2.4.2 Artificial Jamming Signals Types

Cooperative jamming relies on creating the interference at the eavesdropper's side, many artificial jamming signals are used and could be divided into four categories Long *et al.* (2014):

1. Gaussian noise: which is similar to additive noise at the receiver Atallah & Kaddoum (2016, 2017); Atallah & Kaddoum (2019).

2. Jamming signals which are priory known at the legitimate receivers, and thus only impact the eavesdropper's performance. This type of signals is better than the previous one because the jamming signals don't affect the legitimate receiver Long *et al.* (2013); Dong *et al.* (2011).

3. Random codewords of a public codebook which is known by all the nodes including the eavesdroppers, so the legitimate receiver has the ability to decode and cancel the jamming signals, even though it requires a complicated self-interference cancellation receiver to decode the codewords Pierrot & Bloch (2011).

4. Useful signals for the other legitimate nodes; signals of multiple simultaneous source-destination pairs Sheikholeslami *et al.* (2012), or signals of the invited cognitive radio users Stanojev & Yener (2011) and Stanojev & Yener. (2011); this type is difficult to apply because of the change in the multiple transmission pairs.

5. Random fake signals that the legitimate transmitter sends to confuse the eavesdroppers. The legitimate receiver uses self-interference cancellation to cancel these fake messages Atallah & Kaddoum (2019).

In the following subsection, we will explore some applied policies with the cooperative jamming technique to enhance the performance and increase the security.

1.2.4.3 Jamming Policies

Several policies were proposed for relay selection to secure the communication Liu *et al.* (2015); Sun *et al.* (2015); Hui *et al.* (2015); Jameel *et al.* (2018). In Liu *et al.* (2015), four relay selection policies are proposed and compared, particularly random relay and random jammer, best relay and best jammer, random jammer and best relay, and also best relay and no jammer. This work characterizes the proposed relay selection policies, impact and the power of interference constraint on the secrecy performance by deriving new exact closed-form expressions for the secrecy outage probability; it is shown that the jammer's absence raises the outage saturation phenomenon. In Hui *et al.* (2015), selection methods for the relay and the jammer were developed in order to minimize the secrecy outage probability; in these selection methods, the knowledge of the jammer and relay set is kept secret to the eavesdropper while each intermediate node knows its own role. As a result, the maintenance of the privacy of the selection greatly improves the SOP performance of the system. This work assumes a decode and forward relay system, in which through intermediate nodes in the presence of numerous passive eavesdroppers, the destination can communicate with the source. To prohibit the eavesdroppers from the interception of the signal of interest, the intermediate nodes act as jammers or as conventional relays. To determine whether they will be serving as relays or jammers, the intermediate

nodes take the decision based on the receiving information from the destination. Additionally, the eavesdropper is unaware of the selection result to null the interference towards it. In Luo & Yin (2018), a new scheme was provided in two-hops wireless networks. The source communicates with the destination via N relays in the presence of a wiretapper. In each transmission, one of these relays will be selected to jam the wiretapper, while the other $N-1$ relays are retransmitting their received messages from the source towards the destination using distributed beamforming (DBF). Another scheme was provided in Liu *et al.* (2013) where in the first phase, the information bearing signal is transmitted by the source simultaneously as it is cooperating with the destination in jamming the eavesdropper without interference at the relay. In the second phase, a relay is selected optimally, which transmits the decoded source signal. Meanwhile, this relay is cooperating with the source to jam the eavesdropper without creating interference whereat the destination is located. The authors in Lin *et al.* (2013a) proposed a new transmission scheme, where the relaying group and the jamming group are constructed together. The jammers send the jamming signal and the useful message in the same time. This scheme enables to confuse the wiretappers and increase the signal-to-noise ratio at the legitimate receiver's side. In Chen *et al.* (2013), attack strategies were investigated in a multi-relay network that consists of both malicious and cooperative relays, where the malicious relays have the freedom to listen to the transmitter in the first hop (so that they can send interference signals in the second hop). The direct emission of jamming signals in both hops is also investigated. Subsequently, it is shown that the malicious relays should attack in both hops rather than just listening in the first hop and attacking in the second hop. On the other hand, the opportunistic cooperative jamming and the opportunistic relay chatting schemes were compared in Ding *et al.* (2011). It is shown that the chatting scheme where the relay nodes jam the eavesdropper in the both phases, is better than the cooperative jamming scheme in which the eavesdropper is only jammed in the first phase. In Alibeigi & Taherpour (2019), the authors proposed a security scheme in two-hops D2D communications, based on making use of other cellular users as friendly jammers to jam an eavesdropper while this latter is trying to intercept the transmitted message. According to their simulation results, a better secrecy performance is achieved when the number of cellular users or the distance to the eavesdropper is increased. The researchers

in Chen (2018) investigated the security over a two-users Gaussian interference channel, where each source communicates with its corresponding destination. When one of the destinations receives the other destination's message, it will treat it as interference. They showed, for a symmetric case, that the optimal secrecy rate is achieved as long as the interference-to-signal ratio in decibel is no more than $2/3$. Otherwise, cooperative jamming is needed to achieve the optimal secrecy rate in their system. Furthermore, another scheme was studied in Mobini *et al.* (2019) to secure a source-relay-destination link in the presence of an eavesdropper and an external cooperating jammer. Two cooperating protocols were investigated: the full duplex jammer protocol (FDJ), where all the nodes are half duplex except the relay is full duplex, and the half duplex jammer protocol (HDJ), where all the nodes are half duplex. It is shown that, from a secrecy perspective, FDJ is superior to HDJ.

1.2.4.4 Cooperative Jamming with Power Allocation

Since the system's performance in cooperative jamming highly depends on the jamming strategy and power level Park *et al.* (2013), three power allocation strategies were derived in Park *et al.* (2013) for the SOP to be minimized. Moreover, three kinds of jamming power allocation schemes are proposed according to the available CSI at the destination to limit the outage probability. In He *et al.* (2019), the researchers proposed three user-pair selection schemes for untrustworthy relay networks with multiple source-destination pairs, namely opportunistic, greedy and genie-aided user pair selection schemes. They showed that the greedy user-pair selection scheme overcomes the other schemes from a secrecy perspective, due to the cooperation by the source that adds flexibility to the network. The authors in Zhang *et al.* (2015) investigated the cooperative jamming in MISO channels in which the legitimate receiver splits the received power for energy harvesting and information decoding. Another power allocation method is analysed in Long *et al.* (2014) in which the source nodes send jamming signals as a part of their power instead of hiring extra nodes to jam the eavesdropper. Two types of jamming signals are analysed; a priori known jamming signals at the source nodes, and unknown jamming signals at the source nodes. A major finding reported in this work is that, if

the jamming signals are known a priori at the source nodes, the secrecy capacity is improved significantly when compared to the scenario in which the jamming signals are unknown. In Yang *et al.* (2014), besides applying cooperative jamming technique, the base station utilizes a linear precoding scheme, which exploits transmission diversity by weighting the information stream. When the number of the friendly jammer's antennas is no less than the total number of the eavesdropping antennas, an optimal solution is obtained. The authors in Wang *et al.* (2015a) proposed a sequential parametric convex approximation (SPCA) based algorithms to address the power allocation optimization and maximize the ergodic secrecy rate (ESR) lower bound, and show that the secrecy capacity is improved by the optimized power allocation that tends to allocate jamming signals more power. An optimal relay selection criterion and power allocation strategy were derived in Wang & Wang (2014) between the jamming signals and the confidential information for the ESR maximization. Another study in Deng *et al.* (2015) showed that a helper node should allocate its power as a jammer or as a helper depending on the locations of the helper and the eavesdropper. In Do *et al.* (2019), the authors studied the optimal transmit power in the presence of an active eavesdropper that is jamming the destination. The destination tells the source when to transmit the data and when to harvest energy depending on the source's power and the existence of jamming attacks by the eavesdropper. The aim of their policy is to optimize the security and the allocated power at the source when it is transmitting data under the energy harvesting constraint that is applied to the source.

1.2.5 Game Theory for Security

As an effective framework for the design of security mechanisms for wireless networks, Game theory, traditionally applied in the areas of sociology, economics, biology, political science, and resource allocation in wireless systems, has recently emerged. Moreover, jamming policies using game theory methods were proposed in Fakoorian & Swindlehurst (2013); Chen *et al.* (2013); Stanojev & Yener (2013); Li *et al.* (2014b). In Chen *et al.* (2013), a multi-relay network, consisting of both malicious and cooperative relays, applies Nash equilibrium game strategy on its scheme, by modelling the sets of malicious relays and cooperative relays as two

players in a zero sum game with the maximum achievable rate as the utility. The authors in Fakoorian & Swindlehurst (2013) proposed a scheme of two users MISO Gaussian interference channel, where the transmitters aim to maximize the difference between their secrecy rate and that of the others. In this scheme, the weaker link tries to minimize the gap between its secrecy rate and that of the other transmitter, while the transmitter with the stronger link tries to maximize this gap. This paper used Nash equilibrium strategy as a solution in its scheme. In Houjeij *et al.* (2013), using the non-cooperative game theory framework, the interactions in CRNs between secondary users (SU)s and eavesdroppers were analysed. A novel secure channel selection algorithm has been proposed to solve the formulated game; the eavesdroppers and the SUs are enabled to take distributed decisions in order to reach a Nash equilibrium point. As showed by the authors, in terms of the average secrecy rate per SU, the proposed approach yields significant performance improvements especially when compared to a classical spectrum sharing scheme. The researchers in Stanojev & Yener (2013) proposed another game-theoretic model, Stackelberg game, with the legitimate parties being the owners of the spectrum acting as a game leader, and the set of the assisting jammers become the followers. They showed that as the number of potential jammers increases, a chosen jammer's utility will decrease because of the aggressiveness of the game leaders, i.e. the legitimate parties. In Li *et al.* (2014b), it was shown that the strategies of the legitimate transmitters quickly learned by a smart jammer would lead to an adjustment of the jammer's strategy to damage the legitimate transmission. Meanwhile, the existence of the smart jammer is well known from the transmitters. This scenario of anti-jamming is modelled as a Stackelberg game, where the leader is the source node and the follower is the jammer. It is shown that the obtained optimal power control strategies from the Stackelberg equilibrium game can minimize the effect of the damage caused by the jammer. As proposed by the authors in Zhu *et al.* (2010), and based on a reversed Stackelberg game, a secure cooperative spectrum trading scheme in CRNs is applied; the illegal actions of the SU are automatically supervised by the PU, who will adjust it's strategies according to the actions of the SU. In Badia & Gringoli (2019), the authors studied a game theory scenario in the presence of a malicious node for two scenarios: when there is only one friendly jammer and when there are multiple friendly jammers. Their study showed that even though the exis-

tence of multiple friendly jammers enhances the security, it is still not effective enough to stop the malicious node from trying to perform unauthorized transmissions because of the lack of coordination between these jammers. Another interesting dynamic psychological game study, between a soldier and an attacker, was investigated in Hu *et al.* (2019), where the soldier tries to finish his mission in a certain time to pass through the battlefield while keeping connected to the Internet of Battlefield Things (IOBT). In the mean time, the attaker is trying to delay the soldier's connection time with the IOBT by using jamming. Their results showed that by using their proposed Bayesian updating algorithm, the soldier and the attacker can reach ε-like psychological self-confirming equilibrium strategies for their proposed psychological game. However, more studies are still needed to investigate the schemes where there are multiple defenders versus multiple attackers. Additionally, in most of the studies, the assumption of that the defender and the attacker can detect the system state with no error, needs to be relaxed.

1.2.6 Key Generation Technique

Key generation is a technique where two legitimate nodes extract secret symmetric key bits by exploiting the fluctuations and the random characteristics of wireless communication channels. It is a low cost solution since it does not require complex operations. For the model shown in Fig. 1.1 where Bob and Alice want to establish a secure key while the eavesdropper is listening to the legitimate channel between them. Bob, Alice, and Eve can get correlated observations $Y^n = (Y_1, ..., Y_n)$, $X^n = (X_1, ..., X_n)$ and $Z^n = (Z_1, ..., Z_n)$, respectively. Over the legitimate channel, Bob and Alice will exchange a message s while Eve is trying to eavesdrop it. For a sufficiently large n and any $\varepsilon > 0$, R is the achievable key rate if there exists $K^B = g_B(Y^n, s)$ and $K^A = g_A(X^n, s)$ making the key generation satisfy the following Zhang *et al.* (2016a):

- Bob and Alice are generating the same key with high probability $\Pr(K^A \neq K^B) < \varepsilon$.
- No information is leaked to the eavesdropper which means guaranteeing the generated key's secrecy $\frac{1}{n} I(K^A; s, Z^n) < \varepsilon$ where $I(.)$ is the mutual information.

- The key rate R satisfies $R > \frac{1}{n}H(K^A) + \varepsilon$.
- Finally, the generated key is uniformly distributed $\frac{1}{n}\log|\mathscr{K}| < \frac{1}{n}H\left|K^A\right| + \varepsilon$, where $\mathscr{K}$ denotes the alphabet of the generated key.

Moreover, the key capacity which is the largest key rate achieved is given by

$$C_K = \min\left[I(X;Y), I(X;Y \mid Z)\right], \tag{1.14}$$

Most of works studied the key generation technique based on the characteristics of wireless channels, while a few works have investigated schemes with static channels. The authors in Guillaume *et al.* (2015) proposed a new scenario to generate random keys in static channels by using a moving third party to exploit the channels' characteristics between him and the legitimate nodes to generate the key. In Madiseh *et al.* (2012), another scheme is proposed to generate keys in static environments by employing random beamforming. Furthermore, Huang & Wang (2013) also proposed a key generation scheme aided by frequency diversity and opportunistic beamforming for long coherence time channels. In Felkaroski & Petri (2019), the authors generated their keys from the CSI that was extracted from multiple mmWave subcarriers. This generation method yields a very fast bit generation rate, which enabled the communicating legitimate nodes to establish and refresh the shared generated secret key in a very short period of time. Also, the authors in Zhang *et al.* (2018) proposed a two-way secret key generation method, where each legitimate node shares its random signal with the other legitimate node through the reciprocal channel. Then, each node will generate keys benefiting from the randomness that comes from multiplying its received signal by its local signal. By applying this method, there is no need to rely on the CSI to generate keys. The results showed the effectiveness of this method, not only theoretically, but also practically.

1.3 Unrealistic assumptions

In the literature, most of the security methods rely on knowing the eavesdropper's channel, location or both of them. Additionally, for our best of knowledge, the eavesdroppers in all the

scenarios were receiving the whole transmitted message all the time. Many studies investigated in the eavesdroppers' passive behavior, and few considered the colluding one. Also, key generating techniques didn't exploit the presence of having many untrusted nodes, and the secrecy performance in impulsive noise invironments wasn't been analysed yet. Therefore, we covered each of these aforementioned points in our following articles.

CHAPTER 2

SECRECY CAPACITY SCALING WITH UNTRUSTWORTHY AGGRESSIVE RELAYS COOPERATING WITH A WIRE-TAPPER

Michael Atallah[1], and Georges Kaddoum[1]

[1] Department of Electrical Engineering, École de Technologie Supérieure,
1100 Notre-Dame Ouest, Montréal, Québec, Canada H3C 1K3

Paper published in *IEEE Wireless Communications Letters*, August 2016.

2.1 Abstract

In this paper, we investigate the performance of the secrecy capacity in an amplify-and-forward (AF) dual-hop network for both distributed beamforming (DBF) and opportunistic relaying (OR) techniques. We derive the capacity scaling for two sets; U untrustworthy aggressive relays cooperating together with a wire-tapper to intercept the message, and T trustworthy relays, for a large number of nodes. We prove that the capacity scaling in the DBF is bounded by a value depending on a ratio between the number of the trustworthy and the untrustworthy aggressive relays. Finally, we show that DBF is better than OR whose capacity scaling is proved to be upper-bounded by a value tending to zero when the untrustworthy relays are aggressive. Simulation results confirm our analytical derivations.

Keywords: Physical layer security, cooperative jamming, distributed beamforming, opportunistic relaying, amplify and forward.

2.2 Introduction

Security has always played a critical role in wireless cooperative communication systems design. The basic notion of physical layer security is to increase the legitimate links capacity while decreasing the capacity of the illegitimate links, which is achievable via the utilisation of the dynamic nature of wireless channels Liang *et al.* (2008); Gopala *et al.* (2008). Many con-

tributions have been recently made to increase the secrecy capacity by combining advanced strategies in wireless communications like beamforming, multiple antenna schemes, game theory techniques and power allocation methods Atallah *et al.* (2015). Because of the broadcast nature of the wireless network's medium, all the users could be potential eavesdroppers within the transmission range. Considering this point, recent works show that the secrecy rate could be enhanced when treating the untrusted nodes as relays instead of treating them as eavesdroppers Jeong *et al.* (2012); Yener & He (2010). In Jeong *et al.* (2012), this scenario is extended to MIMO scheme with beamforming strategy. Furthermore, asymptotic analysis is often seen in research as the "end of the line"; the attaining of a result that cannot be dramatically improved upon. Therefore, asymptotic analysis is a method of describing limiting behaviour in systems when they are very large. Hence, many works study the scaling performance from a security perspective Sun *et al.* (2012); Kim *et al.* (2015). Using the opportunistic relaying OR scheme as described in Sun *et al.* (2012), the scaling law of the secrecy capacity is investigated for multiple untrustworthy relays. The researchers in Kim *et al.* (2015) have studied the maximum capacity scaling according to the number of the untrustworthy relays by considering all relays as untrustworthy passive nodes. Hence, the capacity scaling where the untrustworthy relays are aggressive by sending their messages to a wire-tapper has not yet been studied in the literature. Therefore, we investigate the following questions in this paper:

- What is the minimum secrecy-capacity scaling according to the number of untrustworthy aggressive relays U and trustworthy relays T?
- Which scenario would be better, DBF or OR?

Our considered cooperative network contains one source, two sets of relays using AF technique, and one destination. Hence, the first set includes untrustworthy relays which are collaborating together to eavesdrop the transmitted messages through an external wire-tapper, and the other set includes trustworthy relays. Moreover, to reduce the eavesdropping capacity of untrustworthy relays, the destination acts as a jammer and transmits a jamming signal to the relays during the first phase of communication. In this paper, an investigation of the asymptotic

performance of DBF and OR using AF technique is performed. The contributions presented in this paper are; 1) The secrecy capacity scaling is provided by showing that DBF has the scaling of $\frac{1}{2}\log_2(\frac{T}{U}+1)$ at either the absence or the presence of the intended jamming (IJ) by the destination. 2) In OR, the secrecy capacity scaling is upper bounded by a value tending to zero for large number of T and U.

Notations: $E[X]$ and $\mathrm{VAR}[X]$ denote the mean expectation and the variance of a random variable (r.v.) X. Furthermore, $f_x(.)$ and $F_x(.)$ denote the probability density function (PDF) and the cumulative distribution function (CDF) of X, respectively. More, $\overset{w.p.1}{\rightarrow}$ denotes the convergence with probability one, $[A]^+$ denotes $\max\{A,0\}$. For two functions $f(x)$ and $g(x)$, $f(x)\sim g(x)$ means that $\lim_{x\to\infty} f(x)/g(x)=1$ and $\lim_{1/x\to 0} f(\frac{1}{x})/g(\frac{1}{x})=1$. For a r.v. X, the notation $X\sim N_c(a,b)$ denotes that X is a complex Gaussian r.v. with mean a and variance b.

2.3 System Model

Consider a two-hop wireless network which consists of a source s communicating with a destination d through a set of amplify-and-forward relays $R_k=\{1,2,...,K\}$ divided into two sets, an untrustworthy set $R_u=\{1,2,...,U\}$ and a trustworthy set $R_t=\{1,2,...,T\}$ of relays, where $R_u\cup R_t=R_k$. The trustworthy relays are considered as an essential part of the network, whereas the untrustworthy relays are the nodes that login to the network for a long enough period of time. Moreover, the destination broadcasts the jamming signal toward all the relays. In our network, each relay has a single antenna operating in half-duplex mode, as shown in Fig. 2.1. On the other hand, the external wire-tapper cooperates with the untrustworthy relays to decode the transmitted symbols of the source thanks to the different replicas of the source's signal relayed by these latter. Moreover, there is no direct link between the source and the destination in our system, i.e. all transmitted information must pass by relays. In our analysis, the channels are assumed to be uncorrelated reciprocal frequency-flat block-fading with the coefficient between nodes i and j being denoted by $h_{i,j}$ and being modelled as a complex Gaussian random variable where $(i,j\in\{s,R_k,d\})$. Therefore, the channel gains $\left|h_{s,k}\right|^2$ and $\left|h_{k,d}\right|^2$ are independent and exponentially distributed r.v.'s whose means are σ_1^2 and σ_2^2 respectively. We assume that the

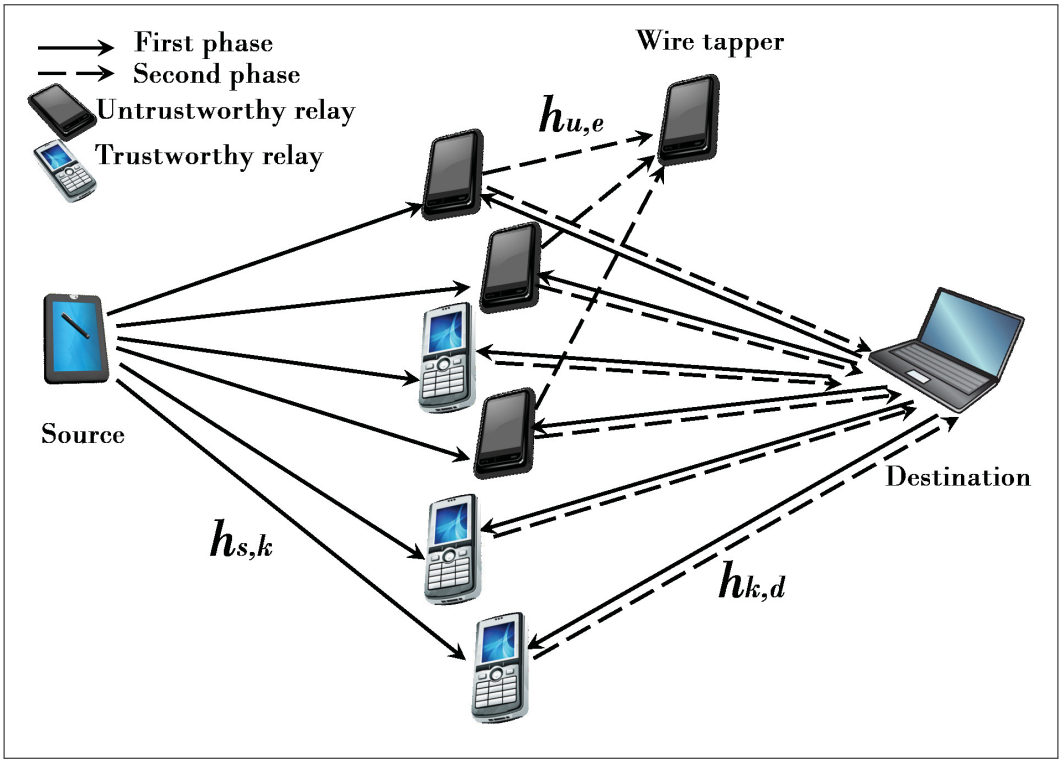


Figure 2.1 System model

noise variance N_0 is the same in the first and the second hop, and the channel state information CSI is known by the receiving nodes. The source broadcasts the message signal x_s in the first hop of transmission to the relays while the destination sends a jamming signal x_d towrds the relays. In the first hop, the received signal at the kth relay is given by

$$y_k = h_{s,k}\sqrt{P_s}x_s + h_{k,d}\sqrt{P_d}x_d + n_k\,. \tag{2.1}$$

Where n_k is a complex additive white Gaussian noise at the kth relay with zero mean and variance N_0. The transmitted powers of the source and the destination are denoted by P_s and P_d respectively. It is assumed that at the kth relay, the received signal-to-interference-plus-noise ratio SINR would be

$$\gamma_k = \frac{\rho_s \left|h_{s,k}\right|^2}{\rho_d \left|h_{k,d}\right|^2 + 1}. \tag{2.2}$$

where the signal to noise ratio SNR is denoted by $\rho'_i \triangleq P_i/N_0$, $i \in \{s,d\}$, $\rho' \subset \rho$ where $\rho_j \triangleq P_j/N_0$, $j \in \{s,t,u,d\}$. In the following subsections, we will derive the secrecy capacities of DBF and OR respectively.

2.3.1 Distributed Beamforming

Using the DBF strategy at the relays' side, the retransmitted signal by the ith relay in the second hop is $x_i = a_i w_i y_i$. where w_i, $i \in \{t,u\}$ represents the optimized beamforming weight. The normalized amplifying coefficient a_k for the kth relay is as follows

$$a_k = \frac{1}{\sqrt{\rho_s \left|h_{s,k}\right|^2 + \rho_d \left|h_{k,d}\right|^2 + N_0}}.$$

The destination receives a signal transmitted by each of the relays, which can be expressed as

$$y_d = h_{k,d} a_k w_k y_k + n_d \,. \tag{2.3}$$

Similarly, the wire-tapper receives a signal transmitted by each of the untrustworthy aggressive relays

$$y_e = h_{u,e} a_u w_u y_u + n_e \,. \tag{2.4}$$

Where $h_{u,e}$ is the channel coefficient between the untrustworthy relay and the external wire-tapper, n_d and n_e are complex AWGN with zero mean and variance N_0 at the destination and at the wire-tapper respectively. After removing the jamming signal x_d at the destination, the received SINR becomes

$$\gamma_d^{DBF} = \sum_{u=1}^{U} \frac{\rho_s \left|h_{s,u}\right|^2 \rho_u \left|h_{u,d}\right|^2}{\rho_s \left|h_{s,u}\right|^2 + (\rho_d + \rho_u)\left|h_{s,u}\right|^2 + 1} + \sum_{t=1}^{T} \frac{\rho_s \left|h_{s,t}\right|^2 \rho_t \left|h_{t,d}\right|^2}{\rho_s \left|h_{s,t}\right|^2 + (\rho_d + \rho_t)\left|h_{t,d}\right|^2 + 1}. \tag{2.5}$$

Whereas the recieved SINR at the wire-tapper becomes

$$\gamma_e = \sum_{u=1}^{U} \frac{\rho_s |h_{s,u}|^2 \rho_u |h_{u,e}|^2}{\rho_u \rho_d \left|h_{u,d}\right|^2 |h_{u,e}|^2 + \rho_s |h_{s,u}|^2 + \rho_d \left|h_{u,d}\right|^2 + \rho_u |h_{u,e}|^2 + 1}. \tag{2.6}$$

Therefore, the instantaneous secrecy capacity of the DBF could be written as

$$C_S^{DBF} = \left[\frac{1}{2} \log_2 \left(1 + \sum_{t=1}^{T} \frac{\rho_s |h_{s,t}|^2 \rho_t \left|h_{t,d}\right|^2}{\rho_s |h_{s,t}|^2 + (\rho_d + \rho_t) \left|h_{t,d}\right|^2 + 1} \right.\right.$$

$$\left.\left. + \sum_{u=1}^{U} \frac{\rho_s |h_{s,u}|^2 \rho_u \left|h_{u,d}\right|^2}{\rho_s |h_{s,u}|^2 + (\rho_d + \rho_u) \left|h_{u,d}\right|^2 + 1} \right) - \frac{1}{2} \log_2 \left(1 + \gamma_e\right) \right]^+$$

$$= \left[C_d^{DBF} - C_w\right]^+. \tag{2.7}$$

The data rate between the wire-tapper and all the untrustworthy relays cooperating with it is denoted by C_w. Since the relays are half-duplex, we use the rate-loss factor value of 1/2.

2.3.2 Opportunistic Relaying

During the second hop, only the best relay b that has the maximum SNR at the destination retransmits the signal. Through the kth relay, the end-to-end SINR is as follows

$$\gamma_{s,k,d} = \frac{\rho_s \left|h_{s,k}\right|^2 \rho_k \left|h_{k,d}\right|^2}{\rho_s \left|h_{s,k}\right|^2 + (\rho_d + \rho_k) \left|h_{k,d}\right|^2 + 1}. \tag{2.8}$$

Hence, the best relay is selected as

$$b = \underset{k \in R_k}{\arg\max} \{\gamma_{s,k,d}\}. \tag{2.9}$$

Therefore, the achievable secrecy capacity becomes

$$\begin{aligned} C_S^{OR} &= \left[\frac{1}{2}\log_2\left(1+\max_k(\gamma_{s,k,d})\right) - \frac{1}{2}\log_2\left(1+\gamma_e\right)\right]^+ \\ &= \left[C_d^{OR} - C_w\right]^+. \end{aligned} \tag{2.10}$$

2.4 SCALING LAW OF SECRECY CAPACITY

2.4.1 Scaling Law of Distributed Beamforming

This subsection shows that the secrecy capacity scaling of untrustworthy aggressive relays in DBF is not the same as the maximum secrecy capacity for trustworthy relays. Without loss of generality, we assume in our analysis that $\rho \triangleq \rho_s = \rho_t = \rho_u = \rho_d$.

Theorem 1. *When $T \to \infty$ and $U \to \infty$ with any finite ρ, the ergodic secrecy capacity of the $\overline{C}_S^{DBF} = E\{C_S^{DBF}\}$ is lower bounded by $\frac{1}{2}\log_2(\frac{T}{U}+1)$.*

Proof. It is shown in Bolcskei *et al.* (2006) that for $T \to \infty$ and any finite ρ, the capacity scaling through trustworthy relays in a dual hop network is upper bounded by $\frac{1}{2}\log_2(T)$. But considering the aggressive behaviour of the untrustworthy relays, the secrecy capacity becomes lower bounded by

$$\begin{aligned} \overline{C}_S^{DBF} &= E\left\{C_S^{DBF}\right\} \\ &= E\left\{\left[\frac{1}{2}\log_2\left(1+\sum_{t=1}^{T}\frac{\rho\left|h_{s,t}\right|^2\rho\left|h_{t,d}\right|^2}{\rho\left|h_{s,t}\right|^2+2\rho\left|h_{t,d}\right|^2+1}\right.\right.\right. \\ &\left.\left.\left.+\sum_{u=1}^{U}\frac{\rho\left|h_{s,u}\right|^2\rho\left|h_{u,d}\right|^2}{\rho\left|h_{s,u}\right|^2+2\rho\left|h_{u,d}\right|^2+1}\right) - \frac{1}{2}\log_2(1+\gamma_e)\right]^+\right\} \\ &\overset{(a)}{\geq}\left[E\left\{\frac{1}{2}\log_2\left(1+\sum_{t=1}^{T}\frac{\rho\left|h_{s,t}\right|^2\rho\left|h_{t,d}\right|^2}{\rho\left|h_{s,t}\right|^2+2\rho\left|h_{t,d}\right|^2+1}\right.\right.\right. \end{aligned}$$

$$+\sum_{u=1}^{U}\frac{\rho\left|h_{s,u}\right|^2\rho\left|h_{u,d}\right|^2}{\rho\left|h_{s,u}\right|^2+2\rho\left|h_{u,d}\right|^2+1}\Bigg)\Bigg\}-E\left\{\frac{1}{2}\log_2(1+\gamma_e)\right\}\Bigg]^+$$

$$=\left[E\left\{C_d^{DBF}\right\}-E\left\{C_w\right\}\right]^+. \tag{2.11}$$

where (a) follows from the fact that $E\{\max(X_1,X_2)\}\geq\max(E\{X_1\},E\{X_2\})$. Let

$$N_u\triangleq\frac{\rho\left|h_{s,u}\right|^2\rho\left|h_{u,d}\right|^2}{\rho^2\left|h_{d,u}\right|^2\left|h_{u,e}\right|^2+\rho\left|h_{s,u}\right|^2+\rho\left|h_{u,e}\right|^2+\rho\left|h_{u,d}\right|^2+1}, \tag{2.12}$$

and

$$M_t\triangleq\frac{\rho\left|h_{s,t}\right|^2\rho\left|h_{t,d}\right|^2}{\rho\left|h_{s,t}\right|^2+\rho\left|h_{t,d}\right|^2+1}. \tag{2.13}$$

M_t satisfies the *Kolmogorov conditions i.e.* $\sum_{t=1}^{T}\frac{VAR[M_t]}{t^2}<\infty$ and $\mu_t=\frac{1}{T}\sum_{t=1}^{T}E\left[M_t\right]<\infty$ are true for any finite ρ Bolcskei *et al.* (2006). N_u also satisfies *Kolmogorov conditions* since $N_u<M_t$, so we can apply the following theorem Serfling (1980):

$$\sum_{u=1}^{U}\frac{N_u}{U}-\sum_{u=1}^{U}\frac{E\left[N_u\right]}{U}\overset{w.p.1}{\rightarrow}0. \tag{2.14}$$

Therefore, $\gamma_d^{DBF}\overset{w.p.1}{\rightarrow}U\,\mu_u$, and $E\left\{C_d^{DBF}\right\}\sim\frac{1}{2}\log_2(T+U)$, where $\mu_u=\frac{1}{U}\sum_{u=1}^{U}E\left[N_u\right]<\infty$. Thus

$$\begin{aligned}\overline{C}_S^{DBF}&\geq\left[E\left\{C_d^{DBF}\right\}-E\left\{C_w\right\}\right]^+\\&\sim\left[\frac{1}{2}\log_2(T+U)-\frac{1}{2}\log_2(U)\right]^+\\&=\frac{1}{2}\log_2\left(\frac{T}{U}+1\right).\end{aligned} \tag{2.15}$$

□

It is clear from (2.15) that the lower bounded secrecy capacity depends on the ratio between T and U. For example, to maintain a certain level of secrecy capacity in a wireless network, the maximum number of untrustworthy aggressive relays should not exceed:

$$U \leq \frac{T}{2^{2\overline{C}_S^{DBF}}}. \tag{2.16}$$

Let's assume that the wire-tapper could receive more signals from other trustworthy relays T' where $T' \leq T$. Hence, the total number of the relays that the wire-tapper could combine the signals from will be U', where $U' = T' + U$. In this case, and by following the same steps in the *proof* of *Theorem 1*, the secrecy capacity scaling in equation (2.15) will be

$$\begin{aligned} \overline{C}_S^{DBF} &\geq \left[\frac{1}{2}\log_2(T+U) - \frac{1}{2}\log_2(U')\right]^+ \\ &= \left[\frac{1}{2}\log_2(T+U) - \frac{1}{2}\log_2(T'+U)\right]^+ \\ &= \frac{1}{2}\log_2\left(\frac{T+U}{T'+U}\right). \end{aligned} \tag{2.17}$$

which tends to zero for $T' = T$.

Moreover, we will show in Theorem 2 that even when the destination is not jamming, the secrecy capacity scaling will tend to the same bound value of DBF with IJ as given in equation (2.15).

Theorem 2. *When $T \to \infty$ and $U \to \infty$ with any finite ρ, the ergodic secrecy capacity of a DBF without IJ tends to the value $\frac{1}{2}\log_2(\frac{T}{U}+1)$.*

Proof. Considering that the ergodic secrecy capacity of a DBF without IJ is given by

$$\overline{C}_{S,NoJam}^{DBF} = E\left\{C_{S,NoJam}^{DBF}\right\}$$

$$= E\left\{\left[\frac{1}{2}\log_2\left(1 + \sum_{t=1}^{T}\frac{\rho\left|h_{s,t}\right|^2\rho\left|h_{t,d}\right|^2}{\rho\left|h_{s,t}\right|^2+\rho\left|h_{t,d}\right|^2+1} + \sum_{u=1}^{U}\frac{\rho\left|h_{s,u}\right|^2\rho\left|h_{u,d}\right|^2}{\rho\left|h_{s,u}\right|^2+\rho\left|h_{u,d}\right|^2+1}\right) -\right.\right.$$

$$\frac{1}{2}\log_2(1+\sum_{u=1}^{U}\frac{\rho_s|h_{s,u}|^2\rho_u|h_{u,e}|^2}{\rho_s|h_{s,u}|^2+\rho_u|h_{u,e}|^2+1})\Bigg]^+\Bigg\}. \tag{2.18}$$

It can be shown by following the same procedure as that in Theorem 1 that $E\left\{C_{S,NoJam}^{DBF}\right\}\sim \frac{1}{2}\log_2(\frac{T}{U}+1)$. □

2.4.2 Scaling Law of Opportunistic Relaying

It was shown that the lower bound for ergodic secrecy capacity tends to zero as the total number of the relays $K\to\infty$ Sun *et al.* (2012). Considering the aggressive behaviour of the untrustworthy relays, we calculate here the upper bound value for the secrecy capacity.

Proof. Let

$$X=1+\max_k(\frac{1}{2}\frac{\rho|h_{s,k}|^2 2\rho|h_{k,d}|^2}{\rho|h_{s,k}|^2+2\rho|h_{k,d}|^2+1}),$$

$$Y=1+\sum_{u=1}^{U}\frac{\rho|h_{s,u}|^2\rho|h_{u,d}|^2}{\rho^2|h_{u,d}|^2|h_{u,e}|^2+\rho|h_{s,u}|^2+\rho|h_{u,e}|^2+\rho|h_{u,d}|^2+1},$$

and $Z=1+\max_k(\frac{\rho|h_{s,k}|^2}{2})$. Then, the secrecy capacity will be upper bounded by

$$\begin{aligned}
E\{C_S^{OR}\} &= E\left\{\left[\frac{1}{2}\log_2(\frac{X}{Y})\right]^+\right\}\\
&< E\left\{\frac{1}{2}\log_2(1+\frac{X}{Y})\right\}\\
&= E\left[\frac{1}{2}\log_2(X+Y)-\frac{1}{2}\log_2(Y)\right]\\
&\overset{(a)}{\leq} \frac{1}{2}\log_2\Big(E[X]+E[Y]\Big)-\frac{1}{2}\log_2\Big(E[Y]\Big)\\
&\overset{(b)}{<} \frac{1}{2}\log_2\Big(E[Z]+E[Y]\Big)-\frac{1}{2}\log_2\Big(E[Y]\Big)
\end{aligned}$$

$$\overset{(c)}{\sim} \frac{1}{2}\log_2\left(\frac{\rho}{2}\log_2 K + U\right) - \frac{1}{2}\log_2(U)$$
$$\sim \frac{1}{2}\log_2\left(\frac{\rho\log_2 K}{2U} + 1\right), \tag{2.19}$$

where (a) follows from Jensen's inequality, (b) follows from the fact that $\frac{\rho\left|h_{s,k}\right|^2 2\rho\left|h_{k,d}\right|^2}{\rho\left|h_{s,k}\right|^2 + 2\rho\left|h_{k,d}\right|^2 + 1} < \frac{\rho\left|h_{s,k}\right|^2 2\rho\left|h_{k,d}\right|^2}{\rho\left|h_{s,k}\right|^2 + 2\rho\left|h_{k,d}\right|^2} \leq \min(\rho\left|h_{s,k}\right|^2, 2\rho\left|h_{k,d}\right|^2) \leq \rho\left|h_{s,k}\right|^2$, (c) follows from the fact that $E\{\max_k(\rho\left|h_{k,d}\right|^2)\} \sim \rho\log_2 K + \mathrm{O}(\log_2\log_2 K)$ Sharif & Hassibi (2005) and $E(Y) = U$ by following the same steps in our *proof* of *Theorem 1*. However, when $T \to \infty$ and $U \to \infty$ with any finite ρ, equation (2.19) tends to zero. □

Therefore, based on the results given in equations (2.15) and (2.19), we can conclude that DBF guarantees better security than OR technique.

Assuming that $\rho \overset{\Delta}{=} \rho_s = \rho_t = \rho_u = \rho_d = 5$ dB and $U = T$, we do the performance comparison of the ergodic secrecy capacity between the lower bound DBF, OR and DBF with and without IJ and we show the outcome in Fig. 2.2. Moreover, we assume that the relays are located near the middle of the source and the destination, and the variances $\sigma_1^2 = \sigma_2^2 = 1$. It is observed in Fig. 2.2 that increasing the total number of relays gives better performance for DBF network, but it reduces the secrecy capacity of OR to zero even at the presence of IJ. Moreover, Fig. 2.2 shows a secrecy capacity gap between DBF without IJ and the one with IJ. Therefore, it can be seen that with the absence of IJ, DBF tends to reach its secrecy capacity scaling quickly.

2.5 Conclusions

The capacity scaling of secure cooperative relaying with DBF and OR through trustworthy and untrustworthy aggressive relays has been investigated in this paper. Considering the aggressiveness of the untrustworthy relays in DBF, we conclude that 1) Secrecy capacity scaling is bounded by a value that depends on the ratio between the number of the trustworthy and the untrustworthy aggressive relays, this value is reached quickly with the absence of IJ. 2) Based

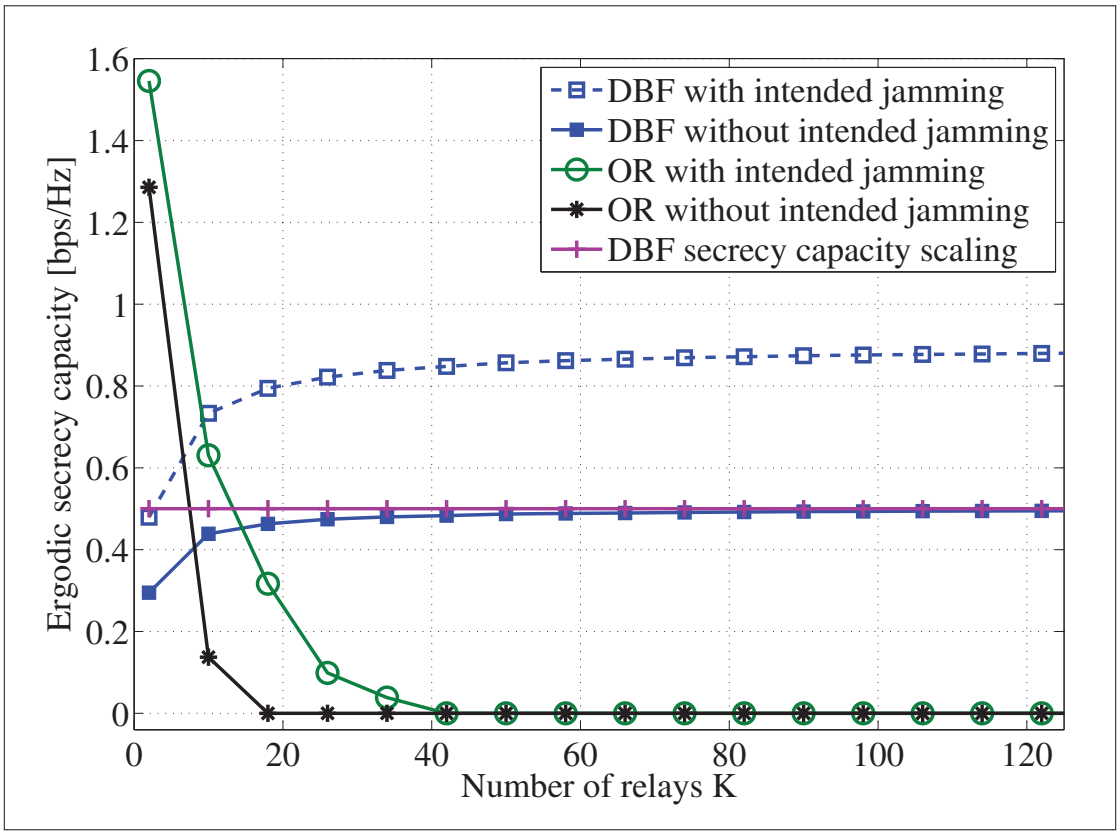


Figure 2.2 Ergodic secrecy capacity: $\rho \stackrel{\Delta}{=} \rho_s = \rho_t = \rho_u = \rho_d = 5$ dB, $\sigma_1^2 = \sigma_2^2 = 1$, and $U = T$

on our results, OR is not recommended for security issues, leading to the priority being handed over to DBF strategy.

CHAPTER 3

SECRECY ANALYSIS IN WIRELESS NETWORK WITH PASSIVE EAVESDROPPERS BY USING PARTIAL COOPERATION

Michael Atallah[1], and Georges Kaddoum[1]

[1] Department of Electrical Engineering, École de Technologie Supérieure,
1100 Notre-Dame Ouest, Montréal, Québec, Canada H3C 1K3

Paper published in IEEE Transactions on Vehicular Technology, 2019.

3.1 Abstract

This paper proposes a new location-based multicasting technique, for dual phase amplify-and-forward (AF) large networks, aiming to improve the security in the presence of non-colluding passive eavesdroppers. These eavesdroppers could also be part of this cooperative network as relays. In order to reduce the impact of these eavesdroppers on the network security, we propose a new transmission strategy where, for the first hop of each transmission time, while the destination is jamming, the source randomly chooses a different subset K of the total T relays, to transmit its message towards the destination. For practical implementation, sectoral transmission can be achieved with analog beamforming at the source's side. In the second hop, using the distributed beamforming technique, the K AF relays retransmit the received signal to the destination. We analytically demonstrated that the proposed technique decreases the probability of choosing the same sector that has certain eavesdroppers again, for each transmission time, to K/T. Moreover, we also show that the secrecy capacity scaling of our technique is still the same as for broadcasting. Hereafter, the lower and upper bounds of the secrecy outage probability are calculated, and it is shown that the security performance is remarkably enhanced, compared to conventional multicasting technique.

Keywords: Physical layer security, jamming, secrecy outage probability, amplify and forward, secrecy capacity, scaling.

3.2 Introduction

Physical layer security (PLS) is considered a promising approach for strengthening the security in wireless communication. One of the most important tools to measure the security performance in PLS is the security rate, in which the channel capacity of the legitimate links should be higher than the capacity of the illegitimate ones. Otherwise, it is equal to zero Gopala *et al.* (2008). In order to achieve a positive secrecy rate, many techniques have been proposed, such as cooperative jamming (CJ) Lee *et al.* (2018); Atallah *et al.* (2015), multi-antenna scenarios Chen *et al.* (2017), beamforming Guo *et al.* (2017), game theory Silva & Cordero (2017), and power allocation schemes Atallah *et al.* (2015). In the literature, the aforementioned techniques were sometimes combined to achieve better security. In Cumanan *et al.* (2017), a CJ technique, by multiple jammers, was combined with an optimal power allocation technique to achieve a better security rate in the presence of multiple eavesdroppers. The authors in Wang *et al.* (2013a) combined cooperative beamforming (CB) and CJ techniques to achieve higher security. The combination of CB and CJ was studied again in Wang & Wang (2015) in the presence of multi-antenna eavesdroppers. Due to the nature of the wireless medium, nodes can join and leave the network frequently. These nodes could be beneficial to the network, when being used as relays, and could also be considered as potential eavesdroppers. However, as demonstrated in Jeong *et al.* (2012) and Yener & He (2010), treating these nodes as relays could be more beneficial to the wireless network, from a security perspective, than treating them as eavesdroppers. In cooperative relaying networks, two main scenarios were studied in the literature, the opportunistic relaying (OR) one, where the best relay is chosen to retransmit the message, and the distributed beamforming (DBF) one, where all the relays retransmit their received messages towards the destination using the beamforming transmission. In A. El-Malek *et al.* (2017), the secrecy performance, considering OR networks, was studied after applying power allocation and jamming techniques, in the presence of interference and many eavesdroppers. Also, the secrecy outage probability (SOP) lower and upper bounds, in OR networks, were investigated in Mabrouk *et al.* (2017) using CJ under outdated channel state information (CSI). Moreover, hybrid schemes that contain DBF and CJ were investigated in Wang & Xia (2015). Hereafter, a

joint cooperative beamforming, jamming, and power-allocation scheme was proposed in Wang *et al.* (2015b) to enhance the security performance in cooperative relay networks. In this direction, the authors in Kim *et al.* (2015) studied the secrecy capacity scaling and the asymptotic performance of a two-hops network, with untrustworthy relays, for both OR and DBF. Thereafter, these scenarios were extended in Atallah & Kaddoum (2016) to study the secrecy scaling laws for dual phase large networks, with wiretappers that are cooperating between each other to intercept the messages. The majority of the proposed techniques in the literature assumed that the wiretappers are receiving the data all the time, which can harm the security. To tackle this challenge, in this paper, we propose a new location-based multicasting technique, based on sending just a part of the information to a certain sector for a certain transmission time, and then switching to other sectors randomly to send the other parts. This transmission strategy can be practically implemented thanks to analog beamforming at the source's side. We mathematically demonstrate that our proposed technique reduces the possibility of an eavesdropper intercepting the whole message, since it's getting just a part of it. Also, we show that the secrecy capacity scaling converges to the same value of the broadcasting method in Kim *et al.* (2015). Moreover, an analysis of secrecy outage probability (SOP) lower and upper bounds is provided, and shows a remarkable improvement compared to the conventional multicasting scenario and OR techniques in A. El-Malek *et al.* (2017) and Mabrouk *et al.* (2017).

Notations: $\mathrm{VAR}[X]$ and $E[X]$ respectively denote the variance and the mean expectation of a random variable (r.v.) X. Also, $F_X(.)$ and $f_X(.)$ denote the cumulative distribution function (CDF) and the probability density function (PDF) of X, respectively. Moreover, $\overset{w.p.1}{\rightarrow}$ denotes the convergence with probability one, and $[A]^+$ denotes $\max\{A,0\}$. For a r.v. X, the notation $X \sim N_c(a,b)$ denotes that X is a complex Gaussian r.v. with variance b and mean a.

3.3 System Model and Problem Formulation

Consider a multi-antennas access point s, T amplify-and-forward (AF) relays clustered into $G = T/K \in \mathbb{N}^+$ clusters, where K is the number of relays in each cluster, a destination d and a passive eavesdropper e, that could also take part of this cooperative network as a relay. Each

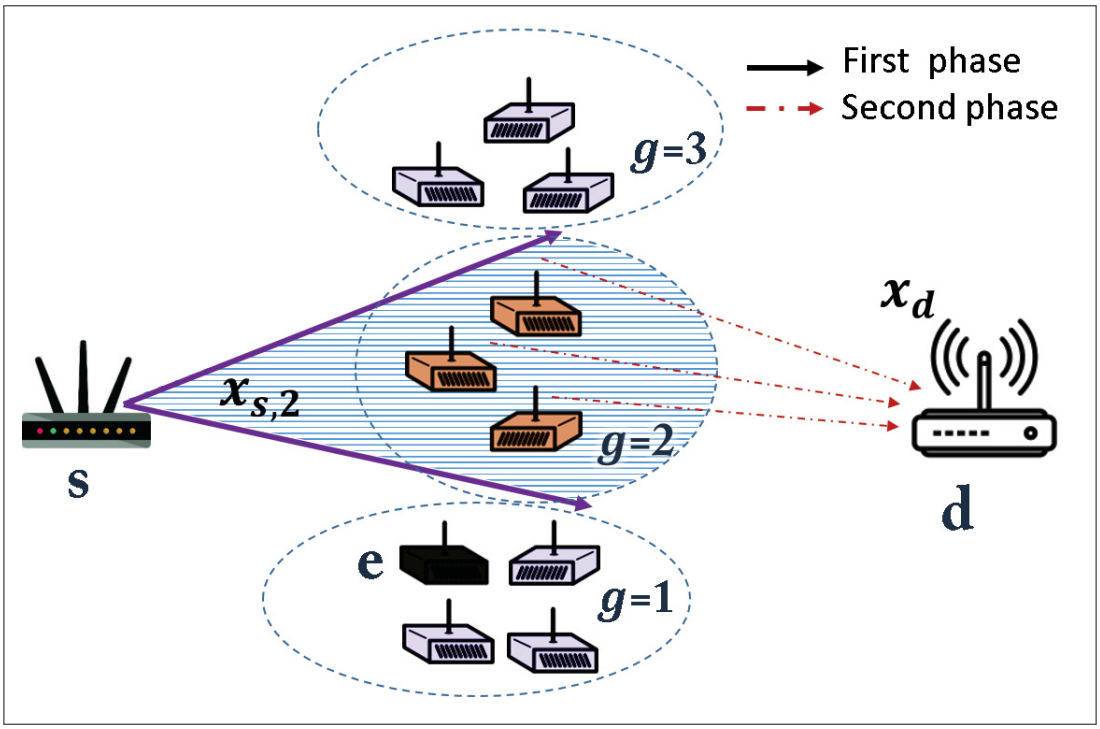


Figure 3.1 System model consisting of a multi-antennas source s, T relays clustered in G sectors, a destination d and an eavesdropper e. In this figure, $T = 9$, $K = 3$ and $G = 3$

relay has a single antenna, as shown in Fig. 3.1, and operates in a half-duplex mode. It is assumed that there is no direct link between the source and the destination, which means that all the transmitted information should be forwarded by the relays. This scenario can represent a D2D cooperative network. As shown in Fig. 3.1, in the first hop of each transmission time, while d is jamming the relays, s will multicast the signal $x_{s,g}$ to the gth cluster that contains K relays in it, where $1 \leq g \leq G$. In the second phase, the K relays will forward the received message towards d, using the distributed beamforming technique, which has been proven to outperform the opportunistic one Kim *et al.* (2015), Atallah & Kaddoum (2016). After each transmission time, s will choose another set of K relays to transmit towards d. Hence, the received signal expression, at a kth relay, where $1 \leq k \leq K$, is given by

$$y_k = \sqrt{P_s}\, h_{s,k} x_{s,g} + \sqrt{P_d}\, h_{d,k} x_d + n_k, \tag{3.1}$$

where $n_k \sim \mathcal{N}_c(0, N_0)$ is the complex additive white Gaussian noise (AWGN) at the kth relay, P_s and P_d are the transmitted powers from the s and d respectively. In our analysis, we assume that the channels are quasi-static block Rayleigh channels, *i.e.* the channel coefficients $h_{l,j}$, where $l \in \{s,k,d\}$ and $j \in \{k,e,d\}$, are constant during the transmission time of one message, but may change independently to different values thereafter. Moreover, we assume that the CSI is known by the receiving nodes. Accordingly, the channel gains $\left|h_{l,j}\right|^2$ follow independent exponential distributions. It is also assumed that the noise variance N_0 has the same value in the first and the second phases. Consequently, the received signal-to-interference-plus-noise ratio (SINR) at the kth relay becomes

$$\gamma_k = \frac{\rho_s \left|h_{s,k}\right|^2}{\rho_d \left|h_{d,k}\right|^2 + 1}, \tag{3.2}$$

where $\rho_i \stackrel{\Delta}{=} P_i / N_0$, and $i \in \{s,k,e,d\}$. If e is not in the sector covered by the antenna beam of the transmitter, then it will not receive the message $x_{s,g}$. Thus, the received signal expression at e can be expressed as

$$y_e = b.\sqrt{P_s}\, h_{s,e}\, x_{s,g} + \sqrt{P_d}\, h_{d,e}\, x_d + n_e, \tag{3.3}$$

where b is a Bernoulli r.v. that takes the value 0 when e is in the uncovered sector, and 1 when e is in the covered sector. Hence, when $b = 0$, the received signal at e is given by

$$y_e = \sqrt{P_d}\, h_{d,e}\, x_d + n_e\,. \tag{3.4}$$

Since the probability of e being in the covered sector is equal to K/T, then the probability mass function of b is expressed as

$$\Pr(b=1) = p_1 = \frac{K}{T}, \tag{3.5}$$

$$\Pr(b=0) = p_0 = 1 - p_1 = 1 - \frac{K}{T}. \tag{3.6}$$

From (3.3), the SINR at e is obtained as

$$\gamma_{e'} = \frac{b.\rho_s \left|h_{s,e}\right|^2}{\rho_d \left|h_{d,e}\right|^2 + 1}, \tag{3.7}$$

The expected value of the SINR at the eavesdropper's side becomes

$$\begin{aligned} \gamma_e &= \sum_{i=0}^{1} \Pr(b=i)\, \gamma_{e'b=i} && (3.8) \\ &= 0 + \frac{K}{T} \frac{\rho_s \left|h_{s,e}\right|^2}{\rho_d \left|h_{d,e}\right|^2 + 1} \\ &= \frac{K}{T} \frac{\rho_s \left|h_{s,e}\right|^2}{\rho_d \left|h_{d,e}\right|^2 + 1}. && (3.9) \end{aligned}$$

In the second hop, the retransmitted message from the kth relay will take the following form $x_k = \alpha_k w_k y_k$, where w_k is the optimized beamforming weight, and α_k represents the normalized amplifying coefficient. From (3.1), α_k can be calculated as $\alpha_k = \frac{1}{\sqrt{\rho_s \left|h_{s,k}\right|^2 + \rho_d \left|h_{d,k}\right|^2 + N_0}}$. In the second hop, the received message, at d, from the K relays, is given as

$$y_d = \sum_{k=1}^{K} h_{k,d}\, \alpha_k\, w_k\, y_k + n_d, \tag{3.10}$$

where $n_d \sim \mathcal{N}_c(0, N_0)$ is the complex AWGN at d. After receiving y_d, the destination will extract $x_{s,g}$, after removing the jamming signal x_d. From Kim *et al.* (2015) and the references therein, the SINR at the destination's side becomes

$$\gamma_d = \sum_{k=1}^{K} \frac{\rho_s \left|h_{s,k}\right|^2 \rho_k \left|h_{k,d}\right|^2}{\rho_s \left|h_{s,k}\right|^2 + (\rho_d + \rho_k) \left|h_{k,d}\right|^2 + 1}. \tag{3.11}$$

From (3.11) and (3.8), the secrecy capacity $C_S = [C_d - C_e]^+$ will be given by

$$C_S = \left[\frac{1}{2} \log_2 \left(1 + \sum_{k=1}^{K} \frac{\rho_s \left|h_{s,k}\right|^2 \rho_k \left|h_{k,d}\right|^2}{\rho_s \left|h_{s,k}\right|^2 + (\rho_d + \rho_k) \left|h_{k,d}\right|^2 + 1} \right) \right.$$

$$-\frac{1}{2}\log_2\left(1+\frac{K}{T}\frac{\rho_s\left|h_{s,e}\right|^2}{\rho_d\left|h_{d,e}\right|^2+1}\right)\Bigg]^+, \tag{3.12}$$

where C_d and C_e are the data rates from s, to d and e, respectively. The loss rate, $1/2$, was used in (3.12) due to the constraint of operating the half-duplex mode at the relays. In the following section, we will calculate the SOP lower and upper bounds of C_S.

3.4 Lower and Upper Bounds of Secrecy Outage Probability

From (3.12), the SOP expression can be written as

$$\begin{aligned} p_{out} &= \Pr\left[C_S < R\right] && (3.13)\\ &= \Pr\left[\frac{1+\sum_{k=1}^{K}\frac{1}{2}\frac{\gamma_{s,k}\,2\,\gamma_{k,d}}{\gamma_{s,k}+2\,\gamma_{k,d}+1}}{1+\frac{K}{T}\frac{\gamma_{s,e}}{\gamma_{d,e}+1}} < u\right] \\ &\sim \Pr\left[\frac{1+\sum_{k=1}^{K}\frac{1}{2}\frac{\gamma_{s,k}\,2\,\gamma_{k,d}}{\gamma_{s,k}+2\,\gamma_{k,d}}}{1+\frac{K}{T}\frac{\gamma_{s,e}}{\gamma_{d,e}+1}} < u\right], && (3.14)\end{aligned}$$

where R is the threshold and $u = 2^{2R}$. We will use the following inequality to calculate the lower and upper bounds of the SOP Mabrouk *et al.* (2017). For any two r.v. X and Y

$$\frac{1}{2}\min\left\{X,Y\right\} \leq \frac{XY}{X+Y} \leq \min\left\{X,Y\right\}. \tag{3.15}$$

From (3.14) and (3.15), we have

$$\frac{1}{2}\min\left\{\gamma_{s,k},2\gamma_{k,d}\right\} \leq \frac{\gamma_{s,k}\,2\,\gamma_{k,d}}{\gamma_{s,k}+2\,\gamma_{k,d}} \leq \min\left\{\gamma_{s,k},2\gamma_{k,d}\right\}.$$

Thus, the SOP lower and upper bounds can be respectively expressed as

$$P_{out} \leq \Pr\left[\frac{1+\frac{1}{4}\sum_{k=1}^{K}\min\left\{\gamma_{s,k},2\,\gamma_{k,d}\right\}}{1+\frac{K}{T}\frac{\gamma_{s,e}}{\gamma_{d,e}+1}} < u\right] = P_{out,UB},$$

$$P_{out} \geq \Pr\left[\frac{1+\frac{1}{2}\sum_{k=1}^{K}\min\left\{\gamma_{s,k},2\,\gamma_{k,d}\right\}}{1+\frac{K}{T}\frac{\gamma_{s,e}}{\gamma_{d,e}+1}} < u\right] = P_{out,LB}.$$

We evaluate the general expression of the SOP bounds as follows

$$P_{out,B} = \Pr\left[\frac{1+\frac{1}{\theta}\sum_{k=1}^{K}\min\left\{\gamma_{s,k},2\,\gamma_{k,d}\right\}}{1+\frac{K}{T}\frac{\gamma_{s,e}}{\gamma_{d,e}+1}} < u\right], \tag{3.16}$$

where θ takes the values 2 and 4 for the SOP lower and upper bounds, respectively.

Theorem 3. *The secrecy outage probability lower and upper bounds, of our proposed technique, are given by*

$$p_{out,B} = 1 - \frac{{\lambda_0}^K}{\Gamma(K)}\left(s_2 - s_3\left(s_4 - s_5\right)\right), \tag{3.17}$$

where s_3, s_2, s_4, and s_5 are respectively given in (3.25)*,* (3.26)*,* (3.29) *and* (3.30)*.*

Proof. From (3.16), the SOP is bounded by

$$\begin{aligned} P_{out,B} &= \Pr\left[\frac{1+\frac{1}{\theta}\sum_{k=1}^{K}\min\left\{\gamma_{s,k},2\,\gamma_{k,d}\right\}}{1+\frac{K}{T}\frac{\gamma_{s,e}}{\gamma_{d,e}+1}} < u\right] \\ &= \Pr\left[\frac{1+\frac{1}{\theta}A}{B} < u\right] \\ &= 1-\Pr\left[B < \frac{\theta+A}{\theta u}\right], \end{aligned} \tag{3.18}$$

where $B = 1+\frac{K}{T}\frac{\gamma_{s,e}}{\gamma_{d,e}+1}$, and $A = \sum_{k=1}^{K}\min\left\{\gamma_{s,k},2\,\gamma_{k,d}\right\}$.

$$\text{We have} \qquad B > 1 \Rightarrow \frac{\theta+A}{\theta u} > 1 \Rightarrow A > \theta u - \theta. \tag{3.19}$$

From (3.18) and (3.19), and assuming that A and B are independent, the SOP bounds are obtained as

$$p_{out,B} = 1 - \int_{\theta u-\theta}^{\infty} F_B\left(\frac{\theta + A}{\theta u}\right) f_A(a)\, da. \tag{3.20}$$

Lemma 1. *The PDF of A and the CDF of B are respectively given by*

$$f_A(a) = a^{K-1} e^{-\lambda_0 a} \frac{{\lambda_0}^K}{\Gamma(K)}, \tag{3.21}$$

$$F_B(b) = 1 - \exp\left[-\lambda_1 (b-1)\frac{T}{K}\right] \frac{\lambda_2}{\lambda_1 (b-1)\frac{T}{K} + \lambda_2}, \tag{3.22}$$

where $\Gamma(X) = \int_0^\infty t^{X-1} e^{-t}\, dt$, *is the Gamma function,*

$$\lambda_1 = \frac{1}{\rho\, \sigma_1^2},\ \lambda_2 = \frac{1}{\rho\, \sigma_2^2},\ \textit{and}\ \ \lambda_0 = \frac{1}{\rho\, \sigma_1^2} + \frac{1}{2\rho\, \sigma_2^2}. \tag{3.23}$$

Where σ_1^2 and σ_2^2 are the means of $\left|h_{s,k}\right|^2$ and $\left|h_{k,d}\right|^2$ respectively.

Proof. Please refer to the Appendix I. □

By using **Lemma 1**'s results, the bounds in (3.20) can be expressed as

$$p_{out,B} = 1 - \int_{\theta u-\theta}^{\infty} \left(1 - \exp\left[-\lambda_1\left(\frac{\theta + A}{\theta u} - 1\right)\frac{T}{K}\right]\right.$$

$$\left. \times \frac{\lambda_2}{\lambda_1\left(\frac{\theta+A}{\theta u} - 1\right)\frac{T}{K} + \lambda_2}\right) a^{K-1} e^{-\lambda_0 a} \frac{{\lambda_0}^K}{\Gamma(K)} da$$

$$= 1 - \frac{{\lambda_0}^K}{\Gamma(K)}\left[s_2 - s_3 \int_{\theta u-\theta}^{\infty} s_1 da\right], \tag{3.24}$$

$$\text{where} \quad s_3 = \frac{\theta u K \lambda_2}{\lambda_1 T} \exp\left(\frac{\lambda_1 T}{K}\left(1-\frac{1}{u}\right)\right), \tag{3.25}$$

$$\begin{aligned} s_2 &= \int_{\theta u-\theta}^{\infty} a^{K-1} e^{-\lambda_0 a}\, da \\ &= \lambda_0^{-K}\Gamma(K) + \lambda_0^{-K}\left[-\Gamma(K) + \Gamma(K, \lambda_0(\theta u-\theta))\right], \end{aligned} \tag{3.26}$$

and

$$\begin{aligned} s_1 &= \frac{a^{K-1}\exp\left(-a\overbrace{\left(\lambda_0+\frac{\lambda_1 T}{K\theta u}\right)}^{\beta}\right)}{a+\underbrace{(\theta-\theta u+\frac{\theta u K\lambda_2}{\lambda_1 T})}_{\phi}} \\ &= \frac{a^{K-1}\exp(-a\beta)}{a+\phi}. \end{aligned} \tag{3.27}$$

Thus, to calculate $\int_{\theta u-\theta}^{\infty} s_1\, da$ in (3.24), we will integrate by parts as follows

$$\int_{\theta u-\theta}^{\infty} s_1\, da = \int_{\theta u-\theta}^{\infty} U dV = \underbrace{VU\Big|_{\theta u-\theta}^{\infty}}_{s_4} - \underbrace{\int_{\theta u-\theta}^{\infty} V dU}_{s_5}, \tag{3.28}$$

where $dV = \frac{\exp(-a\beta)}{a+\phi} da \Rightarrow V = \exp(\beta\phi)\, E_i(-\beta(a+\phi))$, and $U = a^{K-1} \Rightarrow dU = (K-1)\, a^{K-2}\, da$. Here, $E_i(X) = -\int_{-X}^{\infty} \frac{e^{-t}}{t} dt$, is the exponential integral of the r.v. X. From (3.28), s_4 and s_5 are calculated as

$$\begin{aligned} s_4 &= -(\theta u-\theta)^{K-1}\exp(\beta\phi)\, E_i(-\beta(\theta u-\theta+\phi)), \\ s_5 &= (K-1)\, e^{\beta\phi} \int_{\theta u-\theta}^{\infty} a^{K-2} E_i(-\beta(a+\phi))\, da \end{aligned} \tag{3.29}$$

$$\stackrel{(\dagger)}{=} (K-1)\, e^{\beta\phi}\, E_1\left(\beta\left(\theta u-\theta+\phi\right)\right) s_6 - e^{\left(-\beta(\theta u-\theta+\phi)\right)}\, s_7\,. \tag{3.30}$$

$(\dagger)$ follows from using the integral in [Ng (1969), Section 4.1, Eq. 7] after employing the following property $E_1(X) = -E_i(-X)$. Thus, s_6 and s_7 in (3.30) are defined as

$$\begin{aligned} s_6 &= \sum_{m=0}^{K-2} \frac{(-1)^m (K-2)!\,(\theta u-\theta)^{K-m-2}\,(\theta u-\theta+\phi)^{m+1}}{(K-2-m)!\,(m+1)!}, \\ s_7 &= \sum_{m=0}^{K-2} \frac{(K-2)!\,(\theta u-\theta)^{K-m-2}}{(K-2-m)!\,(m+1)!\beta^{m+1}} \\ &\qquad \times \sum_{j=0}^{m} (-1)^j\,(m-j)!\,(\beta\,(\theta u-\theta+\phi))^j. \end{aligned}$$

Substituting (3.25), (3.26), (3.29), and (3.30) in (3.24), we completed the proof. □

3.5 Scaling Law of Secrecy Capacity

In this section, we will show that the secrecy capacity of our proposed technique converges to $\frac{1}{2}log_2(T)$. To prove this, we will show that, for large K and T, the lower and upper bounds of C_S scale to $\frac{1}{2}log_2(T)$. Without loss of generality, in our analysis, we assume that $\rho \stackrel{\Delta}{=} \rho_s = \rho_d = \rho_k$, but the extension using different values of ρ_i is straightforward.

Theorem 4. *The ergodic secrecy capacity $\overline{C}_S = E\{C_S\}$, for any finite ρ, is lower bounded by $\frac{1}{2}log_2(T)$.*

Proof.

$$E\{C_S\} = E\left\{\left[\frac{1}{2}\log_2\left(1+\sum_{k=1}^{K}\frac{\rho\left|h_{s,k}\right|^2\rho\left|h_{k,d}\right|^2}{\rho\left|h_{s,k}\right|^2+2\rho\left|h_{k,d}\right|^2+1}\right) - \frac{1}{2}\log_2\left(1+\frac{K}{T}\frac{\rho\left|h_{s,e}\right|^2}{\rho\left|h_{d,e}\right|^2+1}\right)\right]^+\right\}$$

$$\overset{(\dagger)}{\geq}\left[E\left\{\frac{1}{2}\log_2\left(1+\sum_{k=1}^{K}\frac{\rho\left|h_{s,k}\right|^2\rho\left|h_{k,d}\right|^2}{\rho\left|h_{s,k}\right|^2+2\rho\left|h_{k,d}\right|^2+1}\right)\right\}\right.$$
$$\left.-E\left\{\frac{1}{2}\log_2\left(1+\frac{K}{T}\frac{\rho\left|h_{s,e}\right|^2}{\rho\left|h_{d,e}\right|^2+1}\right)\right\}\right]^+$$

$$=\left[E\left\{C_d\right\}-E\left\{C_e\right\}\right]^+, \tag{3.31}$$

$(\dagger)$ follows from applying *Jensen's inequality* on the convex function $\max\left(X_1,X_2\right)$, which is $E\left\{\max\left(X_1,X_2\right)\right\}\geq\max\left(E\left\{X_1\right\},E\left\{X_2\right\}\right)$. From Bolcskei *et al.* (2006), we have that *Kolmogorov conditions* are satisfied for

$$M_k\overset{\Delta}{=}\frac{\rho\left|h_{s,k}\right|^2\rho\left|h_{k,d}\right|^2}{\rho\left|h_{s,k}\right|^2+\rho\left|h_{k,d}\right|^2+1}.$$

i.e., $\frac{1}{K}\sum_{k=1}^{K}E\left[M_k\right]<\infty$, and $\sum_{k=1}^{K}\frac{VAR[\gamma_k]}{k^2}<\infty$, are true. Since $\gamma_{dk}\overset{\Delta}{=}\frac{\rho\left|h_{s,k}\right|^2\rho\left|h_{k,d}\right|^2}{\rho\left|h_{s,k}\right|^2+2\rho\left|h_{k,d}\right|^2+1}<M_k,\Rightarrow\gamma_{dk}$ also satisfies the *Kolmogorov conditions,* which are $\mu\overset{\Delta}{=}\frac{1}{K}\sum_{k=1}^{K}E\left[\gamma_{dk}\right]<\infty$, and $\sum_{k=1}^{K}\frac{VAR[\gamma_{dk}]}{k^2}<\infty$. Hence, we can apply the following theorem [(Serfling, 1980, 1.8.D)]

$$\sum_{k=1}^{K}\frac{\gamma_k}{K}-\sum_{k=1}^{K}\frac{E\left[\gamma_k\right]}{K}\overset{w.p.1}{\rightarrow}0. \tag{3.32}$$

Resultantly, $\gamma_k\overset{w.p.1}{\rightarrow}K\mu$. Substituting in (3.31), we get

$$\begin{aligned}\overline{C}_S &\geq \left[E\left\{C_d\right\}-E\left\{C_e\right\}\right]^+\\ &= \left[\frac{1}{2}\left(\log_2 K+\log_2\mu\right)-\frac{1}{2}\left(\log_2\frac{K}{T}+\log_2\frac{\rho\left|h_{s,e}\right|^2}{\rho\left|h_{d,e}\right|^2+1}\right)\right]^+\\ &\sim \left[\frac{1}{2}\log_2 K-\frac{1}{2}\log_2\frac{K}{T}\right]^+\\ &= \frac{1}{2}\log_2 T.\end{aligned} \tag{3.33}$$

From Bolcskei *et al.* (2006), the asymptotic capacity scaling upper bound of dual phase relaying networks through trustworthy relays, where the source is broadcasting towards the relays in the first hop, is shown to be $1/2\log_2 T$. Considering, for $K \to \infty$, that our technique acts like broadcasting, the result in Bolcskei *et al.* (2006) will be the asymptotic upper bound of $\overline{C}_S$. Thus, by showing that both the lower and upper bounds coincide with $1/2\log_2 T$, we completed the proof. □

3.6 Simulation Results

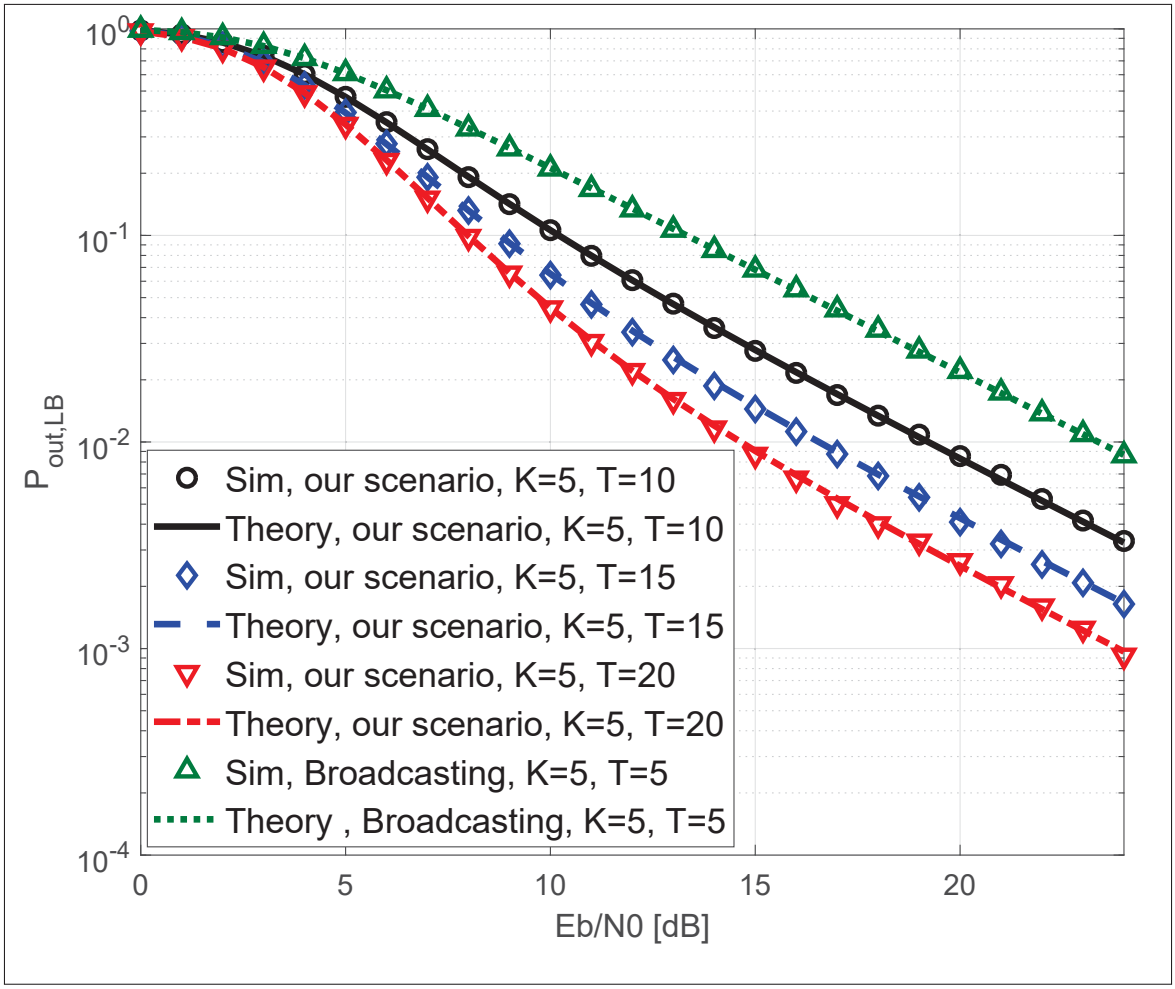


Figure 3.2 Analytical and simulated SOP lower bound performances of the proposed system with jamming: $\left|\overline{h_{s,k}}\right|^2 = \left|\overline{h_{k,d}}\right|^2 = 1$, $R = 1bps/Hz$, and $K = 5$

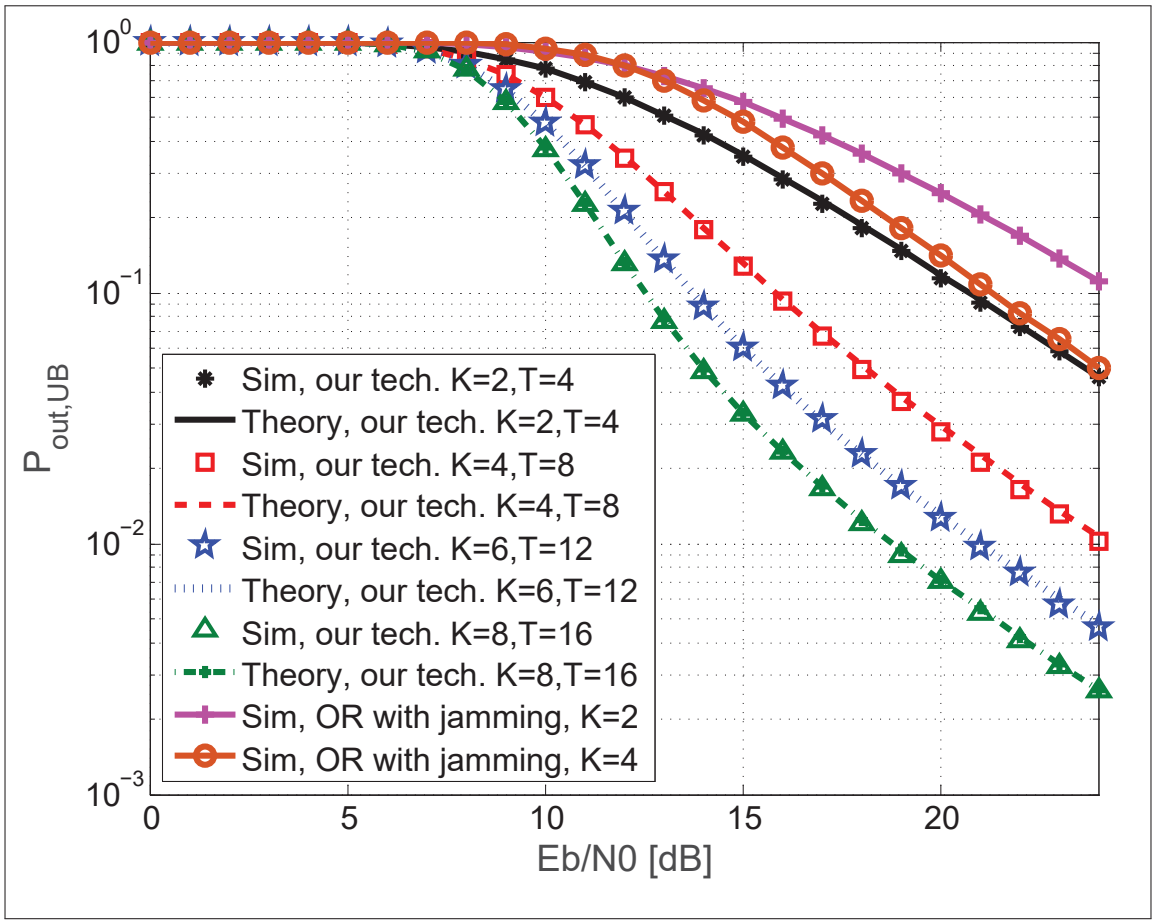


Figure 3.3 Analytical and simulated SOP upper bound performances of the proposed system and OR with jamming: $\left|\overline{h_{s,k}}\right|^2 = \left|\overline{h_{k,d}}\right|^2 = 1$, and $R = 1bps/Hz$

In this section, we evaluate the performance of our scheme by means of analytical and simulation results of the SOP and the secrecy capacity scaling. It's assumed that $\rho \triangleq \rho_s = \rho_d = \rho_k$, $R = 1bps/Hz$ and $\left|\overline{h_{s,k}}\right|^2 = \left|\overline{h_{k,d}}\right|^2 = 1$.

Fig. 3.2 shows a comparison, of the SOP lower bound, between the broadcasting (the green curve), and our proposed technique, which is shown to be, from a security perspective, remarkably better than the former technique. In the simulation results, it is assumed that K is fixed and equal to 5. We can see that the analytical expression, given in (3.17), perfectly matches the SOP lower bound, for different values of T. Also, we can notice that the SOP is improved when

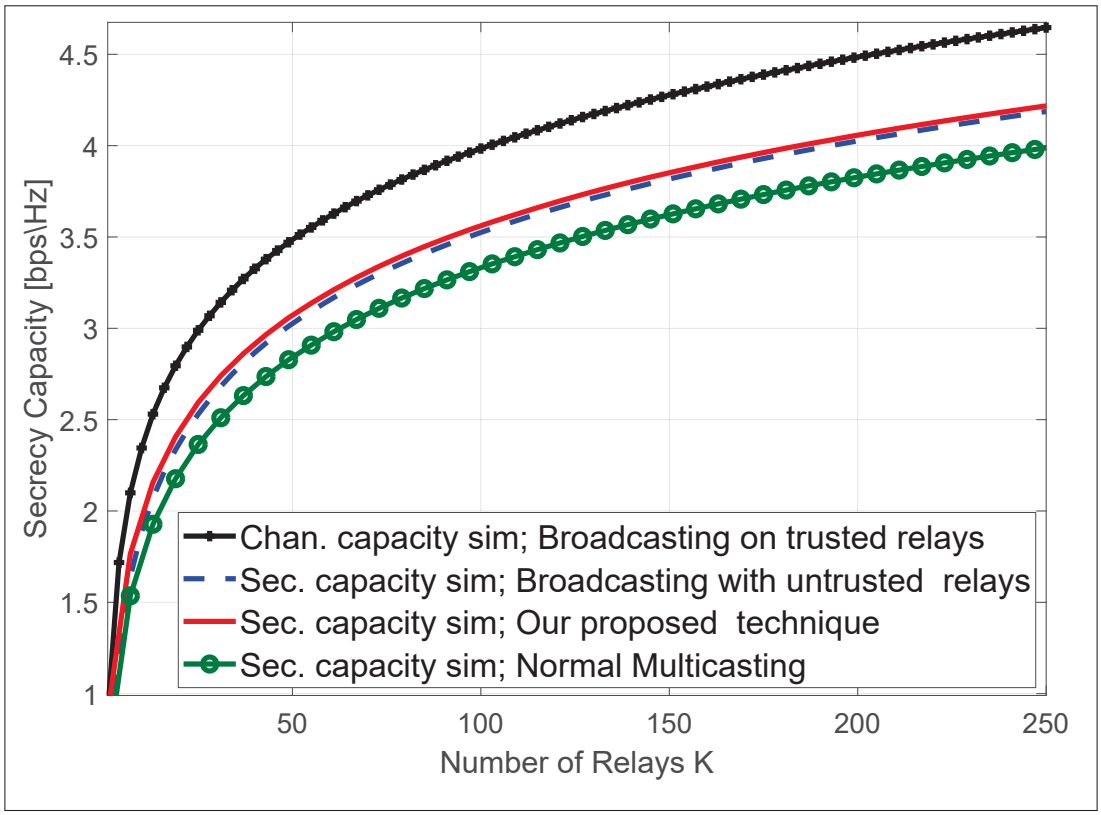


Figure 3.4 Simulated secrecy capacity scaling: $\left|\overline{h_{k,d}}\right|^2 = \left|\overline{h_{s,k}}\right|^2 = 1$, and $\rho \triangleq \rho_s = \rho_d = \rho_k = 10$ dB

the total number of the relays T increases. In fact, the higher the T is, the less the probability that an eavesdropper receives a signal from s, and the better the secrecy performance becomes.

Fig. 3.3 shows a comparison between the SOP upper bound for our technique and the OR technique that was proposed in A. El-Malek *et al.* (2017) and Mabrouk *et al.* (2017), with jamming, for different values of K and T. It is shown that the secrecy performance is remarkably enhanced with adding more relays to the network. Also, a noticeable improvement is shown in our proposed technique compared to the OR technique proposed in A. El-Malek *et al.* (2017) and Mabrouk *et al.* (2017).

Fig. 3.4 shows the secrecy capacity scaling comparison between our proposed technique, the broadcasting, and the conventional multicasting transmission, for $\rho \triangleq \rho_s = \rho_d = \rho_k = 10$ dB

and $T = 3K$. Moreover, we show the performance for the case where all the relays are trusted (the black curve). From Fig. 3.4, we can see that 1) our technique scaled similar to, even slightly better than, the broadcasting technique, which gives an advantage to our proposed technique, since the eavesdropper receives just a part of the message, whereas it receives all the transmitted message when the broadcasting scenario is applied Kim *et al.* (2015). 2) A security enhancement was achieved compared to the conventional multicasting technique.

3.7 Conclusions

In this paper, we proposed a new location-based multicasting cooperation strategy that takes advantage of the locations of all the nodes to enhance the security. We provided an analytical study for the SOP, and we showed that the secrecy capacity scaling, of the proposed technique, converges to values similar to the broadcasting case. Moreover, it was shown that the SOP is improved when the total number of relays T increases. Our results also displayed remarkable security performance improvement, compared to the conventional multicasting technique. As future work, we will further improve the current study by considering aggressive eavesdroppers.

CHAPTER 4

DESIGN AND PERFORMANCE ANALYSIS OF SECURE MULTICASTING COOPERATIVE PROTOCOL FOR WIRELESS SENSOR NETWORK APPLICATIONS

Michael Atallah[1], and Georges Kaddoum[1]

[1] Department of Electrical Engineering, École de Technologie Supérieure,
1100 Notre-Dame Ouest, Montréal, Québec, Canada H3C 1K3

Paper under revision in IEEE Wireless Communication Letters, 2019.

4.1 Abstract

This paper proposes a new security cooperative protocol, for dual phase amplify-and-forward large wireless sensor networks. In such a network, a portion of the K relays can be potential eavesdroppers. The source agrees to share with the destination a given channel state information (CSI) of a source-trusted relay-destination link to encode the message. Then, in the first hop, the source will use this CSI to map the right message to a certain sector while transmitting fake messages to the other sectors using sectoral transmission. In the second hop, the relays retransmit their received signals to the destination, using the distributed beamforming technique. We derived the secrecy outage probability and demonstrated that the probability of receiving the right encoded information by an untrustworthy relay is inversely proportional to the number of sectors. We also showed that the aggressive behavior of the cooperating untrusted relays is not effective compared to the case where each untrusted relay is trying to intercept the transmitted message individually.

Keywords: Physical layer security, secrecy outage probability, amplify and forward, secrecy capacity.

4.2 Introduction

In wireless networks, nodes can join and leave frequently, which increases the risk of the malicious nodes that are penetrating the wireless network. Therefore, the demand for security solutions in the physical layer is becoming more and more essential. One of the important metrics that evaluate the security performance in the physical layer is the secrecy rate, which is the difference between the channel capacity of the legitimate links and the channel capacity of the illegitimate ones Gopala *et al.* (2008). Many techniques have been proposed to achieve a positive secrecy rate, such as multi-antenna scenarios, beamforming, game theory, power allocation schemes and cooperative jamming Wang *et al.* (2014b), Kuhestani *et al.* (2018a), Kuhestani *et al.* (2016) and Atallah *et al.* (2015). A wireless network could benefit from the new joining nodes, by using them as relays, or by treating them as potential eavesdroppers. However, as shown in Kuhestani *et al.* (2016) and Kuhestani *et al.* (2018b), taking advantage of these nodes and using them as relays could be more useful to the wireless network, from a security perspective, than treating them as eavesdroppers. The authors in Kim *et al.* (2015) studied the secrecy performance for the case of multiple passive untrusted relays, where each passive untrusted relay is trying to intercept its received message individually. In Atallah & Kaddoum (2016), the authors studied the secrecy capacity scaling with aggressive untrusted relays. We define the aggressive behavior as when the untrusted relays are cooperating between each other by sending their received messages to an external wiretapper. Both Kim *et al.* (2015) and Atallah & Kaddoum (2016) considered two transmission schemes, namely opportunistic relaying (OR) and distributed beamforming (DBF). They also demonstrated that DBF outperforms OR technique from a secrecy perspective. In Atallah & Kaddoum (2017), a new location-based multicasting technique was proposed considering both passive and aggressive untrusted relays behaviors. It was shown that this technique enhances the security compared to Kim *et al.* (2015) and Atallah & Kaddoum (2016).

On the other hand, the randomness of the channel has been exploited for different purposes, whether to enhance the reliability or to secure the communication system as it was used to generate keys in Li *et al.* (2005). Therefore, in this paper, we combine the channel randomness

with multicasting transmission to propose a new location-based multicasting protocol in two-hops wireless sensor networks (WSN). The goal of this protocol is to increase the security of these networks while taking into account that wireless sensor nodes have limited capabilities. In the proposed protocol, the source and the destination share the channel state information (CSI) to map the source's transmission by sending the useful encoded message towards a specific sector, while sending other fake messages, similar to the useful one, towards the other sectors to confuse the eavesdroppers. Thus, we propose two strategies: the first one is to prevent the eavesdropper from receiving the transmitted message all the time by multicasting the signal to a different sector in each transmission time. Hence, for an eavesdropper located in a certain sector, the probability that it would be in the right sector is inversely proportional to the number of sectors, $p = 1/N \ll 1$. This eavesdropper can still know when there is a transmission towards it and when there isn't. Also, it can know to which sector this transmitted signal is multicasted when this eavesdropper cooperates with other eavesdroppers located in other sectors. Therefore, we came up with the second strategy which is based on sending fake messages towards the other sectors to increase the entropy and the confusion, related to being in the right sector, at the eavesdroppers. We provide analytical expressions for the secrecy outage probability (SOP) of both passive and aggressive untrusted relays. Our numerical results show how our technique enhances the security performance and how immune it is against the aggressive behavior of the untrusted relays. Finally, adopting such a security protocol by allowing a part of the nodes to forward fake messages is promising because of the availability of high number of cheap electronic sensors with limited computational capabilities.

4.3 System Model and Problem Formulation

Consider a source s equipped with multi-sectoral antennas, K amplify-and-forward (AF) cooperative relay sensor nodes with limited capabilities, and a destination d, provided with sectoral antennas. Out of the K relays, there are U untrustworthy relays that could be potential eavesdroppers. Each relay is equipped with a single antenna and works in a half-duplex mode, as shown in Fig.3.1. It is assumed that there is no direct link between s and d, *i.e.* all the transmit-

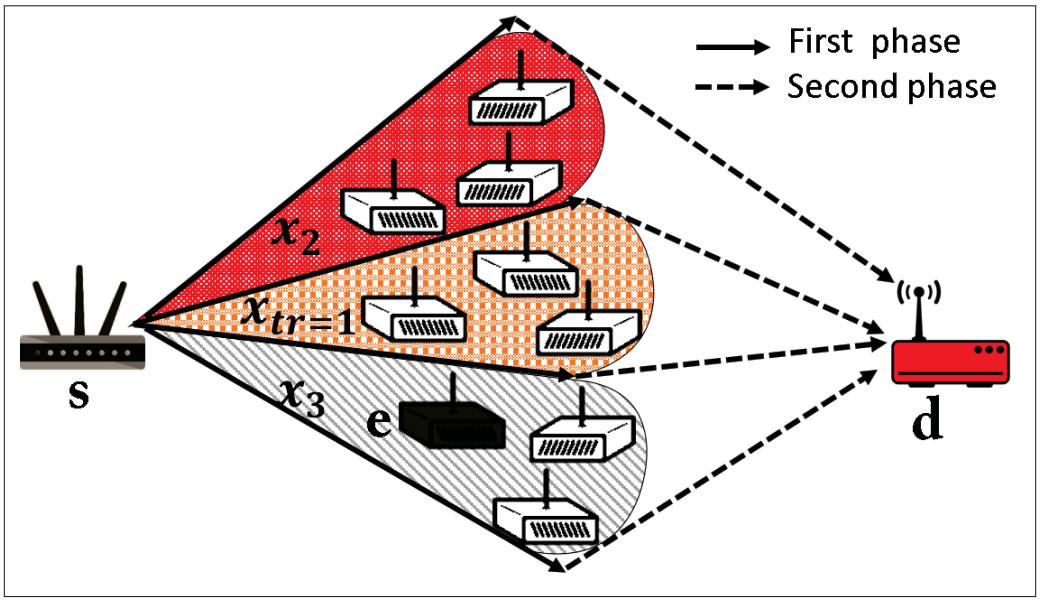


Figure 4.1 In the 1st hop of each transmission, s multicasts the useful message x_{tr} and the fake ones $x_{i\neq tr}$'s towards N sectors. In the 2nd hop, the K relays retransmit their received messages towards d

ted information should be forwarded by the relays. To perform the proposed security method, s and d should share the CSI knowledge of the source-trusted relay-destination link, which is the kernel of our developed security method. This CSI is considered to be the main cause of randomness and it is completely mapped into a vector V of digital values. It should be noted that this security algorithm is implemented just before the communication process starts, and it can be renewed at any time s and d agree on to keep refreshing the source of security and to make it as strong as possible. Moreover, since the received signal-to-noise ratio (SNR) in an AF two-hop wireless network over the first hop is higher than the received SNR after two hops. Therefore, by considering the case where the eavesdropper is in the first hop, we are studying the worst case security scenario. In the first hop, the source will encode the data prior to the transmission by using the vector V. Then, s will use this vector again to map its transmission of the different messages x_i's towards N different sectors, where $1 \leq i \leq N$, $N \in \mathbb{N}^+$. We will denote the desired encoded signal by x_{tr}, whereas the other signals $x_{i\neq tr}$ are the fake ones that are transmitted over the other sectors. Without the knowledge of V, each untrusted relay e will try to randomly guess the useful signal with a probability $1/N$. Even if it succeeds in guessing

and receiving the useful message, the untrusted relay would still need the vector V to decode it. In the second phase, all the K relays will resend their received messages towards d using the DBF technique. Since it has the same vector V, after removing the interference coming from the fake messages by using self-interference cancellation (SIC), the destination will be able to know from which sector the useful message is coming and decode it using V. The received signal, at the kth relay, where $1 \leq k \leq K$, is given by

$$y_k = \sqrt{P_i}\, h_{s,k}\, x_i + n_k, \tag{4.1}$$

where $n_k \sim \mathcal{N}_c\left(0, \sigma^2\right)$ is the complex additive white Gaussian noise (AWGN) at the kth relay, with mean 0 and variance σ^2, P_i is the transmitted power from s towards the ith sector. We assumed that the channels are quasi-static block log-normal channels, *i.e.* the channel coefficient $h_{v,r} \sim \ln\mathcal{N}(\mu_v, \sigma_v^2)$, where $\{v,r\} \subset \{\{s,k\},\{k,d\}\}$, is considered as constant during the transmission time of one message, but it may change independently thereafter, the CSI is known by the receiving nodes, and the noise variance N_0 has the same value in the first and the second phases. It is important to note that adopting such security solution by allowing a part of the nodes to forward fake messages is feasible due to the availability of a high number of electronic sensors with limited capabilities. Consequently, the received signal-to-noise ratio (SNR), at a kth relay, is expressed as

$$\gamma_k = \rho_s \left|h_{s,k}\right|^2, \tag{4.2}$$

where $\rho_j \triangleq P_j / N_0$, $j \in \{s,k,e\}$. In the second hop, the retransmitted message from the kth relay will be $\chi_k = \alpha_k w_k y_k$, where w_k is the beamforming weight, and α_k represents the normalized amplifying coefficient $\alpha_k = \frac{1}{\sqrt{\rho_s \left|h_{s,k}\right|^2 + N_0}}$. The received useful messages at d will be written as

$$y_d = \sum_{m=1}^{M} h_{m,d}\, \alpha_m\, w_m y_m + n_d, \tag{4.3}$$

where M is the number of the relays in the sector that receives the right message. $1 \leq m \leq M$, $n_d \sim \mathcal{N}_c(0, N_0)$ is the complex AWGN at d. After optimizing the beamforming weights from Kim *et al.* (2015) and the references therein, the SNR at the destination is obtained as

$$\begin{aligned} \gamma_d &= \sum_{m=1}^{M} \frac{\rho_s |h_{s,m}|^2 \rho_m \left|h_{m,d}\right|^2}{\rho_s |h_{s,m}|^2 + \rho_m \left|h_{m,d}\right|^2 + 1} \\ &= \sum_{m=1}^{M} \gamma_m. \end{aligned} \tag{4.4}$$

The channel capacity at d will be

$$C_d = \left[\frac{1}{2}\log(1+\gamma_d)\right]^+, \tag{4.5}$$

where $[\xi]^+$ denotes $\max\{\xi, 0\}$.

4.3.1 Non Colluding Eavesdropping Relays

In this scenario, there are two different hypotheses $H1$ and $H2$ as follows :
Hypothesis H_1: the untrusted relay is in the right sector with a probability $p_1 = 1/N$ and it knows how to recover V and decode the message.
Hypothesis H_2: the untrusted relay is in a wrong sector, with a probability $p_0 = 1 - p_1 = 1 - 1/N$. Then, this relay will not impact the security and the channel capacity at the eavesdropper e will be equivalent to zero from a security point of view. Considering the aforementioned two hypotheses, the channel capacity at e will be expressed as

$$C_e = \begin{cases} \frac{1}{2}\log(1+\gamma_e) & H_1 \\ 0 & H_2, \end{cases} \tag{4.6}$$

where $\gamma_e = \rho_s |h_{s,e}|^2$ is the SNR of the useful message at e.

4.3.2 Colluding Eavesdropping Relays

Assuming aggressive untrusted relays, cooperating between each other and sending their messages towards an external wire-tapper A, the received useful signal at A will be written as

$$y_A = \sum_{u=1}^{U_1} h_{u,A}\, \alpha_u\, w_u\, y_u + n_A, \tag{4.7}$$

where U_1 is the number of the untrusted relays that are in the right sector and sending the useful messages x_{tr}, and $1 \leq u \leq U_1 \leq U$. Moreover, $n_A \sim \mathcal{N}_c(0, N_0)$ is the complex AWGN at A. Hence, the SNR at A will become

$$\begin{aligned} \gamma_A &= \sum_{u=1}^{U_1} \frac{\rho_s \left|h_{s,u}\right|^2 \rho_u \left|h_{u,A}\right|^2}{\rho_s \left|h_{s,u}\right|^2 + \rho_u \left|h_{u,A}\right|^2 + 1} \\ &= \sum_{u=1}^{U_1} \gamma_u. \end{aligned} \tag{4.8}$$

We will define two hypotheses for A:
Hypothesis $H_1^{'}$: A receives the right message with a probability $p_1 = 1/N$ and knows how to recover V and decodes the message.
Hypothesis $H_2^{'}$: the colluding relays are just in the wrong sectors, or A con not recover V, which means that A won't have any impact on the security. Hence, the channel capacity at A will be equivalent to

$$C_A = \begin{cases} \frac{1}{2}\log\left(1+\gamma_A\right) & H_1^{'} \\ 0 & H_2^{'}, \end{cases} \tag{4.9}$$

We will define the worst security case as when e, (in the non colluding state), or A, (in the colluding state), knows how to recover V and decode the message. Therefore, the channel capacity at q, where $q \in \{e, A\}$, is given as

$$C_q = \left[\frac{1}{N}.\frac{1}{2}\log\left(1+\gamma_q\right)\right]^+. \tag{4.10}$$

From (4.5) and (4.10), the general secrecy capacity expression of the worst case is calculated as

$$\begin{aligned} C_{S,q} &= \left[C_d - C_q\right]^+ \\ &= \left[\frac{1}{2}\log\left(1+\gamma_d\right) - \frac{1}{2N}\log\left(1+\gamma_q\right)\right]^+. \end{aligned} \tag{4.11}$$

4.4 Secrecy Outage Probability

Theorem 5. *The secrecy outage probability expression of our proposed method $C_{S,q}$, for both passive and aggressive untrusted relays scenarios, is expressed as*

$$\begin{aligned} \Pr\left[C_{S,q} < R\right] = \frac{2}{3}\Phi\left(\left(\ln\left(2^{2R}\left(1+e^{\mu_q}\right)^{\frac{1}{N}}-1\right)-\mu_d\right)\sigma_d^{-1}\right) \\ +\frac{1}{6}\Phi\left(\left(\ln\left(2^{2R}\left(1+e^{\left(\mu_q+\sqrt{3}\sigma_q\right)}\right)^{\frac{1}{N}}-1\right)-\mu_d\right)\sigma_d^{-1}\right) \\ -\frac{1}{6}\Phi\left(\left(\ln\left(2^{2R}\left(1+e^{\left(\mu_q-\sqrt{3}\sigma_q\right)}\right)^{\frac{1}{N}}-1\right)-\mu_d\right)\sigma_d^{-1}\right). \end{aligned} \tag{4.12}$$

Proof. From (4.11), and for a threshold R, the SOP is defined as Kim *et al.* (2015)

$$\begin{aligned} \Pr\left[C_{S,q} < R\right] &= \Pr\left[\frac{1}{2}\log\left(1+\gamma_d\right) - \frac{1}{2N}\log\left(1+\gamma_q\right) < R\right] \\ &= \Pr\left[\gamma_d < 2^{2R}\left(1+\gamma_q\right)^{\frac{1}{N}}-1\right] \\ &= \int_0^\infty F_{\gamma_d}\left(2^{2R}\left(1+\gamma_q\right)^{\frac{1}{N}}-1\right) f_{\gamma_q}\left(\gamma_q\right) d\,\gamma_q. \end{aligned} \tag{4.13}$$

Since γ_q and γ_d are following a log-normal distribution, (please refer to Appendix II for the proof), then their probability density function (PDF) and cumulative distribution function

(CDF) are given as follows

$$f_X(x;\mu,\sigma) = \frac{1}{x\sigma\sqrt{2\pi}}\, e^{-\frac{(\ln x-\mu)^2}{2\sigma^2}}, \tag{4.14}$$

$$F_X(x;\mu,\sigma) = \Phi\left(\frac{\ln x-\mu}{\sigma}\right), \tag{4.15}$$

and Φ is the CDF of the standard normal distribution. Thus, the SOP in (4.13) is obtained as

$$\Pr\left[C_{S,q} < R\right] = \tag{4.16}$$

$$= \int_0^\infty \Phi\left(\frac{\ln\left(2^{2R}\left(1+\gamma_q\right)^{\frac{1}{N}}-1\right)-\mu_d}{\sigma_d}\right) \frac{e^{-\frac{\left(\ln\gamma_q-\mu_q\right)^2}{2\,{\sigma_q}^2}}}{\gamma_q\,\sigma_q\,\sqrt{2\pi}}\, d\,\gamma_q.$$

$$\text{Let} \quad \beta = \ln\left(\gamma_q\right), \ \text{ then } \ \gamma_q = e^{\beta}, \ \text{ and } \ d\,\gamma_q = e^{\beta}\, d\beta. \tag{4.17}$$

β is a normally distributed r.v. $\beta \sim \mathcal{N}(\mu_q, \sigma_q^2)$. Substituting (4.17) in (4.16), the secrecy outage probability $\Pr\left[C_{S,q} < R\right]$ is written as

$$\int_0^\infty \overbrace{\Phi\left(\frac{\ln\left(2^{2R}\left(1+e^{\beta}\right)^{\frac{1}{N}}-1\right)-\mu_d}{\sigma_d}\right)}^{\psi(\beta)} \frac{e^{-\frac{(\beta-\mu_q)^2}{2\,{\sigma_q}^2}}}{\sigma_q\sqrt{2\pi}}\, d\beta. \tag{4.18}$$

It is noticed that (4.18) denotes the expectation of $\psi(\beta)$. We will use *Holtzman* tool Holtzman (1992) to approximate $E\left[\psi(\beta)\right]$ in terms of three points located at μ_q, $\mu_q+\sqrt{3}\,\sigma_q$ and $\mu_q-\sqrt{3}\,\sigma_q$ as follows

$$\Pr\left[C_{S,q} < R\right] = E\left[\psi(\beta)\right] =$$

$$\frac{2}{3}\psi\left(\mu_q\right) + \frac{1}{6}\psi\left(\mu_q+\sqrt{3}\,\sigma_q\right) - \frac{1}{6}\psi\left(\mu_q-\sqrt{3}\,\sigma_q\right). \tag{4.19}$$

Compensating $\psi(\beta)$ from (4.18) in (4.19) yields (4.12). □

4.5 Simulation Results

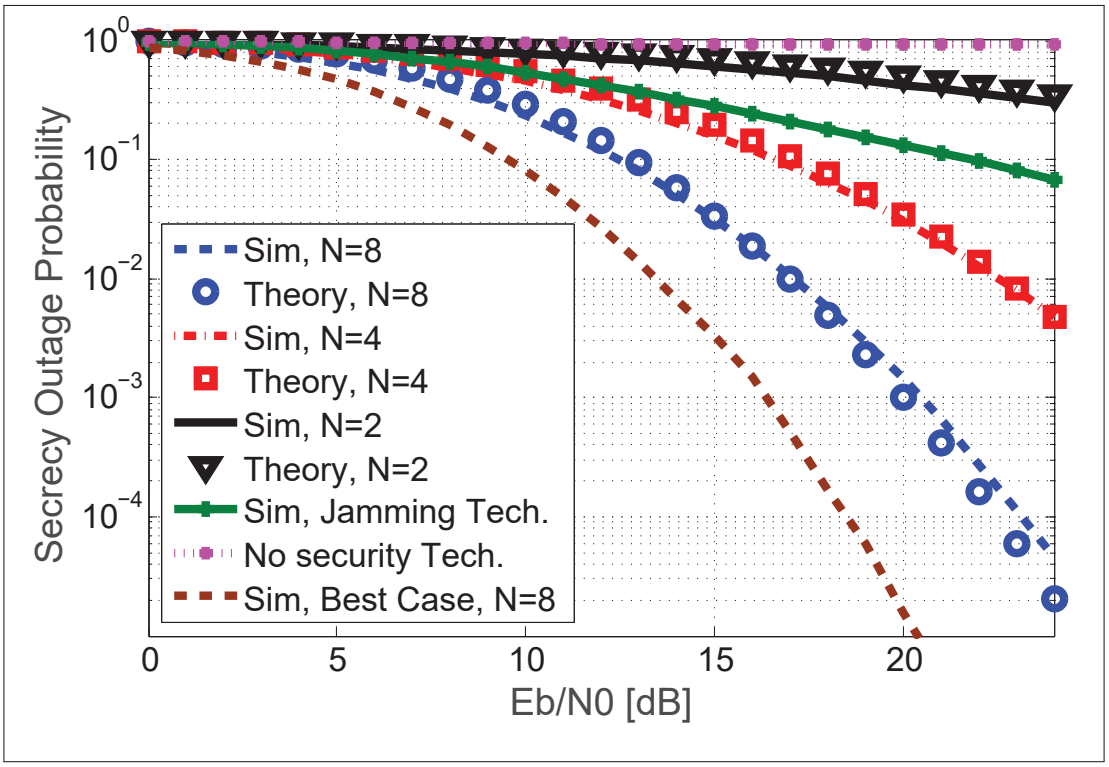


Figure 4.2 SOP with passive untrusted relays: $R = 3$ bps/Hz, $M = 4$, $\sigma_s = \sigma_k = 0.95$ and $\mu_s = \mu_k = 1$

In this section, we demonstrate the validity of our derived results using MATLAB software. Fig.4.2 shows the SOP as a function of the SNR. It is noticed that the derived expressions accurately characterize the simulation results. It is assumed that $R = 3$ bps/Hz, $M = 4$, $\sigma_s = \sigma_k = 0.95$ and $\mu_s = \mu_k = 1$. From Fig.4.2, we can see how the secrecy performance improves when the number of sectors N is increased. For example, to keep the SOP level at 10^{-2}, the source has to increase the number of sectors N from 4 to 8, which will also reduces the required SNR from $23dB$ to $17dB$. Also, it is shown that our performed technique outperforms the conventional jamming technique, where the destination jams the nodes while the source is transmitting in the first hop. As we can see from Fig.4.2, the margin between the worst and the

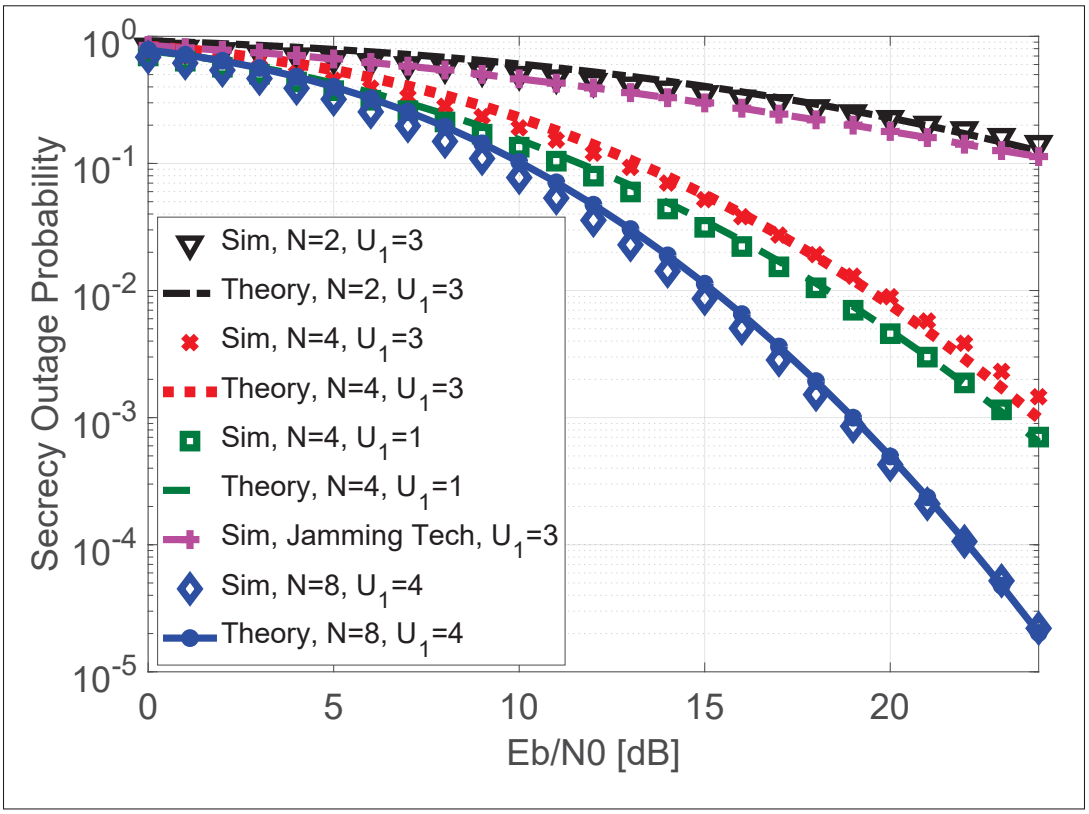


Figure 4.3 SOP with aggressive untrusted relays: $R = 2$ bps/Hz, $M = 4$, $\sigma_s = \sigma_k = 1.1$ and $\mu_s = \mu_k = 0.69$

best case, when e does not know how to recover V, depends on e's capability in recovering V and decoding the message.

Fig.4.3 shows the SOP of our proposed technique for different values of N, when $R = 2$ bps/Hz, $\sigma_s = \sigma_k = 1.1$, and $\mu_s = \mu_k = 0.69$. It can be seen that the greater the number of sectors, the better the secrecy performance. Moreover, we can see from Fig.4.3 that there is not that much of difference between the base of one and that of three aggressive untrusted relays. For example, at SNR level of $18dB$, the SOP just goes from 1.05×10^{-2} to 1.85×10^{-2} after adding two extra aggressive untrusted relays, which means that our proposed technique is immune towards adding more eavesdropping relays that are cooperating with each other. Also, it is shown that the security performance is improved when our technique is applied compared to the jamming technique. To evaluate the diversity order, we calculated the slope at 20dB for the

following cases: when all the relays are trusted, the brown curve in Fig. 3.2, and when all the relays are untrusted and aggressive, the blue curve in Fig. 3.4. For the first case, the slope is 1.1, whereas it becomes 0.7 for the second case.

4.6 Conclusions

In this paper, we proposed a new location-based multicasting protocol that is mapped by the knowledge of a trusted link's CSI in two-hops WSN. We provided an analytical study for the SOP for the passive and the aggressive behaviors of the untrusted relays. The results showed the immunity of our technique towards the untrusted relays aggressive behavior, and an improvement in the security compared to the conventional jamming technique.

CHAPTER 5

SECRECY ANALYSIS OF WIRELESS SENSOR NETWORK IN SMART GRID WITH DESTINATION ASSISTED JAMMING

Michael Atallah[1], Md. Sahabul Alam[1], and Georges Kaddoum[1]

[1] Department of Electrical Engineering, École de Technologie Supérieure,
1100 Notre-Dame Ouest, Montréal, Québec, Canada H3C 1K3

Paper published in IET communications, 2019.

5.1 Abstract

In this paper, we investigate the physical layer security performance over Rayleigh fading channels in the presence of impulsive noise, as encountered, for instance, in smart grid environments. For this scheme, secrecy performance metrics are considered with and without destination assisted jamming at the eavesdropper's side. Specifically, we derive analytical expressions for the secrecy outage probability (SOP), at the legitimate receiver. Finally, numerical results are provided to verify the accuracy of our derivations. From the obtained results, it is verified that the SOP, without destination assisted jamming, is flooring at high signal-to-noise-ratio values and that it can be significantly improved with the use of jamming.

5.2 Introduction

Wireless Sensor Networks (WSN)'s are widely employed in oil, gas, and smart grid (SG) mediums, since they have tremendously reduced the costs, increased the network coverage, and reduced the deployment time Gungor *et al.* (2010); Akyildiz *et al.* (2002). For example, in the context of designing a reliable smart grid, it is crucial to monitor and control the power system parameters in the transmission and distribution segments as well as in substation devices Fang *et al.* (2012). In order to allow such advanced functionalities and to avoid possible disruptions in electric systems due to unexpected failures, a highly reliable, scalable, secure, cost-effective, and robust communication network must be operational within the power grid

that convey data from monitoring sensors in the field to the access point. In this vein, the most promising method of SG monitoring, explored in the literature, is based on WSN's Gungor *et al.* (2011). For such applications, the increase in the infiltration rate for smart sensor networks has raised concerns regarding their security and privacy. Therefore, creating a secure environment for communications, and guaranteeing the privacy of customers, is becoming a significant challenge in SG environments. Since the infrastructures tend to be highly diversified, especially with the continuous deployment of small sensors Baig & Amoudi (2013), the lower layers (physical and data link layer) are oblivious of any security considerations. In this vein, to tackle the security issues, physical layer security (PLS) was suggested as a potential solution Soosahabi & Naraghi-Pour (2012). Recently, many security methods were studied in the PLS field, like game theory , multiple antenna schemes , beamforming , cooperative jamming , and power allocation techniques Atallah *et al.* (2015). Particularly, cooperative jamming strategies have been deemed efficient for reliable secure transmission over wireless mediums Atallah *et al.* (2015); Atallah & Kaddoum (2016, 2017); Liu *et al.* (2013).

5.3 Related Work

In the literature, multiple researches have been depicting the performance of cooperative jamming strategies in the presence of additive white Gaussian noise (AWGN). However, the noise characteristics usually observed in SG environments are remarkably non-Gaussian and are inherently impulsive Middleton (1977); Sarr *et al.* (2017); Neagu & Hamouda (2016). For example, the noise, emitted from power equipments in a power substation, appeared to be impulsive *et al* (2011). On the other hand, the performance of PLS techniques, in the presence of impulsive noise, is not widely acknowledged. In Pittolo & Tonello (2013), the secrecy rate was studied in narrowband power line communications (PLC) networks taking correlated channels into consideration. Thereafter, Pittolo & Tonello (2014) evaluated the security in PLC networks with multi-carrier and multi-user broadcast channels. Both Pittolo & Tonello (2013) and Pittolo & Tonello (2014) showed that a higher secrecy rate could be achieved when deploying wireless channels, rather than utilizing the PLC links. In Salem *et al.* (2017), the researchers

proposed a PLC and wireless hybrid security scheme. However, the analysis in Salem *et al.* (2017) is limited to AWGN only and the effect of impulsive noise is ignored. In Liu *et al.* (2013), the authors studied two-hops wireless networks, with destination assisted jamming, in the presence of an eavesdropper. In their work, both the destination and the transmitter are jamming the eavesdropper. However, the practical case of impulsive noise, whether at the legitimate receiver or at the eavesdropper's side, has not been investigated.

To the best of the authors' knowledge, no existing work has considered PLS in wireless systems, where the effect of the impulsive noise was involved. To fulfill this research gap, our paper provides a mathematical framework to investigate the performance of PLS in the presence of impulsive noise. Here, we consider a Bernoulli-Gaussian (BG) noise model, to take into account the impulsive behavior. This is motivated by the facts that the BG model is tractable and can represent the amplitude distributions of real impulsive noise measurements to a certain level of satisfaction Shongwey *et al.* (2014). We consider a single input single output (SISO) communication network, which consists of a source, a destination, and a passive eavesdropper. The passive eavesdropper is trying to intercept the transmitted message between the source and the destination without interfering with the system. To study the secrecy performance in this system, we consider two scenarios: 1) with destination assisted jamming, where the destination is jamming the eavesdropper while the source is transmitting its signal, and 2) without destination assisted jamming, which is the worst security case. In this network, the wireless channels have a Rayleigh distribution and the noise is characterized by a Bernoulli-Gaussian random process Ghosh (1996), to capture the combined effects of the AWGN and the impulsive noise. Our main contributions summarized are as follows:

- We analyze the secrecy performance of the proposed network in smart grid scenarios, in the presence of impulsive noise.
- We reformulate the secrecy capacity in an alternative approach aiming to make the derivation of the secrecy outage probability (SOP) tractable.

- We also analyze and compare the secrecy outage performance under two different scenarios: i) with destination assisted jamming, where the destination assists by jamming the passive eavesdropper while the source is transmitting its signal, and ii) without considering destination assisted jamming.

- We provide accurate results, in terms of the achievable secrecy capacity and the SOP, for these scenarios. Subsequently, numerical simulations are used to verify the accuracy of our analytical expressions.

5.4 System Model and Problem Formulation

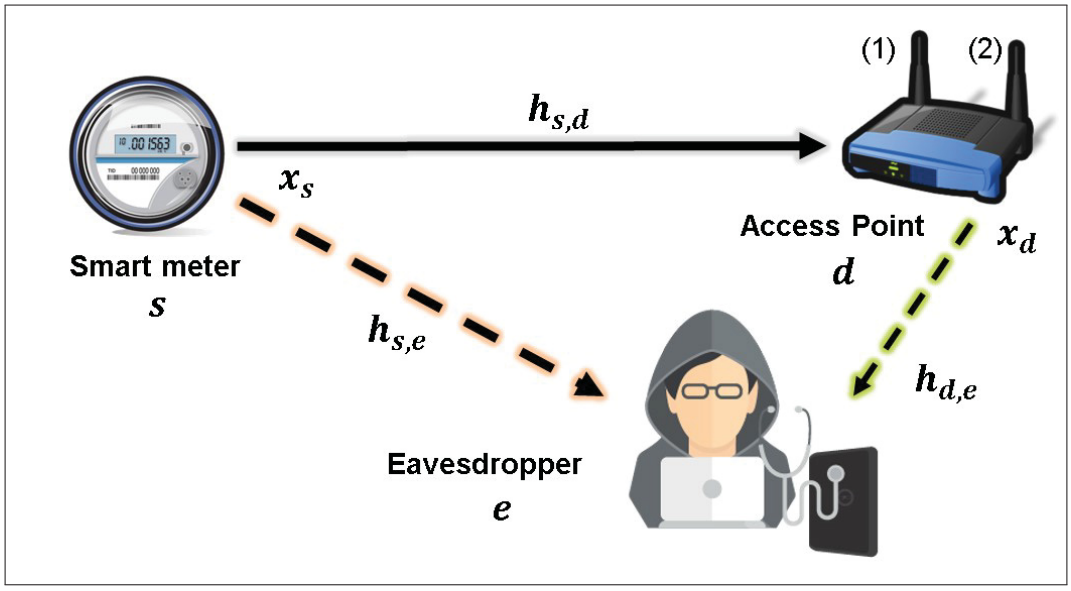


Figure 5.1 The source s transmits x_s to the destination d, while the eavesdropper e is trying to intercept x_s. In the case where d is jamming, d is provided with two independent antennas; (1) is for receiving x_s. (2) is for jamming with artificial noise signal x_d

As shown in Fig. 5.1, a wireless communication system consists of a source s, a destination d, and a passive eavesdropper e. In the demonstrated network, two scenarios can occur; in the first one, the source is broadcasting its signal x_s, and both the destination and the passive eavesdropper are receiving it. The destination has two independent antennas; one is jamming

the passive eavesdropper, with an artificial noise signal x_d, while the other one is receiving the signal, coming from the source. In the second scenario, there is no destination assisted jamming. Thus, the received signals, at the destination and at the eavesdropper's sides, are respectively expressed by

$$y_d^{'} = h_{s,d}\sqrt{P_s}x_s + h_{din}\sqrt{P_d}x_d + n_d, \tag{5.1}$$

$$y_e = h_{s,e}\sqrt{P_s}x_s + h_{d,e}\sqrt{P_d}x_d + n_e, \tag{5.2}$$

where P_s is the source transmit power and P_d is the artificial noise signal x_d power. Also, $h_{s,d}$ is the channel coefficient between the source and the destination and h_{din} is the channel coefficient between the jamming and the receiving antenna at the destination side. In addition, n_d and n_e are respectively the noise terms at the destination and the eavesdropper, that capture the combined effects of AWGN and impulsive interferers. In a specific situation, where no jamming is used at the eavesdropper's side, P_d in (5.2) will be equal to zero. In our analysis, we assume that the channels are quasi-static block Rayleigh channels, i.e. the channel coefficients $h_{s,e}$, $h_{s,d}$, h_{din}, and $h_{d,e}$ are considered as constant during the transmission time of one message, but they may change independently thereafter. Accordingly, the channel gains $|h_{s,e}|^2$, $\left|h_{s,d}\right|^2$, $|h_{din}|^2$, and $\left|h_{d,e}\right|^2$ follow independent exponential distributions. For this model, the thermal noise component at node m, where $m \in \{e,d\}$, is considered complex Gaussian, whereas the impulsive part is modeled as a Bernoulli-complex Gaussian random process Ghosh (1996). Since it is a sum of two complex Gaussian random processes, n_m qualifies as a complex Gaussian noise and can be written as Dubey & Mallik (2015),

$$n_m = n_{m0} + n_{m1}, \tag{5.3}$$

where n_{m0} is the AWGN component at node m, with zero mean and variance σ_{m0}^2, and $n_{m1} = b_m A_m$ is the impulsive component. Moreover, A_m is a complex white Gaussian noise, with zero mean and variance σ_{m1}^2, and b_m is the Bernoulli process. The probability mass function of b_m

is given by,

$$\begin{aligned} \Pr(b_m = 1) &= p_{m1}, \\ \Pr(b_m = 0) &= p_{m0} = 1 - p_{m1}, \end{aligned} \tag{5.4}$$

where p_{m1} and p_{m0} denote the probabilities of occurrence of the impulsive and the thermal noise at node m, respectively. Thus, the noise variance of n_m can be written as

$$N_m = \sigma_0^2 + b_m \sigma_m^2. \tag{5.5}$$

At the destination side, due to the large power difference between x_s and x_d, .i.e. $x_d \gg x_s$, the destination will be able to use successive interference cancellation (SIC) to remove x_d. Hence, after using SIC, the signal at the destination will be given by

$$y_d = h_{s,d}\sqrt{P_s}x_s + n_d. \tag{5.6}$$

Then, the received signal-to-interference-plus-noise-ratio (SINR), at node m, can be expressed as

$$\begin{aligned} \gamma_m &= \frac{P_s |h_{s,m}|^2}{P_d \left|h_{d,m}\right|^2 + N_m} \\ &= \frac{P_s |h_{s,m}|^2}{P_d \left|h_{d,m}\right|^2 + \sigma_{m0}^2 + b_m \sigma_{m1}^2} \\ &= \frac{P_s |h_{s,m}|^2}{P_d \left|h_{d,m}\right|^2 + \sigma_{m0}^2 (1 + b_m \Gamma_m)}, \end{aligned} \tag{5.7}$$

where $\Gamma_m = \frac{\sigma_{m1}^2}{\sigma_{m0}^2}$. By dividing the nominator and the denominator by σ_{m0}^2, the SINR γ_m becomes

$$\gamma_m = \frac{\gamma_{m0}}{\gamma_j + 1 + b_m \Gamma_m}, \tag{5.8}$$

$$\text{where} \quad \gamma_j = \frac{P_d \left|h_{d,e}\right|^2}{\sigma_{e0}^2}, \quad \text{and} \quad \gamma_{m0} = \frac{P_s |h_{s,m}|^2}{\sigma_{m0}^2}. \tag{5.9}$$

Thus, from (5.8), the channel capacity at node m becomes

$$\begin{aligned} C_m &= \log_2(1+\gamma_m) \\ &= \log_2\left(1+\frac{\gamma_{m0}}{\gamma_j+1+b_m\Gamma_m}\right). \end{aligned} \tag{5.10}$$

Finally, the achievable secrecy capacity would be given by

$$\begin{aligned} C_s &= [C_d - C_e]^+ \\ &= \left[\log_2\left(1+\frac{\gamma_{d0}}{1+b_d\Gamma_d}\right) - \log_2\left(1+\frac{\gamma_{e0}}{\gamma_j+1+b_e\Gamma_e}\right)\right]^+, \end{aligned} \tag{5.11}$$

where $[a]^+ = \max(a,0)$. As a consequence, in the following section, we detail the derivations of the secrecy outage probability equations to study the impact of impulsive noise on the PLS. The analysis considers both cases: with and without destination assisted jamming.

5.5 Secrecy Outage Probability Analysis

It is important to mention that a secrecy outage event happens when the target secrecy R is greater than the achievable secrecy capacity C_s, i.e., $C_s < R$. For the two scenarios, the analytical expressions of the SOP can be found as

$$\Pr[C_s < R] = \Pr[\log_2(1+\gamma_d) - \log_2(1+\gamma_e) < R]. \tag{5.12}$$

5.5.1 Secrecy Outage Probability Analysis with Jamming

In this subsection, we study the SOP after applying destination assisted jamming.

Theorem 6. *With jamming, the secrecy outage probability in Rayleigh fading channels, in the presence of impulsive noise, is given by*

$$\Pr\left[C_s < R\right] = \frac{\sum_{i=0}^{1} p_{di} \sum_{k=0}^{1} p_{ek} \left(a_1 \exp\left(a_2\right) E_1\left(a_3\right) + \overline{\gamma_{d0}\gamma_j}\right)}{\overline{\gamma_{d0}\gamma_j}}, \tag{5.13}$$

where a_1,a_2, and a_3 are given in (5.19), (5.20), and (5.22), respectively. Also, $E_1\left(x\right)$ is the exponential integral function of the random variable (r.v.) x and defined as $E_1\left(x\right) = \int_1^\infty \frac{\exp(-tx)}{t} dt$.

Proof. From (5.11) and (5.12), the SOP is demonstrated as

$$\begin{aligned}
\Pr\left[C_s < R\right] &= \Pr\left[\frac{1+\frac{\gamma_{d0}}{1+b_d\Gamma_d}}{1+\gamma_e} < 2^R\right] \\
&= \Pr\left[\left(1+\frac{\gamma_{d0}}{1+b_d\Gamma_d}\right) < 2^R\left(1+\gamma_e\right)\right] \\
&= 1-\Pr\left[2^R\left(1+\gamma_e\right) < \left(1+\frac{\gamma_{d0}}{1+b_d\Gamma_d}\right)\right] \\
&= 1-\Pr\left[\gamma_e < \left(1+\frac{\gamma_{d0}}{1+b_d\Gamma_d}\right)2^{-R}-1\right] \\
&= 1-\sum_{i=0}^{1} p_{di} \int_0^\infty F_{\Upsilon_e}\left(\left(1+\frac{\gamma_{d0}}{1+b_{di}\Gamma_d}\right)\frac{1}{2^R}-1\right) f_{\Upsilon_{d0}}(\gamma_{d0})\, d\,\gamma_{d0},
\end{aligned} \tag{5.14}$$

where $F_{\Upsilon_e}(\gamma_e)$ is the cumulative distribution function (CDF) of γ_e, which is given as

$$\begin{aligned}
F_{\Upsilon_e}(\gamma_e) &= \Pr\left(\Upsilon_e < \gamma_e\right) \\
&= \Pr\left(\frac{\gamma_{e0}}{\gamma_j+1+b_e\Gamma_e} < \gamma_e\right) \\
&= \Pr\left(\gamma_{e0} < \gamma_e\left(\gamma_j+1+b_e\Gamma_e\right)\right) \\
&= \sum_{k=0}^{1} p_{ek} \int_0^\infty F_{\Upsilon_{e0}}\left(\gamma_e\left(\gamma_j+1+b_{ek}\Gamma_e\right)\right) f_{\Upsilon_j}\left(\gamma_j\right) d\,\gamma_j
\end{aligned}$$

$$= \sum_{k=0}^{1} p_{ek} \int_{0}^{\infty} \left(1 - \exp\left(\frac{\gamma_e\left(\gamma_j + 1 + b_{ek}\Gamma_e\right)}{\overline{\gamma_{e0}}}\right)\right) \frac{\exp\left(-\frac{\gamma_j}{\overline{\gamma_j}}\right)}{\overline{\gamma_j}} d\gamma_j$$

$$= \sum_{k=0}^{1} p_{ek} \left(-\frac{\overline{\gamma_{e0}} \exp\left(-\frac{\gamma_e(1+b_{ek}\Gamma_e)}{\overline{\gamma_{e0}}}\right) - \overline{\gamma_j}\gamma_e - \overline{\gamma_{e0}}}{\gamma_e \overline{\gamma_j} + \overline{\gamma_{e0}}}\right). \tag{5.15}$$

Since γ_{m0} follows an exponential distribution, the probability density function (PDF) and the CDF of γ_{m0} are given by Alouini & Goldsmith (1999):

$$f_{\Upsilon_{m0}}(\gamma_{m0}) = \frac{e^{-\gamma_{m0}/\overline{\gamma_{m0}}}}{\overline{\gamma_{m0}}}, \tag{5.16}$$

$$F_{\Upsilon_{m0}}(\gamma_{m0}) = 1 - \exp\left(-\frac{\gamma_{m0}}{\overline{\gamma_{m0}}}\right), \tag{5.17}$$

where $\overline{\gamma_{m0}}$ is the mean of γ_{m0}. Substituting (5.15) and (5.16) in (5.14), the SOP with jamming can be written as

$$\Pr[C_s < R] = 1 - \sum_{i=0}^{1} p_{di} \int_{0}^{\infty} \left(\frac{\exp\left(\frac{-\gamma_{d0}}{\overline{\gamma_{d0}}}\right)}{\overline{\gamma_{d0}}} \sum_{k=0}^{1} p_{ek} \right.$$

$$\left. \times \left(-\frac{\overline{\gamma_{e0}} \exp\left(-\frac{\gamma_e(1+b_{ek}\Gamma_e)}{\overline{\gamma_{e0}}}\right) - \overline{\gamma_j}\gamma_e - \overline{\gamma_{e0}}}{\gamma_e \overline{\gamma_j} + \overline{\gamma_{e0}}}\right)\right) d\gamma_{d0}$$

$$= \frac{1}{\overline{\gamma_{d0}}\,\overline{\gamma_j}} \sum_{i=0}^{1} p_{di} \sum_{k=0}^{1} p_{ek} \left(a_1 \exp(a_2) E_1(a_3) + \overline{\gamma_{d0}\gamma_j}\right), \tag{5.18}$$

$$\text{where} \qquad a_1 = -\overline{\gamma_{e0}}\, 2^R (1 + b_{di}\Gamma_d), \tag{5.19}$$

$$a_2 = \frac{z_2 + b_{di}\Gamma_d \overline{\gamma_j} + b_{ek}\Gamma_e \overline{\gamma_{d0}} + \overline{\gamma_{d0}} + \overline{\gamma_j}}{\overline{\gamma_{d0}\gamma_j}}, \tag{5.20}$$

$$z_2 = -\left(\overline{\gamma_j} - \overline{\gamma_{e0}}\right)(1 + b_{di}\Gamma_d)\, 2^R, \tag{5.21}$$

$$a_3 = \frac{z_3 + z_4 - \overline{\gamma_{d0}\gamma_j}(1 + b_{ek}\Gamma_e)}{\overline{\gamma_j \gamma_{e0} \gamma_{d0}}}, \tag{5.22}$$

$$z_3 = \frac{\left(\overline{\gamma_{e0}}(1+b_{di}\Gamma_d)\left(\overline{\gamma_{e0}} - \overline{\gamma_j}\right) 4^R + \overline{\gamma_{d0}\gamma_j}(1 + b_{ek}\Gamma_e)\right)}{2^R}, \tag{5.23}$$

$$z_4 = \left(b_{ek}\Gamma_e \overline{\gamma_{d0}} + b_{di}\Gamma_d \overline{\gamma_j} + \overline{\gamma_{d0}} + \overline{\gamma_j}\right) \overline{\gamma_{e0}}. \tag{5.24}$$

□

5.5.2 Secrecy Outage Probability Analysis without Jamming

Here, we consider the worst security case, without destination assisted jamming, to measure the security performance of our proposed scenario.

Theorem 7. *Without jamming, the secrecy outage probability in Rayleigh fading channels, in the presence of impulsive noise, is given by*

$$\Pr[C_s < R] = \sum_{i=0}^{1} p_{di} \sum_{k=0}^{1} p_{ek}$$

$$\times \left(1 - \frac{\exp\left(\frac{1-2^R(1+b_{di}\Gamma_d)}{\overline{\gamma_{d0}}}\right)(1+b_{ek}\Gamma_e)\,\overline{\gamma_{d0}}}{(1+b_{ek}\Gamma_e)\,\overline{\gamma_{d0}} + 2^R(1+b_{di}\Gamma_d)\,\overline{\gamma_{e0}}} \right). \tag{5.25}$$

Proof. Without jamming, $P_d = 0$, then γ_j in (5.9) is equal to zero, and (5.11) is further simplified. Revisiting (5.12), the SOP, under this condition, becomes

$$\begin{aligned} \Pr[C_s < R] &= \Pr\left[\log_2 \left(\frac{1 + \frac{\gamma_{d0}}{1+b_d\Gamma_d}}{1+\gamma_e} \right) < R \right] \\ &= \Pr\left[\gamma_{d0} < \left(2^R(1+\gamma_e) - 1\right)(1+b_d\Gamma_d) \right]. \end{aligned} \tag{5.26}$$

By substituting (5.16) and (5.17) in (5.26), we can write the SOP as

$$\Pr[C_s < R] = \sum_{i=0}^{1} p_{di} \sum_{k=0}^{1} p_{ek} \int_0^{\infty} F_{\Upsilon_{d0}}(z_1)\, f_{\Upsilon_{e0}}(\gamma_{e0}) d\,\gamma_{e0} \tag{5.27}$$

$$= \sum_{i=0}^{1} p_{di} \sum_{k=0}^{1} p_{ek} \int_0^{\infty} \left(1 - \exp\left(\frac{-z_1}{\overline{\gamma_{d0}}} \right) \right) \frac{\exp\left(\frac{-\gamma_{e0}}{\overline{\gamma_{e0}}}\right)}{\overline{\gamma_{e0}}} d\,\gamma_{e0} \tag{5.28}$$

$$= \sum_{i=0}^{1} p_{di} \sum_{k=0}^{1} p_{ek} \left(1 - \frac{\exp\left(\frac{1-2^R(1+b_{di}\Gamma_d)}{\overline{\gamma_{d0}}}\right)(1+b_{ek}\Gamma_e)\,\overline{\gamma_{d0}}}{(1+b_{ek}\Gamma_e)\,\overline{\gamma_{d0}} + 2^R(1+b_{di}\Gamma_d)\,\overline{\gamma_{e0}}} \right) \tag{5.29}$$

where z_1 in (5.27) becomes

$$z_1 = \left(2^R \left(1 + \frac{\gamma_{e0}}{1 + b_{ek}\Gamma_e}\right) - 1\right)(1 + b_{di}\Gamma_d). \tag{5.30}$$

□

Although this paper considers the secrecy analysis for the case of memoryless impulsive noise, modeled by a Bernoulli-Gaussian process, the analysis could be easily extended to consider the presence of any kind of impulsive or Gaussian mixture noise.

5.6 Simulation Results

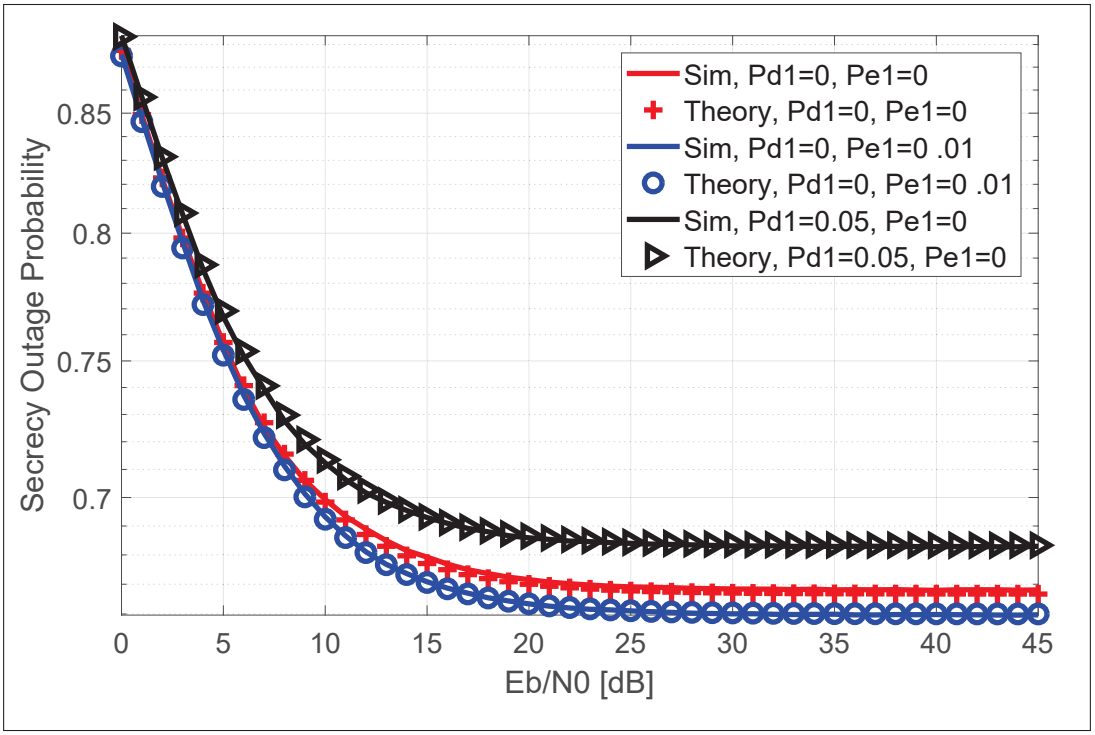


Figure 5.2 Analytical and simulated SOP performances of the proposed system without jamming: $\overline{\gamma_{d0}} = \overline{\gamma_{e0}}$, $\Gamma_d = \Gamma_e = 1000$, $\left|\overline{h_{s,d}}\right|^2 = \left|\overline{h_{s,e}}\right|^2 = \left|\overline{h_{d,e}}\right|^2 = 1$, and $R = 1\,bps/Hz$

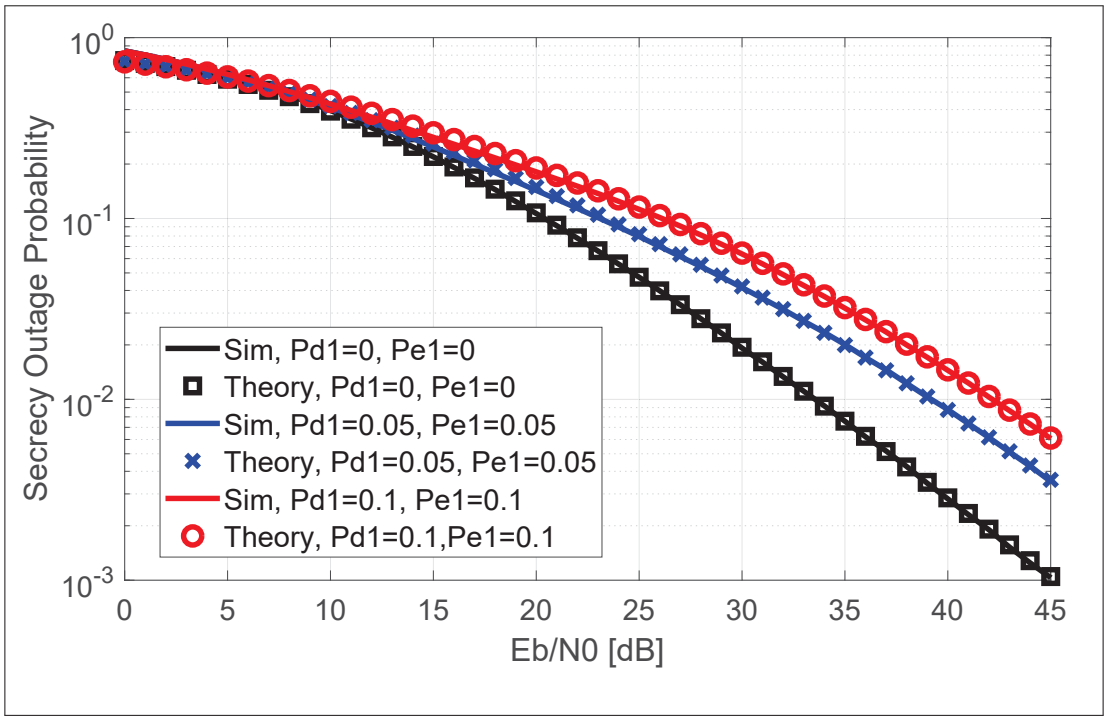


Figure 5.3 Analytical and simulated SOP performances of the proposed system with jamming: $\left|\overline{h_{s,d}}\right|^2 = |\overline{h_{s,e}}|^2 = \left|\overline{h_{d,e}}\right|^2 = 1$, $\Gamma_d = \Gamma_e = 100$, $\overline{\gamma_{d0}} = \overline{\gamma_{e0}}$, $\overline{\gamma_j} = \frac{1}{2}\overline{\gamma_{d0}}$, and $R = 1 bps/Hz$

In this section, we present the SOP performances of SG networks, with and without destination assisted jamming. In the simulation results, performed using MATLAB software, it is assumed that the probability of having impulsive noise P_{m1}, ranges from 0.01 to 0.1, and Γ_m takes the values 100 and 1000. These values are chosen to represent the characteristics of the impulsive noise, as observed in SG environments Middleton (1977). On the other hand, it is also assumed that the threshold $R = 1 bps/Hz$, $E_b/N_0 = \overline{\gamma_{d0}} = \overline{\gamma_{e0}}$, $\overline{\gamma_j} = \frac{1}{2}\overline{\gamma_{d0}}$, $\left|\overline{h_{s,d}}\right|^2 = |\overline{h_{s,e}}|^2 = \left|\overline{h_{d,e}}\right|^2 = 1$, and the background noise $\sigma_{d0}^2 = \sigma_{e0}^2 = 1$.

Fig.5.2 shows the analytical results derived in (5.25), and simulated SOP performances without destination assisted jamming. From Fig.5.2, it is seen that the analytical results perfectly match the simulations. Moreover, we can observe that the security performance is directly proportional to the impulsive noise at the eavesdropper, and is inversely proportional to the impulsive noise at the destination. We also exposed that when $E_b/N_0 > 25dB$, the security

is flooring; due to the effect of the noise becoming negligible, and therefore, the SOP scales towards a constant value.

Fig.5.3 shows the analytical results given in (5.13), and simulated SOP performances when considering destination assisted jamming. This figure further confirms the correctness of the analysis through the simulations. From Fig.5.3, We can see the degradation in the security performance due to the presence of the impulsive noise. Subsequently, compared to Fig.5.2, it is also observed that by adding jamming, the security performance is remarkably enhanced. This confirms that the destination assisted jamming technique can be beneficial to SG environments.

5.7 Conclusions

We have presented the SOP expressions, in wireless SG environments, with and without destination assisted jamming. Our analytical expressions allow the measurement of the security performance; when either both of the destination and the wiretapper or any of them is affected by impulsive noise. From the obtained results, we verified that the analytical results agree with the simulations. We also showed that the achievable security is enhanced when the occurrence probability of impulsive noise is higher at the eavesdropper's side than at the legitimate receiver. Moreover, the results show that destination assisted jamming can significantly enhance the security of the network, making it a promising security solution for SG networks. In this paper, we didn't consider any aggressive action by the eavesdropper, which would be an interesting topic for future works.

CONCLUSION AND RECOMMENDATIONS

This thesis concentrated on the security in the physical layer in wireless networks. The environment's characteristics were exploited to provide secure protocols in wireless systems. A jamming technique was applied in most of the works, whether to analyse its presence, to add more security to the studied systems, or to compare its performance with our novel protocols to show the superiority of our protocols against the conventional jamming technique. The domain was exploited to design spatial transmission protocols. Rayleigh and log-normal fadings were considered. Also, the presence of impulsive noise has been investigated. The proposed protocols showed their strength against the eavesdroppers' passive and colluding behaviors. Finally, a novel approach to study the security performance in impulsive noise environments is proposed and analysed. Hence, we investigated the secrecy capacity scaling with the presence of colluding eavesdroppers in large wireless networks. To reduce the probability of having access to the whole message by the eavesdroppers, we proposed new location based protocols for that purpose. Our techniques were liberated from the need to know the CSI or the location of the eavesdroppers. Also, by exploiting the presence of having many trusted nodes in large wireless networks, we proposed a novel key generating and mapping technique. In addition, we provided new secrecy capacity expressions for the environments that are affected by the impulsive noise. Thus, from the second chapter, we showed how the secrecy performance was enhanced after applying cooperative jamming technique, and how the distributed beamforming overcomes the opportunistic relaying technique for large number of relays. However, opportunistic relaying can still be used for small number of relays and its performance could be enhanced by increasing the transmitted power. In the third chapter, a novel location based protocol was proposed to reduce the probability that an eavesdropper will receive the whole transmitted message. Even though the multicasting technique is applied in each transmission time, the secrecy capacity scaling was not just similar, but also slightly better than the broadcasting technique applied in the second chapter. We applied cooperative jamming technique

along with our proposed protocol to boost the security. The results showed how increasing the number of the sectors or the number of the relays could remarkably enhance the security performance. Our proposed protocol could be exploited to optimize the selection strategy of the sectors to avoid choosing the weak clusters and to focus on the stronger ones. Since the passive behavior of the eavesdroppers was considered in this chapter, there was a need to investigate in the colluding behavior to provide the most secure protocol for wireless networks. Thus, we proposed a new key mapping technique, in the fourth chapter, that was proved to be immune towards the colluding behavior of the untrusted eavesdroppers. This protocol also exploited the presence of the large number of trusted relays to generate keys to encode the transmitted signals and to map the transmission towards different clusters. By applying this protocol, the destination and the relays can benefit from the transmitted power in all the sectors to harvest the energy. Here, the destination didn't need to drain its energy by jamming the relays. That's due to the fact that our proposed protocol is strong enough to be operated by itself and to achieve good security results. Furthermore, This protocol is promising due to the availability of high number of cheap electronic sensor nodes. In another topic, since the smart grid environment suffers from the impulsive noise, we provided in the fifth chapter the secrecy analyses for two cases: before and after applying the destination assisted jamming technique, with the presence of impulsive noise. Besides reformulating the secrecy capacity equations, we showed in our results that the impulsive noise has an impact on the security since it's affecting both the destination and the eavesdropper, which means that implementing good impulsive noise receivers could be taken into consideration to enhance the security performance. Also, the results showed how the security was enhanced after applying destination assisted jamming technique, especially for the systems that are transmitting with high power. It should be noted that the simulations in this thesis were performed using MATLAB software.

6.1 Future Work

As extensions to the current works, the imperfect CSI could be considered in the future studies to cover more general cases. The full duplex mode could be investigated, whether at the transmitter, the receiver or at the relays to see its impact on the security with our proposed security protocols. Moreover, analysing and comparing the cooperation strategies when the relays are decoding and forwarding or compressing and forwarding the information could also be considered, especially since these relays will have different capabilities and permissions on the access to the information. The aggressive behaviour of the eavesdroppers when they cooperate together to intercept the transmitted messages could be analysed to show its effect on some of the proposed protocols. Our proposed security techniques, that rely on the space diversity, could be optimized by checking which sectors are the best to be chosen and which sectors should be avoided whether from the power or the security perspective. Multi-antennas techniques could be applied and investigated at both the legitimate and illegitimate nodes. The case where the eavesdroppers are attacking the network by jamming the legitimate nodes could also be investigated whether to find alternative ways to route the transmitted information or other solutions to reduce the attack effect on the legitimate nodes. Moreover, the impulsive noise environments could benefit from a deeper investigation and analysis in the context of several physical layer security techniques. Deep or reinforcement learning could be implemented to detect jamming behavior. Additionally, more research efforts need to be focused towards exploiting relay positioning and cross layered scenarios, which this latter could be used to gain more benefits from secure cooperative schemes.

APPENDIX I

PROOFS FOR CHAPTER 2

1. Proof of Lemma1

1. Here, we will prove that $A = \sum_{k=1}^{K} \min\left\{\gamma_{s,k}, 2\gamma_{k,d}\right\}$ has the PDF given in (3.21)

Lemma 2. *Let $Y = \min\left\{\gamma_{s,k}, 2\gamma_{k,d}\right\}$'s, then Y is an exponentially distributed r.v. with a rate parameter $\lambda_0 = \frac{1}{\rho\,\sigma_1^2} + \frac{1}{2\rho\,\sigma_2^2}$.*

Proof. Since $\gamma_{s,k}$ and $2\gamma_{k,d}$ are exponentially distributed r.v.'s, their PDF and CDF will be respectively given by the following equations Alouini & Goldsmith (1999)

$$f_{\Upsilon}(\gamma) = \lambda e^{-\lambda\gamma}, \tag{A I-1}$$

$$F_{\Upsilon}(\gamma) = 1 - \exp(-\lambda\,\gamma), \tag{A I-2}$$

where λ is the rate of the exponentially distributed r.v. γ. Hence, to prove that Y has an exponential distribution, we will first find the complement of the CDF of Y as follows; for some $v > 0$,

$$\begin{aligned}
\Pr(Y > v) &= \Pr\left(\min\{\gamma_{s,k}, \gamma_{k,d}\} > v\right) \\
&= \Pr\left(\gamma_{s,k} > v, \gamma_{k,d} > v\right) \\
&= \left(1 - F_{\gamma_{s,k}}(v)\right)\left(1 - F_{\gamma_{k,d}}(v)\right) \\
&= e^{-\lambda_1 v} e^{-\frac{\lambda_2 v}{2}} \\
&= e^{-v\left(\lambda_1 + \frac{\lambda_2}{2}\right)}.
\end{aligned} \tag{A I-3}$$

Then, the CDF of y will be calculated as

$$F_Y(v) = 1 - \Pr(Y > v) = 1 - e^{-v\left(\lambda_1 + \frac{\lambda_2}{2}\right)},$$

where λ_1 and λ_2 are defined in (3.23). We can see from (A I-3) that the CDF of Y has exactly the form of the CDF of an exponentially distributed r.v. given in (A I-2), with a rate parameter of $\lambda_0 = \lambda_1 + \frac{\lambda_2}{2} = \frac{1}{\rho\,\sigma_1^2} + \frac{1}{2\rho\,\sigma_2^2}$. □

Since A is a sum of K exponential r.v.'s, it has a Gamma distribution with a shape parameter K and a rate parameter λ_0, and its PDF is given by (3.21).

2. Since $\gamma_{s,e}$ $\gamma_{d,e}$ follow exponential distributions, the forms of their CDF and PDF are respectively given in (A I-1) and (A I-2). Thus, the CDF of a r.v. $Z_e = \frac{\gamma_{s,e}}{\gamma_{d,e}+1}$ is expressed as

$$\begin{aligned}
\Pr[Z<u] &= \Pr\left[\gamma_{s,e} < \left(\gamma_{d,e}+1\right)u\right] \\
&= \int_0^\infty F_{\Upsilon_{s,e}}\left(\left(\gamma_{d,e}+1\right)u\right) f_{\Upsilon_{d,e}}\left(\gamma_{d,e}\right) d\,\gamma_{d,e} \\
&= \int_0^\infty \left(1-\exp\left(-\lambda_1\,u\left(\gamma_{d,e}+1\right)\right)\right)\left(\lambda_2\,e^{-\lambda_1\,\gamma_{d,e}}\right) d\,\gamma_{d,e} \\
&= 1-\exp\left(-\lambda_1\,u\right)\frac{\lambda_2}{\lambda_1\,u+\lambda_2}. \qquad \text{(A I-4)}
\end{aligned}$$

where λ_1 and λ_2 are defined in (3.23).

Since $B = 1+\frac{K}{T}Z$, the CDF of B is calculated as

$$\begin{aligned}
F_B(b) &= \Pr\left[1+\frac{K}{T}Z < b\right] \\
&= \Pr\left[Z < (b-1)\frac{T}{K}\right] \\
&= 1-\exp\left[-\lambda_1\,(b-1)\frac{T}{K}\right]\frac{\lambda_2}{\lambda_1\,(b-1)\frac{T}{K}+\lambda_2}. \qquad \text{(A I-5)}
\end{aligned}$$

Thus, we completed the proof.

APPENDIX II

PROOFS FOR CHAPTER 3

We will prove that γ_q and γ_d are following a log-normal distribution. First, we will define the SNR $\gamma_{i,j}$ as follows

$$\gamma_{i,j} = \rho_i \left|h_{i,j}\right|^2, \tag{A II-1}$$

where $i \in \{s,m\}$ and $j \in \{m,e,d\}$.

Lemma 3. *Let* $X \sim \ln \mathcal{N}(\mu, \sigma^2)$*, then* $aX \sim \ln \mathcal{N}(\mu + \ln a,\ \sigma^2)$*, and* $X^a \sim \ln \mathcal{N}(a\mu, a^2\ \sigma^2)$*,* $a \in \mathbb{R}$.

From **Lemma 3**, where $a = 2$, the channel gain $\left|h_{i,j}\right|^2 \sim \ln \mathcal{N}(2\mu_{\gamma_{i,j}}, 4\sigma^2_{\gamma_{i,j}})$. By using the properties in **Lemma 3**, we find that $\gamma_{i,j} \sim \ln \mathcal{N}(\mu_{\gamma_{i,j}}, \sigma^2_{\gamma_{i,j}})$, where $\mu_{\gamma_{i,j}} = 2\,\mu_i + \ln(\rho_i)$, $\ln(\rho_i) = \ln(P_i) - \ln(N_0)$, and $\sigma^2_{\gamma_{i,j}} = 4\,{\sigma_i}^2$. Hence, $\gamma_e \sim \ln \mathcal{N}(\mu_{\gamma_{s,e}}, \sigma^2_{\gamma_{s,e}})$.

Now, we will find the distribution of γ_m (4.4) with the following approximation for high SNRs, as follows

$$\gamma_m = \frac{\gamma_{s,m}\,\gamma_{m,d}}{\gamma_{s,m} + \gamma_{m,d} + 1} \approx \frac{\gamma_{s,m}\,\gamma_{m,d}}{\gamma_{s,m} + \gamma_{m,d}} = \frac{1}{\frac{1}{\gamma_{s,m}} + \frac{1}{\gamma_{m,d}}} = \frac{1}{z}, \tag{A II-2}$$

where $z = z_1 + z_2$, $z_1 = \frac{1}{\gamma_{s,m}}$ and $z_2 = \frac{1}{\gamma_{m,d}}$.

Lemma 4. *Let* $X_j \sim \ln \mathcal{N}(\mu_j, \sigma_j^2)$ *are independent log-normally distributed variables with varying* σ *and* μ *parameters, and* $Y = \sum_{j=1}^{n} X_j$*. Then the distribution of* Y *has no closed form expression, but can be reasonably approximated by another log-normal distribution* Z *with parametersFenton (1960)*

$$\mu_Z \quad = \ln\left[\sum e^{\mu_j + \sigma_j^2/2}\right] - \frac{\sigma_Z^2}{2}, \tag{A II-3}$$

$$\sigma_Z^2 \quad = \ln\left[\frac{\sum e^{2\mu_j+\sigma_j^2}(e^{\sigma_j^2}-1)}{(\sum e^{\mu_j+\sigma_j^2/2})^2}+1\right]. \qquad \text{(A II-4)}$$

Form **Lemma 3**, where $a=-1$, we find that $Z_1 \sim \ln \mathcal{N}(-\mu_{\gamma_{s,m}}, \sigma^2_{\gamma_{s,m}})$ and $Z_2 \sim \ln \mathcal{N}(-\mu_{\gamma_{m,d}}, \sigma^2_{\gamma_{m,d}})$. Also, from **Lemma 4**, $Z \sim \ln \mathcal{N}(\mu_z, \sigma_z^2)$, where

$$\sigma_z{}^2 = \ln\left(\left(\exp\left(\sigma_{z_1}^2\right)-1\right)/2+1\right),$$

$$\mu_z = \ln\left(2\exp\left(\mu_{z_1}\right)\right)+0.5\left(\sigma_{z_1}^2-\sigma_z^2\right).$$

Thus, from **Lemma 3** and (A II-2), we get $\gamma_m \sim \ln \mathcal{N}(\mu_{\gamma_m}, \sigma^2_{\gamma_m})$, where $a=-1$, $\mu_{\gamma_m} = -\mu_z$, and $\sigma^2_{\gamma_m} = \sigma_z^2$. From (4.4), since γ_d is a sum of many γ_m, we will again use **Lemma 4** to find that $\gamma_d \sim \ln \mathcal{N}(\mu_{\gamma_d}, \sigma^2_{\gamma_d})$, where

$$\sigma_d{}^2 = \ln\left(\left(\exp\left(\sigma_{\gamma_m}^2\right)-1\right)/M+1\right),$$

$$\mu_d = \ln\left(M\exp\left(\mu_{\gamma_m}\right)\right)+0.5\left(\sigma_{\gamma_m}^2-\sigma_d^2\right).$$

Since the expressions of γ_u and γ_A in (4.8) are similar to γ_m and γ_d respectively, by following the same steps, we show that $\gamma_u \sim \ln \mathcal{N}(\mu_{\gamma_m}, \sigma^2_{\gamma_m})$ and $\gamma_A \sim \ln \mathcal{N}(\mu_{\gamma_A}, \sigma^2_{\gamma_A})$ where

$$\sigma_A{}^2 = \ln\left(\left(\exp\left(\sigma_{\gamma_m}^2\right)-1\right)/U_1+1\right),$$

$$\mu_A = \ln\left(U_1\exp\left(\mu_{\gamma_m}\right)\right)+0.5\left(\sigma_{\gamma_m}^2-\sigma_A^2\right).$$

SUBMITTED PAPERS

APPENDIX III

A SURVEY ON COOPERATIVE JAMMING APPLIED TO PHYSICAL LAYER SECURITY

Michael Atallah[1], Georges Kaddoum[1], and Long Kong[1]

[1] Department of Electrical Engineering, École de Technologie Supérieure,
1100 Notre-Dame Ouest, Montréal, Québec, Canada H3C 1K3

Paper published in *IEEE International Conference on Ubiquitous Wireless Broadband (ICUWB)* , November 2015.

1. Abstract

Security has always played a critical role in wireless cooperative communication systems design. Eavesdropping and jamming are two common threats to the information security in wireless networks. However, jamming can be used in a cooperative manner to enable a secure communication link between the legitimate transmitter and the intended receiver. This paper presents a comprehensive survey on different jamming methods used to enhance the physical layer security. This survey outlines first the underlying concept and challenges with respect to security in wireless network design followed by a comprehensive literature review and analysis of jamming techniques with their applications in this field. For each jamming protocol, the paper categorizes different techniques within the existing literature by elaborating on their application, and corresponding performances.

Keywords: Physical layer security, cooperative jamming, beamforming, power allocation, artificial noise, multiple antennas, MIMO, game theory.

2. Introduction

Wireless communications is playing an integral part in our lives and also has a significant social impact. Privacy and confidentiality with respect to the transmitted information over the wireless medium becomes vital, especially for applications concerning medical informa-

tion, e-banking, and e-commerce. However, wireless communications are often vulnerable to eavesdropping and signal interception Hong *et al.* (2013). Many security tasks are involved in wireless networks design, like integrity and confidentiality checks, authentication, spectrum access control Lou & Ren (2009); Shiu *et al.* (2011). Confidentiality refers to the prevention of unauthorized information disclosure. Integrity ensures that the transmitted information is utilized and modified by the legitimate user. Authentication refers to the identity confirmation of different terminals. Spectrum access control refers to prevention of denial-of-service type attacks. Conventionally, these security tasks are addressed mostly in the upper layers of the network protocol stack using cryptographic encryption and decryption methods. When employing symmetric-key cryptosystems, the two users have to share a common private key to encrypt and decrypt the confidential message Hong *et al.* (2013). However, for the secret keys sharing, this requires a secure channel or protocol. The difficulties in secret key distribution and management Schneier (1998) lead to security vulnerabilities in wireless systems. Alternatively, public-key cryptosystems allow the use of a public key for encryption and a separate private key for decryption. The public key is available to all users whereas the private key is known only to the receiver. However, the cryptographic methods rely on the computational hardness on decrypting the message to achieve security when the secret key is not available. As the computational power increases, e.g., with the development of quantum computers, the computational hardness of certain mathematical problems, for which the encryption and decryption are based on, may no longer hold, causing many current cryptosystems to break downHong *et al.* (2013). Many coding and signal processing techniques in the physical layer have been developed in the recent years, to support and to further enhance security in wireless systems, many researchers have made contributions to find alternative security solutions to fit the requirements of the current and emerging wireless networks Goel & Negi (2008); Gopala *et al.* (2008); Shannon (1949); Bloch & Barros (2011). Even though the fast channel variations and the wireless medium's broadcast nature may cause additional challenges, physical layer security technique exploits the properties of the wireless transmissions to secure the communication channel in a better wayHong *et al.* (2013).

Interference, in general, is regarded as undesired phenomenon in wireless communications. But in secure communications, interference can benefit the system if it is used in a proper way. The idea is to create an interference and put the eavesdropper in a disadvantage comparing to the legitimate nodes Park *et al.* (2013). Several applications use interference to increase the security in the physical layer, one of the security applications that has become a very common and promising technique in the physical security field is the cooperative jamming which is accomplished by the friendly terminals in which one of the legitimate parties sacrifices his entire rate to jam the eavesdropper.

In this paper a continuation and update of the recent achievements in the field of physical layer security is presented with emphasis on different jamming methods and protocols of such schemes. Hence, our contribution can be summarized as follows:

1. Providing a brief overview of physical layer system model and the challenges in this field.
2. Developing a literature review of the different jamming techniques within the existing recent literature with their advantages and disadvantages, followed by a discussion on their subsequent application.

The remainder of this paper is outlined as follows. The concept of physical layer security is depicted in Section 3. Cooperative Jamming and techniques to enhance physical layer security via cooperative jamming are presented in section 4. Finally, the concluding remarks are given in section 5.

3. Physical Layer security and cooperative jamming

3.1 Physical Layer Security

As shown in Fig. III-1, a generic wireless communication network model which consists of three nodes is taken into consideration: the legitimate transmitter (Alice), the intended receiver (Bob) and the eavesdropper (Eve). The link between Alice and Bob is called the main channel,

while the link between Alice and Eve is named as a wiretap channel. This model exemplifies the specific features of most multi-user secure communication systems. The secrecy capacity is defined as the maximum achievable secrecy rate. In Bloch *et al.* (2008), the secrecy capacity over additive white Gaussian noise (AWGN) channel $C_{s,A}$ and Rayleigh fading channel $C_{s,R}$ are given by

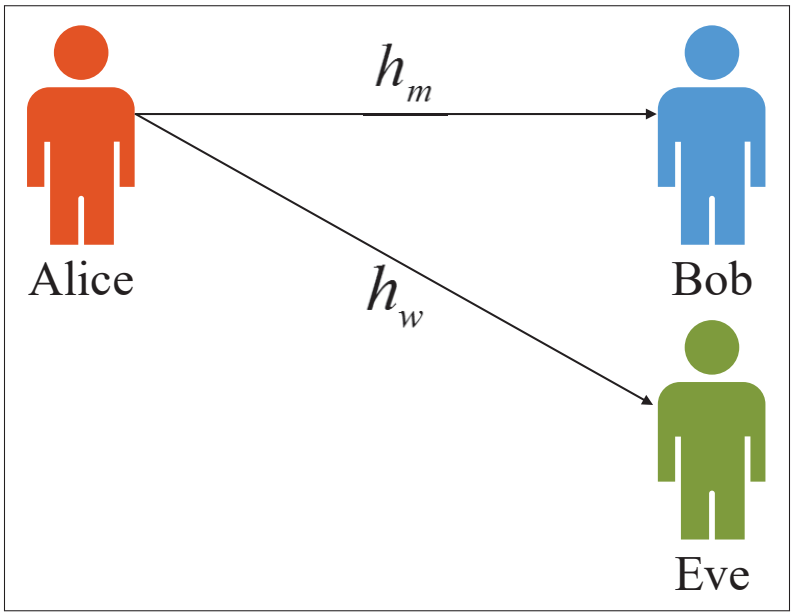


Figure-A III-1 Wireless wiretap system model

$$C_{s,A} = \left[\frac{1}{2}\log_2\left(1+\frac{P}{\sigma_m^2}\right) - \frac{1}{2}\log_2\left(1+\frac{P}{\sigma_w^2}\right)\right]^+, \tag{A III-1}$$

$$C_{s,R} = \left[\log_2\left(1+\frac{P|h_m|^2}{\sigma_m^2}\right) - \log_2\left(1+\frac{P|h_w|^2}{\sigma_w^2}\right)\right]^+, \tag{A III-2}$$

where P is the transmitted power, σ_m and σ_w are the noise power of the main channel and wiretap channel. h_m and h_w are the Rayleigh fading coefficients of main channel and wiretap channel respectively. $[x]^+ = \max\{0,x\}$. Also, the received signal-to-noise ratio (SNRs) at Bob and Eve are defined as $\gamma_m = \frac{P|h_m|^2}{\sigma_m^2}$ and $\gamma_w = \frac{P|h_w|^2}{\sigma_w^2}$, respectively.

In Fig. III-2, an average secrecy capacity of Rayleigh fading channel is compared (equation (A III-2)) with that of Gaussian wiretap channel (equation (A III-1)). Strikingly, one can observe

that the secrecy capacity over Rayleigh fading channels is higher than that of an AWGN channel, in other words, we can use the fading property of the physical layer channel to decrease the SNR of wiretap channel. Besides using the fading characteristics of wireless channel, many other methods are applied to improve the secrecy performance of the wireless communication systems. All the existing physical layer security methods in Shiu *et al.* (2011) are classified into five major approaches: theoretical secrecy capacity, multiple-input-multiple-output (MIMO) channel, coding schemes (channel coding and network coding), power allocation, and signal design (artificial noise). Additionally, cooperative relay Han *et al.* (2015); Wang *et al.* (2013a); Chen *et al.* (2013), cooperative jamming Ibrahim *et al.* (2015) and energy harvesting Xing *et al.* (2014) are other useful methods. Among the aforementioned methods, cooperative jamming is a promising technique and has attracted significant attention. It was originally proposed for a multiple access wiretap channel, where multiple legitimate users wish to have simultaneous secure communications with an intended receiver in the presence of an eavesdropper.

3.2 Cooperative jamming

Cooperative jamming is a special technique where artificial noise is introduced by a helpful interferer to confuse the eavesdropper.

In the following section, we will introduce the cooperative jamming techniques which are used to enhance the physical layer security. To improve the secrecy capacity, we should either increase the legitimate receiver's SNR or decrease the eavesdropper's SNR. A natural approach by which to achieve the latter (decreasing the eavesdropper's SNR) is to introduce interferers into the system.

3.3 Artificial Jamming Signals types

Cooperative jamming depends on creating the interference at the eavesdropper's side, many artificial jamming signals are used and could be divided into four categories Long *et al.* (2014):

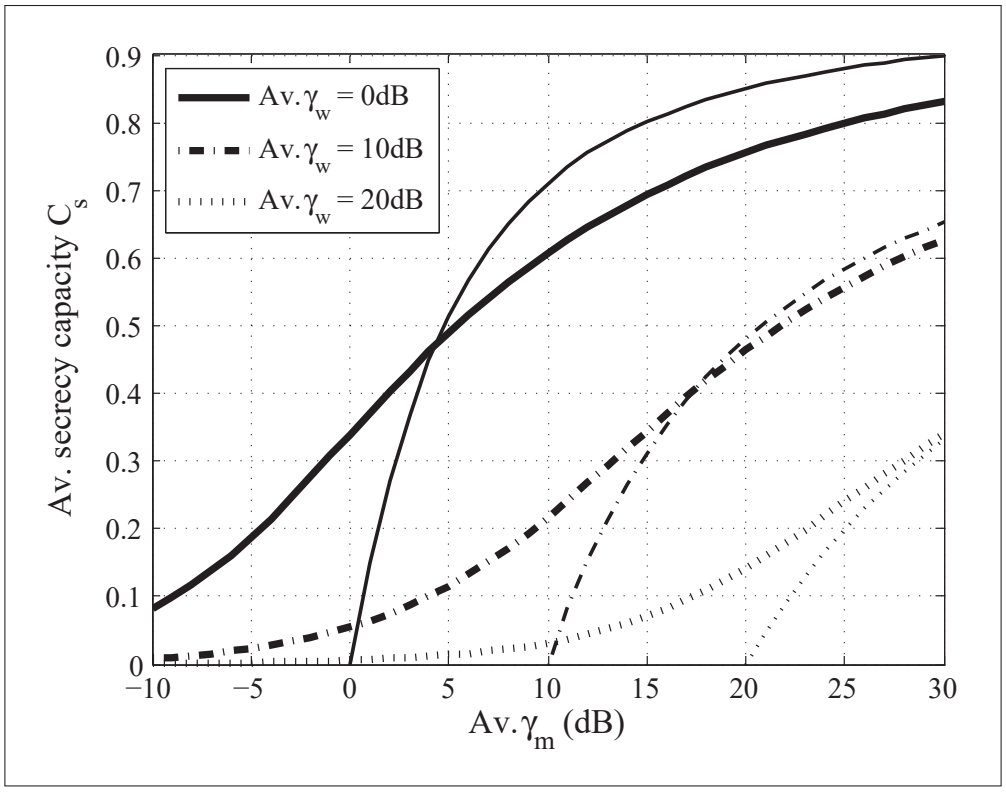


Figure-A III-2 Normalized average secrecy capacity versus $\overline{\gamma}_m$, for selected values of $\overline{\gamma}_w$. The thicker lines correspond to the normalized average secrecy rate capacity of Rayleigh fading channel while the thinner lines correspond to the secrecy capacity of a Gaussian wiretap channel

1. Gaussian noise: which is the same as the additive noise at the receiver Bassily & Ulukus (2013); He & Yener (2013); Zhang *et al.* (2011).

2. Jamming signals which are priory known at legitimate receivers, which has an impact only on the eavesdropper's performance. This type of signals is better than the previous one because the jamming signals don't affect the legitimate receiver Long *et al.* (2013); Dong *et al.* (2011).

3. Random codewords of a public codebook which is known by all the nodes including the eavesdroppers, so the legitimate receiver has the ability to decode and cancel the jamming signals, even though it requires a complicated self-interference cancellation receiver to decode the codewords Pierrot & Bloch (2011).

4. Useful signals for the other legitimate nodes; like the downlink and the uplink of the neighbouring cells Popovski & Simeone (2009), signals of multiple simultaneous source-destination pairs Sheikholeslami *et al.* (2012), or signals of the invited cognitive ratio users Stanojev & Yener (2011) and Stanojev & Yener. (2011), this type is difficult to apply because of the change of the multiple transmission pairs.

Many applications are used in conjunction with the cooperative jamming strategy to enhance the performance and increase the security, these include the usage of multiple antennas, beamforming, game theory, and power allocation methods.

4. Application of cooperative jamming

4.1 Cooperative Jamming with Multiple Antennas and Beamforming

Many works apply multiple antennas method with cooperative jamming technique to enhance the physical layer securityYang *et al.* (2013); Zhang *et al.* (2015); Li *et al.* (2014a); Wang *et al.* (2014b); Banawan & Ulukus (2014); Xing *et al.* (2014); Vishwakarma & Chockalingam (2014). The authors in Yang *et al.* (2013) assume a scenario that the base station has to send multiple independent data streams to multiple legitimate users; during the transmission, many eavesdroppers with multiple antennas have interests in the transmission stream of the base station. The eavesdroppers may collude or not, and maximize the signal-to-interference-plus-noise ratio (SINR) of the desired streams using the beamforming method. The cooperative jammer will work on keeping the SINR at the eavesdroppers below a certain threshold level to guarantee a confidential transmission between the base station and the legitimate users. Another scenario in Li *et al.* (2014a) studies the Gaussian wiretap channel's secrecy capacity aided by an external jammer. Each of the receiver and the transmitter has a single antenna, while the jammer and the eavesdropper are equipped with multiple antennas. The authors in Wang *et al.* (2014b) reveal a scenario for secure transmission within a two-hop amplify-and-forward relay network scheme, such that for large number of antennas at the source, the ergodic

secrecy capacity (ESC) is independent of the number of antennas; whereas, for a large number of antennas at the destination, the ESC is dependent on the number of antennas.

Beamforming is a very efficient method also when it is used with the cooperative jamming technique. However, these two techniques are adopted separately in most worksWang *et al.* (2013a); Tran & Kong (2014); Wang *et al.* (2013b); Han *et al.* (2015); Vishwakarma & Chockalingam (2014). In Wang *et al.* (2013a), a scheme with joint cooperative jamming and beamforming is proposed to enhance the security of a cooperative relay network, where part of the nodes uses a distributed beamforming mechanism while the others jam the eavesdropper simultaneously. In Tran & Kong (2014), another scheme of using the beamforming is proposed; by preventing the eavesdroppers from using the beamformers to suppress the jamming signals. It uses also two orthogonal dimensions for transmitting and receiving signals. A hybrid cooperative jamming and beamforming scheme is proposed in Wang *et al.* (2013b) also; the idea is in both cooperative transmission phases, some intermediate nodes relay the signals to the legitimate receivers by adopting the beamforming distribution, while, simultaneously, the other nodes jam the eavesdropper, which eventually leads in protection of the transmitted data. The authors in Han *et al.* (2015) develop an optimal relay assignment algorithm to solve the secrecy capacity maximization problem, and a smart jamming algorithm is proposed to increase the secrecy capacity of the system.

4.2 Cooperative jamming with Power Allocation method

Since the system's performance in cooperative jamming depends highly on the jamming strategy as well as the power level of the jamming Park *et al.* (2013), three power allocation strategies are derived in Park *et al.* (2013) to minimize the outage probability of the secrecy rate, besides that, three kinds of jamming power allocation schemes are proposed according to the available channel state information (CSI) at the destination to minimize the outage probability. The authors in Zhang *et al.* (2015) propose another scenario investigates the MISO channels with power splitting scheme used by the legitimate receiver to split the received signal for both information decoding and energy harvesting. Another power allocation method in Long *et al.*

(2014) is analysed in which the source nodes should send jamming signals as a part of their power instead of hiring extra nodes to jam the eavesdropper. Two types of jamming signals are analysed; a priori known jamming signals at the source nodes, and unknown jamming signals at the source nodes. A major finding reported in this work is that, if the jamming signals are known a priori at the source nodes, the secrecy capacity is improved significantly when compared to the scenario in which the jamming signals are unknown at the source nodes. In Yang *et al.* (2014), a linear precoding scheme is utilized at the base station, which exploits transmit diversity by weighting the information stream, this is studied with the cooperative jamming strategy. An optimal solution is obtained when the number of antennas at the friendly jammer is no less than the total number at the eavesdropping antennas. The authors in Wang *et al.* (2015a) propose a sequential parametric convex approximation (SPCA) based algorithms to address the power allocation optimization and maximize the ergodic secrecy rate (ESR) lower bound, and then it is shown that the optimized power allocation tends to allocate more power to the jamming signals to improve the secrecy capacity. An optimal relay selection criterion and power allocation strategy are derived in Wang & Wang (2014) between the jamming signals and the confidential information for the ESR maximization. Another study in Deng *et al.* (2015) shows that a helper node should allocate its power as a jammer or as a helper depending on the locations of the helper and the eavesdropper.

4.3 Jamming Policies

Several policies are proposed for relay selection Liu *et al.* (2015); Sun *et al.* (2015); Hui *et al.* (2015). In Liu *et al.* (2015), four relay selection policies are proposed and compared, namely random relay and random jammer, random jammer and best relay, best relay and best jammer, and best relay and no jammer; and it characterizes the joint impact of the proposed relay selection policies and the interference power constraint on the secrecy performance by deriving new exact closed-form expressions for the secrecy outage probability; it is shown then that the jammer's absence gives rise to the outage saturation phenomenon. Two relay and jammer selection methods are developed in Hui *et al.* (2015) for minimizing the secrecy outage probability; in both these selection methods, each intermediate node knows its own role while the

knowledge of the jammer and relay set is kept secret from all the eavesdroppers. It is shown that maintaining the privacy of the selection result improves greatly the secrecy outage probability performance. This work assumes a decode and forward relay system, in which the source communicates with the destination through many intermediate nodes in the presence of several passive eavesdroppers. The intermediate nodes act as either jammers or as conventional relays to hinder the eavesdroppers from intercepting the signal of interest. The destination broadcasts information that allows the intermediate nodes to determine whether they will serve as relays or jammers, but this information does not allow the eavesdroppers to know the selection result. In Park *et al.* (2013), a scheme is provided which has a destination, relay and a source; the destination starts to send jamming signals towards the eavesdropper while the source is sending the message to the relay, and the destination then removes the jamming noise perfectly via self-interference cancellation at the second phase. Another scheme in Liu *et al.* (2013) is provided; in the first phase, the source transmits the information bearing signal, simultaneously as it cooperates with the destination in jamming the eavesdropper without interference at the relay. In the second phase, a relay is selected optimally, which transmits the decoded source signal, at the same time, this relay cooperates with the source to jam the eavesdropper without creating interference at the destination. The authors in Lin *et al.* (2013a) propose a new transmission scheme, where the relaying group and the jamming group are constructed together, this scheme enables to block the eavesdroppers simultaneously and further increase the signal-to-noise ratio at the destination. In Chen *et al.* (2013), attack strategies are investigated in a multi-relay network that consists of both malicious and cooperative relays, where the malicious relays are given the freedom to listen to the source in the first phase (so that they can send interfering signals in the second phase), or to directly emit jamming signals in both phases. Subsequently, it is shown that the malicious relays should attack in both phases rather than just listening in the first phase and attack in the second phase. On the other hand, the opportunistic cooperative jamming and the opportunistic relay chatting schemes are compared in Ding *et al.* (2011). It is shown that the chatting scheme is better for implementing the relay nodes to jam the eavesdropper in the both phases comparing with cooperative jamming scheme in which only the eavesdropper jams in the first phase.

Moreover, jamming policies using game theory methods are proposed in Fakoorian & Swindlehurst (2013); Chen *et al.* (2013); Stanojev & Yener (2013); Li *et al.* (2014b). In Fakoorian & Swindlehurst (2013), a scheme of two user multiple-input-single output Gaussian interference channel is considered, where each transmitter aims to maximize the difference between its secrecy rate and the other's secrecy rate, in this scheme, the weaker link tries to minimize the extra secrecy rate of the other transmitter, while the transmitter with the stronger link tries to maximize it. This paper uses Nash equilibrium strategy as a solution in its scheme. A multi-relay network is considered in Chen *et al.* (2013) that consists of both malicious and cooperative relays, and applies Nash equilibrium game strategy on its scheme, by modelling the cooperative relays set and the malicious relays set as two players in a zero sum game with the maximum achievable rate as the utility. The authors in Stanojev & Yener (2013) propose another game-theoretic model, Stackelberg game, with the legitimate parties being spectrum owners acting as a game leader, and the set of the assisting jammers which are constituting the follower. It shows that when the potential jammers' number increases, utility of a chosen jammer for any scheme will start to decrease as the legitimate parties can be more aggressive when leading the game. In Li *et al.* (2014b), a smart jammer can quickly learn the transmission strategies of the legitimate transmitters, then he would adjust his strategy to damage the legitimate transmission. Meanwhile, the transmitters are aware of the existence of the smart jammer. This anti-jamming scenario is modeled as a Stackelberg game, where the leader is the source node and the follower is the jammer. It is shown that the optimal power control strategies obtained from the Stackelberg equilibrium game can decrease the damage caused by the jammer.

5. Conclusion

Unlike its conventional applications, jamming techniques are used to enhance the security of transmission in wireless communication networks. In this paper, we have surveyed the different challenges related to the physical layer security in wireless networks and we developed a literature review of the different jamming techniques within the existing recent literature with their advantages and disadvantages.

Based on this review we can conclude that there are still many issues to be resolved around jamming techniques applications such as communication architectures for energy harvesting, protocols, and interference management.

Acknowledgment

This work has been supported by the ETS' research chair of physical layer security in wireless networks.

APPENDIX IV

SECRECY ANALYSIS OF COOPERATIVE NETWORK WITH UNTRUSTWORTHY RELAYS USING LOCATION-BASED MULTICASTING TECHNIQUE

Michael Atallah[1], and Georges Kaddoum[1]

[1] Department of Electrical Engineering, École de Technologie Supérieure,
1100 Notre-Dame Ouest, Montréal, Québec, Canada H3C 1K3

Paper published in *5th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)* , November 2017.

1. Abstract

This paper studies the secrecy capacity scaling in an Amplify-and-Forward (AF) dual-phase large network containing K relays. In our model, part of these K relays are assumed to be potential eavesdroppers. Before transmitting the message in the first phase, the multi-antennas source divides it to partial messages and multicasts each part to a different disjoint sector. During the second phase, the K relays use the distributed beamforming (DBF) technique to retransmit the message to the destination. We investigate the ergodic secrecy capacity considering two different behaviours of the untrustworthy relays; the passive behaviour, when the untrustworthy relays work separately from each other to intercept the signal, and the aggressive one, when the untrusted relays collaborate to hijack the message. As demonstrated, our location-based multicasting scenario is significantly increasing the security compared to the recent works that employ broadcasting schemes. Additionally, it also increases the secrecy capacity scaling remarkably. Finally, our analytical derivations are confirmed by the simulation.

Keywords: Physical layer security, location-based multicasting, amplify and forward, distributed beamforming, secrecy capacity.

2. Introduction

Over the last few years, security has always been considered a critical issue in wireless networks' design. The vital concept of the secrecy capacity is built on whether increasing the legitimate channel capacity or decreasing the capacity of the illegitimate channels, which is attainable via the usage of the dynamic nature of the wireless channels Gopala *et al.* (2008). Therefore, many contributions have been recently accomplished to escalate the secrecy capacity by associating advanced techniques in wireless communications, such as multiple antenna schemes, game theory techniques, beamforming and power allocation methods Atallah *et al.* (2015). Wireless security appears to be a crucial matter in today's communication systems as both the diversity and the number of users in wireless networks keep growing. According to these security challenges, leading researchers are seeking more information theoretical methods to accomplish almost perfect security in wireless channels. With this approach, considerable efforts have been made by authors in Gopala *et al.* (2008); Bloch *et al.* (2008) to develop information-theoretical security, which raises the opportunity to have a secure communication in an existence of eavesdroppers. The foundations of information-theoretic security were led by Wyner (1975); Leung-Yan-Cheong & Hellman (1978). Obviously, many facts haven't been considered in this domain's primal works, such as the wireless channels that are susceptible to fading or that the communicating devices constitute *networks* out of *unknown topology*. A few decades later, channel propagation effect has been considered in Gopala *et al.* (2008); Bloch *et al.* (2008). In this direction, the authors in Gopala *et al.* (2008) investigated the secrecy capacity of wireless fading channels considering the channel state information (CSI). The authors in Bloch *et al.* (2008) found the average secrecy capacity and the outage probability expressions of quasi-static fading channels for both the perfect and the imperfect CSI scenarios. Considering random topologies, the secrecy capacity has been investigated in Haenggi (2008). Following this direction, the researchers in Koyluoglu *et al.* (2012) studied the secrecy capacity scaling laws. The secrecy capacity of unicast links with the existence of multiple wiretappers was investigated in Vuppala & Abreu (2013), where the transmission to the k-th legitimate node was based on the order of the distance between the source and the destination. Henceforth, relay aided transmission has been taken into consideration as an effective way to escalate the transmission reliability, throughput and coverage probability in the literatureLaneman *et al.*

(2004); Lin *et al.* (2014). Several strategies have been studied in literature for relay aided transmission, particularly amplify and forward, decode and forward and demodulate and forward. As the nature of the wireless medium previously explained, some of the relays could possibly be eavesdroppers within the transmission area. In Kim *et al.* (2015), the secrecy capacity scaling and the diversity order were calculated with the presence of potential passive eavesdroppers with the destination-assisted jamming, in which the destination transmits jamming messages to the relays. However, in Atallah & Kaddoum (2016), the authors went deeper to find the capacity scaling in a worse scenario; the possibility that potential aggressive eavesdroppers could cooperate together to intercept the received message.

In this paper, we introduce a new system model that remarkably improves the security, especially compared to the recent works Kim *et al.* (2015); Atallah & Kaddoum (2016). We propose a two-hop AF relaying model. It is also assumed that the source divides its message to parts and sends each part to a different directional antenna in which each element covers a disjoint area. Whereas in the second phase, using the distributed beamforming technique (DBF), the relays retransmit the received message towards the destination. This DBF method is proved to be very efficient compared to other methods like opportunistic relaying technique Kim *et al.* (2015); Atallah & Kaddoum (2016). Again, we assume two types of relays, trustworthy and untrustworthy. Two kinds of untrusted relays are studied; passive, where each relay tries to intercept the message individually, and aggressive, where each untrustworthy relay sends its received signal to a concurrent eavesdropper which in its turn aggregates the received signals to decipher the message. The main contributions presented in this paper are finding the ergodic secrecy capacity under location-based multicasting scenario in two cases:

- The potential untrustworthy relays are passive where they work apart to interpret the message.

- The potential untrustworthy relays are aggressive by collaborating between each other to hijack the message.

Notations: $\overline{X}$ and $E[X]$ denote the mean expectation of a random variable (r.v.) X. Furthermore, $[A]^+$ denotes $\max\{A,0\}$. For a r.v. X, the notation $X \sim \mathcal{N}_c(a,b)$ denotes that X is a complex Gaussian r.v. with mean a and variance b. $X \overset{w.p.1}{\rightarrow}$ denotes the convergence with probability 1.

3. SYSTEM MODEL

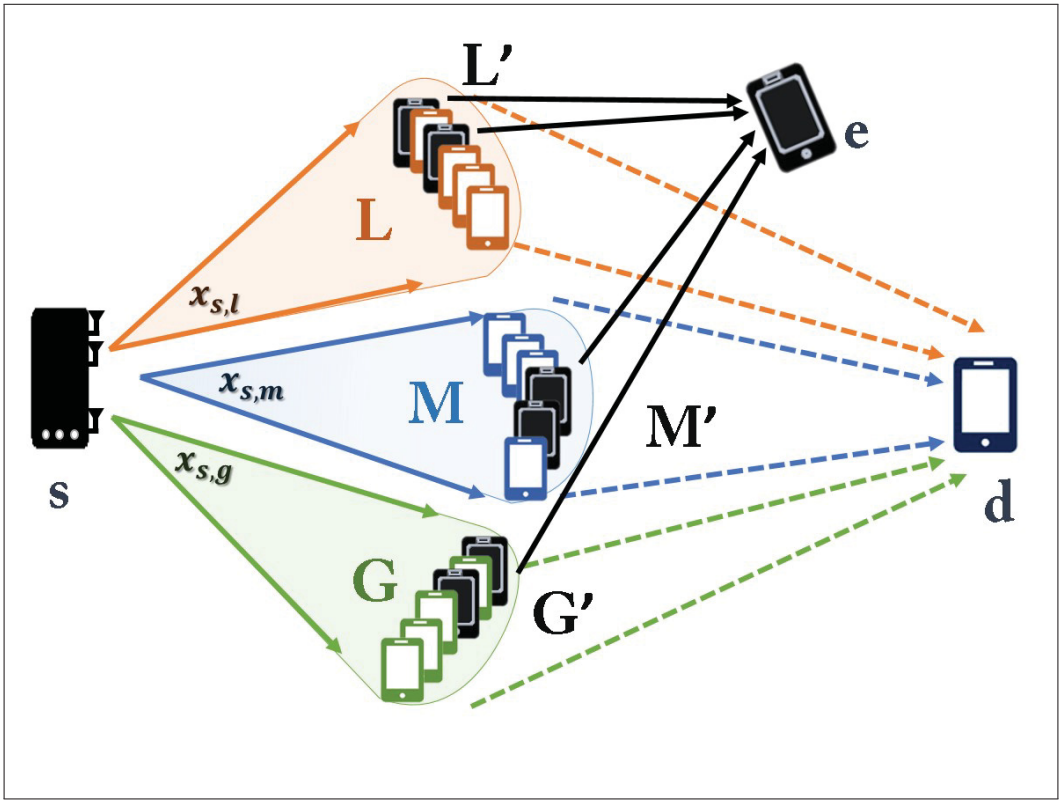


Figure-A IV-1 System model. The source s sends its message to the destination d by multicasting its partial signals in the first hop, $x_{s,l}, x_{s,m}$ and $x_{s,g}$, towards different sections L,M and G. In the second hop, the relays retransmit the signals to the destination d using beamforming technique DBF

Consider a two-hop wireless network consisting of K relays with a destination d and a multi-antennas source s. In our network, as shown in Fig. IV-1, each relay has a single antenna operating in a half-duplex mode. In addition, we assume that there is no direct link between the source s and the destination d, i.e. all the transmitted information must be forwarded by relays.

In our analysis, the channels are assumed to be reciprocal frequency-flat block-fading with the coefficient between nodes i and j being denoted by $h_{i,j}$ and being modelled as a Gaussian r.v. $h_{i,j} \sim \ln \mathcal{N}(\mu_{ij}, \sigma_{ij}^2)$ where $(i, j \in \{s,k,d\})$. The channel gains $\left|h_{s,k}\right|^2$ and $\left|h_{k,d}\right|^2$ are independent and exponentially distributed r.v.'s. We assume that the noise variance N_0 is the same in the first and the second phase, and the CSI is known by the receiving nodes. Instead of broadcasting the message in the first phase, the source will divide the signal into multiple parts and multicast each part to a specified sector, as demonstrated in Fig. IV-1. Each section will be denoted by the total number of the relays that it has. Without loss of generality, we study the case where the source divides its message into three partial messages and sends them to three different disjoint areas, due to the use of directional antennas. This given configuration is used to make the derivation easy to follow. Therefore, the general form of the secrecy capacity using multicasting with many partial messages is given at the end of the analysis part. As shown in Fig. IV-1, the first, the second and the third sections will be denoted by L, M and G respectively. We will use the same letters L, M and G to denote the total number of relays in its corresponding section. Hence, $K = L + M + G$. We will also denote the partial message by $x_{s,r}$, when it is sent to the section R, where $r \in \{l,m,g\}$, $R \in \{L,M,G\}$ and $1 \leq r \leq R$. The received signal at the rth relay is expressed by

$$y_r = h_{s,r}\sqrt{P_{s,r}}x_{s,r} + n_{s,r}, \tag{A IV-1}$$

where $n_{s,r}$ is a complex additive white Gaussian noise at the rth relay with zero mean and variance N_0. The transmitted powers of the source are denoted by $P_{s,r}$. It is assumed that at the rth relay, the received signal-to-interference-plus-noise ratio SINR would be

$$\gamma_r = \rho_{s,r}\left|h_{s,r}\right|^2, \tag{A IV-2}$$

where the signal to noise ratio is denoted by $\rho_{s,r} \triangleq P_{s,r}/N_0$, $r \in \{l,m,g\}$. We will assume that the signal to noise ratios are equal $\rho \triangleq \rho_{s,r}$, but the extension using different $\rho_{s,r}$ values is straightforward. In the following subsections, we will find the secrecy capacity scaling for our system in two cases; when there are untrusted relays trying to intercept their received messages

individually, and when these untrusted relays work together to intercept the message. We will later use L', M' and G' to denote the total number of the untrustworthy aggressive relays in each of L, M and G sectors respectively, where $L > L', M > M'$ and $G > G'$.

4. Secrecy Capacity for Passive Untrustworthy relays

In this case, each untrustworthy passive relay works individually to intercept the received message without any kind of cooperation with any other relays. The received SINR at any potential untrusted passive relay would be given by

$$\gamma_k = \rho_{s,k} \left| h_{s,k} \right|^2, \tag{A IV-3}$$

Considering that each relay has just a part of the message, and that the message is already encrypted in the upper layers before it is divided to partial messages, its interpretation is impossible considering the other parts are missing.

Using the distributed beamforming strategy DBF in the second phase, the retransmitted signal by the rth relay is $x_r = a_r y_r$. The normalized amplifying coefficient a_r for the rth relay is as follows

$$a_r = \frac{1}{\sqrt{\rho_{s,r} \left| h_{s,r} \right|^2 + N_0}}. \tag{A IV-4}$$

However, the destination can receive a signal either from a trustworthy or untrustworthy relay. The received signal at the destination, from a random relay, can be expressed as

$$y_d = h_{r,d} a_r y_r + n_d \,. \tag{A IV-5}$$

where n_d is a complex additive white Gaussian noise AWGN with zero mean and variance N_0 at the destination. The received SINR from the rth relay becomes

$$\gamma_r = \frac{\rho_{s,r}\left|h_{s,r}\right|^2 \rho_{r,d}\left|h_{r,d}\right|^2}{\rho_{s,r}\left|h_{s,r}\right|^2 + \rho_{r,d}\left|h_{r,d}\right|^2 + 1}, \tag{A IV-6}$$

for $r \in \{l, m, g\}$. The channel capacity from the source to the destination would be given by

$$C_d = \frac{1}{2}\log\left(1 + \sum_{l=1}^{L}\gamma_l\right) + \frac{1}{2}\log\left(1 + \sum_{m=1}^{M}\gamma_m\right) + \frac{1}{2}\log\left(1 + \sum_{g=1}^{G}\gamma_g\right). \tag{A IV-7}$$

whereas C_w is the secrecy capacity between a potential untrusted passive relay and the source, and it is given as follows

$$C_w = \frac{1}{2}\log\left(1 + \max_k\left(\rho_{s,k}\left|h_{s,k}\right|^2\right)\right). \tag{A IV-8}$$

We consider the maximum SINR in Eq. (A IV-8) to evaluate the worst case in which the eavesdropper could obtain the maximum amount of information. From Eq.(A IV-7) and Eq. (A IV-8), the ergodic secrecy capacity could be written as

$$\begin{aligned} \overline{C}_P &= E\{C_P\} \\ &= E\left\{[C_d - C_w]^+\right\} \\ &\overset{(a)}{\geq} [E\{C_d\} - E\{C_w\}]^+, \end{aligned} \tag{A IV-9}$$

where C_P is the instantaneous secrecy capacity.

(a) follows from Jensen's inequality

$$E\{\max(X_1, X_2)\} \geq \max(E\{X_1\}, E\{X_2\}). \tag{A IV-10}$$

For $R \to \infty$, γ_r in Eq.(A IV-6) satisfies the *Kolmogorov conditions i.e.*

$$\sum_{r=1}^{R} \frac{\mathrm{VAR}\left[\gamma_r\right]}{r^2} < \infty, \tag{A IV-11}$$

and

$$\mu_r = \frac{1}{R} \sum_{r=1}^{R} E\left[\gamma_r\right] < \infty, \tag{A IV-12}$$

are true for any finite ρ Bolcskei *et al.* (2006) where $R \in \{L, M, G\}$.

Thus, we can apply the following theorem [15, Theorem 1.8.D] :

$$\sum_{r=1}^{R} \frac{\gamma_r}{R} - \sum_{r=1}^{R} \frac{E\left[\gamma_r\right]}{R} \overset{w.p.1}{\to} 0. \tag{A IV-13}$$

Therefore, $\gamma_r \overset{w.p.1}{\to} R\mu_r$ and

$$E\left\{\frac{1}{2}\log\left(1 + \sum_{r=1}^{R} \gamma_r\right)\right\} \sim \frac{1}{2}\log\left(R\right). \tag{A IV-14}$$

Fact 1: $\max\limits_{k}\left(\rho_{s,k}\left|h_{s,k}\right|^2\right)$ behaves like $\rho_{s,k}\log\left(K\right) + \mathscr{O}\left(\log\log\left(K\right)\right)$ for $K \to \infty$ and limited ρ [16, Lemma 4].

From Fact 1 and Eq.(A IV-8), $\overline{C_w}$ will be as follows

$$\overline{C_w} \sim \frac{1}{2}\log\log\left(K\right). \tag{A IV-15}$$

The secrecy capacity in Eq.(A IV-9) can be represented by

$$\overline{C}_P \geq \frac{1}{2}\log\left(L\right) + \frac{1}{2}\log\left(M\right) + \frac{1}{2}\log\left(G\right) - \frac{1}{2}\log\log\left(K\right),$$

$$\overline{C}_P \gtrsim \frac{1}{2}\log(LMG). \tag{A IV-16}$$

Since the relays are half-duplex, we use the rate-loss factor value of 1/2.

5. Aggressive Untrustworthy Relays

The aggressive untrustworthy relays are the relays that collaborate together by retransmitting their received signals to a one wiretapper to decipher the message. The wiretapper could be internal *i.e.* one of the relays, or external. In our scheme, we will assume that the wiretapper e is external, as shown in Fig. IV-1. We will denote the total number of all the untrusted aggressive relays in the network by U. We will assume that these untrusted aggressive relays are distributed equally between all the sectors L, M and G. From Fig. IV-1, L', M' and G' denote the total number of the untrustworthy aggressive relays in each of L, M and G sectors, respectively.

The retransmitted signal from each untrusted aggressive relay towards the wiretapper e will be denoted by $y_{r'}$ where $r' \in \{l', m', g'\}$. Hence, the received signal at the wiretapper e from each of the untrustworthy aggressive relays would be

$$y_e = h_{r',e} a_{r'} y_{r'} + n_e, \tag{A IV-17}$$

where $h_{r',e}$ is the channel coefficient between an untrustworthy relay and the wire-tapper, n_e is a complex AWGN with zero mean and variance N_0 at the wire-tapper. The received SINR at the wire-tapper becomes

$$\gamma_{r'} = \frac{\rho_{s,r'} \left|h_{s,r'}\right|^2 \rho_{r',e} \left|h_{r',e}\right|^2}{\rho_{s,r'} \left|h_{s,r'}\right|^2 + \rho_{r',e} \left|h_{r',e}\right|^2 + 1}, \tag{A IV-18}$$

The instantaneous channel capacity at the wiretapper will be given by

$$C_e = \frac{1}{2}\log\left(1 + \sum_{l'=1}^{L'} \gamma_{l'}\right) + \frac{1}{2}\log\left(1 + \sum_{m'=1}^{M'} \gamma_{m'}\right) + \frac{1}{2}\log\left(1 + \sum_{g'=1}^{G'} \gamma_{g'}\right). \tag{A IV-19}$$

Consequently, the ergodic secrecy capacity with the presence of the aggressive relays could be written as

$$\overline{C}_A = E\{C_A\} = E\left\{[C_d - C_e]^+\right\} \tag{A IV-20}$$

$$\overset{(a)}{\geq} [E\{C_d\} - E\{C_e\}]^+, \tag{A IV-21}$$

where (a) follows from the fact that $E\{\max(X_1, X_2)\} \geq \max(E\{X_1\}, E\{X_2\})$. By applying the steps followed for the Eq.(A IV-14) in the previous subsection, the secrecy capacity scaling for untrusted aggressive relays will take the form

$$\overline{C}_A = \frac{1}{2}\log(L) + \frac{1}{2}\log(M) + \frac{1}{2}\log(G) -$$

$$\frac{1}{2}\log(L') + \frac{1}{2}\log(M') + \frac{1}{2}\log(G')$$

$$= \frac{1}{2}\log(LMG) - \frac{1}{2}\log(L'M'G')$$

$$\overline{C}_A = \frac{1}{2}\log\left(\frac{LMG}{L'M'G'}\right), \tag{A IV-22}$$

Without loss of generality, we will assume that

$$\frac{K}{U} = \frac{L}{L'} = \frac{M}{M'} = \frac{G}{G'} = T. \tag{A IV-23}$$

By compensating Eq.(A IV-23) in Eq.(A IV-22), the secrecy capacity would be

$$\overline{C}_A = \frac{1}{2}\log(T^3). \tag{A IV-24}$$

Then, by generalizing Eq.(A IV-24) to multicast V partial messages towards V different sections instead of three, the secrecy capacity scaling will be expressed as

$$\overline{C}_A = \frac{1}{2}\log\left(T^V\right) = \frac{V}{2}\log\left(T\right), \tag{A IV-25}$$

$$\overline{C}_A = \frac{V}{2}\log\left(\frac{K}{U}\right). \tag{A IV-26}$$

6. Simulation results

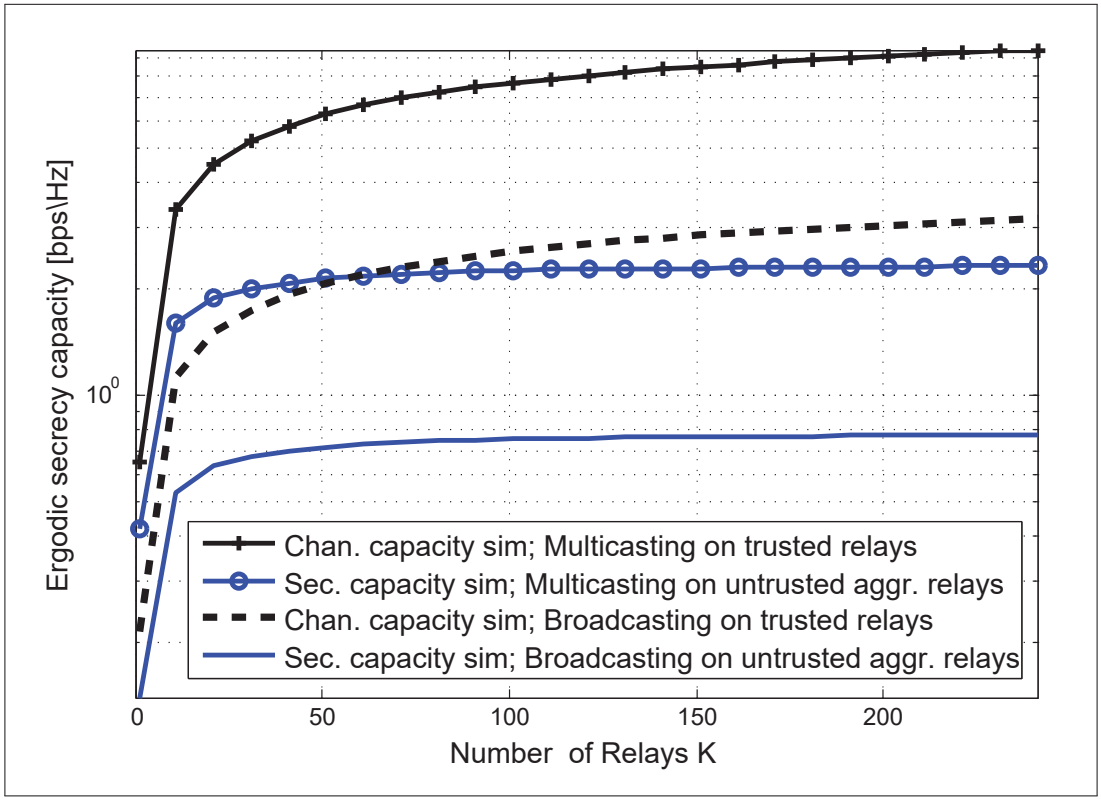


Figure-A IV-2 Ergodic secrecy capacity: $\rho \triangleq \rho_{s,k} = \rho_{k,d} = \rho_{k,e} = 5dB$, $\left|\overline{h_{s,k}}\right|^2 = \left|\overline{h_{k,e}}\right|^2 = \left|\overline{h_{k,d}}\right|^2 = 1$ and $U = \frac{1}{3}K$

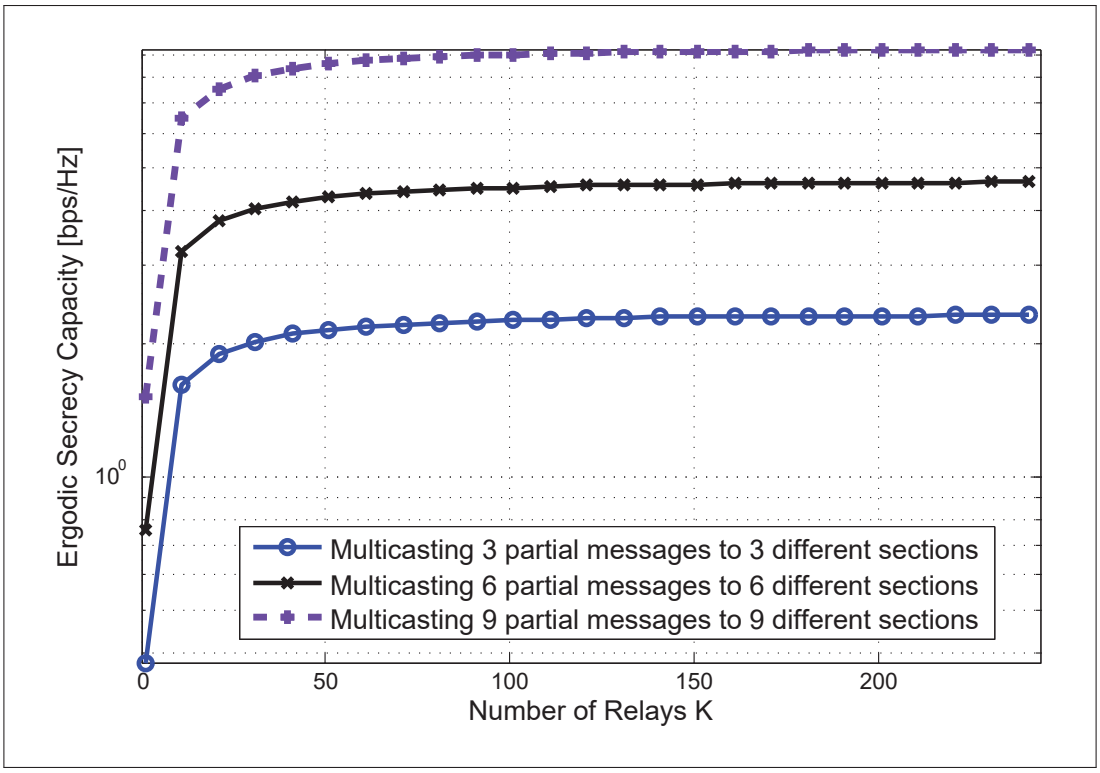


Figure-A IV-3 Ergodic secrecy capacity when using Location-Besed Multicasting technique with the presence of untrusted aggressive relays for different values of V which is identified in Eq.(A IV-26): $\rho \triangleq \rho_{s,k} = \rho_{k,d} = \rho_{k,e} = 5dB$, $\left|\overline{h_{s,k}}\right|^2 = \left|\overline{h_{k,e}}\right|^2 = \left|\overline{h_{k,d}}\right|^2 = 1$ and $U = \frac{1}{3}K$

Assuming that $\rho \triangleq \rho_{s,k} = \rho_{k,d} = \rho_{k,e} = 5dB$, $\left|\overline{h_{s,k}}\right|^2 = \left|\overline{h_{k,e}}\right|^2 = \left|\overline{h_{k,d}}\right|^2 = 1$ and $U = \frac{1}{3}K$, in Fig.IV-2, we do the performance comparison between our scenario, where the source multicasts each part of the message, and the other scenarios, from recent studies, in which the source just broadcasts the signal Kim *et al.* (2015); Atallah & Kaddoum (2016). The results, which are simulated in Matlab, show the improvement in the secrecy capacity of our scenario compared to the broadcasting one. For the passive untrusted relays' case, considering that the message is already encrypted in the upper layers before dividing it to partial messages, the secrecy capacity is not affected as long as the eavesdroppers cannot have an access to the other parts of the message, which gives a lot of enhancements in the security perspective and eliminates the need for some of the other security solutions like cooperative jamming. On the other hand, for aggressive eavesdroppers cooperating between each other to assemble the message's parts,

the secrecy capacity is considerably enhanced a lot, as a result of ameliorating the channel capacity from $\frac{1}{2}\log(K) = \frac{1}{2}\log(L+M+G)$ in Kim *et al.* (2015),Atallah & Kaddoum (2016) to $\frac{1}{2}\log(LMG)$ as shown in our study. In Fig.3.4, we simulate the ergodic secrecy capacity with the presence of untrustworthy aggressive relays when V, identified in Eq.(A IV-26), takes the values $3, 6$ and 9. As shown in Fig.3.4, the more we multicast partial messages towards different sectors, the more the security is enhanced in our network.

7. Conclusions

In this paper, we have investigated the secrecy capacity scaling in large networks within two contrasting roles of potential eavesdroppers; the passive and the aggressive one. We showed that using our location-based multicasting technique will not only increase the secrecy capacity in the presence of the aggressive relays, but prohibit the individual attempts, by passive eavesdroppers to intercept the message as well. In addition, our proposed scheme is less energy consuming compared to some techniques in physical layer security like cooperative jamming methods. Besides, it does not need complicated calculations or advanced security algorithms, which opens the door for it to be applied in Internet of Things world.

BIBLIOGRAPHY

A. El-Malek, A. H., Salhab, A. M., Zummo, S. A. & Alouini, M.-S. (2017). Power allocation and cooperative jamming for enhancing physical layer security in opportunistic relay networks in the presence of interference. *Trans. Emerging Telecommun. Technol.*, 28(11), e3178. doi: 10.1002/ett.3178. e3178 ett.3178.

Akhlaghpasand, H., Björnson, E. & Razavizadeh, S. M. (2019). Jamming Suppression in Massive MIMO Systems. *IEEE Trans. Circuits Syst. II, Exp. Briefs*, 1-1. doi: 10.1109/TCSII.2019.2902074.

Akyildiz, I. F., Su, W., Sankarasubramaniam, Y. & Cayirci, E. (2002). Wireless sensor networks: a survey. *Computer networks*, 38(4), 393–422.

Alibeigi, M. & Taherpour, A. (2019). Optimisation of secrecy rate in cooperative device to device communications underlaying cellular networks. *IET Commun.*, 13(5), 512-519. doi: 10.1049/iet-com.2018.5507.

Alouini, M. S. & Goldsmith, A. J. (1999). Capacity of Rayleigh fading channels under different adaptive transmission and diversity-combining techniques. 48(4), 1165-1181. doi: 10.1109/25.775366.

Alsaba, Y., Leow, C. Y. & Abdul Rahim, S. K. (2019). Null-Steering Beamforming for Enhancing the Physical Layer Security of Non-Orthogonal Multiple Access System. *IEEE Access*, 7, 11397-11409. doi: 10.1109/ACCESS.2019.2890822.

Arafa, A., Shin, W., Vaezi, M. & Poor, H. V. (2018, Dec). Securing Downlink Non-Orthogonal Multiple Access Systems by Trusted Relays. *IEEE Global Commun. Conf. (GLOBECOM)*, pp. 1-6. doi: 10.1109/GLOCOM.2018.8648037.

Atallah, M. & Kaddoum, G. (2016). Secrecy Capacity Scaling With Untrustworthy Aggressive Relays Cooperating With a Wire-Tapper. *IEEE Wireless Commun. Lett.*, 5(4), 376-379. doi: 10.1109/LWC.2016.2561285.

Atallah, M. & Kaddoum, G. (2017, Aug). Secrecy Analysis of Cooperative Network with Untrustworthy Relays Using Location-Based Multicasting Technique. *2017 5th Intern. Conf. on Future Internet of Things and Cloud Workshops (FiCloudW)*, pp. 206-210. doi: 10.1109/FiCloudW.2017.74.

Atallah, M. & Kaddoum, G. (2019). Secrecy Analysis in Wireless Network with Passive Eavesdroppers by Using Partial Cooperation. *IEEE Trans. Veh. Technol.*, 1-1. doi: 10.1109/TVT.2019.2913934.

Atallah, M. & Kaddoum, G. (2019). Design and Performance Analysis of Secure Multicasting Cooperative Protocol for Wireless Sensor Network Applications. *IEEE Wireless Commun. Lett.*

Atallah, M., Kaddoum, G. & Kong, L. (2015, Oct). A Survey on Cooperative Jamming Applied to Physical Layer Security. *2015 IEEE Int. Conf. Ubiquitous Wireless Broadband (ICUWB),*, pp. 1-5. doi: 10.1109/ICUWB.2015.7324413.

Atallah, M., Alam, M. S. & Kaddoum, G. (2019). Secrecy analysis of wireless sensor network in smart grid with destination assisted jamming. *Institution of Eng. Technol.*, -(0). Consulted at https://digital-library.theiet.org/content/journals/10.1049/iet-com.2018.5344.

Badia, L. & Gringoli, F. (2019). A Game of One/Two Strategic Friendly Jammers Versus a Malicious Strategic Node. *IEEE Netw. Lett.*, 1(1), 6-9. doi: 10.1109/LNET.2019.2893536.

Baig, Z. A. & Amoudi, A.-R. (2013). An Analysis of Smart Grid Attacks and Countermeasures. *JCM*, 8, 473-479.

Banawan, K. & Ulukus, S. (2014, Sept.). Gaussian MIMO wiretap channel under receiver side power constraints. *Annu. Allerton Conf. Commun., Control, and Computing (Allerton),*, pp. 183-190. doi: 10.1109/ALLERTON.2014.7028454.

Barros, J. & Rodrigues, M. (2006, July). Secrecy Capacity of Wireless Channels. *IEEE Int. Symp. Inform. Theory.*, pp. 356-360. doi: 10.1109/ISIT.2006.261613.

Bassily, R. & Ulukus, S. (2012). Deaf Cooperation for Secrecy With Multiple Antennas at the Helper. *IEEE Trans. Inform. Forens. Security.*, 7(6), 1855-1864. doi: 10.1109/TIFS.2012.2215325.

Bassily, R. & Ulukus, S. (2013). Deaf Cooperation and Relay Selection Strategies for Secure Communication in Multiple Relay Networks. *IEEE Trans. Signal Process.*, 61(6), 1544-1554. doi: 10.1109/TSP.2012.2235433.

Bloch, M., Barros, J., Rodrigues, M. & McLaughlin, S. (2008). Wireless Information-Theoretic Security. *IEEE Trans. Inform. Theory.*, 54(6), 2515-2534. doi: 10.1109/TIT.2008.921908.

Bloch, M. & Barros, J. (2011). *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press.

Bolcskei, H., Nabar, R., Oyman, O. & Paulraj, A. (2006). Capacity scaling laws in MIMO relay networks. *IEEE Trans. Wireless Commun.*, 5(6), 1433-1444. doi: 10.1109/TWC.2006.1638664.

Chen, H. C., Lin, T. H., Kung, H. T., Lin, C. K. & Gwon, Y. (2012, Oct). Determining RF angle of arrival using COTS antenna arrays: A field evaluation. *MILITARY COMMUN. CONF. MILCOM*, pp. 1-6. doi: 10.1109/MILCOM.2012.6415851.

Chen, J. (2018, Oct). Secure Communication over Interference Channel: To Jam or Not to Jam? *56th Ann. Allerton Conf. Commun. Control, and Computing*, pp. 1120-1127. doi: 10.1109/ALLERTON.2018.8635988.

Chen, M.-H., Lin, S.-C., Hong, Y.-W. & Zhou, X. (2013). On Cooperative and Malicious Behaviors in Multirelay Fading Channels. *IEEE Trans. Inform. Forensics and Security*, 8(7), 1126-1139. doi: 10.1109/TIFS.2013.2262941.

Chen, X., Ng, D. W. K., Gerstacker, W. H. & Chen, H. H. (2017). A Survey on Multiple-Antenna Techniques for Physical Layer Security. *IEEE Commun. Surveys Tuts.*, 19(2), 1027-1053. doi: 10.1109/COMST.2016.2633387.

Cover, T. M. & Thomas, J. A. (2006). *Elements of Information Theory (Wiley Series in Telecommunications and Signal Processing)*. Wiley-Interscience.

Csiszar, I. & Korner, J. (1978). Broadcast channels with confidential messages. *IEEE Trans. Inform. Theory.*, 24(3), 339-348. doi: 10.1109/TIT.1978.1055892.

Cumanan, K., Alexandropoulos, G. C., Ding, Z. & Karagiannidis, G. K. (2017). Secure Communications With Cooperative Jamming: Optimal Power Allocation and Secrecy Outage Analysis. *IEEE Trans. Veh. Technol.*, 66(8), 7495-7505. doi: 10.1109/TVT.2017.2657629.

Dahmane, S., Kerrache, C. A., Lagraa, N. & Lorenz, P. (2017, May). WeiSTARS: A weighted trust-aware relay selection scheme for VANET. *IEEE Intern. Conf. on Commun. (ICC)*, pp. 1-6. doi: 10.1109/ICC.2017.7996451.

Deng, H., Wang, H.-M., Guo, W. & Wang, W. (2015). Secrecy Transmission With a Helper: To Relay or to Jam. *IEEE Trans. Inf. Forensics and Security.*, 10(2), 293-307. doi: 10.1109/TIFS.2014.2374356.

Ding, Z., Leung, K., Goeckel, D. & Towsley, D. (2011). Opportunistic Relaying for Secrecy Communications: Cooperative Jamming vs. Relay Chatting. *IEEE Trans. Wireless Commun.*, 10(6), 1725-1729. doi: 10.1109/TWC.2011.040511.101694.

Do, Q. V., Hoan, T. N. K. & Koo, I. (2019). Optimal Power Allocation for Energy-efficient Data Transmission Against Full-duplex Active Eavesdroppers in Wireless Sensor Networks. *IEEE Sensors J.*, 1-1. doi: 10.1109/JSEN.2019.2904523.

Dong, L., Yousefi'zadeh, H. & Jafarkhani, H. (2011, June). Cooperative Jamming and Power Allocation for Wireless Relay Networks in Presence of Eavesdropper. *IEEE Int. Conf. Commun. (ICC)*, pp. 1-5. doi: 10.1109/icc.2011.5963094.

Dubey, A. & Mallik, R. K. (2015). PLC System Performance With AF Relaying. *IEEE Trans. Commun.*, 63(6), 2337-2345. doi: 10.1109/TCOMM.2015.2427171.

El Shafie, A., Mabrouk, A., Tourki, K., Al-Dhahir, N. & Hamila, R. (2017). Securing Untrusted RF-EH Relay Networks Using Cooperative Jamming Signals. *IEEE Access*, 5, 24353-24367. doi: 10.1109/ACCESS.2017.2768508.

Fakoorian, S. A. A. & Swindlehurst, A. L. (2013). Competing for Secrecy in the MISO Interference Channel. *IEEE Trans. Signal Process.*, 61(1), 170-181. doi: 10.1109/TSP.2012.2223689.

Fang, X., Misra, S., Xue, G. & Yang, D. (2012). Smart Grid - The New and Improved Power Grid: A Survey. *IEEE Commun. Surveys Tuts.*, 14(4), 944-980. doi: 10.1109/SURV.2011.101911.00087.

Felkaroski, N. & Petri, M. (2019, Feb). Secret Key Generation Based on Channel State Information in a mmWave Communication System. *SCC; 12th Int. ITG Conf. Syst. Commun. and Coding*, pp. 1-6. doi: 10.30420/454862049.

Fenton, L. (1960). The Sum of Log-Normal Probability Distributions in Scatter Transmission Systems. *IRE Trans. Commun. Syst.*, 8(1), 57-67.

Ghosh, M. (1996). Analysis of the effect of impulse noise on multicarrier and single carrier QAM systems. *IEEE Trans. Commun.*, 44(2), 145-147. doi: 10.1109/26.486604.

Goel, S. & Negi, R. (2008). Guaranteeing Secrecy using Artificial Noise. *IEEE Trans. Wireless Commun.*, 7(6), 2180-2189. doi: 10.1109/TWC.2008.060848.

Gopala, P. K., Lai, L. & El Gamal, H. (2008). On the Secrecy Capacity of Fading Channels. *IEEE Trans. Inform. Theory.*, 54(10), 4687-4698. doi: 10.1109/TIT.2008.928990.

Guillaume, R., Ludwig, S., Muller, A. & Czylwik, A. (2015, Oct). Secret key generation from static channels with untrusted relays. *IEEE 11th Int. Conf. Wireless and Mobile Comput. Networking and Commun. (WiMob).*, pp. 635-642. doi: 10.1109/WiMOB.2015.7348022.

Gungor, V. C., Lu, B. & Hancke, G. P. (2010). Opportunities and Challenges of Wireless Sensor Networks in Smart Grid. *IEEE Trans. Ind. Electron*, 57(10), 3557-3564. doi: 10.1109/TIE.2009.2039455.

Gungor, V. C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C. & Hancke, G. P. (2011). Smart Grid Technologies: Communication Technologies and Standards. *IEEE Trans. Ind. Informat.*, 7(4), 529-539. doi: 10.1109/TII.2011.2166794.

Guo, H., Yang, Z., Zhang, L., Zhu, J. & Zou, Y. (2017). Joint Cooperative Beamforming and Jamming for Physical-Layer Security of Decode-and-Forward Relay Networks. *IEEE Access*, 5, 19620-19630. doi: 10.1109/ACCESS.2017.2752199.

Haenggi, M. (2008). A Geometric Interpretation of Fading in Wireless Networks: Theory and Applications. *IEEE Trans. Inform. Theory*, 54(12), 5500 - 5510.

Han, B., Li, J., Su, J., Guo, M. & Zhao, B. (2015). Secrecy Capacity Optimization via Cooperative Relaying and Jamming for WANETs. *IEEE Trans. Parallel and Distributed Systems*, 26(4), 1117-1128. doi: 10.1109/TPDS.2014.2316155.

He, B., Ni, Q., Chen, J., Yang, L. & Lv, L. (2019). User-Pair Selection in Multiuser Cooperative Networks With an Untrusted Relay. *IEEE Trans. Veh. Techn.*, 68(1), 869-882. doi: 10.1109/TVT.2018.2882178.

He, X. & Yener, A. (2008, Nov). Two-Hop Secure Communication Using an Untrusted Relay: A Case for Cooperative Jamming. *IEEE Global Telecommun. Conf. (GLOBECOM).*, pp. 1-5. doi: 10.1109/GLOCOM.2008.ECP.185.

He, X. & Yener, A. (2013). The Role of Feedback in Two-Way Secure Communications. *IEEE Trans. Inform. Theory.*, 59(12), 8115-8130. doi: 10.1109/TIT.2013.2281711.

Holtzman, J. M. (1992). A simple, accurate method to calculate spread-spectrum multiple-access error probabilities. *IEEE Trans. Commun.*, 40(3), 461-464. doi: 10.1109/26.135712.

Hong, Y.-W. P., Lan, P.-C. & Kuo, C.-C. J. (2013). *Signal Processing Approaches to Secure Physical Layer Communications in Multi-Antenna Wireless Systems*. Springer Publishing Company, Incorporated.

Houjeij, A., Saad, W. & Bascar, T. (2013, June). A game-theoretic view on the physical layer security of cognitive radio networks. *IEEE Int. Conf. Commun. (ICC).*, pp. 2095-2099. doi: 10.1109/ICC.2013.6654835.

Hu, Y., Sanjab, A. & Saad, W. (2019). Dynamic Psychological Game Theory for Secure Internet of Battlefield Things (IoBT) Systems. *IEEE Internet of Things J.*, 1-1. doi: 10.1109/JIOT.2018.2890431.

Huang, P. & Wang, X. (2013, April). Fast secret key generation in static wireless networks: A virtual channel approach. *IEEE Proc. INFOCOM.*, pp. 2292-2300. doi: 10.1109/INFCOM.2013.6567033.

Hui, H., Swindlehurst, A., Li, G. & Liang, J. (2015). Secure Relay and Jammer Selection for Physical Layer Security. *IEEE Signal Process. Lett.*, 22(8), 1147-1151. doi: 10.1109/LSP.2014.2387860.

Ibrahim, D., Hassan, E. & El-Dolil, S. (2014, Dec.). Improving physical layer security in two-way cooperative networks with multiple eavesdroppers. *Int. Conf. Informatics and Syst. (INFOS)*, pp. ORDS-8-ORDS-13. doi: 10.1109/INFOS.2014.7036690.

Ibrahim, D. H., Hassan, E. S. & El-Dolil, S. A. (2015). Relay and jammer selection schemes for improving physical layer security in two-way cooperative networks. *Comput. & Security*, 50(0), 47 - 59. doi: http://dx.doi.org/10.1016/j.cose.2015.02.002.

Jameel, F., Wyne, S., Kaddoum, G. & Duong, T. Q. (2018). A Comprehensive Survey on Cooperative Relaying and Jamming Strategies for Physical Layer Security. *IEEE Commun. Surveys Tuts.*, 1-1. doi: 10.1109/COMST.2018.2865607.

Jeong, C., Kim, I.-M. & Kim, D. I. (2012). Joint Secure Beamforming Design at the Source and the Relay for an Amplify-and-Forward MIMO Untrusted Relay System. *IEEE Trans. Signal Process.*, 60(1), 310-325. doi: 10.1109/TSP.2011.2172433.

Kaddoum, G., Gagnon, F. & Richardson, F. (2012, Aug). Design of a secure Multi-Carrier DCSK system. *2012 Int. Symp. Wireless Communication Syst. (ISWCS)*, pp. 964-968. doi: 10.1109/ISWCS.2012.6328511.

Khisti, A. & Wornell, G. W. (2010). Secure Transmission With Multiple Antennas I: The MISOME Wiretap Channel. *IEEE Transactions on Inform. Theory.*, 56(7), 3088-3104. doi: 10.1109/TIT.2010.2048445.

Kim, J.-B., Lim, J. & Cioffi, J. (2015). Capacity Scaling and Diversity Order for Secure Cooperative Relaying With Untrustworthy Relays. *IEEE Trans. Wireless Commun.*, 14(7), 3866-3876. doi: 10.1109/TWC.2015.2413784.

Kong, L. & Kaddoum, G. (2019). Secrecy Characteristics with Assistance of Mixture Gamma Distribution. *IEEE Wireless Commun. Lett.*, 1-1. doi: 10.1109/LWC.2019.2907083.

Kong, L., He, J., Kaddoum, G., Vuppala, S. & Wang, L. (2016, Sep.). Secrecy Analysis of a MIMO Full-Duplex Active Eavesdropper with Channel Estimation Errors. *IEEE 84th Veh. Technol. Conf. (VTC-Fall)*, pp. 1-5. doi: 10.1109/VTCFall.2016.7881216.

Kong, L., Kaddoum, G., da Costa, D. B. & Bou-Harb, E. (2018a, June). On Secrecy Bounds of MIMO Wiretap Channels with ZF detectors. *14th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, pp. 724-729. doi: 10.1109/IWCMC.2018.8450477.

Kong, L., Vuppala, S. & Kaddoum, G. (2018b). Secrecy Analysis of Random MIMO Wireless Networks Over α-μ Fading Channels. *IEEE Trans. Veh. Technol.*, 67(12), 11654-11666. doi: 10.1109/TVT.2018.2872884.

Koyluoglu, O. O., Koksal, C. E. & Gamal, H. E. (2012). On Secrecy Capacity Scaling in Wireless Networks. *IEEE Trans. Inform. Theory*, 58(5), 3000 - 3015.

Kuhestani, A., Mohammadi, A. & Masoudi, M. (2016). Joint optimal power allocation and relay selection to establish secure transmission in uplink transmission of untrusted relays network. *IET Networks*, 5(2), 30-36. doi: 10.1049/iet-net.2015.0035.

Kuhestani, A., Mohammadi, A., Wong, K., Yeoh, P. L., Moradikia, M. & Khandaker, M. R. A. (2018a). Optimal Power Allocation by Imperfect Hardware Analysis in Untrusted Relaying Networks. *IEEE Trans. Wireless Commun.*, 17(7), 4302-4314. doi: 10.1109/TWC.2018.2822286.

Kuhestani, A., Mohammadi, A. & Yeoh, P. L. (2018b). Optimal Power Allocation and Secrecy Sum Rate in Two-Way Untrusted Relaying Networks With an External Jammer. *IEEE Trans. Commun.*, 66(6), 2671-2684. doi: 10.1109/TCOMM.2018.2802951.

Lai, L. & El Gamal, H. (2008). The Relay-Eavesdropper Channel: Cooperation for Secrecy. *IEEE Trans. Inform. Theory.*, 54(9), 4005-4019. doi: 10.1109/TIT.2008.928272.

Laneman, J. N., Tse, D. N. C. & Wornell, G. W. (2004). Cooperative Diversity in Wireless Networks: Efficient protocols and outage behavior. *IEEE Trans. Inform. Theory.*, 50(12), 3062-3080.

Lee, K., Hong, J. P., Choi, H. H. & Levorato, M. (2018). Adaptive Wireless-powered Relaying schemes with Cooperative Jamming for Two-hop Secure Communication. *IEEE Internet of Things Journal*, 1-1. doi: 10.1109/JIOT.2018.2830880.

Leung-Yan-Cheong, S. & Hellman, M. (1978). The Gaussian wire-tap channel. *IEEE Trans. Inform. Theory.*, 24(4), 451-456. doi: 10.1109/TIT.1978.1055917.

Li, L., Chen, Z. & Fang, J. (2014a). On Secrecy Capacity of Gaussian Wiretap Channel Aided by A Cooperative Jammer. *IEEE Signal Process. Lett.*, 21(11), 1356-1360. doi: 10.1109/LSP.2014.2336803.

Li, W., Xin, M., Yue, M., Yinglei, T. & Yong, Z. (2013). Security-oriented transmission based on cooperative relays in cognitive radio. *China, Commun.*, 10(8), 27-35. doi: 10.1109/CC.2013.6633742.

Li, X., Chen, M. & Ratazzi, E. P. (2005, June). Space-time transmissions for wireless secret-key agreement with information-theoretic secrecy. *IEEE 6th Workshop on Signal Process. Advances in Wireless Commun.*, pp. 811-815. doi: 10.1109/SPAWC.2005.1506252.

Li, Y., Xiao, L., Liu, J. & Tang, Y. (2014b, Nov.). Power control Stackelberg game in cooperative anti-jamming communications. *Int. Conf. Game Theory for Networks (GAMENETS)*, pp. 1-6. doi: 10.1109/GAMENETS.2014.7043719.

Liang, Y., Poor, H. & Shamai, S. (2008). Secure Communication Over Fading Channels. *IEEE Trans. Inform. Theory.*, 54(6), 2470-2492. doi: 10.1109/TIT.2008.921678.

Lin, M., Ge, J. & Yang, Y. (2013a). An Effective Secure Transmission Scheme for AF Relay Networks with Two-Hop Information Leakage. *IEEE Commun. Lett.*, 17(8), 1676-1679. doi: 10.1109/LCOMM.2013.062113.131012.

Lin, P.-H., Lai, S.-H., Lin, S.-C. & Su, H.-J. (2013b). On Secrecy Rate of the Generalized Artificial-Noise Assisted Secure Beamforming for Wiretap Channels. *IEEE J. Sel. Areas Commun.*, 31(9), 1728-1740. doi: 10.1109/JSAC.2013.130907.

Lin, Z., Gao, Y., Zhang, X. & Yang, D. (2014, June). Stochastic Geometry Analysis of Achievable Transmission Capacity for Relay-assisted Device-to-Device Networks. *Proc. IEEE Int. Conf. on Commun. Mobile and Wireless Networking Symp.*

Liu, X., Li, B., Chen, H., Sun, Z., Liang, Y. & Zhao, C. (2019). Detecting Pilot Spoofing Attack in MISO Systems With Trusted User. *IEEE Commun. Lett.*, 23(2), 314-317. doi: 10.1109/LCOMM.2018.2889491.

Liu, Y., Wang, L., Duy, T. T., Elkashlan, M. & Duong, T. (2015). Relay Selection for Security Enhancement in Cognitive Relay Networks. *IEEE Wireless Commun. Lett.*, 4(1), 46-49. doi: 10.1109/LWC.2014.2365808.

Liu, Y., Li, J. & Petropulu, A. (2013). Destination Assisted Cooperative Jamming for Wireless Physical-Layer Security. *IEEE Trans. Inform. Forensics and Security.*, 8(4), 682-694. doi: 10.1109/TIFS.2013.2248730.

Long, H., Xiang, W., Wang, J., Zhang, Y. & Wang, W. (2013, Apr.). Cooperative jamming and power allocation in three-phase two-way relaying wiretap systems. *IEEE Wireless Commun. and Networking Conf. (WCNC).*, pp. 4175-4179. doi: 10.1109/WCNC.2013.6555247.

Long, H., Xiang, W., Wang, J., Zhang, Y. & Wang, W. (2014). Cooperative jamming and power allocation with untrusty two-way relay nodes. *Commun. IET*, 8(13), 2290-2297. doi: 10.1049/iet-com.2013.0580.

Lou, W. & Ren, K. (2009). Security, privacy, and accountability in wireless access networks. *IEEE Wireless Commun.*, 16(4), 80-87. doi: 10.1109/MWC.2009.5281259.

Luo, M. & Yin, Q. (2018, Oct). Security Transmission Designs in Two-Way Relay Wireless Networks. *TENCON IEEE Region 10 Conf.*, pp. 0150-0155. doi: 10.1109/TENCON.2018.8650482.

Mabrouk, A., Tourki, K., Hasna, M. O. & Hamdi, N. (2017). Performance analysis of secure AF relay networks using cooperative jamming under outdated CSI. *IET Commun.*, 11(14), 2199-2205. doi: 10.1049/iet-com.2017.0412.

Madiseh, M. G., Neville, S. W. & McGuire, M. L. (2012). Applying Beamforming to Address Temporal Correlation in Wireless Channel Characterization-Based Secret Key Generation. *IEEE Trans. Inf. Forens. Security*, 7(4), 1278-1287. doi: 10.1109/TIFS.2012.2195176.

Mavoungou, S., Kaddoum, G., Taha, M. & Matar, G. (2016). Survey on Threats and Attacks on Mobile Networks. *IEEE Access*, 4, 4543-4572. doi: 10.1109/ACCESS.2016.2601009.

Middleton, D. (1977). Statistical-Physical Models of Electromagnetic Interference. *IEEE Trans. Electromagn. Compat.*, EMC-19(3), 106-127. doi: 10.1109/TEMC.1977.303527.

Mobini, Z., Mohammadi, M. & Tellambura, C. (2019). Wireless-Powered Full-Duplex Relay and Friendly Jamming for Secure Cooperative Communications. *IEEE Trans. Inf. Forens. Security*, 14(3), 621-634. doi: 10.1109/TIFS.2018.2859593.

Neagu, O. & Hamouda, W. (2016, April). Performance of smart grid communication in the presence of impulsive noise. *2016 Intern. Conf. on Selected Topics in Mobile Wireless Netw. (MoWNeT)*, pp. 1-5. doi: 10.1109/MoWNet.2016.7496614.

Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G. & Ghani, N. (2019). Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-scale IoT Exploitations. *IEEE Commun. Surveys Tuts.*, 1-1. doi: 10.1109/COMST.2019.2910750.

Ng,Edward W.; Geller, M. (1969). A Table of Integrals of the Exponential Integral. *J. of Res. of the Nat. Bureau of Standards*, 73B(3), 1-20. doi: 10.1109/TIFS.2018.2834301.

Oggier, F. & Hassibi, B. (2011). The Secrecy Capacity of the MIMO Wiretap Channel. *IEEE Trans. Inf. Theory.*, 57(8), 4961-4972. doi: 10.1109/TIT.2011.2158487.

Oohama, Y. (2007, June). Capacity Theorems for Relay Channels with Confidential Messages. *IEEE Int. Symp. Inform. Theory. ISIT.*, pp. 926-930. doi: 10.1109/ISIT.2007.4557113.

Park, K.-H., Wang, T. & Alouini, M.-S. (2013). On the Jamming Power Allocation for Secure Amplify-and-Forward Relaying via Cooperative Jamming. *IEEE J. Selected Areas in Commun.*, 31(9), 1741-1750. doi: 10.1109/JSAC.2013.130908.

Pierrot, A. & Bloch, M. (2011). Strongly Secure Communications Over the Two-Way Wiretap Channel. *IEEE Trans. Inform. Forensics and Security*, 6(3), 595-605. doi: 10.1109/TIFS.2011.2158422.

Pittolo, A. & Tonello, A. M. (2013, March). Physical layer security in PLC networks: Achievable secrecy rate and channel effects. *IEEE 17th Intern. Symp. Power Line Commun. and Its Appl.*, pp. 273-278. doi: 10.1109/ISPLC.2013.6525863.

Pittolo, A. & Tonello, A. M. (2014). Physical layer security in power line communication networks: an emerging scenario, other than wireless. *IET Commun.*, 8(8), 1239-1247. doi: 10.1049/iet-com.2013.0472.

Popovski, P. & Simeone, O. (2009). Wireless Secrecy in Cellular Systems With Infrastructure-Aided Cooperation. *IEEE Trans. Inform. Forensics and Security.*, 4(2), 242-256. doi: 10.1109/TIFS.2009.2020776.

Salem, A., Hamdi, K. A. & Alsusa, E. (2017). Physical Layer Security Over Correlated Log-Normal Cooperative Power Line Communication Channels. *IEEE Access*, 5, 13909-13921. doi: 10.1109/ACCESS.2017.2729784.

Sarr, N. B., Yazbek, A. K., Boeglen, H., Cances, J. P., Vauzelle, R. & Gagnon, F. (2017, May). An impulsive noise resistant physical layer for smart grid communications. *2017 IEEE Intern. Conf. on Commun. (ICC)*, pp. 1-7. doi: 10.1109/ICC.2017.7996876.

Schneier, B. (1998). Cryptographic Design Vulnerabilities. *IEEE Comput.*, 31(9), 29-33.

Serfling, R. (1980). *Approximation Theorems of Mathematical Statistics*. Wiley.

Shannon, C. (1949). Communication theory of secrecy systems. *The Bell Syst. Technical J.*, 28(4), 656-715. doi: 10.1002/j.1538-7305.1949.tb00928.x.

Sharif, M. & Hassibi, B. (2005). On the capacity of MIMO broadcast channels with partial side information. *IEEE Trans. Inform. Theory.*, 51(2), 506-522. doi: 10.1109/TIT.2004.840897.

Sheikholeslami, A., Goeckel, D., Pishro-Nik, H. & Towsley, D. (2012, Mar.). Physical layer security from inter-session interference in large wireless networks. *Proc. IEEE INFOCOM.*, pp. 1179-1187. doi: 10.1109/INFCOM.2012.6195477.

Shiu, Y.-S., Chang, S. Y., Wu, H.-C., Huang, S.-H. & Chen, H.-H. (2011). Physical layer security in wireless networks: a tutorial. *IEEE Wireless Commun.*, 18(2), 66-74. doi: 10.1109/MWC.2011.5751298.

Shongwey, T., Vinck, A. J. H. & Ferreira, H. C. (2014, March). On impulse noise and its models. *18th IEEE Int. Symp. on Power Line Commun. and Its Appl.*, pp. 12-17. doi: 10.1109/ISPLC.2014.6812360.

Shrestha, A. P., Riazul Islam, S. M., Dhakal, R. & Kwak, K. S. (2019, Jan). Physical Layer Security for Cooperative Multihop Routing in Wireless Networks. *IEEE 9th Annu. Comput. Commun. Workshop Conf. (CCWC)*, pp. 0910-0915. doi: 10.1109/CCWC.2019.8666507.

Silva, N. M. O. & Cordero, C. V. (2017, Oct). Towards physical layer security systems design using game theory approaches. *2017 CHILEAN Conf. on Elect. Electron. Eng. Inform. and Commun. Technol. (CHILECON)*, pp. 1-6. doi: 10.1109/CHILECON.2017.8229597.

Simeone, O. & Popovski, P. (2008). Secure Communications via Cooperating Base Stations. *IEEE ASSP Mag. Commun. Lett.*, 12(3), 188-190. doi: 10.1109/LCOMM.2008.071836.

Song, C. (2018). Achievable Secrecy Rate of Artificial Fast-Fading Techniques and Secret-Key Assisted Design for MIMO Wiretap Channels With Multiantenna Passive Eavesdropper. *IEEE Trans. Veh. Technol.*, 67(10), 10059-10063. doi: 10.1109/TVT.2018.2856764.

Soosahabi, R. & Naraghi-Pour, M. (2012). Scalable PHY-Layer Security for Distributed Detection in Wireless Sensor Networks. *Trans. Inf. Forens. Security*, 7(4), 1118-1126. doi: 10.1109/TIFS.2012.2194704.

Stanojev, I. & Yener., A. (2011, May). Cooperative jamming via spectrum leasing. *Int. Symp. Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt)*, pp. 265-272. doi: 10.1109/WIOPT.2011.5930026.

Stanojev, I. & Yener, A. (2011, Sept.). Recruiting multi-antenna transmitters as cooperative jammers: An auction-theoretic approach. *Annual Allerton Conf. Commun., Control, and Computing (Allerton)*, pp. 1106-1112. doi: 10.1109/Allerton.2011.6120291.

Stanojev, I. & Yener, A. (2013). Improving Secrecy Rate via Spectrum Leasing for Friendly Jamming. *IEEE Trans. Wireless Commun.*, 12(1), 134-145. doi: 10.1109/TWC.2012.120412.112001.

Sun, L., Zhang, T., Li, Y. & Niu, H. (2012). Performance Study of Two-Hop Amplify-and-Forward Systems With Untrustworthy Relay Nodes. *IEEE Trans. Vehicular Technology.*, 61(8), 3801-3807. doi: 10.1109/TVT.2012.2207438.

Sun, L., Ren, P., Du, Q., Wang, Y. & Gao, Z. (2015). Security-Aware Relaying Scheme for Cooperative Networks With Untrusted Relay Nodes. *IEEE Commun. Lett.*, 19(3), 463-466. doi: 10.1109/LCOMM.2014.2385095.

Tekin, E. & Yener, A. (2008). The General Gaussian Multiple-Access and Two-Way Wiretap Channels: Achievable Rates and Cooperative Jamming. *IEEE Trans. Inform. Theory.*, 54(6), 2735-2751. doi: 10.1109/TIT.2008.921680.

et al, G. M. (2011). Impacts of impulsive noise from partial discharges on wireless systems performance: application to MIMO precoders. *EURASIP J. Wireless Commun. Netw.*, 2011(1), 186. doi: 10.1186/1687-1499-2011-186.

Tolossa, Y. J., Vuppala, S., Kaddoum, G. & Abreu, G. (2018). On the Uplink Secrecy Capacity Analysis in D2D-Enabled Cellular Network. *IEEE Syst. J.*, 12(3), 2297-2307. doi: 10.1109/JSYST.2017.2700438.

Tran, D., Tran, H., Ha, D. & Kaddoum, G. (2019). Secure Transmit Antenna Selection Protocol for MIMO NOMA Networks Over Nakagami-m Channels. *IEEE Syst. J.*, 1-12. doi: 10.1109/JSYST.2019.2900090.

Tran, T. T. & Kong, H. Y. (2014). CSI-Secured Orthogonal Jamming Method for Wireless Physical Layer Security. *IEEE Commun. Lett.*, 18(5), 841-844. doi: 10.1109/LCOMM.2014.040214.140109.

Vishwakarma, S. & Chockalingam, A. (2014, Feb.). MIMO decode-and-forward relay beamforming for secrecy with cooperative jamming. *Nat. Conf. Commun. (NCC)*, pp. 1-6. doi: 10.1109/NCC.2014.6811256.

Vuppala, S. & Abreu, G. (2013). Unicasting on the Secrecy Graph. *IEEE Trans. Inf. Forens. Security*, 8(9), 1469 - 1481.

Vuppala, S., Tolossa, Y. J., Kaddoum, G. & Abreu, G. (2018). On the Physical Layer Security Analysis of Hybrid Millimeter Wave Networks. *IEEE Trans. Commun.*, 66(3), 1139-1152. doi: 10.1109/TCOMM.2017.2776944.

Wang, C. & Wang, H. (2015). Robust Joint Beamforming and Jamming for Secure AF Networks: Low-Complexity Design. *IEEE Trans. Veh. Techn.*, 64(5), 2192-2198. doi: 10.1109/TVT.2014.2334640.

Wang, C. & Wang, H.-M. (2014, June). Joint relay selection and artificial jamming power allocation for secure DF relay networks. *IEEE Int. Conf. Commun. Workshops (ICC)*, pp. 819-824. doi: 10.1109/ICCW.2014.6881301.

Wang, C., Wang, H.-M. & Xia, X.-G. (2015a). Hybrid Opportunistic Relaying and Jamming With Power Allocation for Secure Cooperative Networks. *IEEE Trans. Wireless Commun.*, 14(2), 589-605. doi: 10.1109/TWC.2014.2354635.

Wang, H. & Xia, X. (2015). Enhancing wireless secrecy via cooperation: signal design and optimization. *IEEE Commun. Mag.*, 53(12), 47-53. doi: 10.1109/MCOM.2015.7355565.

Wang, H., Liu, F. & Yang, M. (2015b). Joint Cooperative Beamforming, Jamming, and Power Allocation to Secure AF Relay Systems. *IEEE Trans. Veh. Technol.*, 64(10), 4893-4898. doi: 10.1109/TVT.2014.2370754.

Wang, H.-M., Luo, M., Xia, X.-G. & Yin, Q. (2013a). Joint Cooperative Beamforming and Jamming to Secure AF Relay Systems With Individual Power Constraint and No Eavesdropper's CSI. *IEEE Signal Process. Lett.*, 20(1), 39-42. doi: 10.1109/LSP.2012.2227725.

Wang, H.-M., Luo, M., Yin, Q. & Xia, X.-G. (2013b). Hybrid Cooperative Beamforming and Jamming for Physical-Layer Security of Two-Way Relay Networks. *IEEE Trans. Inform. Forensics and Security.*, 8(12), 2007-2020. doi: 10.1109/TIFS.2013.2287046.

Wang, H.-M., Zheng, T. & Mu, P. (2014a, June). Secure MISO wiretap channels with multi-antenna passive eavesdropper via artificial fast fading. *IEEE Int. Conf. Commun. (ICC).*, pp. 5396-5401. doi: 10.1109/ICC.2014.6884179.

Wang, H.-M., Zheng, T. & Xia, X.-G. (2015c). Secure MISO Wiretap Channels With Multi-antenna Passive Eavesdropper: Artificial Noise vs. Artificial Fast Fading. *IEEE Trans. Wireless Commun.*, 14(1), 94-106. doi: 10.1109/TWC.2014.2332164.

Wang, L., Elkashlan, M., Huang, J., Tran, N. & Duong, T. (2014b). Secure Transmission with Optimal Power Allocation in Untrusted Relay Networks. *IEEE Wireless Commun. Lett.*, 3(3), 289-292. doi: 10.1109/WCL.2014.031114.140018.

Wang, T. & Yang, Y. (2013, April). Analysis on perfect location spoofing attacks using beamforming. *IEEE Proc. INFOCOM.*, pp. 2778-2786. doi: 10.1109/INFCOM.2013.6567087.

Wang, T. & Yang, Y. (2012, Oct). Enhancing wireless communication privacy with artificial fading. *IEEE 9th Int. Conf. Mobile Adhoc and Sensor Syst. (MASS).*, pp. 173-181. doi: 10.1109/MASS.2012.6502515.

Waqas, M., Ahmed, M., Li, Y., Jin, D. & Chen, S. (2018). Social-Aware Secret Key Generation for Secure Device-to-Device Communication via Trusted and Non-Trusted Relays. *IEEE Trans. Wireless Commun.*, 17(6), 3918-3930. doi: 10.1109/TWC.2018.2817607.

Wen, Y., Huo, Y., Ma, L., Jing, T. & Gao, Q. (2019). A Scheme for Trustworthy Friendly Jammer Selection in Cooperative Cognitive Radio Networks. *IEEE Trans. Veh. Technol.*, 1-1. doi: 10.1109/TVT.2019.2895639.

Wyner, A. D. (1975). The Wire-Tap Channel. *Bell System Technical Journal*, 54(8), 1355–1387. doi: 10.1002/j.1538-7305.1975.tb02040.x.

Xing, H., Chu, Z., Ding, Z. & Nallanathan, A. (2014, Dec.). Harvest-and-jam: Improving security for wireless energy harvesting cooperative networks. *IEEE Global Commun. Conf. (GLOBECOM).*, pp. 3145-3150. doi: 10.1109/GLOCOM.2014.7037289.

Yang, J., Kim, I.-M. & Kim, D. I. (2013). Optimal Cooperative Jamming for Multiuser Broadcast Channel with Multiple Eavesdroppers. *IEEE Trans. Wireless Commun.*, 12(6), 2840-2852. doi: 10.1109/TWC.2013.040413.120972.

Yang, J., Kim, I.-M. & Kim, D. I. (2014). Joint Design of Optimal Cooperative Jamming and Power Allocation for Linear Precoding. *IEEE Trans. Commun.*, 62(9), 3285-3298. doi: 10.1109/TCOMM.2014.2345659.

Yener, A. & He, X. (2010). Cooperation With an Untrusted Relay: A Secrecy Perspective. *IEEE Trans. Inform. Theory.*, 56(8), 3807-3827. doi: 10.1109/TIT.2010.2050958.

Zeng, M., Nguyen, P., Dobre, O. & Poor, H. V. (2019). Securing Downlink Massive MIMO NOMA Networks with Artificial Noise. *IEEE J. Sel. Topics. Signal Process.*, 1-1. doi: 10.1109/JSTSP.2019.2901170.

Zhang, J., Duong, T., Marshall, A. & Woods, R. (2016a). Key Generation from Wireless Channels: A Review. *IEEE Access.*, PP(99), 1-1. doi: 10.1109/ACCESS.2016.2521718.

Zhang, J., Firooz, M. H., Patwari, N. & Kasera, S. K. (2008). Advancing Wireless Link Signatures for Location Distinction. *Proc. 14th ACM Int. Conf. Mobile Comput. and Networking*, (MobiCom '08), 26–37. doi: 10.1145/1409944.1409949.

Zhang, M., Liu, Y. & Zhang, R. (2016b). Artificial Noise Aided Secrecy Information and Power Transfer in OFDMA Systems. *IEEE Trans. Wireless Commun.*, PP(99), 1-1. doi: 10.1109/TWC.2016.2516528.

Zhang, Q., Huang, X., Li, Q. & Qin, J. (2015). Cooperative Jamming Aided Robust Secure Transmission for Wireless Information and Power Transfer in MISO Channels. *IEEE Trans. Commun.*, 63(3), 906-915. doi: 10.1109/TCOMM.2015.2405063.

Zhang, R., Song, L., Han, Z. & Jiao, B. (2011, June). Distributed Coalition Formation of Relay and Friendly Jammers for Secure Cooperative Networks. *IEEE Int. Conf. Commun. (ICC).*, pp. 1-6. doi: 10.1109/icc.2011.5962513.

Zhang, S., Jin, L., Lou, Y., Huang, K. & Zhong, Z. (2018, Oct). High-Rate Secret Key Generation Method Using Two-Way Random Signal. *Int. Conf. Cyber-Enabled Distrib. Comput. and Knowl. Discovery (CyberC)*, pp. 32-324. doi: 10.1109/CyberC.2018.00017.

Zhu, Y., Suo, D. & Gao, Z. (2010, Aug). Secure Cooperative Spectrum Trading in Cognitive Radio Networks: A Reversed Stackelberg Approach. *Int. Conf. Multimedia Commun. (Mediacom).*, pp. 202-205. doi: 10.1109/MEDIACOM.2010.33.