ΠΑΝΕΠΙΣΤΗΜΙΟ
ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

Ασφάλεια στο Φυσικό Επίπεδο σε Ασύρματα Κανάλια με Διαλείψεις

Αρίστος Καράμπελας-Τιμοτίεβιτς

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΕΠΙΒΛΕΠΩΝ

Θεόδωρος Τσιφτσής
Καθηγητής

Λαμία, Ιανουάριος 2023

ΠΑΝΕΠΙΣΤΗΜΙΟ
ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

Ασφάλεια στο Φυσικό Επίπεδο σε Ασύρματα Κανάλια με Διαλείψεις

Αρίστος Καράμπελας-Τιμοτίεβιτς

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΕΠΙΒΛΕΠΩΝ

Θεόδωρος Τσιφτσής
Καθηγητής

Λαμία, Ιανουάριος 2023

SCHOOL OF SCIENCE

DEPARTMENT OF COMPUTER SCIENCE & TELECOMMUNICATIONS

Physical Layer Security Over Fading Channels

Aristos Karampelas-Timotievits

FINAL THESIS

SUPERVISOR

Theodoros Tsiftsis
Professor

Lamia, January 2023

«Με ατομική μου ευθύνη και γνωρίζοντας τις κυρώσεις [(1)], που προβλέπονται από της διατάξεις της παρ. 6 του άρθρου 22 του Ν. 1599/1986, δηλώνω ότι:

1. *Δεν παραθέτω κομμάτια βιβλίων ή άρθρων ή εργασιών άλλων αυτολεξεί χωρίς να τα περικλείω σε εισαγωγικά και χωρίς να αναφέρω το συγγραφέα, τη χρονολογία, τη σελίδα. Η αυτολεξεί παράθεση χωρίς εισαγωγικά χωρίς αναφορά στην πηγή, είναι λογοκλοπή. Πέραν της αυτολεξεί παράθεσης, λογοκλοπή θεωρείται και η παράφραση εδαφίων από έργα άλλων, συμπεριλαμβανομένων και έργων συμφοιτητών μου, καθώς και η παράθεση στοιχείων που άλλοι συνέλεξαν ή επεξεργάσθηκαν, χωρίς αναφορά στην πηγή. Αναφέρω πάντοτε με πληρότητα την πηγή κάτω από τον πίνακα ή σχέδιο, όπως στα παραθέματα.*

2. *Δέχομαι ότι η αυτολεξεί παράθεση χωρίς εισαγωγικά, ακόμα κι αν συνοδεύεται από αναφορά στην πηγή σε κάποιο άλλο σημείο του κειμένου ή στο τέλος του, είναι αντιγραφή. Η αναφορά στην πηγή στο τέλος π.χ. μιας παραγράφου ή μιας σελίδας, δεν δικαιολογεί συρραφή εδαφίων έργου άλλου συγγραφέα, έστω και παραφρασμένων, και παρουσίασή τους ως δική μου εργασία.*

3. *Δέχομαι ότι υπάρχει επίσης περιορισμός στο μέγεθος και στη συχνότητα των παραθεμάτων που μπορώ να εντάξω στην εργασία μου εντός εισαγωγικών. Κάθε μεγάλο παράθεμα (π.χ. σε πίνακα ή πλαίσιο, κλπ), προϋποθέτει ειδικές ρυθμίσεις, και όταν δημοσιεύεται προϋποθέτει την άδεια του συγγραφέα ή του εκδότη. Το ίδιο και οι πίνακες και τα σχέδια*

4. Δέχομαι όλες τις συνέπειες σε περίπτωση λογοκλοπής ή αντιγραφής.

Ημερομηνία: ……/…../20……

Ο – Η Δηλ.

(1) «Οποιος εν γνώσει του δηλώνει ψευδή γεγονότα ή αρνείται ή αποκρύπτει τα αληθινά με έγγραφη υπεύθυνη δήλωση
του άρθρου 8 παρ. 4 Ν. 1599/1986 τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών. Εάν ο υπαίτιος αυτών των πράξεων
σκόπευε να προσπορίσει στον εαυτόν του ή σε άλλον περιουσιακό όφελος βλάπτοντας τρίτον ή σκόπευε να βλάψει άλλον, τιμωρείται με κάθειρξη μέχρι 10 ετών.»

Περίληψη

Στην σύγχρονη εποχή οι ασύρματες επικοινωνίες γίνονται όλο και πιο διαδεδομένες. Τεχνολογίες όπως η ασύρματη μετάδοση πληροφορίας, η ασύρματη διάδοση ενέργειας και οι τηλεπικοινωνίες εξελίσσονται συνεχώς. Τα συστήματα ασύρματης μετάδοσης σημάτων μπορούν εύκολα να βρεθούν υπό τον κίνδυνο της μη εξουσιοδοτημένης πρόσβασης τρίτου. Επομένως η αξιολόγηση των καναλιών μετάδοσης της πληροφορίας για την ποιότητα της ασφάλειας που εμφανίζουν αλλά και η μελέτη τους υπό διάφορες συνθήκες είναι μείζονος σημασίας. Η παρούσα πτυχιακή εργασία αποσκοπεί στην μελέτη, αξιολόγηση και προσομοίωση της βασικής μετρικής ασφαλείας των ασύρματων καναλιών, ήτοι η πιθανότητα διακοπής ασφάλειας. Αρχικά γίνεται μια εισαγωγή στις διάφορες έννοιες που θα παρουσιαστούν. Εν συνεχεία παρουσιάζονται αναλυτικά και μέσω προσομοιώσεων τα μοντέλα συστημάτων για πέντε ασύρματα κανάλια με την παρουσία διαλείψεων, Rayleigh, Weibull, Rice, Nakagami-μ και Generalized Gamma. Τέλος, εκφράζονται συμπεράσματα για την αξιολόγηση της ασφάλειας του κάθε καναλιού, καθώς και μελλοντικές επεκτάσεις.

Abstract

In modern times, wireless communications are becoming more and more widespread. Technologies such as wireless information transmission, wireless power propagation and telecommunications are constantly evolving. Wireless signal transmission systems can easily come under the risk of unauthorized access by third parties. Therefore, evaluating information transmission channels for their security quality and studying them under various conditions is of major importance. This thesis aims to study, evaluate, and simulate the key security metric of wireless channels, namely the secrecy outage probability. First, an introduction to the various concepts to be presented is given. Then the system models for five wireless channels in the presence of flat fading, Rayleigh, Weibull, Rice, Nakagami-M and Generalized Gamma, are presented in detail and through simulations. Finally, conclusions are expressed for the security evaluation of each channel, as well as for future extensions.

Contents

Section 1. Introduction

1.1. Wireless Communications

Wireless communication refers to the transfer of information or power between two or more points that are not connected by a physical link. The most common wireless technologies are radio, infrared and microwave. The whole basis of communication relies on the use of electromagnetic waves to transmit information from one point to another. These waves can be either guided, such as those transmitted over a wire or cable, or unguided, such as those transmitted through the air.

There are several factors that can affect the performance of a wireless communication system, the distance between the transmitter and receiver (Friis' equation), the presence of obstacles or interference (Rayleigh), and the frequency of the electromagnetic waves being used.

1.2. Flat-Fading Channels

A flat fading channel is a type of wireless communication channel that experiences constant, or flat, fading over the duration of a transmitted signal. Flat fading occurs when the signal strength of the transmitted signal remains constant, or nearly constant, over time. Flat-fading channels are typically found in wireless systems that operate over short distances, such as those used in indoor environments or in personal area networks (PANs). These channels are characterized by low levels of fading, or signal variation, over time.

There are several factors that can cause flat fading in a wireless communication channel, including reflections from nearby objects, scattering from small obstacles, and the movement of the transmitter or receiver. One way to mitigate effects of flat fading is to use multiple antennas on both the transmitter and the receiver. This can help to improve the signal-to-noise ratio (SNR) and increase the reliability of the communication link. Other techniques, such as error correction coding and frequency-hopping, can also be used to improve the performance of a wireless system in a flat-fading channel.

1.3. Performance evaluation and metrics

Thus, it is important to evaluate the performance of a wireless channel since wireless communications are prone to various types of interference and noise that can degrade the quality of the signal. By evaluating the performance of a wireless channel, it is possible to identify any problems or limitations in the system and take steps to improve communication performance. The performance can be evaluated using a variety of metrics, including:

1. Signal strength: This metric refers to the power of the signal at the receiving end. Stronger signal results in better communication performance.
2. Data rate: This measures the speed at which data is transmitted over the wireless channel.
3. Bandwidth: This measures the amount of data that can be transmitted over the wireless channel in each period.
4. Error rate: This measures the percentage of transmitted data that is received incorrectly at the receiving end.
5. Interference: This measures the amount of noise or other signals that can disrupt communication over the wireless link.

Additionally, there are some metrics that are considered crucial about the evaluation of a digital wireless communication system. Those are, the signal-to-noise ratio (SNR), the outage probability and the average bit-error rate. SNR is probably the most common and well understood performance measure metric of a digital communication system, and overall communication systems. Most often it is measured at the output of the receiver and is strongly related to the data detection process. It is characterized as the easiest metric to evaluate and is a valid indicator about the overall quality of the system. In the concern of communications under fading channels, the more appropriate metric is the average SNR, where the term average denotes the statistical average of the random variable, subject to the fading distribution model. The random variable in these systems is the instantaneous SNR, which acts as the random variable of the distribution.

Evaluating the performance of a wireless channel can also be important for optimizing the use of the wireless spectrum. By understanding how different types of interference and noise affect the performance of a wireless system, it is possible to design and deploy the system in a way that maximizes its efficiency and minimizes its impact on other users of the spectrum.

1.4. Secrecy as a performance metric

1.4.1. Definition

Secrecy, or the ability to keep the content of a communication private, can also be considered a performance metric in wireless channels, particularly in situations where the security of the communication is important. In wireless systems, secrecy can be achieved through various methods, such as encryption, which transforms the data into a form that can only be understood by someone with the proper decryption key. Other methods for achieving secrecy in wireless systems include using secure protocols for communication, authenticating the identity of the sender and receiver, and using techniques to detect and prevent unauthorized access to the communication.

Evaluating the performance of a wireless channel in terms of secrecy can involve measuring the effectiveness of the methods used to protect the communication from being intercepted or compromised. For example, the strength of the encryption algorithm and the robustness of the authentication protocols can be evaluated to determine the level of secrecy that can be achieved. Overall, secrecy is an important performance metric in wireless channels, particularly in situations where the security of communication is critical, such as in military, financial, or healthcare applications.

1.4.2. Secrecy outage probability

The secrecy outage probability (SOP) is the probability that the mutual information between the transmitter and the intended receiver is less than the mutual information between the transmitter and an eavesdropper, given a certain level of transmit power and channel conditions

[1] [2]. In other words, it is the probability that the transmitted message cannot be kept secret from an eavesdropper due to poor channel conditions or insufficient transmit power. Evaluating SOP is an important task metric in the field of secure communication, as it determines the probability that the transmitted message will be successfully intercepted by an eavesdropper. To ensure the security of a communication system, it is important to minimize the secrecy outage probability as much as possible. [2]

The evaluation of a system based on its secrecy demonstrates a variety of applications, including military communications, financial transactions, and private messaging. It is also used to design and optimize secure communication systems, by determining the necessary transmit power and channel conditions required to achieve the desired level of security.

1.5. Physical layer security

Having referred to SOP, there should be a mention to the general field of Physical Layer Security or PLS. Most systems require some kind of security to retain the data integrity and confidentiality. The most common tactic in the need of securing a system is to apply cryptographic techniques, which rely on secret keys [3]. The most common type of malevolent attack are the eavesdropping attacks. A simple antenna placement is enough to have the transmitted data stolen from an unauthorized third-party. In the wake of these problems, cryptographic techniques demand trusted infrastructures in order to execute secret key distribution and management. Unfortunately, wireless networks are a very hard system to secure.

The need for secure connections and confidential transmissions can be satisfied through PLS, which is now emerging as an effective means of achieving perfect secrecy against eavesdropping attacks. By exploiting the physical characteristics of the wireless channel, PLS can potentially secure any wireless system. Presently, extensive efforts have been devoted to the research and development of wireless secrecy capacity enhancement techniques to combat fading effects. Such efforts are analyzed in the following section.

Section 2. Literature Review

Security is a broadly researched aspect of communications, on both wired and wireless applications. This interest in the subject of security prompted many research teams to conduct studies on the matter at hand and yield a clearer picture for the scientific community. Notably, some of the recent, increasingly sophisticated attacks on the wireless edge (e.g., jamming, or false base stations) can be implemented with a price tag as low as US$1000 using low-cost software defined radios [4]. In addition, we are experiencing an expansion of the attack surface with artificial intelligence becoming more prominent as the years go by. This section is dedicated in showcasing the state of the art in wireless communication channel security, while also presenting the source of inspiration for the rest of the thesis.

The first and most notable mention is the paper, "The Wiretap Channel", published in 1975 by Abraham Wyner [5]. In that paper, Wyner introduced and analyzed the wiretap channel, a communication system where a sender wishes to transmit a message to a legitimate receiver over a noisy channel but wants to keep the message confidential from an eavesdropper who also observes the transmission. In that paper the fundamental limits of information-theoretic security where analyzed, in such a scenario and showed that a secure communication is possible if and only if the legitimate receiver's channel quality is better than that of the eavesdropper's. Wyner also introduced the notion of secrecy capacity, which is the maximum rate at which the sender can transmit a message securely and showed that it is a well-defined quantity that depends on the channel quality of both the legitimate receiver and the eavesdropper. The wiretap channel model and the concept of secrecy capacity have since become fundamental tools in information-theoretic security and have found numerous applications in cryptography and network security.

Wyner's study has been referenced in most of the research papers, but even with it being a seminal contribution to the field of information-theoretic security, it cannot be considered the ultimate reference for wireless security. Wireless security is a complex and multifaced problem that involves not only information-theoretic considerations but also practical issues such as authentication, key management, secure protocols, and physical layer security. There is a significant amount of scientific papers and publications that have extended on Wyner's wiretap model, applying its contents into the field of physical layer wireless channel security.

The measurement that is also the main interest of the current thesis is the secrecy outage probability. Since its appearance, the concept of secrecy outage probability has become an important tool for the analysis and design of secure communication systems, particularly in wireless networks. It has been studied extensively in the literature and has found numerous applications in various fields of wireless security, such as physical layer security, cooperative communication, and jamming-resistant communication. In their study, Zhao et al. [6] designed a simple approximation for the secrecy outage probability over generalized-K fading channels. It was observed that as the SNR of the wiretap channel decreased, the approximation became tighter. Based on the derived simple expression, the authors attempted an asymptotic analysis of the secrecy outage probability, in the high SNR region of the main channel. Besides simplifying the expression of the SOP, the asymptotic expression revealed the secrecy diversity order in a general case. Numerical results demonstrated high accuracy of the proposed approximation results.

Another application of SOP can be found in the scientific paper by Wang et al. [3] In that paper, the authors considered a wireless ad hoc network consisting of multiple source nodes transmitting to their respective destinations, where an eavesdropper attempts to intercept their transmissions. Given the previous system model, the authors proposed an optimal transmission scheduling scheme to defend against the eavesdropper, where a source node having the highest secrecy rate is scheduled to access the wireless medium for transmitting to its destination in an opportunistic manner. The secrecy rate between a pair of source and destination nodes, in the presence of an eavesdropper varies temporarily due to the presence of fading. The proposed optimal transmission scheduling scheme selects a source node with the highest secrecy rate to transmit its data for the sake of maximizing the security of the ad hoc network against eavesdropping attacks. The authors compared their custom scheme to the round robin scheduling as the benchmark. The transmission channel also demonstrated Rayleigh fading. The numerical results show that the proposed scheduling outperformed the Round Robin in terms of its secrecy outage probability. In this application, SOP is used to show that the exploitation of the transmission scheduling yields security benefits, resulting in the protection of wireless ad hoc networks against eavesdropping.

In turn, Alotaibi et al. [7] analyzed the SOP in a cooperative network for an independent but non-identically distributed Rayleigh fading channel. By using multi-trusted decode and forward relays, the model assumes direct links between sender and receiver nodes, where between the receivers lies an eavesdropper. The protocol selects the best relay with the highest SNR in relation

to the destination. The eavesdropper's CSI is unavailable to the sender and the best relay, while maximum ratio combining (MRC) is used at Bob and the eavesdropper. The authors validate their theoretical analysis through simulations, with the results showing that the performance of the system is enhanced with an increasing number of relays in the event of a direct link between the sender and the receiver's terminals. The pre-existing direct links between sender and receiver nodes improve the SOP of a cooperative communication system with non-identical distribution, while the cluster of relays is trusted. Since the optimal relay is chosen such as it maximizes the SNR at the receiver, and this means that the ratio of the SNR in the receiver and the one in the eavesdropper is also maximized, the physical layer security is enhanced, since there is secrecy in the channel.

Another attempt was made by Anastasov et al. [8], where they tried to investigate the secrecy performance of traditional Wyner's wiretap channel [5], but over an α-F fading channel. The mathematical expressions for evaluating the SOP and the probability of intercept are numerically derived during the course of the paper. Based on the obtained results and the channel information, the authors studied the physical layer security metrics of the system model. They concluded that secrecy transmission can be enhanced by proper exploitation of the propagation characteristics of both legitimate and illegitimate wireless channels. The obtained results showed that favorable conditions over the main channel could upgrade the secure transmission. Lighter shadowing conditions over the main channel decrease the SOP only in the presence of high SNRs of the main link. The proposed analysis yielded the main advantage that it can be recursively applied to special cases of α-F fading models, them being the Rayleigh, Weibull, Nakagami-m, α-μ and many more fading models.

At last, Lei et al. [1] studied the secrecy performance of the classic Wyner's wiretap channel [5] over the generalized Gamma fading channels. The authors managed to derive closed forms for the strictly positive secrecy capacity and the lower bound secrecy outage probability. The closed-forms were verified through Monte-Carlo simulations, with the resulting simulation curves matching the corresponding analysis results.

Many other groups have investigated the security of complex system models through analysis and performance evaluations based on SOP. Therefore, the current thesis strives to present the SOP analysis of various fading channels through theoretical derivations and simulations, but also

it can provide a gentle gateway to any individual, interested in studying about physical layer security and the applications of SOP in system model analysis.

Section 3. Rayleigh Fading Channel

The Rayleigh fading or Rayleigh channel is a statistical model for the effect of a propagation environment on a radio signal, such as that used by wireless devices. Rayleigh fading models assume that the magnitude of a signal that has passed through such a transmission medium will vary randomly, or fade, according to a Rayleigh distribution. [2] [9] This distribution is the radial component of the sum of two uncorrelated Gaussian random variables. Rayleigh fading is viewed as a reasonable model for tropospheric and ionospheric signal propagation as well as the effect of heavily built-up urban environments on radio signals. Rayleigh fading is most applicable when there is no dominant propagation along a line of sight between the transmitter and receiver. If there is a dominant line of sight, Rician fading may be more applicable.

3.1. System model of Rayleigh fading channel

As foretold, the scatters model is a reasonable one when there are many objects in the environment that scatter the radio signal before it arrives at the receiver. The central limit theorem holds that, if there is sufficiently much scatter, the channel impulse response will be well-modelled as a Gaussian process irrespective of the distribution of the individual components. This means the impulse response varies based on time and the symbol delay. If there is no dominant component to the scatter, then such a process will have zero mean and phase evenly distributed between 0 and 2π radians. The envelope of the channel response will therefore be Rayleigh distributed.

Calling this random variable R, it will have a pdf:

$$\boldsymbol{p_R(r) = \frac{2r}{\Omega} e^{-\frac{r^2}{\Omega}}, \qquad r \geq 0} \tag{1}$$

Where $\Omega = E(R^2)$ which is the second moment of the random variable, in other words it is called mean-squared value, which is the mean of its square and not the square of its mean. When the distribution is centered on zero, then the second moment is the variance of the random variable since:

$$\sigma_R^2 = E[R^2] - E^2[R]$$

As told, the distribution is zero-centered, which means that $E[R] = 0$, thus $E^2[R] = 0$. This means that:

$$\sigma_R^2 = E[R^2]$$

Rayleigh fading is exhibited by the assumption that the real and imaginary parts of the response are modelled by independent and identically distributed zero-mean Gaussian processes so that the amplitude of the response is the sum of two such processes.

Based on the GG distribution of the random variable R is given by:

$$\boldsymbol{f_R(r) = \frac{ac^c r^{ac-1}}{\Gamma(c)\bar{r}^{ac}} e^{-c\left(\frac{r}{\bar{r}}\right)^a}, \qquad a > 0, c > 0} \tag{2}$$

In this equation the a is the fading parameter, c is the normalized variance of the channel envelope R, and $\bar{r}$ is the a[th] mean square of the channel envelope. The gamma function is the following:

$$\Gamma(c) = \int_0^\infty t^{c-1} e^{-t}\, dt \tag{3}$$

By changing the parameters of the GG distribution, we can obtain other famous distributions like Rayleigh, Rice, Weibull and Nakagami-μ. Beginning the substitution using the Rayleigh parameters, where $\alpha = 2$ and $c = 1$.

$$f_R(r) = \frac{2 \cdot 1^1 \cdot r^{2-1}}{\Gamma(1) \cdot \bar{r}^{2 \cdot 1}} e^{-1 \cdot \left(\frac{r}{\bar{r}}\right)^2} \Rightarrow f_R(r) = \frac{2r}{\Gamma(1)\bar{r}^2} e^{-\frac{r^2}{\bar{r}^2}}$$

Before returning to this equation, we should calculate the gamma function:

$$\Gamma(1) = \int_0^\infty t^0 e^{-t} dt = [-e^{-t}]_0^\infty = \left[-\lim_{t \to +\infty} e^{-t} - e^0\right] = -[-1] = 1$$

Since $\Gamma(1) = 1$, then:

$$f_R(r) = \frac{2r}{\bar{r}^2} e^{-\frac{r^2}{\bar{r}^2}}$$

The upper equation is the exact same as the Rayleigh model that was presented in Eq. (1). The $\bar{r}^2 = E[R^2] = \Omega$, thus the final model equation is:

$$f_{R(r)} = \frac{2r}{\Omega} e^{-\frac{r^2}{\Omega}}$$

The problem must be approached from a channel perspective. The main metric for a channel is the capacity and the SNR, in other words the quality of the transmitted signal. Thus, we are going to assume that in our earlier formulas, the main random variable corresponded to the SNR of the channel and not the actual scale. Doing that we are talking about the distribution of the SNR which varies with time. The general pdf of the SNR for a GG fading channel is given as:

$$f_k(\gamma) = \frac{a_k c_k^{c_k} \gamma^{\frac{a_k c_k}{2}-1}}{2(\overline{\gamma_k})^{\frac{\alpha_k c_k}{2}} \Gamma(c_k)} e^{-c_k\left(\frac{\gamma}{\overline{\gamma_k}}\right)^{\frac{a_k}{2}}}$$

In the upper formula, the parameter k is assigned as the Destination (D) or the Eavesdropper (E) channel. $\boldsymbol{c_k}$ are the normalized variances of the two channel envelopes based on the bandwidth. The average SNR is defined as:

$$\overline{\gamma_k} = \frac{E[R_k^2]Eb}{N_o}$$

The ratio $\frac{E_b}{N_o}$ is the energy per bit to the noise power spectral density. By substituting the parameters for the Rayleigh fading ($a = 2, c = 1$), and assuming that the parameters are the same for both the main and eavesdropper channels, we have the following equation:

$$f_k(\gamma) = \frac{1}{\overline{\gamma_k}} e^{-\frac{\gamma}{\overline{\gamma_k}}}$$

As for the cumulative density function, we have the following equation, which is based on the lower gamma function.

$$F_k(\gamma) = \frac{\Upsilon\left(1, \frac{\gamma}{\overline{\gamma_k}}\right)}{\Gamma(1)} = \Upsilon\left(1, \frac{\gamma}{\overline{\gamma_k}}\right)$$

We know that the lower gamma function has the following expression:

$$\Upsilon(a, x) = \int_0^x e^{-t} t^{a-1} dt$$

Thus, the previous equation becomes.

$$\Upsilon\left(1, \frac{\gamma}{\overline{\gamma_k}}\right) = \int_0^{\frac{\gamma}{\overline{\gamma_k}}} e^{-t} dt$$

The former can be solved very easily using integration by parts, resulting in the following final expression:

$$\Upsilon\left(1, \frac{\gamma}{\overline{\gamma_k}}\right) = 1 - e^{-\frac{\gamma}{\overline{\gamma_k}}}$$

The upper formulas are valid when it is known that the channel is overcome by Rayleigh fading.

3.2. Secrecy outage probability analysis

Secrecy Outage Probability is defined as the probability that the instantaneous secrecy capacity falls below a predesignated target bitrate. Simplifying the definition, this is the probability that the channel will seize being secure, and that the eavesdropper can discern critical information about the transmitted data. Thus, SOP is an important performance measurement, which is widely used to characterize a wireless communication system.

SOP can be defined as:

$$SOP = P\{C_S(\gamma_D, \gamma_E) \leq C_{th}\}$$

By considering that we are using bit transmission we have the capacity as it was defined by the Shannon-Hartley theorem. In the upper formula the C_{th} describes the predesignated threshold capacity for the secrecy outage. Respectively, the $C_s(\gamma_D, \gamma_E)$ describes the ratio of the destination capacity to eavesdropper capacity.

$$C = \log_2(1 + SNR)$$

This capacity is normalized by the channel bandwidth. Thus, we have the following:

$$SOP = P\{\log_2(1 + \gamma_D) - \log_2(1 + \gamma_E) \leq C_{th}\}$$

We will apply some simplifications on the previous expression by using the 2^x function which is 1-to-1, keeping the monotony of the function unchanged.

$$SOP = P\left\{\frac{1 + \gamma_D}{1 + \gamma_E} \leq 2^{C_{th}}\right\} = P\{\gamma_D \leq 2^{C_{th}} + 2^{C_{th}}\gamma_E - 1\}$$

To calculate the probability, we need to calculate the area below the pdf up until the break point. This is achievable by using the cumulative distribution function:

$$F_x(x) = P(X \leq x) = \int_{-\infty}^{x} f_x(t)dt$$

We set $\lambda = 2^{C_{th}}$, and then apply the first integral:

$$\int_0^{\lambda+\lambda\gamma_E-1} f_D(\gamma_D)d\gamma_D$$

And then we also integrate for the second SNR, which is the eavesdropper's channel.

$$\int_0^{\infty} \int_0^{\lambda+\lambda\gamma_E-1} f_D(\gamma_D)d\gamma_D \, f_E(\gamma_E)d\gamma_E$$

We solve the inner integral by using the formula of the CDF, and we have the following:

$$\int_0^{\infty} F_D(\lambda + \lambda\gamma_E - 1) f_E(\gamma_E)d\gamma_E$$

Both the cumulative and the density functions are known from earlier calculations. We can also notice that the cumulative is irrespective of $\boldsymbol{\gamma_E}$ which allows us to place it on the outside of the integral. Then we will attempt to solve it:

$$F_k(\gamma) = 1 - e^{-\frac{\gamma}{\overline{\gamma_k}}}$$

$$F_D(\lambda + \lambda\gamma_E - 1) = 1 - e^{-\frac{(\lambda+\lambda\gamma_E-1)}{\overline{\gamma_k}}}$$

Respectively, we have the following:

$$f_D(\gamma_D) = \frac{1}{\overline{\gamma_D}} e^{-\frac{\gamma_D}{\overline{\gamma_D}}}$$

$$f_E(\gamma_E) = \frac{1}{\overline{\gamma_E}} e^{-\frac{\gamma_E}{\overline{\gamma_E}}}$$

The final integral to be solved is the following:

$$SOP = \int_0^\infty \left(1 - e^{-\frac{(\lambda+\lambda\gamma_E-1)}{\overline{\gamma_D}}}\right) \frac{1}{\overline{\gamma_E}} e^{-\frac{\gamma_E}{\overline{\gamma_E}}} d\gamma_E$$

We will now attempt to simplify the equation:

$$SOP = \frac{1}{\overline{\gamma_E}} \int_0^\infty \left(1 - e^{-\frac{(\lambda+\lambda\gamma_E-1)}{\overline{\gamma_D}}}\right) e^{-\frac{\gamma_E}{\overline{\gamma_E}}} d\gamma_E$$

Our solution of the upper integral assumes that the big terms in the exponential powers will be simplified by substituting them with some placeholder variables.

$$e^{-\frac{(\lambda+\lambda\gamma_E-1)}{\overline{\gamma_D}}} = e^{\frac{-\lambda-\lambda\gamma_E+1}{\overline{\gamma_D}}} = e^{-\frac{\lambda\gamma_E}{\overline{\gamma_D}}} \cdot e^{\frac{-\lambda+1}{\overline{\gamma_D}}}$$

Using this separation, we will execute the multiplication inside the integral

$$e^{-\frac{\gamma_E}{\overline{\gamma_E}}} - e^{-\frac{\lambda\gamma_E}{\overline{\gamma_D}}} \cdot e^{\frac{-\lambda+1}{\overline{\gamma_D}}} \cdot e^{-\frac{\gamma_E}{\overline{\gamma_E}}}$$

Thus, the integral will be transfigured as such:

$$SOP = \frac{1}{\overline{\gamma_E}} \int_0^\infty e^{-\frac{\gamma_E}{\overline{\gamma_E}}} - e^{-\frac{\lambda\gamma_E}{\overline{\gamma_D}}} \cdot e^{\frac{-\lambda+1}{\overline{\gamma_D}}} \cdot e^{-\frac{\gamma_E}{\overline{\gamma_E}}} d\gamma_E \Rightarrow$$

$$SOP = \frac{1}{\overline{\gamma_E}}\left[\int_0^{\infty} e^{-\frac{\gamma_E}{\overline{\gamma_E}}} d\gamma_E - e^{\frac{-\lambda+1}{\overline{\gamma_D}}} \cdot \int_0^{\infty} e^{-\frac{\lambda\gamma_E}{\overline{\gamma_D}}} \cdot e^{-\frac{\gamma_E}{\overline{\gamma_E}}} d\gamma_E\right]$$

We will solve each integral separately:

$$I_1 = \int_0^{\infty} e^{-\frac{\gamma_E}{\overline{\gamma_E}}} d\gamma_E = -\overline{\gamma_E}\left[-e^{-\frac{\gamma_E}{\overline{\gamma_E}}}\right]_0^{\infty} = \overline{\gamma_E}$$

$$I_2 = \int_0^{\infty} e^{-\frac{\lambda\gamma_E}{\overline{\gamma_D}}} \cdot e^{-\frac{\gamma_E}{\overline{\gamma_E}}} d\gamma_E = \int_0^{\infty} e^{-\frac{\lambda\gamma_E}{\overline{\gamma_D}}-\frac{\gamma_E}{\overline{\gamma_E}}} d\gamma_E = \int_0^{\infty} e^{-\left(\frac{\lambda}{\overline{\gamma_D}}+\frac{1}{\overline{\gamma_E}}\right)\gamma_E} d\gamma_E = \frac{1}{\frac{\lambda}{\overline{\gamma_D}}+\frac{1}{\overline{\gamma_E}}}$$

Substituting the solutions in the initial integral we have

$$SOP = \frac{1}{\overline{\gamma_E}}\left[\overline{\gamma_E} - e^{\frac{-\lambda+1}{\overline{\gamma_D}}} \cdot \frac{1}{\frac{\lambda}{\overline{\gamma_D}}+\frac{1}{\overline{\gamma_E}}}\right] = 1 - e^{\frac{-\lambda+1}{\overline{\gamma_D}}} \cdot \frac{\overline{\gamma_D}}{\lambda\overline{\gamma_E}+\overline{\gamma_D}}$$

Since we know that $\lambda = 2^{C_{th}}$, then we can simulate the expression using various values of the threshold channel capacity and see how the SOP changes, responding to the capacity.

3.3. Simulations

To simulate the secrecy outage probability of the Rayleigh fading channel we divided the procedure into two discrete experiments. The first demonstrates the theoretical calculations based on user given values for the various communication parameters. The second seeks to validate the theoretical results by implementing a simple communication system and evaluating the SOP, through realistic experimental values.

3.3.1. Simulation of the analytical expression

The analytical experiment of the SOP is going to be based on the closed form expression we calculated in the previous section.

$$SOP = 1 - e^{\frac{-\lambda+1}{\overline{\gamma_D}}} \cdot \frac{\overline{\gamma_D}}{\lambda\overline{\gamma_E} + \overline{\gamma_D}}$$

The during the simulation of the analytical closed form, it is assumed that the threshold secrecy capacity is $C_{th} = 1$, the noise SNR is $N(dB) = 20\ dB$ and that the ratio of the legitimate receiver (destination) to the eavesdropper is a vector K. The vector K receives has values in the range -10 to 20, and it is measured in dB. The simulation can be divided into three distinct simulations. The first simulation investigates the relationship between the eavesdropper average SNR and the SOP. During the second simulation, the corresponding relation with the destination average SNR is visited. Finally, the final relation is between the ratio K and the SOP.

The first two simulations are very straightforward. The simulations are created by defining a vector of values for the eavesdropper average SNR and for the destination average SNR. During each simulation, the complementary factor, it being the eavesdropper during the destination simulation and vice-versa, is a constant value. For simulation values for the average eavesdropper SNR varying from 0 to 10 and step 0.1, the experiment yielded the following graph for the Secrecy Outage Probability.

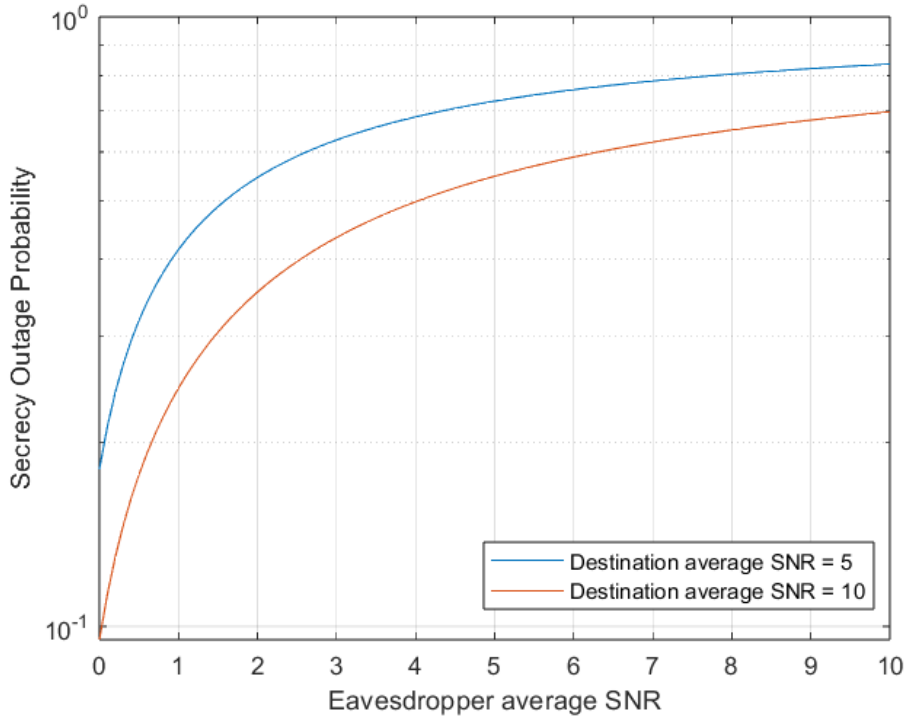

Figure 1: Logarithmic scale plot of the SOP during varying eavesdropper SNR

As it is obvious, the SOP demonstrates an ascending figure, which translates to the probability of secrecy outage increasing as the eavesdropper SNR is increased. The corresponding simulation for varying destination average SNR is plotted in Fig.2.

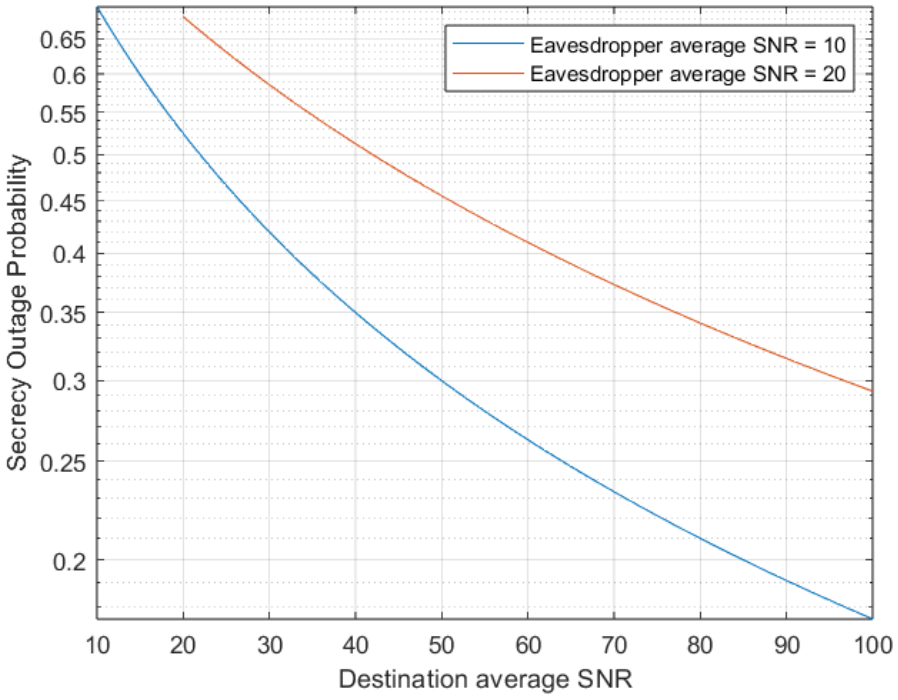

Figure 2: Logarithmic scale plot of the SOP during varying destination SNR

It is plainly witnessed that the SOP is decreasing in response to the increase of the average destination SNR. In simpler words, the destination's SNR is becoming much greater than the eavesdropper suggests that the channel is secure enough for transmission.

The final simulation, which exploits the relationship between the destination and the eavesdropper, the SNR ratio of the two receivers requires some additional steps. The first step in this simulation is to convert the decibels of the K ratio into numbers using the standard dB conversion.

$$SNR = 10^{\frac{SNR(dB)}{10}}$$

Continuing, random values for the eavesdropper average SNR are chosen. Another assumption is that the legitimate receiver's average SNR (destination SNR) is K-times greater than the eavesdropper's average SNR:

$$\overline{\gamma_D} = K \cdot \overline{\gamma_E}$$

Finally, from the analytical solution we have that $\lambda = 2^{C_{th}}$. The MATLAB script which implements the simulation can be found in Appendix 1 (*add link*). The generated figure is shown in Fig.3.

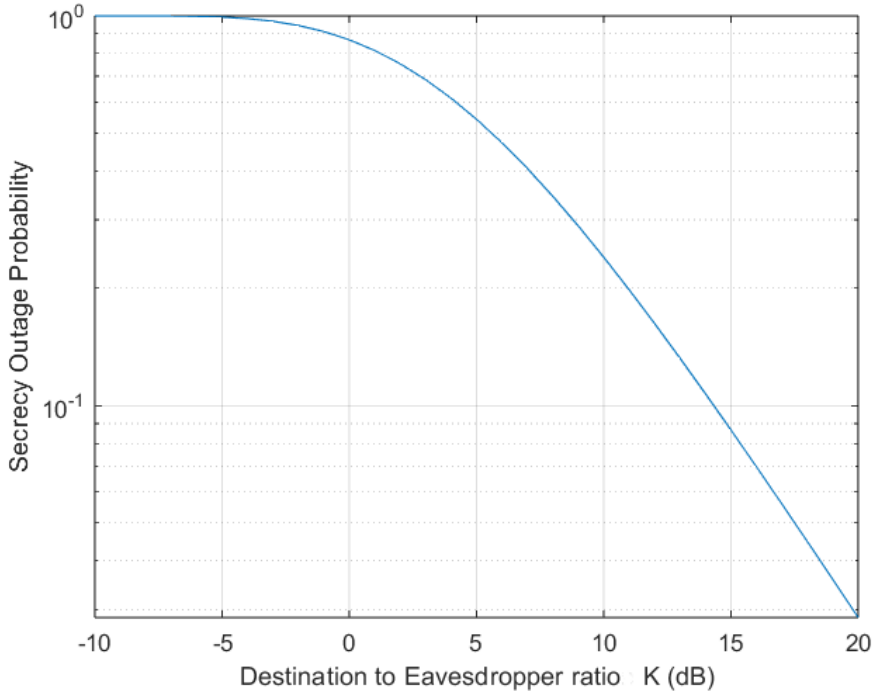

Figure 3: Simulation plot of the analytical SOP expression

We can see that as the ratio increases, the SOP decreases. This is because the eavesdropper receives a much smaller SNR than the legitimate user, making the signal detection much harder for the eavesdropper. We can see that the probability of security outage is most unlikely the larger the ratio of the SNR becomes.

Finally, the influence of threshold capacity is shown in Fig.4, where the simulation is run for the same parameters as the K-ratio simulation, but with also, varying threshold capacity in the range from 2 to 5.

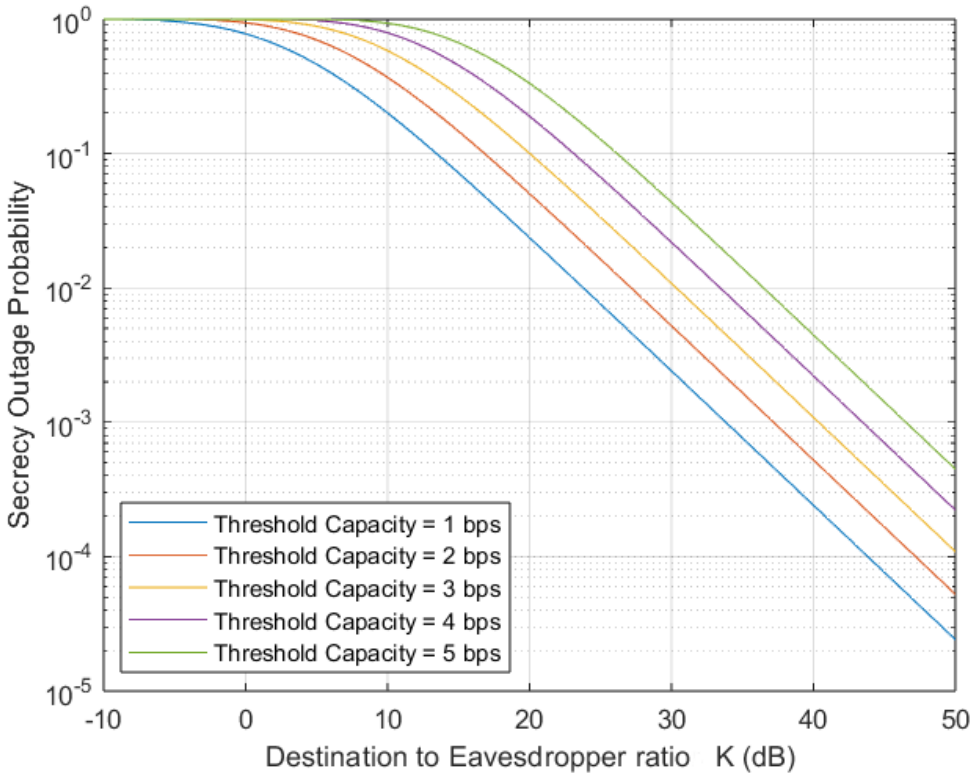

Figure 4: Simulation plot of the analytical SOP expression in respect to varying K ratio and threshold capacity

It is clearly shown that an increasing threshold capacity increases the insecure ratio, which is logical as the greater the threshold, the longer the security outage duration.

3.3.2. Simulation of a realistic system model

The system model we are going to use in our simulation is (Fig. 5):

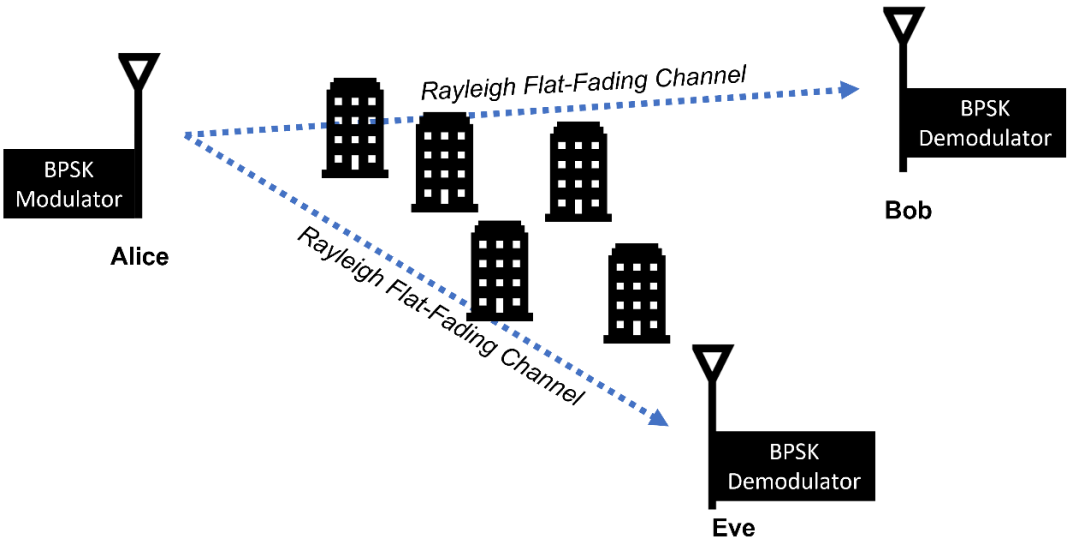

Figure 5: The system model for the Rayleigh channel simulation

To calculate the secrecy outage probability in a system with BPSK modulation scheme and a Rayleigh flat fading channel, where there are two receivers (a legitimate and an eavesdropper) and the secrecy outage probability is calculated in respect to the ratio of their signal-to-noise ratios (SNRs), the required steps are as follows:

1. Definition of the system parameters, such as the number of bits, the modulation type, and the noise SNR.
2. Generation of a sample of 1000 random bits using the randi function.
3. Modulation of the bits using BPSK modulation by mapping each bit to a complex-valued symbol.
4. Generation of a sample of channel gains from the Rayleigh distribution using the randraw function for both the destination and the eavesdropper.
5. Calculation of the received signal at the destination and the eavesdropper by multiplying the transmitted signal by the channel gains.
6. AWGN addition to the received signal using the AWGN function, with the noise SNR specified in dB.
7. Demodulation of the received signal at the destination and the eavesdropper using BPSK demodulation.

8. Calculation of the SNR of the received signal at the destination and the eavesdropper using the following formula:

$$SNR = \frac{P_s}{P_n}$$

where P_s is the power of the signal and P_n is the power of the noise.

9. Calculation of the secrecy outage probability as the fraction of transmitted bits where the ratio of the SNRs of the destination and the eavesdropper is less than a certain threshold.

The signal-to-noise ratio (SNR) of a symbol is typically calculated after demodulation in the receiver. This is because the SNR is a measure of the strength of the signal relative to the background noise, and it is usually calculated in the baseband domain after the signal has been demodulated.

In actuality, the received SNR can be measured by the following formula.

$$SNR = \frac{|h|^2}{N} \cdot E_s$$

Where h is the channel gain and N the signal power. In the specific system model, since the BPSK modulation scheme is used, the signal energy is equal to the bit energy. Hence the value of $\boldsymbol{E_s}$ is either 0 or 1. To calculate the probability of secrecy outage a sample of at total of 1000 transmissions of 10000 symbols was selected (Monte-Carlo Simulation). The SOP is calculated by dividing the number of samples with a K value below the threshold capacity by the total number of samples. The K value represents the ratio of the mean SNR of the destination to the mean SNR of the eavesdropper. The probability of each transmission is stored in a vector and is plotted against the average K value of each transmission in dB on a logarithmic scale (Fig. 6). The results of the simulation can be used to analyze the security of the communication system.

The ratio of the average SNR between the destination and eavesdropper is miniscule, but it is visible that the SOP decreases as the ratio increases. The general monotony of the scatter plot follows the theoretical curve shown in the previous section (Fig. 3). The yielded simulation results demonstrate that the secrecy outage probability remains below 0.6 and it has a descending rate, with the secrecy becoming more and more stable as the SNR ratio increases.

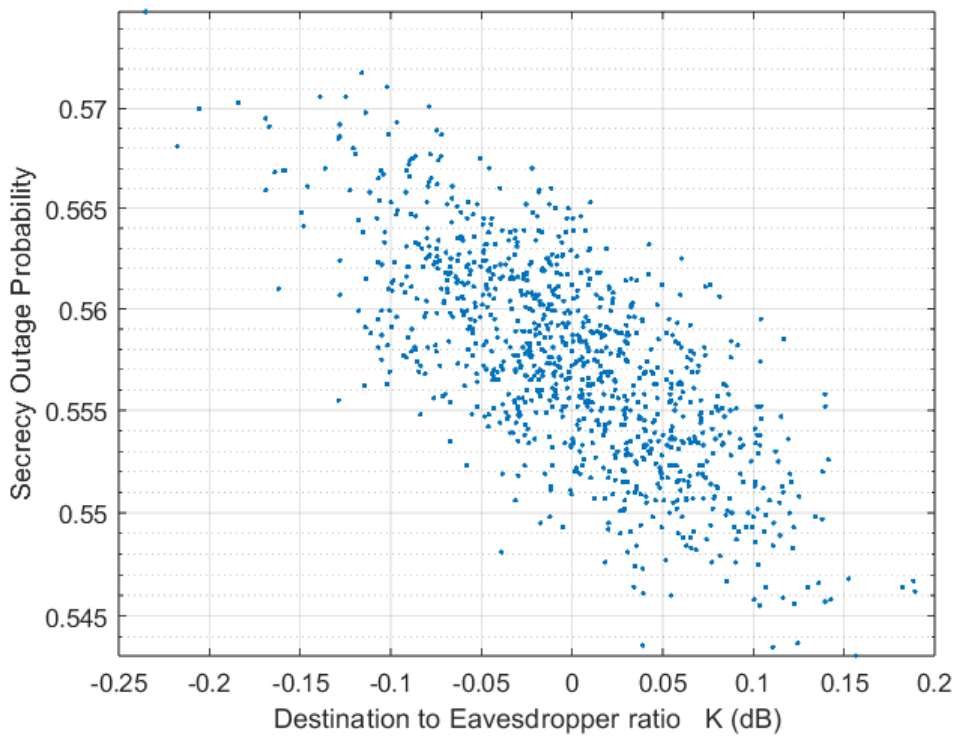

Figure 6: Demonstration of a realistic Rayleigh simulation (Monte-Carlo Simulation).

Section 4. Weibull Fading Channel

Weibull fading is a type of radio frequency signal fading that is commonly used to model the effects of signal attenuation in wireless communication systems. The Weibull distribution is a probability distribution that is widely used in reliability and survival analysis to model the failure of mechanical and electrical systems. In the context of wireless communication, the Weibull distribution is used to model the attenuation of radio waves as they travel through a medium. Like Rayleigh fading, Weibull fading is a statistical model that is used to represent the randomness and unpredictability of signal attenuation in a wireless channel.

The main difference between Weibull fading and Rayleigh fading is the shape of the probability distribution that is used to model the signal attenuation. The Weibull distribution has a more general shape than the Rayleigh distribution, which makes it a more flexible model for a wider range of wireless environments. In particular, the Weibull distribution can be used to model wireless channels with non-uniform attenuation, while the Rayleigh distribution is best suited to modeling channels with uniform attenuation.

The non-uniform nature of the Weibull fading describes a propagation environment where the obstacles are not uniformly distributed. The amplitude of the signal is modeled by a Weibull distribution, which is characterized by two parameters: a shape parameter, k, that determines the severity of the fading, and a scale parameter, λ, that determines the location of the distribution. Weibull fading is commonly observed in environments with non-uniform terrain, such as mountainous or hilly areas.

4.1. System model of Weibull fading channel

Based on the Generalized Gamma Distribution of the SNR and [Reference], the Weibull SNR distribution PDF is:

$$p_\gamma(\gamma) = \frac{c}{2}\left(\frac{\Gamma\left(1+\frac{2}{c}\right)}{\bar{\gamma}}\right)^{\frac{c}{2}} \gamma^{\frac{c}{2}-1} \exp\left[-\left(\frac{\gamma}{\bar{\gamma}}\Gamma\left(1+\frac{2}{c}\right)\right)^{\frac{c}{2}}\right], \quad \gamma \geq 0$$

The corresponding CDF is:

$$P_\gamma(\gamma) = 1 - \exp\left[-\left(\frac{\gamma}{\bar{\gamma}}\Gamma\left(1+\frac{2}{c}\right)\right)^{\frac{c}{2}}\right],\ \gamma \geq 0$$

The Rayleigh fading PDF can be derived from the previous PDF by substituting $c = 2$. The expression becomes:

$$p_\gamma(\gamma) = \frac{\Gamma(2)}{\bar{\gamma}}\exp\left(-\frac{\gamma}{\bar{\gamma}}\Gamma(2)\right)$$

Knowing that $\Gamma(2) = 1$, we have that:

$$p_\gamma(\gamma) = \frac{1}{\bar{\gamma}}\exp\left(-\frac{\gamma}{\bar{\gamma}}\right)$$

Which is the Rayleigh PDF. Thus, the Weibull fading model is a generalization of the Rayleigh fading model.

4.2. Secrecy outage probability analysis

To calculate the secrecy outage probability of the Weibull fading channel, we have to solve the following expression, previously derived in Section 3.

$$SOP = \int_0^{+\infty} F_D(\Theta\gamma_E + \Theta - 1)\cdot f_E(\gamma_E)d\gamma_E$$

Where the constant $\Theta = 2^{C_{th}}$. Substituting the expressions inside the integral, we have the following definite integral.

$$SOP = \int_0^{+\infty} \frac{1}{2}c\cdot e^{-(q\gamma_E)^{\frac{c}{2}}}\cdot\left(1 - e^{-\left(p(\Theta\gamma_E+\Theta-1)\right)^{\frac{c}{2}}}\right)\cdot\xi\gamma_E^{\ -1+\frac{c}{2}}\,d\gamma_E$$

The constants appearing inside the integral for simplicity reasons are:

$$q = \frac{\Gamma\left(1+\frac{2}{c}\right)}{\overline{\gamma_E}}$$

$$p = \frac{\Gamma\left(1+\frac{2}{c}\right)}{\overline{\gamma_D}}$$

$$\xi = \frac{c}{2} \cdot \left(\frac{\Gamma\left(1+\frac{c}{2}\right)}{\overline{\gamma_E}}\right)$$

To simplify the complex expression, a series of algebraic transformations must be done.

$$SOP = \frac{1}{2} c \cdot \xi \int_0^{+\infty} \left(e^{-(q\gamma_E)^{\frac{c}{2}}} - e^{-(q\gamma_E)^{\frac{c}{2}}} \cdot e^{-\left(p(-1+\Theta+\Theta\gamma_E)\right)^{\frac{c}{2}}}\right) \cdot \gamma_E^{-1+\frac{c}{2}} d\gamma_E \Leftrightarrow$$

$$SOP = \frac{c\xi}{2} \int_0^{+\infty} e^{-(q\gamma_E)^{\frac{c}{2}}} \cdot \gamma_E^{-1+\frac{c}{2}} - e^{-(q\gamma_E)^{\frac{c}{2}}} \cdot e^{-\left(p(-1+\Theta+\Theta\gamma_E)\right)^{\frac{c}{2}}} \cdot \gamma_E^{-1+\frac{c}{2}} d\gamma_E \Leftrightarrow$$

$$SOP = \frac{c\xi}{2} \left[\int_0^{+\infty} e^{-(q\gamma_E)^{\frac{c}{2}}} \cdot \gamma_E^{-1+\frac{c}{2}} d\gamma_E - \int_0^{+\infty} e^{-(q\gamma_E)^{\frac{c}{2}}} \cdot e^{-\left(p(-1+\Theta+\Theta\gamma_E)\right)^{\frac{c}{2}}} \cdot \gamma_E^{-1+\frac{c}{2}} d\gamma_E\right] \Leftrightarrow$$

Having two integrals, each is solved separately.

$$I_1 = \int_0^{+\infty} e^{-(q\gamma_E)^{\frac{c}{2}}} \cdot \gamma_E^{-1+\frac{c}{2}} d\gamma_E \Leftrightarrow I_1 = \frac{2q^{-\frac{c}{2}}}{c}, \;\; Re\{c\} > 0 \;\&\&\; Re\left\{q^{\frac{c}{2}}\right\} > 0$$

The second integral is too difficult to solve analytically. We can firstly check, if for shape parameter, equal to 2, the integral will yield the Rayleigh fading channel.

Assuming that $c = 2$, the second integral is solved as such:

$$I_2 = \int_0^{+\infty} e^{-qx-p(-1+\Theta+\Theta x)} dx \Leftrightarrow I_2 = \frac{e^{p-p\Theta}}{q+p\Theta}, \;\; Re\{q+p\Theta\} > 0$$

Substituting the two integrals in the initial expression we have, while c = 2:

$$SOP = \frac{1}{q} - \frac{e^{p-p\Theta}}{q+p\Theta}, Re\{c\} > 0, Re\left\{q^{\frac{c}{2}}\right\} > 0, Re\{q+p\Theta\} > 0$$

The following step is the substitution of the constant parameters q, p and Θ. For c=2, the parameters are evaluated as:

$$p = \frac{\Gamma(1+1)}{\overline{\gamma_D}} = \frac{1}{\overline{\gamma_D}}$$

$$q = \frac{\Gamma(2)}{\overline{\gamma_E}} = \frac{1}{\overline{\gamma_E}}$$

$$\xi = \frac{2}{2} \cdot \frac{\Gamma(2)}{\overline{\gamma_E}} = \frac{1}{\overline{\gamma_E}}$$

$$SOP = \frac{c\xi}{2}\left[\frac{1}{q} - \frac{e^{p-p\Theta}}{q+p\Theta}\right], Re\{c\} > 0, Re\{q\} > 0, Re\{q+p\Theta\} > 0$$

The upper expression can be further simplified as such:

$$SOP = \frac{1}{\overline{\gamma_E}} \cdot \left[\frac{1}{\frac{1}{\overline{\gamma_E}}} - \frac{\exp\left(p(1-\Theta)\right)}{\frac{1}{\gamma_{\bar{E}}} + \frac{\Theta}{\overline{\gamma_D}}}\right] = \frac{1}{\overline{\gamma_E}} \cdot \left[\overline{\gamma_E} - \frac{\exp\left(\frac{1}{\overline{\gamma_D}}(1-\Theta)\right)}{\frac{1}{\overline{\gamma_E}} + \frac{\Theta}{\overline{\gamma_D}}}\right] = SOP$$

$$= 1 - \exp\left(\frac{1}{\overline{\gamma_D}}(1-\Theta)\right) \cdot \frac{1}{1 + \frac{\Theta\overline{\gamma_E}}{\overline{\gamma_D}}}$$

By completing the algebraic simplifications, we have the final closed form SOP expression which is the SOP for the Rayleigh channel.

$$SOP = 1 - \exp\left(\frac{-\Theta+1}{\overline{\gamma_D}}\right) \cdot \frac{\overline{\gamma_D}}{\overline{\gamma_D} + \Theta\overline{\gamma_E}}$$

Continuing, we can solve the second integral for even shape parameters. The appearance of odd shape parameters leads to irrational exponents, which are harder to solve and require more complex analytical calculations. Thus, the second achievable closed form is presented for shape parameter equal to 4.

$$I_2 = \int_0^{+\infty} e^{-q^2x^2 - p^2(-1+t+tx)^2} x\, dx \Leftrightarrow$$

$$I_2 = \frac{e^{-p^2(-1+t)^2}\left(\sqrt{q^2+p^2t^2} - e^{\frac{p^4(-1+t)^2t^2}{q^2+p^2t^2}} p^2\sqrt{\pi}(-1+t)t \cdot \mathrm{Erfc}\left[\frac{p^2(-1+t)t}{\sqrt{q^2+p^2t^2}}\right]\right)}{2(q^2+p^2t^2)^{3/2}}$$

The conditions for the upper integral are:

$$\mathrm{Re}[q^2+p^2t^2] \geq 0 \;\&\&\; (\mathrm{Re}[p^2(-1+t)t] > 0 \;||\mathrm{Re}[q^2+p^2t^2]) > 0$$

Since all the parameters are strictly positive by default, the final SOP closed form expression for a shape parameter of 4 is:

$$SOP = \frac{c\xi}{2}\left[\frac{1}{q^2} - \frac{e^{-p^2(-1+t)^2}\left(\sqrt{q^2+p^2t^2} - e^{\frac{p^4(-1+t)^2t^2}{q^2+p^2t^2}} p^2\sqrt{\pi}(-1+t)t \cdot \mathrm{Erfc}\left[\frac{p^2(-1+t)t}{\sqrt{q^2+p^2t^2}}\right]\right)}{2(q^2+p^2t^2)^{3/2}}\right]$$

The upper form is not going to be simplified further, the parameter values are going to be filled during the simulations. The closed forms for bigger shape parameters are solvable by using integration by parts, but the complexity of the calculations is also increasing. For simplicity reasons, only the first two even shape parameters are derived.

4.3. Simulations

Following the same procedure as the Rayleigh fading channel simulation, both the c=2 and c=4 SOP are going to be presented in the same axis. As with the previous simulation, the axis is semilogarithmic as it is mostly common.

4.3.1. Analytical expression simulations

In order to simulate the SOP under Weibull fading channel some initial conditions must be assumed. The threshold capacity is once again set at 1 dB, while the c parameter is going to be changed inside the code. The first simulation is expected to be like the Rayleigh simulation, since it was already proven mathematically in an earlier section. The first simulation will concentrate on demonstrating the connection between the legitimate receiver, or destination and the SOP. It is expected that as the destination average SNR is increasing, the SOP will be decreasing, since the ratio of destination to eavesdropper is maximized. By running the simulation, the following results are taken (Fig. 7).

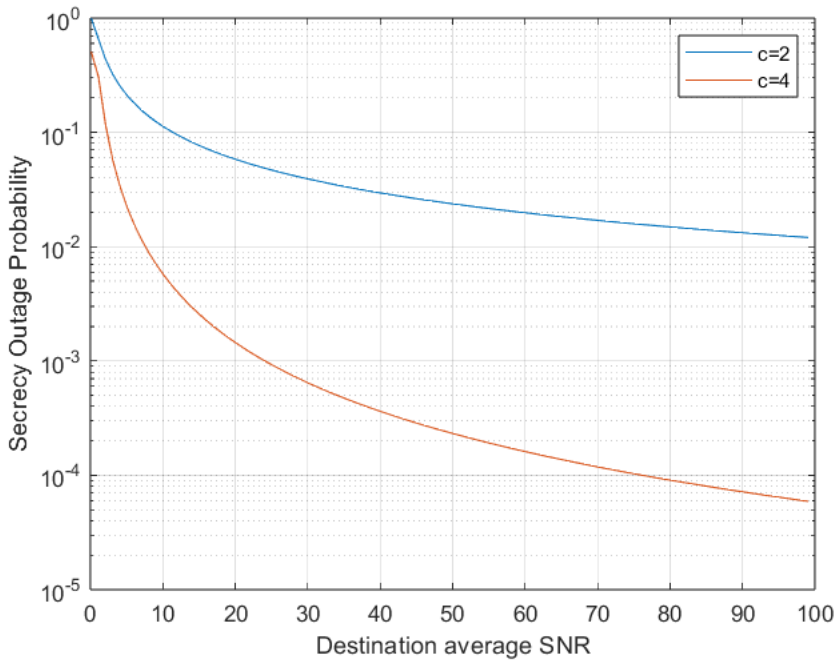

Figure 7: Simulation of Weibull Fading channel in respect to the Destination average SNR

As it is clearly communicated by the curves, when the shape parameter becomes equal to 2, the Weibull fading becomes equal to the Rayleigh fading. This is easily noticed by observing the corresponding curve in the previous section (Fig. 2). In this simple system model, when the shape parameter becomes equal to 4, the SOP is noticeably better. The curve is much steeper than the Rayleigh one, which indicates a higher decrease rate. Thus, it can be assumed that for higher shape parameters the curve will only become steeper, due to the mathematical expression.

The simulation for when the eavesdropper average SNR increases and c=4 could not be implemented due to the extreme steepness of the curve. Incorrect initial conditions may yield erroneous results. The simulation for c=2 can be easily implemented, with the resulting curve (Fig. 8) being like the corresponding Rayleigh simulation (Fig. 1).

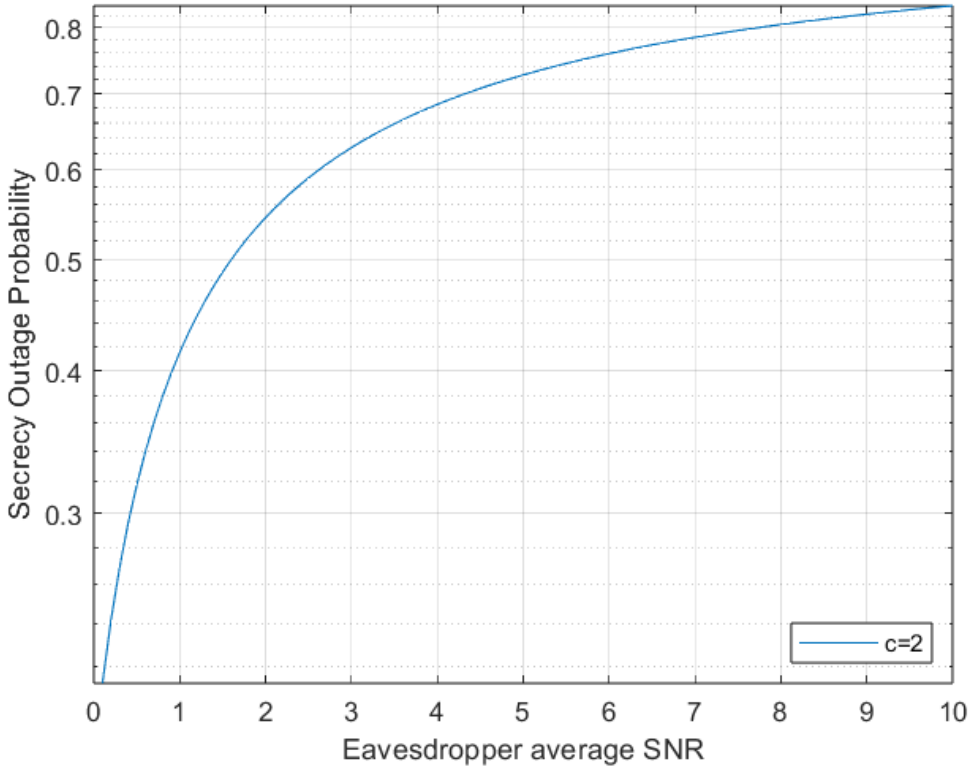

Figure 8: Simulation of increasing eavesdropper SNR, verifying that for c=2, Weibull fading becomes Rayleigh fading

The last simulation to be run is the ratio of destination to eavesdropper. To simulate the SOP correctly, certain initial parameters are needed. It is assumed that the ratios go from 0 to 100 dB, with the average SNR at the eavesdropper being 0.1 and the average SNR at the destination being a multiplicand of the eavesdropper, with their ratio being increased. The other simulation parameters remain unchanged, resulting in the following curve (Fig. 9).

In the figure it is once again observed that the Weibull fading for shape parameter 4 displays a higher decrement rate than the Rayleigh fading (shape parameter c = 2). This simulation result allows the assumption that the Weibull fading for shape parameter c = 4 demonstrates higher secrecy than the Rayleigh fading.

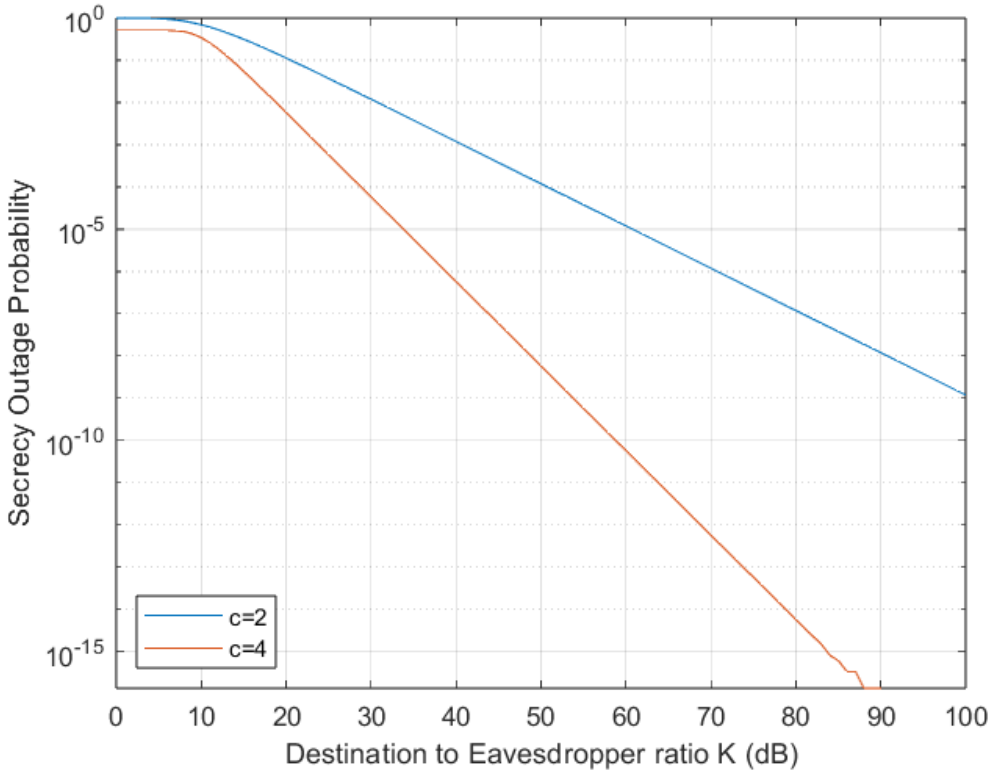

Figure 9: Simulation plot of the Destination to Eavesdropper ratio for the Weibull fading channel.

4.3.2. Realistic system model simulations

By reconfiguring the previous realistic system model simulation program in MATLAB, it is possible to demonstrate results for different fading channels, while simultaneously keeping the initial simulation parameters unchanged. By denoting a Weibull of shape parameter 2 and scale parameter $\lambda = \sqrt{2}\sigma$, we receive the simulation for the Rayleigh fading channel (Fig. 10).

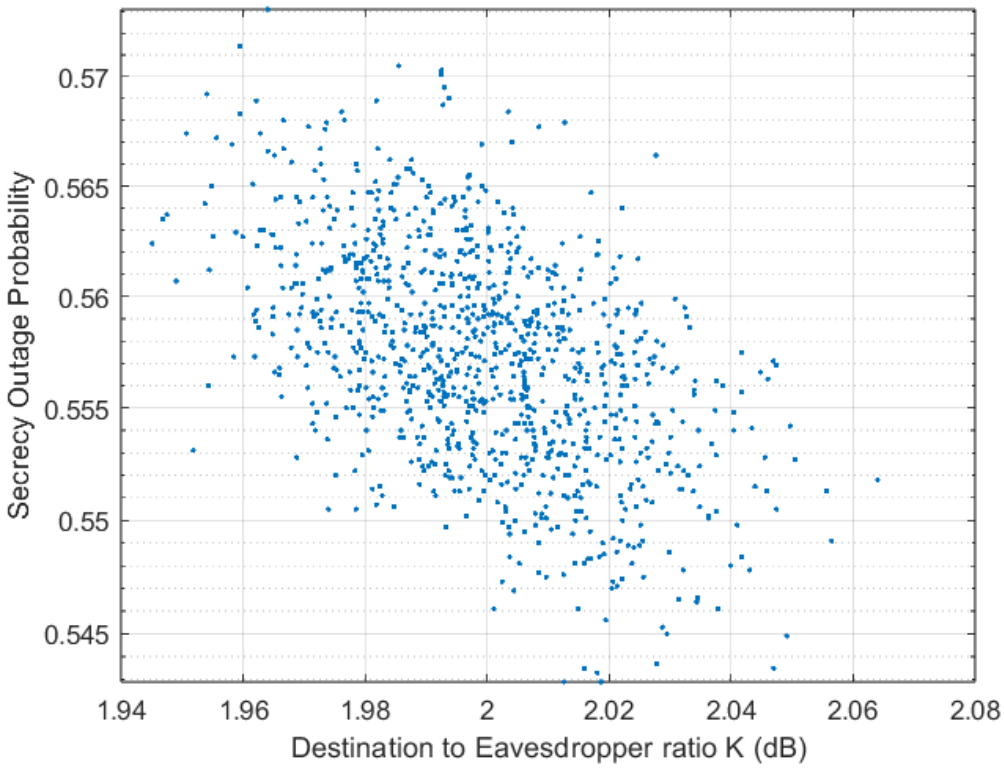

Figure 10: Demonstration of a realistic Weibull (c = 2) simulation (Monte-Carlo Simulation).

Due to other parameters being unchanged, the simulation scatter plot displays a larger scattering than the corresponding scatter plot in the previous section. Regardless, the scatter plot displays a similar decreasing tendency, which is expected. The second simulation is executed for a shape parameter equal to 4 and the rest of the parameters remain the same. The generated scatter plot can be seen in the following figure (Fig.11),

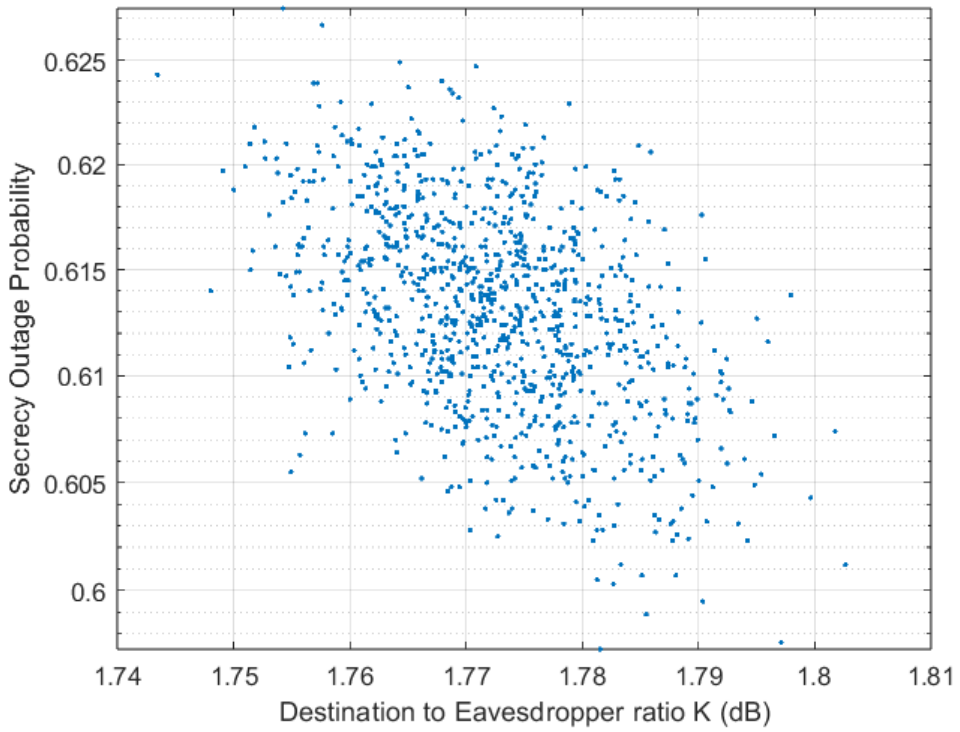

Figure 11: Demonstration of a realistic Weibull (c = 4) simulation (Monte-Carlo Simulation).

To verify the result, the curve fitting method is used. By finding the curve that best fits the scattered data, it is easily observed that the best fitting curve has the shape of the previously demonstrated SOP curves (Fig. 12). The curve fitting method is a mathematical technique used to find a function that best describes a set of data points. The goal is to find a curve that passes through or near the data points and captures the general trend of the data. The curve fitting process involves selecting a type of curve, choosing a fitting algorithm, specifying the data to be fitted, and adjusting fitting options. The choice of the type of curve and the fitting algorithm depends on the specific characteristics of the data and the desired level of accuracy. In this example, the curve that was used was a simple 2^{nd} order polynomial. Regardless, the resulted curve managed to verify the initial conjecture that the data were following the SOP curve.

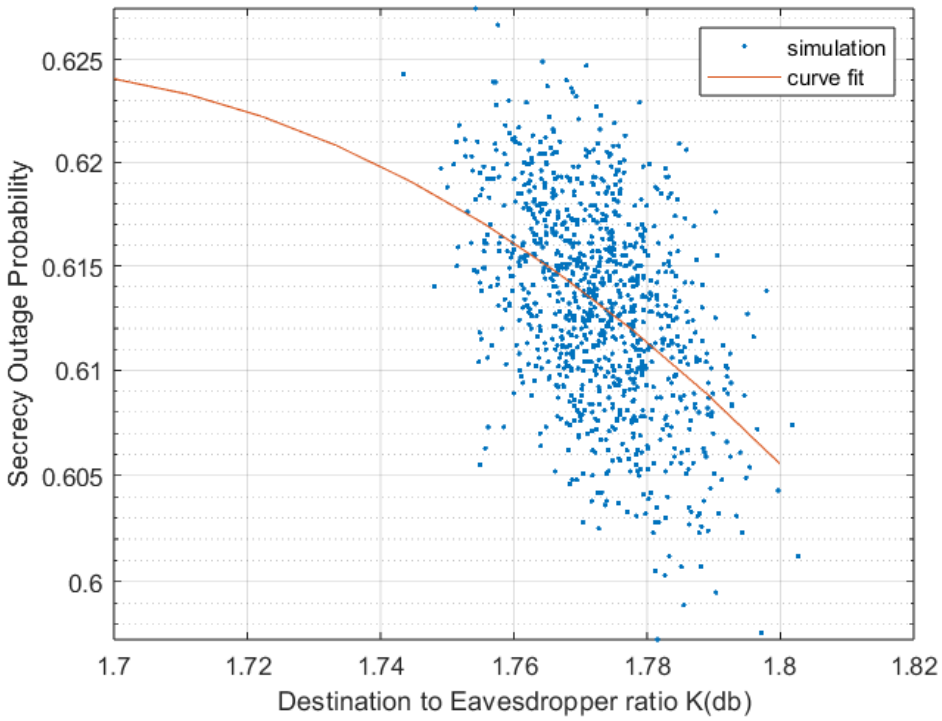

Figure 12: Demonstration of a realistic Weibull (c=4) simulation (Monte-Carlo Simulation) along with the best fitting curve

Section 5. Rician Fading Channel

The current section aims to present the Rician Fading channel from a more theoretical view. The Rician fading channel is a mathematical model used to describe the effect of multipath propagation in wireless communication systems. In a Rician fading channel, the signal from the transmitter is received by the receiver through multiple paths, which can result in constructive or destructive interference at the receiver. The Rician fading channel is characterized by two parameters: the Rician K-factor and the average signal power. The Rician K-factor represents the ratio of the power in the line-of-sight (LOS) path to the power in the non-line-of-sight (NLOS) paths. The LOS path is the direct path from the transmitter to the receiver, while the NLOS paths are the indirect paths that reflect off objects in the environment.

The Rician fading channel is often used to model wireless communication systems in which there is a strong LOS path, such as in satellite communications or microwave links. The Rician fading channel can also be used to model communication systems in urban environments, where there are many reflections from buildings and other structures. In Rician fading channel models, the received signal power is typically assumed to be distributed according to a Rician distribution, which is a combination of a Gaussian distribution and a non-central chi-squared distribution. The Rician distribution can be used to model the distribution of the received signal power in a Rician fading channel, which can be used to calculate various performance metrics, such as the bit error rate or the channel capacity.

5.1. Secrecy Outage Probability

To analyze the SOP on a simple wiretap channel in the presence of Rician fading, extensive mathematical knowledge is required. The Rician or Nakagami-n PDF of SNR is:

$$P_\gamma(\gamma) = \frac{(1+n^2)e^{-n^2}}{\bar{\gamma}} e^{-\left(\frac{(1+n^2)\gamma}{\bar{\gamma}}\right)} I_o\left(2n\sqrt{\frac{(1+n^2)\gamma}{\bar{\gamma}}}\right), \qquad n \geq 0$$

Where n is the fading parameter of the channel. Respectively, I_o is the 0^{th} order modified Bessel function of the first kind.

$$I_a(x) = i^{-a}J_a(ix) = \sum_{m=0}^{\infty} \frac{1}{m!\,\Gamma(m+a+1)}\left(\frac{x}{2}\right)^{2m+a}$$

The Rician K-factor is defined as:

$$k = n^2$$

The K-factor is defined as the power of the LOS component to the average power of the scattered component. It is easily proved that for LOS component equal to 0, the distribution becomes a Rayleigh distribution. Thus, in the same manner as with the Rayleigh fading channel, the secrecy outage probability can be measured by the following formula.

$$SOP = \int_0^{\infty} F_D(\lambda + \lambda\gamma_E - 1) f_E(\gamma_E) d\gamma_E$$

To calculate the closed form, or an approximation, we must first calculate the cumulative density function (CDF) of the Rician PDF. The following integral must be solved.

$$F_x(x) = \int_{-\infty}^{x} \frac{(1+n^2)e^{-n^2}}{\bar{\gamma}} e^{-\left(\frac{(1+n^2)\gamma}{\bar{\gamma}}\right)} I_o\left(2n\sqrt{\frac{(1+n^2)\gamma}{\bar{\gamma}}}\right) d\gamma$$

Moreover, to solve this integral, it is required to substitute the complicated constant values with simple letters/parameters. We have the following form.

$$F_x(x) = \int_{-\infty}^{x} a e^{-n^2} e^{-(a\gamma)} I_o\left(2n\sqrt{a\gamma}\right) d\gamma, \;\; where, \;\; a = \frac{1+n^2}{\bar{\gamma}}$$

Considering that the previous integral appears similar to a known integral [9] (p.699),

$$\int_0^{\infty} e^{-ax^2} I_\nu(\beta x)\, dx = \frac{\sqrt{\pi}}{2\sqrt{a}} e^{\left(\frac{\beta^2}{8a}\right)} I_{\frac{\nu}{2}}\left(\frac{\beta^2}{8a}\right), when\ Re\{\nu\} > -1\ and\ Re\{a\} > 0$$

And by also considering $\beta = 2n$ and $x = \sqrt{a\gamma}$, there is a possible solution for $\nu = 0$.

$$\int_0^{\infty} e^{-a^2\gamma} I_0\left(2n\sqrt{a\gamma}\right) dx = \frac{\sqrt{\pi}}{2\sqrt{a}} e^{\left(\frac{n^2}{4a}\right)} I_0\left(\frac{n^2}{4a}\right)$$

The upper mathematical expression corresponds to the CDF of the Rician PDF of SNR. The calculation of SOP using Eq. # results in rigorous mathematical calculations which require further knowledge of more advanced concepts. There is a given formula to calculate the SOP in presence

of Rician fading [10], but the given formula is not of closed form, which contrasts the goal of the current thesis in presenting closed forms. The simulations in [10] inferred that the SOP decreases with the increased values of the receiver's average SNR and increases with the increased values of the eavesdropper's average SNR (Fig. 13). This result is logical, as it was also verified as such in earlier sections. During the simulations the LOS component for both legitimate and illegitimate receivers was placed as $K_D = K_E = 2$.

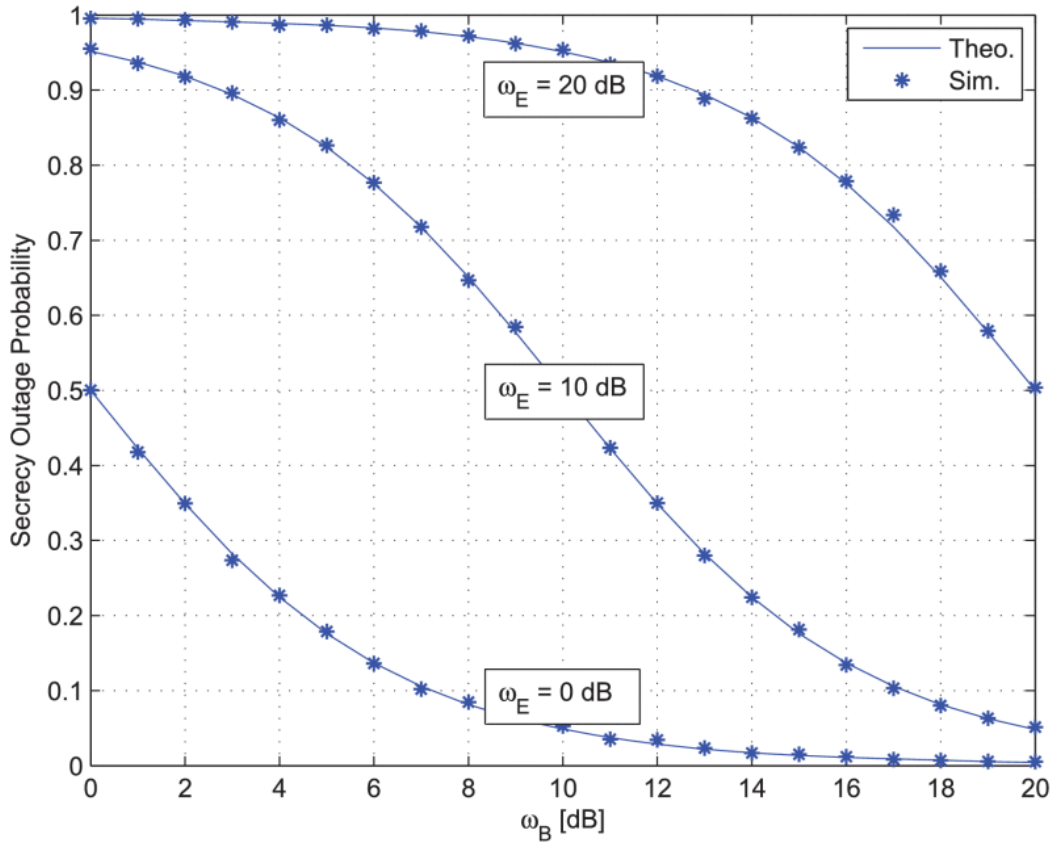

Figure 13: Secrecy Outage Probability versus ω_B, with LOS components equal to 2 and maximum frequency of 20 Hz. The simulation is executed in respect to varying values of the illegitimate receiver's average SNR (ω_E). [10]

5.2. Realistic system model simulation

Even though it was not possible to derive closed theorical (analytical) forms, it is possible to execute the realistic system model simulation that was implemented in the Rayleigh fading simulations. In this example the chosen parameters were the noncentrality parameter, which is related to the LOS component, set to 1 and the scale parameter set to 3. The results Fig.14 demonstrated a similar decreasing tendency, much like the curves in Fig.13.

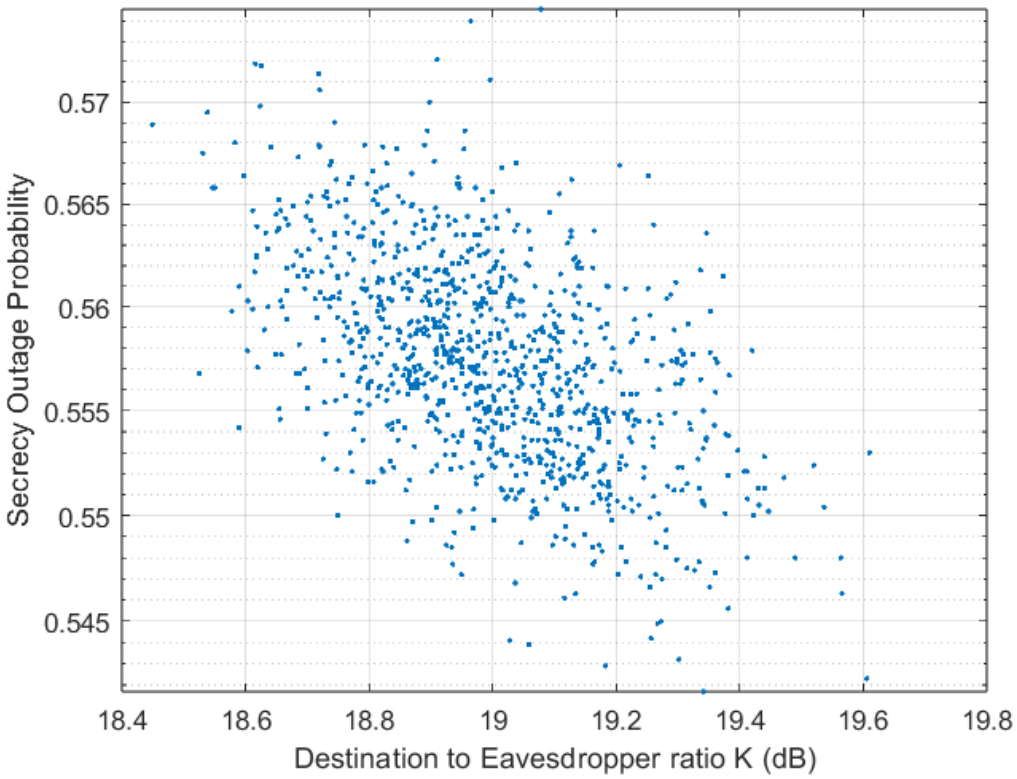

Figure 14: Demonstration of realistic Rician fading channel.

In order to further observe the decreasing tendency, the curve fitting technique was used. The results (Fig.15) demonstrate that the best fitting curve (3rd Order Polynomial function) contains a negative gradient, meaning that the function is decreasing the higher the K-ratio becomes.

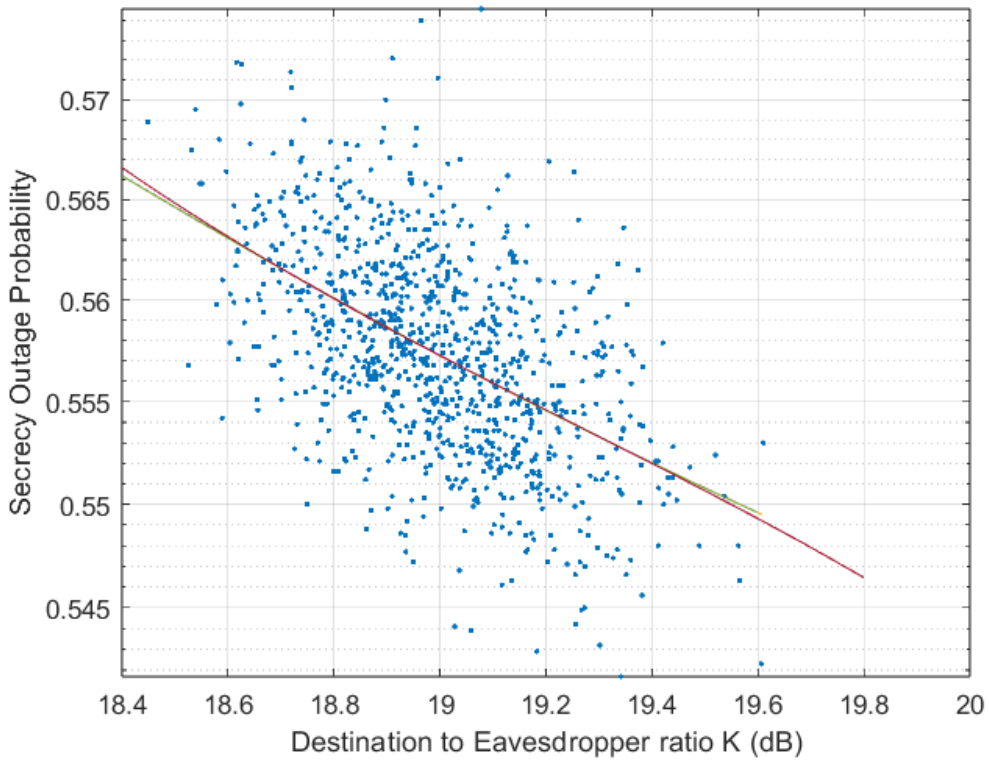

Figure 15: Demonstration of a realistic Rician fading channel SOP, along with the best fitting curve.

Section 8. Conclusion

The completion of this thesis has yielded multiple conclusions. Firstly, an introduction to the field of security at the physical level was performed, by presenting its most important concepts. Then, these concepts were studied and used to extract important information on the field of wireless communications. Dealing with the solution of mathematical expressions and verification through simulations was a vigorous introduction to university research and study. Through mathematics it became possible to verify properties and derive closed forms of difficult statistical models, while properties and hypotheses were also verified through simulations. It was shown that it is possible to exploit the physical information of the channel in order to evaluate the quality of transmission, the integrity of the transmitted information and the security of the data. This thesis may well be extended in the future through the study of more complex system models and through the application of more complex techniques.

Bibliography

[1] **H. Lei, C. Gao, Y. Guo and G. Pan, "On Physical Layer Security over Generalized Gamma Fading Channels," *IEEE Communications Letters,* vol. 19, no. 7, pp. 1257-1260, 2015.**

[2] **M. K. Simon and M.-S. Alouini, Digital Communication over Fading Channels, Second Edition ed., Wiley-Interscience, 2005.**

[3] **W. Yajun, L. Tongqing and W. Chuanan, "An anti-eavesdrop transmission scheduling scheme based on maximizing secrecy outage probability in ad hoc networks," *China Communications,* vol. 13, no. 1, pp. pp. 176-184, 2016.**

[4] **A. Chorti, A. N. Barreto, S. Köpsell, M. Zoli, M. Chafii, P. Sehier, G. Fettweis and H. V. Poor, "Context-Aware Security for 6G Wireless: The Role of Physical Layer Security," *IEEE Communications Standards Magazine,* vol. 6, no. 1, pp. pp. 102-108, 2022.**

[5] **A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal,* vol. 54, no. 8, pp. pp. 1355-1387, 1975.**

[6] **H. Zhao, Y. Liu, A. Sultan-Salem and M. -S. Alouini, "A Simple Evaluation for the Secrecy Outage Probability Over Generalized-K Fading Channels," *IEEE Communication Letters,* vol. 23, no. 9, pp. pp. 1479-1483, 2019.**

[7] **E. R. Alotaibi and K. A. Hamdi, "Secrecy Outage Probability Analysis for Cooperative Communication with Relay Selection Under Non-Indentical Distribution," *2016 IEEE Wireless Conference and Networking Conference,* pp. pp. 1-6, 2016.**

[8] **J. A. Anastasov, A. S. Panajotović, N. M. Sekulović, D. N. Milić and D. M. Milović, "Secrecy outage probability and intercept probability analysis over α-F fading channels," *2022 57th International Scientific Conference on Information, Communication and Energy Systems and Technologies (ICEST),* pp. pp. 1-4, 2022.**

[9] **A. P. Prudnikov, Y. A. Brychkov and O. I. Marichev, Integrals and Series Volume 3: More Special Functions, Gordon and Breach Science Publishers, 1990.**

[10] **M. Abughalwa, A. Omri and M. O. Hasna, "On the Average Secrecy Outage Rate and Average Secrecy Outage Duration of Wiretap Channels with Rician Fading," *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC),* pp. pp. 736-740, 2018.**

[11] **A. P. Prudnikov, Y. A. Brychkov and O. I. Marichev, Integrals and Series Volume 2: Special Functions, Gordon and Breach Science Publishers, 1986.**

[12] **G. Euthimioglou, Telecommunication Systems Simulation and Performance, Kallipos, 2015.**

[13] **M. Bloch, J. Barros, M. R. D. Rodrigues and S. W. McLaughlin, "Wireless Information-Theoretic Security," *IEEE Transactions on Information Theory,* vol. 54, no. 6, pp. pp. 2515-2534, 2008.**

[14] **S. Ö. Ata, "Secrecy Performance Analysis Over Double Nakagami-m Fading Channels," *2018 41st International Conference on Telecommunications and Signal Processing (TSP),* pp. pp. 1-4, 2018.**

Appendix