

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΥΠΕΥΘΥΝΟΣ

Θεόδωρος Τσιφτσής

Καθηγητής

Λαμία, Ιανουάριος 2023

Ασφάλεια στο Φυσικό Επίπεδο σε Ασύρματα Κανάλια με Διαλείψεις

Αρίστος Καράμπελας-Τιμοτίεβιτς

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ



ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

Ασφάλεια στο Φυσικό Επίπεδο σε Ασύρματα Κανάλια με Διαλείψεις

Αρίστος Καράμπελας-Τιμοτίεβιτς



ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΥΠΕΥΘΥΝΟΣ

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

ADVISOR

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)*   *«Όποιος 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.»*

### ΠΕΡΙΛΗΨΗ

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 τέσσερα ασύρματα κανάλια με την παρουσία διαλείψεων, Rayleigh, Rice, Nakagami-μ και Weibull. 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 four wireless channels in the presence of flat fading, Rayleigh, Rice, Nakagami-M and Weibull, are presented in detail and through simulations. Finally, conclusions are expressed for the security evaluation of each channel, as well as for future extensions.

Table of Contents

[ΠΕΡΙΛΗΨΗ i](#_Toc123254752)

[ABSTRACT iii](#_Toc123254753)

[SECTION 1. Introduction 1](#_Toc123254754)

[1.1. Wireless Communications 1](#_Toc123254755)

[1.1. Definition 1](#_Toc123254756)

[1.2. Flat-Fading Channels 1](#_Toc123254757)

[SECTION 2. LITERATURE REVIEW 2](#_Toc123254758)

[(Υποκεφάλαιο 2.1) 2](#_Toc123254759)

[(Ενότητα 2.1.α) 2](#_Toc123254760)

[SECTION 3. Rayleigh Fading Channel 3](#_Toc123254761)

[3.1. System model of Rayleigh fading channel 3](#_Toc123254762)

[3.2. Secrecy Outage Probability Analysis 5](#_Toc123254763)

[3.3. Simulations 8](#_Toc123254764)

[3.3.1. Simulation of the analytical expression 8](#_Toc123254765)

[3.3.2. Simulation 9](#_Toc123254766)

[SECTION 4 ……… 11](#_Toc123254767)

[(Υποκεφάλαιο 4.1) 11](#_Toc123254768)

[(Ενότητα 4.1.α) 11](#_Toc123254769)

[SECTION 5 Συμπεράσματα 12](#_Toc123254770)

[ΒΙΒΛΙΟΓΡΑΦΙΑ 13](#_Toc123254771)

# SECTION 1. Introduction

## 1.1. Wireless Communications

### 1.1. Definition

## 1.2. Flat-Fading Channels

# SECTION 2. LITERATURE REVIEW

## (Υποκεφάλαιο 2.1)

### (Ενότητα 2.1.α)

# 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. 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 , it will have a pdf:

Where 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:

As told, the distribution is zero-centered, which means that , thus . This means that:

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 [1] the GG distribution of the random variable R is given by:

In this equation the a is the fading parameter, c is the normalized variance of the channel envelope R, and is the ath mean square of the channel envelope. The gamma function is the following:

By changing the parameters of the GG distribution, we can obtain other famous distributions like Rayleigh, Rice, Weibull and Nakagami-m. Beginning the substitution using the Rayleigh parameters, where and .

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

Since , then:

The upper equation is the exact same as the Rayleigh model that we presented in relation (1). The , thus the final model equation is:

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:

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

The ratio is the energy per bit to the noise power spectral density. By substituting the parameters for the Rayleigh fading (, and assuming that the parameters are the same for both the main and eavesdropper channels, we have the following equation:

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

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

Thus, the previous equation becomes

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

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:

By considering that we are using bit transmission we have the capacity as it was defined by Shannon-Hartley. In the upper formula the describes the predesignated threshold capacity for the secrecy outage. Respectively, the describes the ratio of the destination capacity to eavesdropper capacity.

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

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

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:

We set , and then apply the first integral:

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

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

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

Respectively, we have the following:

The final integral to be solved is the following:

We will now attempt to simplify the equation:

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.

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

Thus, the integral will be transfigured as such:

We will solve each integral separately:

Substituting the solutions in the initial integral we have

Since we know that , 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.

The during the analytical simulation it is assumed that the threshold secrecy capacity is , the noise SNR is , the sample size is equal to 1000 symbols 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 first step in this simulation is to convert the decibels of K into numbers using the standard dB conversion. Continuing, random values for the eavesdropper average SNR are chosen. Another assumption is that the legitimate receiver’s average SNR is K-times the eavesdropper’s average SNR:

Finally, from the analytical solution we have that . The MATLAB script which implements the simulation can be found in Appendix 1 **(*add link*)**. The generated figure is shown in Fig.#

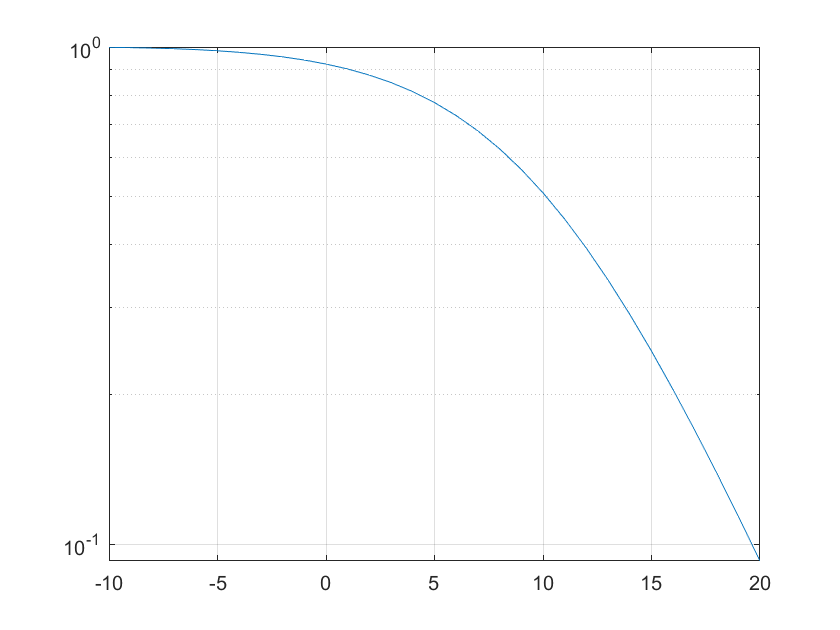


Figure 1: Simulation plot of the analytical SOP expression

We can see that as the ratio increases, the SOP decreases. This is due to the fact that 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.

### 3.3.2. Simulation

The system model we are going to use in our simulation is (Picture #):

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

Define the parameters of the system, such as the number of bits, the modulation type, and the noise SNR.

Generate a sample of 1000 random bits using the randi function.

Modulate the bits using BPSK modulation by mapping each bit to a complex-valued symbol. You can use the pskmod function to do this.

Generate a sample of channel gains from the Rayleigh distribution using the raylrnd function for both the destination and the eavesdropper.

Calculate the received signal at the destination and the eavesdropper by multiplying the transmitted signal by the channel gains.

Add noise to the received signal using the awgn function, with the noise SNR specified in dB.

Demodulate the received signal at the destination and the eavesdropper using BPSK demodulation. You can use the pskdemod function to do this.

Calculate the SNR of the received signal at the destination and the eavesdropper. You can use the formula:

SNR = P\_s / P\_n

where P\_s is the power of the signal and P\_n is the power of the noise.

Calculate 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.

# SECTION 4 ………

## (Υποκεφάλαιο 4.1)

### (Ενότητα 4.1.α)

# SECTION 5 Συμπεράσματα

# ΒΙΒΛΙΟΓΡΑΦΙΑ

Εδώ θα προστεθεί όλη η βιβλιογραφία