Develop an Effective Security Model to Protect Wireless Network

Somya Khidir Mohmmed Ataelmanan[1*] Mostafa Ahmed Hassan Ali[2]

[1] Computer Science Department, College of Computer Engineering & Science, Prince Sattam Bin Abdulaziz University, P.O.Box 422, Alkharj 11942, Saudi Arabia

[2]Communication Engineering Departments, Faculty of Engineering
AL-Neelain University. Khartoum, Sudan

*Corresponding Author
Somya Khidir Mohmmed Ataelmanan
Computer Science Department, College of Computer Engineering & Science, Prince Sattam Bin Abdulaziz University, P.O.Box 422, Alkharj 11942, Saudi Arabia

Abstract
Security is an important issue for wireless communications and poses many challenges. Most security schemes have been applied to the upper layers of communications networks. Since in a typical wireless communication, transmission of data is over the air, third party receiver(s) may have easy access to the transmitted data. This work examines a new security technique at the physical layer for the sake of enhancing the protection of wireless communications against eavesdroppers. We examine the issue of secret communication through Rayleigh fading channel in the presence of an eavesdropper in which the transmitter knows the channel state information of both the main and eavesdropper channel. Then, we analyze the capacity of the main channel and eavesdropper channel we also analyze for the symbol error rate of the main channel, and the outage probability is obtained for the main transmission. This work elucidate that the proposed security technique can safely complement other Security approaches implemented in the upper layers of the communication network. Lastly, we implement the results in Mat lab

Keywords:
Wireless Networks, Security Model, Rayleigh fading channel.

.1. Introduction

Security is a critical side of concerning issues for communication networks due to the multiple attacks that have been reported in recent years (Devi &Suganthi, 2014). Security is significant for the designers of wireless networks. The traditional security measures provided for a specific type of network might be impractical for other types of networks (Debbah et al., 2010).

The physical radio transmission aspects of wireless systems have been studied and addressed separately from the security issues in wireless networks. On the other hand, new network architectures are emerging and not compatible with traditional security measures like data encryption for secured communication. Moreover, the increasing neediness for security of physical environment has also increased the interest in proposing possible physical features for secure communication (Debbah et al., 2010).

Recently, wireless networks have gained the attention of security researchers due to the huge advances in wireless network technologies and the attempt to build a secured reliable communication. Wireless security aims to preventillegitimate Users from damaging the resources of wireless network (Sreedhar et al., 2010).

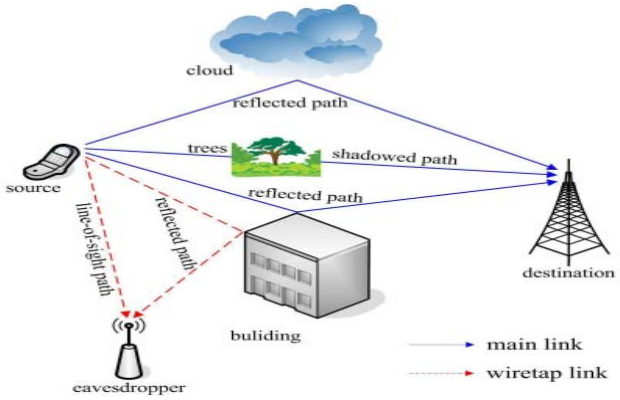

Figure 1.1: Wireless data transmission

Figure 1 shows the scenario of wireless data transmission from Source Node (SN) to Destination Node (DN) with the existence of eavesdropper. Main link refers to the channel span from source to destination, while wiretap refers to the channel span from source to destination and to eavesdropper (Zou et al., 2016).

Radio signal transmission occurs between source and destination by sending multiple delayed signals by source node and they are received by the destination node. The signals are sent over various paths because of experience of signal diffraction, scattering, and reflection (Zou et al., 2016).

Manuscript received March 5, 2021
Manuscript revised March 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.3.7

Multiple-Input-Multiple Output (MIMO) systems are broadly realized as effective ways to mitigate the impact of wireless fading. MIMO wiretap channel is a MIMO broadcast channel that denoted to broadcast confidential information of the SN to the legitimate DN and to the eavesdropper (Zou et al., 2016).

To secure the communication between sender and receiver, the signal to noise ratio of the wireless main channel must be greater than the rate of eavesdropper channel. The communication conditions change due the multipath propagation and interferences in wireless channels (Padala and Kommana, 2018).

2. Related work

In this section, we review the work and studies on the subject that is currently being discussed with regard to problems and security solutions. , Identify some advantages and disadvantages of each study and conclude with the major contributions and improvements offered by the study.

The paper of [6] introduced a new framework for assisting managers in assessing and understanding the diverse threats of using wireless networks. After reviewing and discussing a set of currently implemented techniques to counter wireless network threats, a new model was presented. Access points, clients and transmission media were discussed and described in addition to the corresponding countermeasures to avoid security risks. On the other hand, the paper did not cover the importance of awareness of employees about the procedures for safe wireless network transmissions.

In another paper, [6] has provided an analysis and study of the current infrastructure of wireless network in the Institute of AminuddinBaki. It has identified the vulnerabilities associated with wireless networks and the differences between threats and risks. The proper countermeasures have been outlined for each risk to determine the significant areas that participate in achieving network integrity, security, confidentiality, and authentication. The correct monitoring framework can be designed and developed in accordance with the identified area. However, the paper did not include the issues of interception and interference in the medium of wireless networks.

The communication security cannot be assured absolutely, but rather it can be raised up to mitigate risks threatening the data transmitted over media. In the paper of [5] has presented a solution based on quantum cryptography toward communication security through information encoding and then sending over air. Further, the paper has explored different aspects and implications of quantum cryptography application in wireless connections. Therefore, it introduced a new method for security integrated with quantum cryptography to secure the transmission of encryption keys. The results show the effectiveness of the proposed method in terms of security of IEEE 802.11 protocol. However, it cannot serve comprehensive security of wireless networks due to the limitations of the employed framework.

Similarly, [7] evaluated the wireless network environment in Jordan considering the settings and equipment of security. It also provided a set of recommendations with best practice of secure wireless networks. The attention of wireless communication security has attracted the existence of wireless network interest. The results showed that the equipment for security is not fully secured. It used Net Stumbler and Kismet freeware tools for war driving that have been developed to help network administrators to secure systems and networks. It has carried out the wireless local area network security with proposing security countermeasures to enhance the wireless networks. However, this study has focused only on user training and education regardless other security perspectives.

A set of authentication methods was examined and evaluated in the paper [8] in terms of their benefits and shortcomings. Hence, it included a proposed unified authentication protocol to be contained by radius protocol which is relatively fast and feasible. It employed the utilization of public key infrastructure to demonstrate the performance of proposed protocol. The results showed that the proposed mechanism is robust and simple as well as there is no requirement for extra security infrastructure or measures to guarantee security. Further, the proposed protocol was fast compared to other protocols. However, the proposed technique has not taken into account the IP mobility between wireless networks.

In [9], a computationally lightweight security framework was presented to achieve security objectives against sensor networks attacks. It contained four interacting components including malicious node detection mechanism, secure routing mechanism, secure triple-key management scheme and secure localization technique. Separately, every component is able to achieve a particular level of security. For example, routing mechanism provides a secure node to base station in both directions and triple-key management scheme provides one cluster deployed key and two network pre-deployed keys. These keys mitigate the authentication and confidentiality related attacks. Malicious node detection mechanism secures the network against insiders and outsiders attacks, while secure localization mechanism addresses issues of location determination in terms of security. It guarantees a high level of security using the developed framework. It takes into account the computation and communication limitations of sensor networks. Thus, a trade-off between performance and security always exists. It needs experimental results to

confirm the ability of proposed framework in achieving high level of security with neglected overhead.

The paper [3] has studied the security settings of wireless local area network (WLAN) in terms of their vulnerabilities and different solutions of securing LAN. A comprehensive assessment of wireless network security was presented by showing their results of large wireless LAN. The method applied in the paper has been employed based on physical observation of 5 access points located within 5 categories of network using network performance metrics parameters. A set of interviews were conducted with the personnel at information technology centres to investigate the performance of WLAN. In terms of physical observation, considering 5 formations that were visited, they are running on WPA and MAC address security, IEEE 802.11a, b and g were used as network channels radio type. These security types are not capable enough to protect the network from attacks. The proposed wireless LAN lacks the best security settings that can be broken by network hackers using software tools. Wireless network deployment using IEEE 802.11 is based on SSID, WEP, and MAC address.

The paper [1] explored the application of quantum cryptography aspects in wireless networks by presenting a new methodology to integrate security of IEEE 802.11 and quantum cryptography wireless networks with respect to encryption keys distribution. SARG04 OKD protocol (which is an enhanced version of BB84) was proposed to overcome the security issues of ley distribution. The current IEEE 802.11i protocol was modified without affecting the current frame format. It was applicable to the users equipped with quantum devices. However, if they are not equipped, they still continue with the current Wi-Fi communication. It has many potential works of improvements and extensions such as the security of new level of absolute quantum cryptography. The network security was improved in WLANs with integrated wireless networks with quantum cryptography. Classical cryptographic algorithms are difficult to be used based on key management and distribution. The use of QKD for distribution network key increases the security and then make the capacity of eavesdropping more difficult in interrupting communication. The paper has achieved the key objectives of security improvements for WLANs.

A framework for analysis and specification of security for mobile wireless networks communication protocols was presented in [10]. It introduced new addressed issues in classical protocol analysis techniques. The major complication stems in the connectivity of intermediate nodes cannot be abstracted in one unstructured adversarial environment that formulates the system security. The scenario was modelled faithfully through a broadcast Calculus to create a clear difference between network connectivity graph and the protocol processes in the independent changing protocol actions. An important aspect of security was identified as a property of security setting to express the use of behavioral calculus equivalences. The approach was complemented with a control flow of analysis to enable automatic check of given network property and attack specification. The traditional security protocol analysis has been pointed to develop a new model of novel security properties provided and expanded by the proposed framework.

3. Analyses

3.1 System Model

The system model consists of three entities, the transmitter Alice, the receiver Bob and an eavesdropper, Alice and Bob are connected through the main channel while Alice and eavesdropper are connected through a wiretap link as depicted in Fig 3.1.

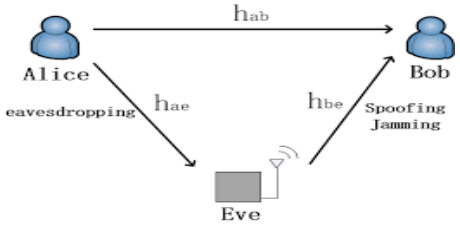

Fig 3.1

In the system model illustrated in Figure 3.1, a legitimate user, named Alice (A), wants to communicate with another user, named Bob (B), while the eavesdropper (E) attempts to eavesdrop the information. The links between any pair of entities are modeled using the Rayleigh fading channels. It is assumed that the transmitter (Alice), receiver (Bob) and eavesdropper have a single antenna. Furthermore, hab and hae denote the channel coefficients from transmitter to legitimate receiver (main channel) and from transmitter to eavesdropper (eve channel), respectively.

4. Simulation Results

The results are obtained from numerical analysis and using MATLAB. Investigations of the outage probability, symbol error rate and secrecy capacity of the system are carried out with different channel mean power Ωb from Alice to Bob and channel mean power Ωe from Alice to Eavesdropper. The results are observed for the outage probability when the SNR threshold γth is selected as 3 dB and the transmit SNR varies from 1 to 20 dB.

4.1 Outage Probability

The outage probability is calculated as the CDF of received SNR Ωb of the eligible receiver Bob at given outage threshold of 3 dB. In Figure 4.1, the outage probability is plotted with respect to the transmitted SNR for different values of channel mean power.

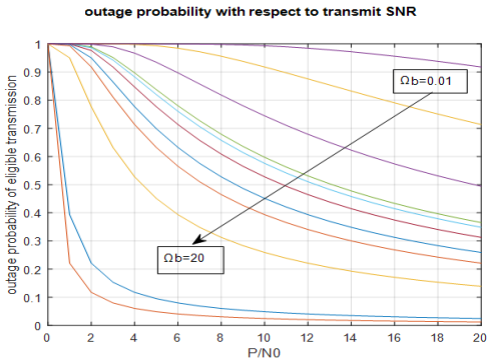

Figure 4.1: Outage probability with respect to transmit SNR

Figure 4.1 represents the 2D plot of outage probability versus the transmit SNR P/No. It is observed that as the transmit SNR increases and for increase in Ωb with a range of 0.01 to 20, the outage probability is being decreased and tends to be zero for very large values of SNR Ωb. Also, when the SNR is increased to 20 dB, the system performance is improved as the outage is being decreased.

```
f = 1 - exp(1./-snr.*1./omega*yth); omega=6; snr=[0:20]; yth=3;
plot(snr,f) f= 1 - exp(1./-snr.*1./omega*yth); hold on omega=12;
f = 1 - exp(1./-snr.*1./omega*yth); omega=12; hold on
plot(snr,f) omega=0.12; f = 1 - exp(1./-snr.*1./omega*yth);
hold on plot(snr,f) omega=0.22;
f = 1 - exp(1./-snr.*1./omega*yth);
hold on plot(snr,f) omega=0.33;
f = 1 - exp(1./-snr.*1./omega*yth);
hold on plot(snr,f) omega=0.35;
f = 1 - exp(1./-snr.*1./omega*yth);
hold on plot(snr,f) omega=0.4;
f = 1 - exp(1./-snr.*1./omega*yth);
hold on plot(snr,f) omega=0.5;
f = 1 - exp(1./-snr.*1./omega*yth);
hold on plot(snr,f) omega=0.6; f = 1 - exp(1./-snr.*1./omega*yth);
hold on plot(snr,f) omega=1; f = 1 - exp(1./-snr.*1./omega*yth);
hold on plot(snr,f) omega=0.06;
f = 1 - exp(1./-snr.*1./omega*yth);
hold on plot(snr,f) xlabel('P/N0') ylabel('outage probability of
eligible transmission')
title('Figure 4.1outage probability with respect to transmit SNR')
grid snr=0:20; omega=0:2;
yth=3; [omega snr]=meshgrid(omega,snr);
z = 1 - exp(1./-snr.*1./omega*yth);
surf(omega,snr,z) omega=0.05;
surf(omega,snr,z) xlabel('Ωb')
ylabel('P/N0') zlabel('outage probability of eligible transmission')
title('Figure 4.2 outage probability for constant Ωe = 0.05')
```

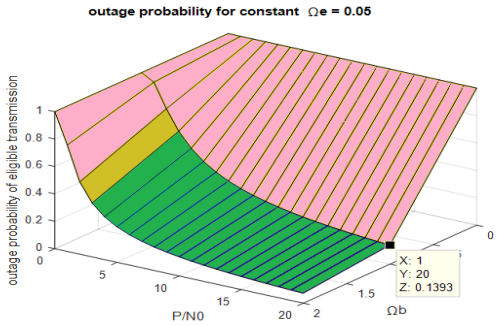

Figure 4.2: Outage probability for constant Ωe=0.05

Figure 4.2 represents the 3D plot of the outage probability of the eligible transmission versus channel mean power Ωb and transmit SNR, for a constant channel mean power value of Ωe = 0.05. It is observed that the outage decreases with the increase in transmit SNR and outage decreases with the increase of Ωb.

```
snr=0:20; omega=0:2; yth=3;
[omega snr]=meshgrid(omega,snr);
z = 1 - exp(1./-snr.*1./omega*yth);
surf(omega,snr,z) omega =  0.0500
surf(omega,snr,z) xlabel('P/N0')
xlabel('Ωb') ylabel('P/N0') zlabel('outageprobability of
eligible transmission')
label('Figure 4.2 outage probability for constant Ωe = 0.05')
title('Figure 6.2 outage probability for constant Ωe = 0.05')
zlabel('outage probability of eligible transmission')
```

4.2 Secrecy Capacity

In this section, the secrecy capacity of the proposed system is depicted as 3D plots. Firstly, we investigate secrecy capacity with channel mean power Ωb and transmit SNR P/No, for a constant channel mean power Ωe. Secondly, we investigate of secrecy capacity with channel mean power Ωe and transmit SNR, for a constant channel mean power Ωb. Finally, the secrecy capacity is investigated for channel mean power Ωb and channel mean power Ωe

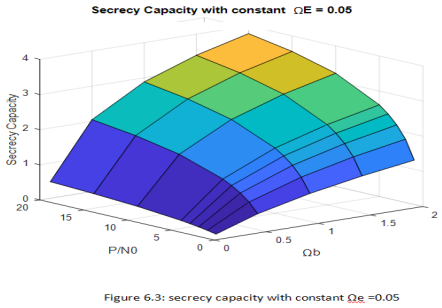

Figure 6.3: secrecy capacity with constant Ωe =0.05

Figure 4.3: Secrecy Capacity with constant Ωe=0.05

```
omegab=[0.1,0.5,1,1.5,2];
snr=[0:5,10,15,20]; [snromegab ]=meshgrid(snr,omegab);
 c=-./log(2)*exp(1./snr.*1./omegab).
*ei(-./snr.*1./omegab)+1./log(2).*exp(1./snr.*1./0.05).*ei(
-1./snr*1./0.05);
 surf(omegab,snr,c)
xlabel('Ωb') ylabel('P/N0')
zlabel('Secrecy Capacity')
title('Figure 6.3 Secrecy Capacity with constant ΩE = 0.05')
```

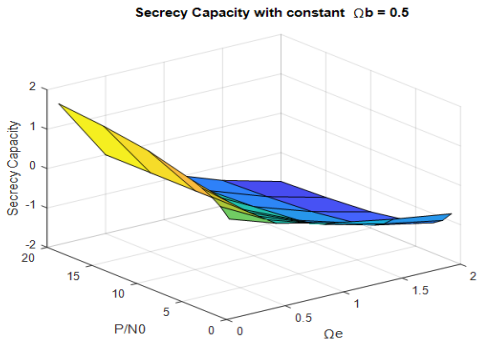

Figure 4.4: secrecy capacity with constant Ωb =0. 5

Figure 5.4 represents the 3D plot of secrecy capacity versus the channel mean power Ωe and the transmit SNR. It is observed that for a constant value of Ωb = 0.5, the secrecy capacity increases with increase in transmit SNR. The secrecy capacity decreases with increase in Ωe as long as Ωe ≥ Ωb , when Ωe becomes greater than Ωb, secrecy capacity becomes zero.

```
c=-
1./log(2)*exp(1./snr.*1./0.5).*ei(-./snr.*1./0.5)+1./log(2).
*exp(1./snr.*1./omegae).*ei(-1./snr*1./omegae);
surf(omegae,snr,c)
c=-1./log(2)*exp(1./snr.*1./0.5).*ei(-./snr.
*1./0.5)+1./log(2).*exp(1./snr.*1./omegae).*ei(-
1./snr*1./omegae);
surf(omegae,snr,c)  omegae=[0.1,0.5,1,1.5,2];
snr=[0:5,10,15,20];  [snromegae ]=meshgrid(snr,omegae);
c=-1./log(2)*exp(1./snr.*1./0.5).*ei(-./snr.*1./0.5)
+1./log(2).*exp(1./snr.*1./omegae).*ei(-1./snr*1./omegae);
surf(omegae,snr,c) xlabel('Ωe') ylabel('Ωb') ylabel('P/N0')
zlabel('Secrecy Capacity')
 title('Figure 6.4 Secrecy Capacity with constant Ωb = 0.5')
```

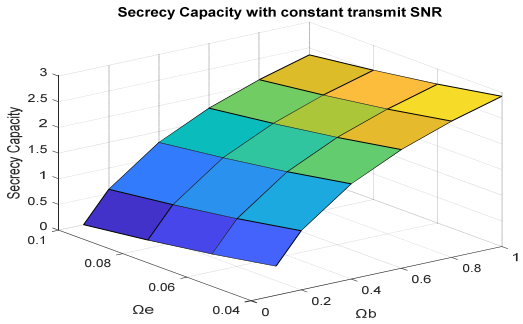

Figure 4.5: secrecy capacity constant transmit with SNR

Figure 4.5 represents the 3D plot of secrecy capacity versus channel mean power Ωb and channel mean power Ωe for SNR being constant. It is observed that, for given values of Ωb being increased the secrecy capacity increases and for the given values of Ωe being increased the secrecy capacity decreases and gives a value less than zero respectively.

```
omegae=[0.04,0.06,0.08,0.1];
omegab = [0,0.2,0.4,0.6,0.8,1];
[omegabomegae ]=meshgrid(omegab,omegae);
c=-1./log(2)*exp(1./20.*1./omegab).*ei(-./20.
*1./omegab)+1./log(2).*exp(1./20.*1./omegae).*ei(-
1./20*1./omegae);
surf(omegab,omegae,c)
c=-1./log(2)*exp(1./18.*1./omegab).
*ei(-./18.*1./omegab)+1./log(2).*exp(1./18.*1./omegae).*
ei(-1./18*1./omegae);
surf(omegab,omegae,c)  surf(omegab,omegae,c)
omegab = [-1,0.2,0.4,0.6,0.8,1];
omegae=[0.04,0.06,0.08,0.1];
[omegabomegae ]=meshgrid(omegab,omegae);
c=-1./log(2)*exp(1./18.*1./omegab).
*ei(-./18.*1./omegab)+1./log(2).*exp(1./18.*1./omegae).*
ei(-1./18*1./omegae);
surf(omegab,omegae,c) omegab = [0.1,0.2,0.4,0.6,0.8,1];
omegae=[0.04,0.06,0.08,0.1];
[omegabomegae ]=meshgrid(omegab,omegae);
c=-1./log(2)*exp(1./18.*1./omegab).
*ei(-./18.*1./omegab)+1./log(2).*exp(1./18.*1./omegae).*
ei(-1./18*1./omegae);
```

```
surf(omegab,omegae,c)
xlabel('Ωb') ylabel('Ωe') zlabel('Secrecy Capacity')
title('Secrecy Capacity with constant transmit SNR')
```

4.3 Symbol Error Rate

In this figure, the symbol error rate of the eligible transmission is plotted in two dimensions for different values of transmit SNR in range of 1 to 20 dB for channel mean power Ωb from 0.01 to 20 dB. We select the MPSK modulation scheme with M =4.

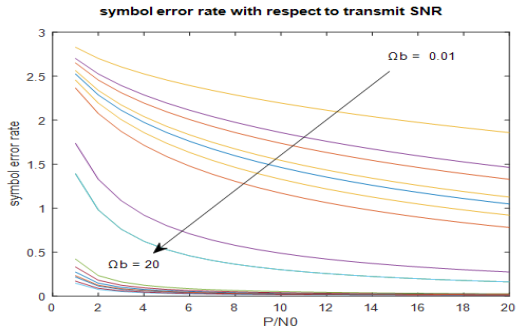

Figure 4.6: symbol error rate with respect to transmit SNR

Figure 4.6 represents the 2D plot of the symbol error rate versus the transmit SNR P/No. It is observed that as the transmit SNR increases and for increase in Ωb with a range of 0.01-20, the symbol error rate is being decreased and tends to be zero for very large values of SNR and Ωb. Also, when the SNR is increased to 20 dB, the system performance is improved as the symbol error rate is being decreased.

```
=(a.*sqrt(b)./2.*(sqrt(pi).*(sqrt (pi./b)-sqrt(pi./(b-(-
1./snr.*1./omega))))));
omega=0.08; a=2; b = sin(pi./4).^2; b = sin(pi./4).^2;
snr=[1:20]; b = sin(pi./4).^2;
plot(snr,p) a=0.1; p=(a.*sqrt(b)./2.*(sqrt(pi).*(sqrt (pi./b)-
sqrt(pi./(b-(-1./snr.*1./omega))))); hold on
plot(snr,p) a=2; p=(a.*sqrt(b)./2.*(sqrt(pi).*(sqrt (pi./b)-
sqrt(pi./(b-(-1./snr.*1./omega))))));
hold on plot(snr,p) plot(snr,p) snr=[0:20];
p=(a.*sqrt(b)./2.*(sqrt(pi).*(sqrt (pi./b)-sqrt(pi./(b-(-
1./snr.*1./omega))))));
hold on plot(snr,p) snr=[1:20];
p=(a.*sqrt(b)./2.*(sqrt(pi).*(sqrt (pi./b)-sqrt(pi./(b-(-
1./snr.*1./omega))))));
hold on plot(snr,p) omega=0.05;
p=(a.*sqrt(b)./2.*(sqrt(pi).*(sqrt (pi./b)-sqrt(pi./(b-(-
1./snr.*1./omega))))));
hold on plot(snr,p)
omega=0.1; p=(a.*sqrt(b)./2.*(sqrt(pi).*(sqrt (pi./b)-
sqrt(pi./(b-(-1./snr.*1./omega))))));
hold on plot(snr,p) omega=0.5;
p=(a.*sqrt(b)./2.*(sqrt(pi).*(sqrt (pi./b)-sqrt(pi./(b-(-
1./snr.*1./omega))))));
hold on plot(snr,p) omega=6;
p=(a.*sqrt(b)./2.*(sqrt(pi).*(sqrt (pi./b)-sqrt(pi./(b-(-
1./snr.*1./omega))))));
hold on plot(snr,p)
omega=20; p=(a.*sqrt(b)./2.*(sqrt(pi).*(sqrt (pi./b)-
sqrt(pi./(b-(-1./snr.*1./omega))))));
hold on plot(snr,p) omega=17;
p=(a.*sqrt(b)./2.*(sqrt(pi).*(sqrt (pi./b)-sqrt(pi./(b-(-
1./snr.*1./omega))))));
hold on plot(snr,p)
omega=13; p=(a.*sqrt(b)./2.*(sqrt(pi).*(sqrt (pi./b)-
sqrt(pi./(b-(-1./snr.*1./omega))))));
hold on plot(snr,p)
omega=0.13; p=(a.*sqrt(b)./2.*(sqrt(pi).*(sqrt (pi./b)-
sqrt(pi./(b-(-1./snr.*1./omega))))));
hold on plot(snr,p) omega=0.07;
p=(a.*sqrt(b)./2.*(sqrt(pi).*(sqrt (pi./b)-sqrt(pi./(b-(-
1./snr.*1./omega))))));
hold on plot(snr,p) omega=0.04;
p=(a.*sqrt(b)./2.*(sqrt(pi).*(sqrt (pi./b)-sqrt(pi./(b-(-
1./snr.*1./omega))))));
hold on plot(snr,p) omega=0.9;
p=(a.*sqrt(b)./2.*(sqrt(pi).*(sqrt (pi./b)-sqrt(pi./(b-(-
1./snr.*1./omega))))));
hold on plot(snr,p) plot(snr,p) omega=8;
p=(a.*sqrt(b)./2.*(sqrt(pi).*(sqrt (pi./b)-sqrt(pi./(b-(-
1./snr.*1./omega))))));
hold on plot(snr,p) omega=10;
p=(a.*sqrt(b)./2.*(sqrt(pi).*(sqrt (pi./b)-sqrt(pi./(b-(-
1./snr.*1./omega))))));
hold on plot(snr,p) omega=12;
p=(a.*sqrt(b)./2.*(sqrt(pi).*(sqrt (pi./b)-sqrt(pi./(b-(-
1./snr.*1./omega))))));
hold on plot(snr,p) omega=0.02;
p=(a.*sqrt(b)./2.*(sqrt(pi).*(sqrt (pi./b)-sqrt(pi./(b-(-
1./snr.*1./omega))))));
hold on plot(snr,p) xlabel('P/N0')
ylabel('symbol error rate') title('Figure 6.6 symbol error
rate with respect to transmit SNR')
```

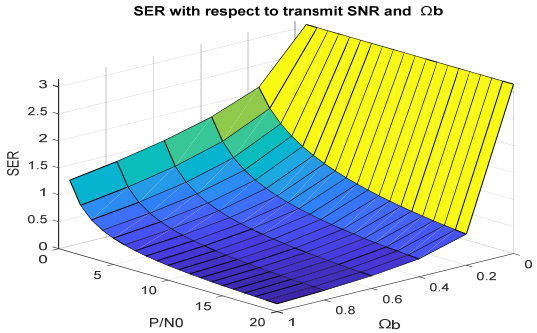

Figure 4.7: SER with respect to transmit SNR and Ωb

Figure 4.7 represents the 3D plot of symbol error rate versus transmit SNR and channel mean power Ωb. It is observed that the symbol error rate decreases for the increase in transmit SNR and symbol error rate decreases with increase in channel mean power Ωb.

```
snr=[1:20]; a=2; b = sin(pi./4).^2; [omega snr]=meshgrid(omega,snr);
p=(a.*sqrt(b)./2.*(sqrt(pi).*(sqrt (pi./b)-sqrt(pi./(b-(-1./snr.*1./omega))))));
 surf(omega,snr,p) omega=0.1;
p=(a.*sqrt(b)./2.*(sqrt(pi).*(sqrt (pi./b)-sqrt(pi./(b-(-1./snr.*1./omega))))));
 [omega snr]=meshgrid(omega,snr); surf(omega,snr,p) a=2;
 b = sin(pi./4).^2; surf(omega,snr,p) omega=[0:0.2:1];
snr=[1:20]; b = sin(pi./4).^2; a=2; [omega snr]=meshgrid(omega,snr);
p=(a.*sqrt(b)./2.*(sqrt(pi).*(sqrt (pi./b)-sqrt(pi./(b-(-1./snr.*1./omega))))));
surf(omega,snr,p) xlabel('Ωb') ylabel('P/N0') zlabel('SER') title('SER')
title('SER with respect to transmit SNR and Ωb')
surf(omega,snr,p)
```

5. Conclusions and Future Works

The inherent openness of wireless medium makes information security one of the most important and difficult problems in wireless networks. Physical layer security, which achieves the information-theoretic security by exploiting the differences between the physical properties of signal channels such that a degraded signal at an eavesdropper is always ensured and thus the original data can be hardly recovered regardless of how the signal is processed at the eavesdropper, has been studied as a promising approach to providing a strong form of security.

In this paper, we have analyzed the SNR at the eligible receiver and eavesdropper. Then, the average capacity of the transmission from the transmitter to the eligible receiver and the eavesdropper has been obtained.

Numerical results have been provided for different values of the channel mean power Ωb of main channel and channel mean power Ωe of the eavesdropper. the results of secrecy capacity have then been performed for different values of SNR and the channel mean power Ωb of the main channel and channel mean power Ωe of the eavesdropper.

The symbol error rate at the main channel has analysed. Lastly, all the results are performed in MATLAB.

In future, the extension of this paper may include the investigation of other performance parameters, Can be used for the realization of secrecy capacity. Where an efficient wireless transmission mechanism can be developed

Reference

[1] Padala, A. N. S. R., &Kommana, K. (2018),Performance of physical layer security with different service integrity parameters.

[2] Li, X., Wang, H., Dai, H. N., Wang, Y., & Zhao, Q. (2016), An Analytical Study on Eavesdropping Attacks in Wireless Nets of Things, *Mobile Information Systems*, *2016*.

[3] Wu, Y., Khisti, A., Xiao, C., Caire, G., Wong, K. K., &Gao, X. (2018), A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead. *arXiv preprint arXiv:1801.05227*.

[4] Zou, Y., Zhu, J., Wang, X., &Hanzo, L. (2016). A survey on wireless security: Technical challenges, recent advances, and future trends. *Proceedings of the IEEE*, *104*(9), 1727-1765.

[5] Devi, L., &Suganthi, A. (2014). Denial of service attacks in wireless networks: The case of jammers. *Int. J. Comput. Sci. Mobile Comput.*, *3*(1), 548-558.

[6] Tupakula, U., &Varadharajan, V. (2013), Security techniques for counteracting attacks in mobile healthcare services. *Procedia Computer Science*, *21*, 374-381.

[7] OOzanKoyluoglu, Can EmreKoksal, and Hesham El Gamal. On secrecy capacity scaling in wireless networks, IEEE Trans. Inf. Theory, 58(5):3000–3015,2012.

[8] HyoungsukJeon, Namshik Kim, Jinho Choi, Hyuckjae Lee, and JeongseokHa.Bounds on secrecy capacity over correlated ergodic fading channels at high snr. IEEE Trans. Inf. Theory, 57(4):1975 – 1983, Apr. 2011.

[9] Weng Chon Ao and Kwang-Cheng Chen. Broadcast transmission capacity ofheterogeneous wireless ad hoc networks with secrecy outage constraints. In IEEEGlobal Telecommunications Conference (GLOBECOM), pages 1–5, 2011.

[10] Zou, Y., Zhu, J., Wang, X., & Leung, V. C. (2015), Improving physical-layer security in wireless communications using diversity techniques , IEEE Network, 29(1), 42-48.