RESEARCH PROJECT

ON

Impact of Security Level on Throughput in Wireless Network

PREPARED BY:

MD. Murad Ahmad

ID: 2012-2-55-051

Toukir Ahamed

ID: 2012-2-56-027

Department of Electronics and Communications Engineering

East West University

SUPERVISED BY:

Professor Dr.Mohamed Ruhul Amin

Department of ECE

East West University

Professor Dr. Md. Imdadul Islam

Department of ECE

East West University

EAST WEST UNIVERSITY

PROJECT TITLE

Impact of Security Level on Throughput in Wireless Network

PREPARED BY:

MD. Murad Ahmad

ID: 2012-2-55-051

Toukir Ahamed

ID: 2012-2-56-027

Department of Electronics and Communications Engineering

East West University

This project report is submitted in accordance with the rules of the Department of Electronics and Communications Engineering, East West University as part of the requirements for the Degree of B.Sc. in Electronic and Telecommunication Engineering. We declare that our work presented in this report is our own except where reference or acknowledgement is presented as to work of other.

Signature:

…………………………………….	…………………………………….
MD. Murad Ahmad	Toukir Ahmed
ID: 2012-2-55-051	ID: 2012-2-56-027
Department of ECE	Department of ECE
East West University	East West University

Signature of Supervisors:

…………………………………….	…………………………………….
Professor Dr.Mohamed Ruhul Amin	Professor Dr. Md. Imdadul Islam
Department of ECE	Department of ECE
East West University	East West University

ACKNOWLEDGEMENT

First of all, we would like to express our sincere gratitude to our advisor Dr. Md. Imdadul Islam and Dr.Mohamed Ruhul Amin for the continuous support throughout the course of this project effort. Their guidance helped us in all the time. Without their initial effort this project would not have been undertaken. We have successfully executed the goal of the project due to their continuous and patient mentoring throughout the entire process. We are extremely grateful to them as they gives us the opportunities and exposure that we could never had if we did not worked with them.

In addition, we would like to thank all the faculty members of ECE department for their guidance and support towards completing our B.Sc. Degree and also this project work. We also like to thank the authors mentioned in the reference page, without their work we would be nowhere.

We are thankful to our honorable parents for their great support and inspiration until the end of this project. We would also like to thanks all our friends and batch-mates for supporting us and encouraging us. The name without whom our thanksgiving is incomplete is the Almighty Allah, Who allowed us to reach here today.

Thank you all for your great support to us.

Signature:

....

MD. Murad Ahmad

ID: 2012-2-55-051

Department of ECE

East West University

....

Toukir Ahamed

ID: 2012-2-56-027

Department of ECE

East West University

ABSTRACT

In both wire and wireless communication data are encrypted before transmission to protect activeand passive intruder. This project work deals with mathematical model among the relation of:security level, length of encrypted block, SNR at receiving end and throughput. The throughputof a network is governed by probability of bit error which is again depends on SNR. Based onabove concept impact of modulation scheme on the throughput is also analyzed in this projectwork. Here, we consider 16-QAM, QPSK and BPSK modulation schemes. We found thatperformance of 16-QAM is far better than QPSK and BPSK at higher SNR.

Table of Contents

List of Figures

CHAPTER ONE

INTRODUCTION

A computer Network is a gathering of PCs and related gadgets associated with one another keeping in mind the end goal to give correspondence, data sharing and assets sharing. The PC can be situated in a little zone, in a city or everywhere throughout the world. They can be associated through metallic links, optical links or satellite connections relying upon the zone of their good.

Many of us may have listened about Internet. It is a substantial system spread all over world associating small networks. It gives such a large number of advantages such as immediate correspondence data exchange, email etc. You can recognize a message, forward it, store, recover or add connections to it. Comparative systems permit you to share asset like applications, printers, modems, scanners, plate space and so on. Despite the fact that it gives such a variety of administrations however now a day the fundamental fascination on it is electronic gatherings, video conferencing and so on that is made conceivable through extraordinary programming called groupware.

The system needs security against aggressors and hackers. System Security incorporates two fundamental securities. The first is the security of information data i.e. to shield the data from unapproved access and misfortune. The second is PC security i.e. to ensure information and to ruin hackers. Here system security not just means security in a solitary system rather in any system or system of systems.

Presently our need of system security has broken into two needs. One is the need of data security and other is the need of PC security.

On web or any system of an association, a great many essential data is traded every day. This data can be abused by aggressors. The data security is required for the accompanying given reasons i.e. to ensure the mystery data clients on the net as it were. No other individual ought to see or get to it, to shield the data from undesirable altering, inadvertently or deliberately by unapproved clients, to shield the data from misfortune and make it to be conveyed to its destination legitimately.

To oversee for affirmation of message got by any hub keeping in mind the end goal to shield from dissent by sender in particular circumstances. For instance let a client requests to buy a couple offers XYZ to the more extensive and denies for the request following two days as the rates go down.

To confine a client to send some message to another client with name of a third one. For instance a client X for his own advantage makes a message containing some positive directions and sends it to client Y in such a way, to the point that Y acknowledges the message as originating from Z, the supervisor of the association.

To shield the message from undesirable deferral in the transmission lines/course keeping in minds the end goal to convey it to required destination in time, if there should be an occurrence of earnestness.

To shield the information from meandering the information parcels or data bundles in the system for boundlessly long time and in this way expanding blockage in the line on the off chance that destination machine neglects to catch it as a result of some inward blames.

Another piece of system security incorporates the PC security. PC security intends to shield your PC framework from undesirable harms brought about because of system. One of the real purpose behind such harms are the infections and spywares that can wipe off all the data from your hard plate or here and there they might be sufficient ruinous and might bring about equipment issues as well. Unquestionably the system must be shielded from such kind of harming programming. The general population who deliberately put such programming on the system is called Hackers. As the system PCs are a piece of it, so the PC security from Hackers is additionally a piece of system security. The necessities of PC security from Hackers are as per the following i.e. it ought to be shielded f rom repeating and catching infections from tainted records, it needs a legitimate insurance from worms and bombs, there is a need of assurance from Trojan Horses as they are sufficient hazardous for PC.

System security is a muddled subject, generally just handled by very much prepared and experienced specialists. Be that as it may, as more individuals get to be wired, an expanding number of individuals need to comprehend the essentials of security in an arranged world. This record was composed with the fundamental PC client and data frameworks supervisor at the top of the priority list, disclosing the ideas expected to peruse through the buildup in the commercial center and comprehend dangers and how to manage them.

Some history of systems administration is incorporated, and additionally a prologue to TCP/IP and internetworking. We go ahead to consider danger administration, system dangers, firewalls, and more exceptional specific usefulness.

System Security is the procedure of taking physical and programming safeguard measures to shield the hidden systems administration framework from unapproved access, abuse, breakdown, change, devastation, or dishonorable revelation, in this way making a safe stage for PCs, clients and projects to perform. Network security comprises of the strategies received to forestall and screen unapproved access, abuse, alteration, or disavowal of a PC system and system open assets. System security includes the approval of access to information in a system, which is controlled by the system chairman.

In this project we deal with four parameters, these are throughput, SNR, encrypted block length and security, related to these terms.

The relation between block length and security is as below:

The computational validity require by the aggressor or attacker to break the cipher increments exponentially with the block length. Therefore the relation between the security and block length is exponential that implies if the block length expands, security will increment exponentially with the expansion of block length. For instance, it is harder to split 128 bit AES contrasted with a 64 bit DES.

The relation between SNR and throughput is as below:

The SNR of an access point signal, measured at the client device, diminishes as range to the client increments in light of the fact that the appropriate free space loss between the client and the access point minimize the signal level. SNR straightforwardly effects the representation of a wireless LAN connection. A higher SNR rate implies that the signal quality is more stronger in connection to the noise levels, which permits higher data rates and less retransmission – all of which offers better throughput. Obviously the inverse is likewise true. A lower SNR requires wireless LAN gadgets to work at lower data rates, which diminishes throughput.

For the maximum SNR, the opportunistic node of mobile encrypts the message with the reducing cipher block length and forward the protected data. The modes of cipher block used in the encryption are: cipher feedback (CFB) mode, output feedback (OFB) mode, and the Counter (CTR) mode. The security measure is characterized as the logarithmic estimation of encrypted block length, and is standardized with a maximum block length with in the given time. The interpretation of applying a unique key for every encryption block per session keeps the message leakage because of key disclosure. The optimization of an encoded block length relies on upon fixed channel conditions. Finally, the trade-off between the throughput and security is set up as far as transmission rate and bit error probability. The standardized throughput maximizes the transmission rate in the system. This convention analyzes the SNR and forward error correction (FEC) codes and their impact on secure communication channel.

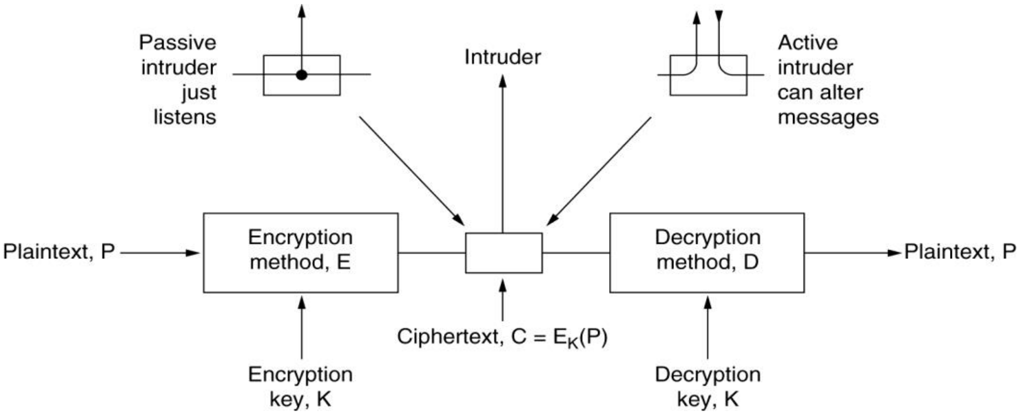
CHAPTER TWO

NETWORK SECURITY

Computer networks are regularly a common asset utilized by numerous applications representing different interests. The Internet is especially generally shared, being utilized by contending organizations, commonly hostile governments, and entrepreneurial offenders. Unless securities to establish safety are taken, a network discussion or a dispersed application might be traded off by an adversary.

Cryptography is one of the main tools for securing networked systems. Cryptography originates from the Greek words for 'secret writing.' It has a long and brilliant history doing a reversal a large number of years. Experts make a distinction between cipher and codes. A cipher is a character-for-character or bit-for-bit change, without respect to the phonetic structure of the messages. Conversely, a code supplants single word with another word or image. Historically four gatherings of individuals have utilized and added to the art of cryptography: the military, the discretionary corps, diarists and mates.

The messages to be encoded, known as plaintext, are changed by a capacity that parameterized by a key. The output of the encryption process called cipher text, is then transmitted, frequently by delivery person or radio. We accept that the adversary or intruder hears and precisely duplicates down the complete cipher text.



The encryption model (for a symmetric-key cipher)

Sometimes the intruder can only listen to the communication channel which is called passive intruder. Active intruder is an intruder who can change the messages before get to the receiver. The art of breaking codes is called cryptanalysis & the cryptography is collectively known as cryptology.

If both participants in a communication use the same key that is called symmetric- key cipher. In other words, by using a particular key to encrypt a message, the same key is required for decrypting the message. Symmetric key used for known communication. On the other hand, if both participants in a communication use the different key that is called public-key. Here, a public key needs by the transmitter for encrypting the message to be sent to the receiver and at the receiver end must be needed a private key to decrypt the message.

Public key algorithms are slower algorithm and more secure than symmetric key algorithms. RSA (Rivest, Shamir, Adleman) is a public key encryption algorithm. Its key size is 1024 bit or 2048 bit. Most popular public key algorithm. In RSA, at the transmitting end public key is used to encrypt a message and private key is used to decrypt the message at the receiving end.

AES (Advanced Encryption Standard) algorithm is the symmetric block cipher. It's full design must be public. The key lengths of the AES algorithm of 128,192 and 256 bits supported. The AES algorithm required both hardware and software implementations.

To get access into a computer, computer network, an online service or website hackers are using many methods. Brute force attack is one of them.

2.1 Brute Force Attack Model

Brute force attack is the least difficult sort of technique to access a site it tries usernames and passwords, again and again until it gets in. A more unpredictable Brute force attack includes attempting each key combination until the right password is found. A Brute force attack can take quite a while to finish the process due to the quantity of conceivable mixes of letters, numbers and images. The higher the kind of encryption utilized (64-bit, 128-bit or 256-bit encryption), the more it can take. These attacks can take a few hours, days, months, and even years to run. An ideal opportunity to finish an attack relies on upon the secret word, the quality of the encryption, how well the attacker knows the objective, and the quality of the computer(s) used to lead the attack. Brute force attacks might be utilized by offenders to break scrambled information, or by security experts to test an association's system security. A Brute force attack might likewise be referred to as Brute force cracking.

Thus, to discover hidden pages, the attacker tries to figure the name of the page, sends demands, and sees the reaction. On the off chance that the page does not exist, it will indicate reaction 404(reaction 404 means server not found) and on achievement the reaction will be 200(reaction 200 means the request has succeeded). Along these lines, it can discover hidden pages on any site.

A reverse Brute force attack is another term that is connected with password cracking. It takes a converse methodology in password cracking. Here, attacker tries one password against various usernames. Think in the event that you know a password yet don't have any thought of the usernames. For this situation, you can attempt the same password and guess the different user names until you locate the working combination.

There are many popular instruments for Brute force attack. Aircrack NG is one of them.

Aircrack NG is a mainstream remote password cracking instrument accessible for nothing. This instrument accompanies WEP/WPA/WPA2-PSK cracker and examination instruments to perform attack on WIFi 802.11. Aircrack NG can be utilized for any NIC, which supports raw monitoring mode. It fundamentally performs Brute force attacks against a remote system to figure the password. The better and successful the password reference is the more probable it is that it will break the password. It is accessible for Windows and Linux stages. It has likewise been ported to keep running on iOS and Android stages.

John the Ripper is another great instrument of Brute force attack. it supports fifteen distinct stages including Unix, Windows, DOS, BeOS, and OpenVMS. By utilizing utilize this either to distinguish weak passwords or to crack passwords for breaking verification. It can consequently distinguish the kind of hashing utilized as a part of a password. It can likewise keep running against encrypted password storage. Fundamentally it can perform Brute force attack with every single conceivable password by joining content and numbers.

Rainbow Crack is also a well known Brute forcing instrument utilized for password cracking. It creates rainbow tables for utilizing while performing the attack. Rainbow tables are pre-figured. It helps in reducing the time in performing the attack. It is accessible for both Windows and Linux and backings every single most recent versions of these stages.

There is a distinction in the middle of online and offline Brute force attacks. For instance, if an attacker needs to Brute force their way into any important mail account, they can start to attempt each and every conceivable password however Google will rapidly cut them off. Administrations that give access to such records will throttle access attempts and boycott IP delivers that attempt to sign in such a large number of times. In this manner, an attack against an online administration wouldn't work too well in light of the fact that not very many attempts can be made before the attack would be stopped. For example, after a couple failed login attempts, Gmail will demonstrate to you a CATPCHA picture to confirm you aren't a PC naturally attempting passwords. They'll likely stop your login attempts totally on the off chance that you figured out how to proceed for quite some time.

2.2 Adversarial Attack Model

In cryptography, an adversary is a malicious substance whose point is to keep the clients of the cryptosystem from accomplishing their objective (essentially security, integrity, and accessibility of information). An adversary's attempts may take the type of attempting to find secret information, corrupting a percentage of the information in the framework, spoofing the character of a message sender or receiver, or constraining framework downtime.

Real adversaries, rather than glorified ones, are referred to as attackers. As anyone might expect, the previous term prevails in the cryptographic and the last in the PC security writing. Eve, Mallory, Oscar and Trudy are all adversarial characters broadly utilized as a part of both sorts of writings.

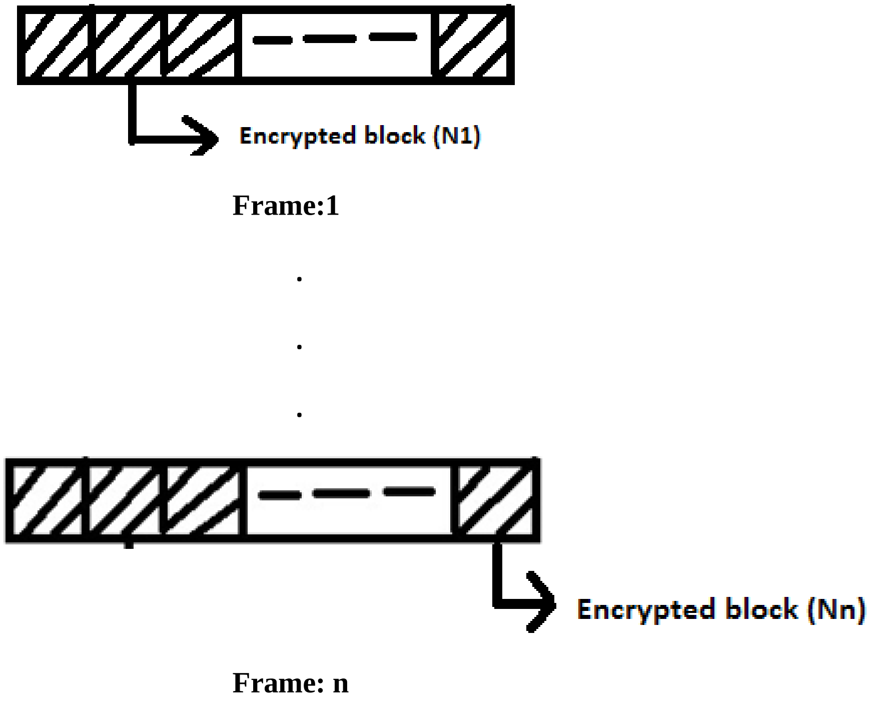
This idea of an adversary helps both natural and formal casting so as to think about cryptosystems security examination of cryptosystems as an "amusement" between the users and a halfway co-ordinate enemy. The thought of security of a cryptosystem is significant just regarding specific attacks (more often than not attempted to be completed by specific sorts of adversaries).

There are a few sorts of enemies relying upon what abilities or expectations they are ventured to have. Enemies might be computationally limited or unbounded (i.e. as far as time and capacity assets), eavesdropping or Byzantine (i.e. inactively listening on or effectively undermining information in the channel), static or versatile (i.e. having altered or evolving conduct), mobile or non-portable (e.g. in the connection of system security), In real security practice, the attacks allotted to such adversaries are frequently seen, so such notional examination is not just hypothetical.

CHAPTER THREE

MATHEMATICAL MODEL OF SECURITY-THROUGHPUT

Let us suppose, a massage of n frames, of which each frames are equally important. Each frame is divided into equal length encrypted block N_i .To get the whole massage it is mandatory to decrypt each frame. Each frame is integral multiple of its encrypted block.



Frame:1

Frame: n

Fig. 3.1: Encrypted block length

The mean security level,

$$\overline{S} = \frac{1}{nS_{\max}} \sum_{i=1}^{n} \log_2 N_i \ , \qquad \left(0 \le \overline{S} \le 1 \right)$$

Where

$$S_{\max} = \log_2 N_{\max} \qquad \left[N_i \in Q_N \right].$$

Here, Q_N is the set where all the encrypted block length is listed.

3.1 Brute Force Attack Model

Mean security,

$$\overline{S} = \frac{1}{nS_{max}} \sum_{i=1}^{n} \log_2 N_i$$

$$\Rightarrow \bar{S} = \frac{1}{nS_{max}} (\log_2 N_1 + \log_2 N_2 + \cdots + \log_2 N_n)$$

$$\Rightarrow \bar{S} = \frac{1}{nS_{max}} \log_2 (N_1 . N_2 \ldots N_n)$$

$$\Rightarrow \bar{S} = \frac{1}{nS_{max}} \log_2 \prod_{i=1}^{n} N_i$$

Security of the i-th frame is.

$$S_i = \log_2 N_i$$

$$\Rightarrow N_i = 2^{S_i}.$$

The throughput is calculated according to

$$T = \frac{1}{nR_{max}} \sum_{i=1}^{n} R_i (1 - N_i P_i),$$

Which can also be written as

$$T = \frac{1}{nR_{max}}\sum_{i=1}^{n} R_i(1-2^{S_i}P_i),$$

Where P_i is the function of SNR

By using the Lagrange optimization technique the object function can be written as

$$C = \frac{1}{nR_{max}}\sum R_i(1-N_iP_i) + \lambda\left(\frac{1}{nS_{max}}\sum_{i=1}^{n}\log_2 N_i - s_{req}\right)$$

To find out the value of the object function(C) for the block length N_i we differentiate the upper equation by $\frac{d}{dN_i}$ and set the value of the equation to zero.

$$\Rightarrow \frac{dC}{dN_i} = \frac{1}{nR_{max}}(-P_iR_i) + \lambda\frac{1}{nS_{max}} \times \frac{1}{N_i \ln 2} = 0$$

$$\Rightarrow \frac{\lambda}{nS_iN_i \ln 2} = \frac{P_iR_i}{nR_{max}}$$

$$\Rightarrow N_i = \frac{\lambda R_{max}}{P_iR_iS_{max}\ln 2} \qquad (1)$$

Here R_i = frame; λ= Langrage multiplier; s_{req} = required level of security.

From the constraint,

$$\frac{1}{nS_{max}}\sum_{i=1}^{n}\log_2 N_i = s_{req}$$

We get,

$$\Rightarrow \frac{1}{nS_{max}}(\log_2 N_1 + \log_2 N_2 + \cdots + \log_2 N_n) = s_{req}$$

$$\Rightarrow \frac{1}{nS_{max}}\log_2 \prod_{i=1}^{n}(N_i) = s_{req}$$

$$\Rightarrow \frac{\ln \sum_{i=1}^{n}(N_i)}{\ln 2} = ns_{req}S_{max}$$

$$\Rightarrow \prod_{i=1}^{n}(N_i) = e^{n s_{req} S_{max}\ln 2} \tag{2}$$

From (1)

$$\prod_{i=1}^{n} N_i = \left(\frac{\lambda R_{max}}{S_{max}\ln 2}\right)^{n} \prod_{i=1}^{n}\left(\frac{1}{P_i R_i}\right)$$

$$\Rightarrow e^{n s_{req}\ln 2} = \left(\frac{\lambda R_{max}}{S_{max}\ln 2}\right)^{n} \prod\left(\frac{1}{P_i R_i}\right)$$

$$\Rightarrow \frac{\lambda R_{max}}{S_{max}\ln 2} = \left\{\frac{e^{n s_{req} S_{max}\ln 2}}{\prod\left(\frac{1}{P_i R_i}\right)}\right\}^{\frac{1}{n}}$$

$$\Rightarrow \lambda = \frac{S_{max}\ln 2}{R_{max}} . \frac{e^{n s_{req} S_{max}\ln 2}}{\left\{\frac{1}{\prod(P_i R_i)}\right\}^{\frac{1}{n}}} \tag{3}$$

From (1)

$$N_i = \frac{e^{s_{req} S_{max}\ln 2} \times S_{max}\ln 2}{R_{max}\left\{\prod\left(\frac{1}{P_i R_i}\right)\right\}^{\frac{1}{n}}} \times \frac{R_{max}}{P_i R_i S_{max}\ln 2}$$

$$\Rightarrow N_i = \frac{e^{s_{req} S_{max}\ln 2}}{P_i R_i \left\{\prod\left(\frac{1}{P_i R_i}\right)\right\}^{\frac{1}{n}}}$$

$$\Rightarrow N_i = \frac{e^{s_{req}S_{max}\ln 2}}{P_iR_i \times \frac{1}{\{\prod(P_iR_i)\}^{\frac{1}{n}}}}$$

$$\Rightarrow N_i = \frac{\{\prod(P_iR_i)\}^{\frac{1}{n}}.e^{s_{req}S_{max}\ln 2}}{P_iR_i}$$

CHAPTER FOUR

RESULTS AND DICUSSION

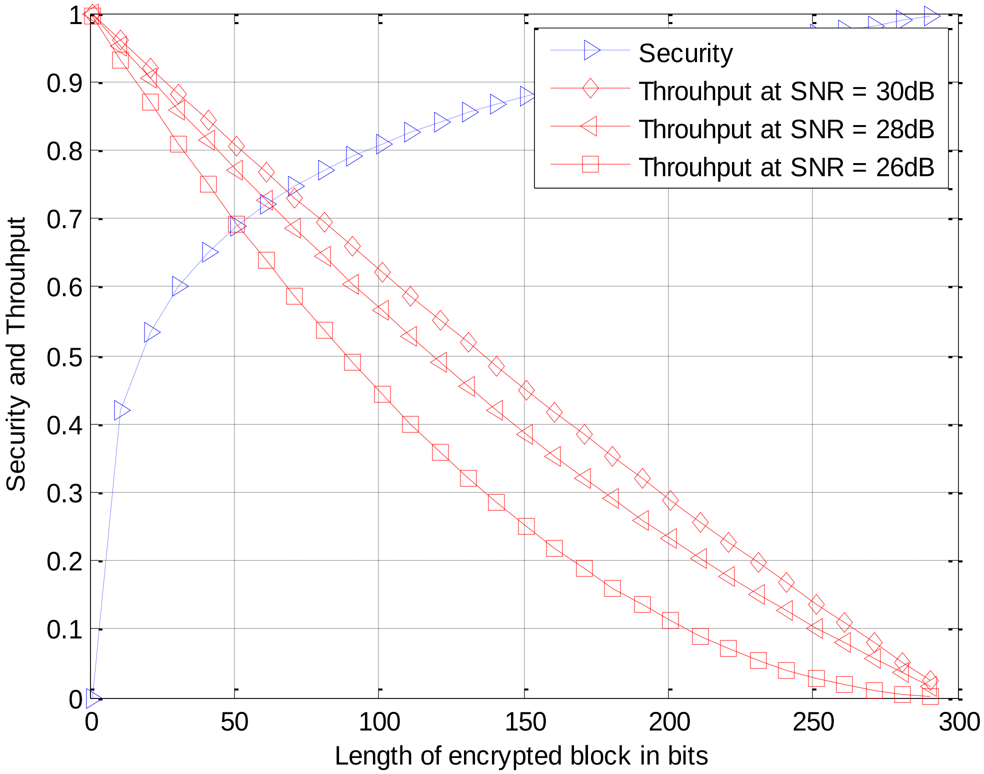


Fig. 4.1: Variations of security and throughput against length of encrypted block (bits)

The above figure shows the variation of both security and throughput against the length of encrypted block (bits). From the figure it is visualize that the security level increases with increasing the length of the encrypted block, since breaking of long a encrypted block requires more permutation and combination under brute force attack. Again the throughput of a message block decreases with the increase in length of the encrypted block. A larger encrypted block provides more security but requires large number of redundant bits; hence the ratio of message length and encrypted block length becomes smaller. From above phenomenon throughput i.e. message per unit time decreases for larger blocks like channel coding technique in communication system. Throughput of a communication system is heavily affected by the probability of bit error, since in case of any erroneous reception the block need to be retransmitted. Again we know probability of bit error decreases with increase in received SNR. Therefore the throughput of a secured communication system increases for larger received SNR but decreased with increase in length of the encrypted block like Fig. 1 where, 3 curves of throughput are shown for 30db, 28db and 26db.

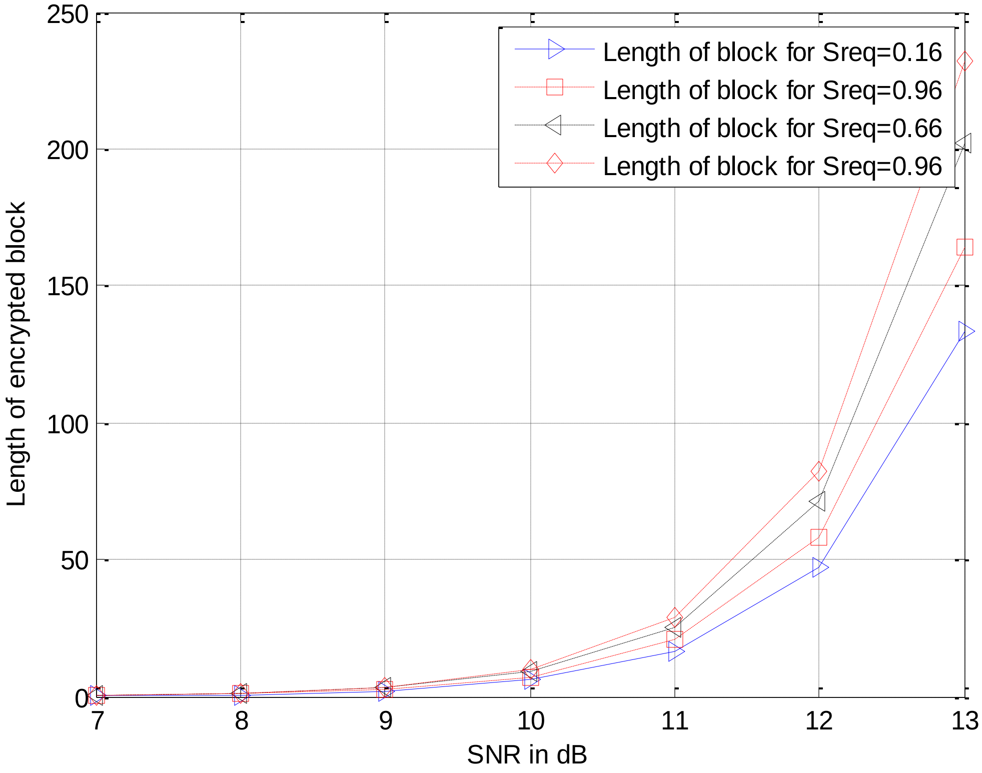


Fig. 4.2: Length of encrypted block against SNR

In Fig. 2 the length of encrypted block is plotted against the received SNR in db taking security level as a parameter. The graph reveals the result similar to Fig. 1, where length of encrypted block increases with the enhancement of security level.

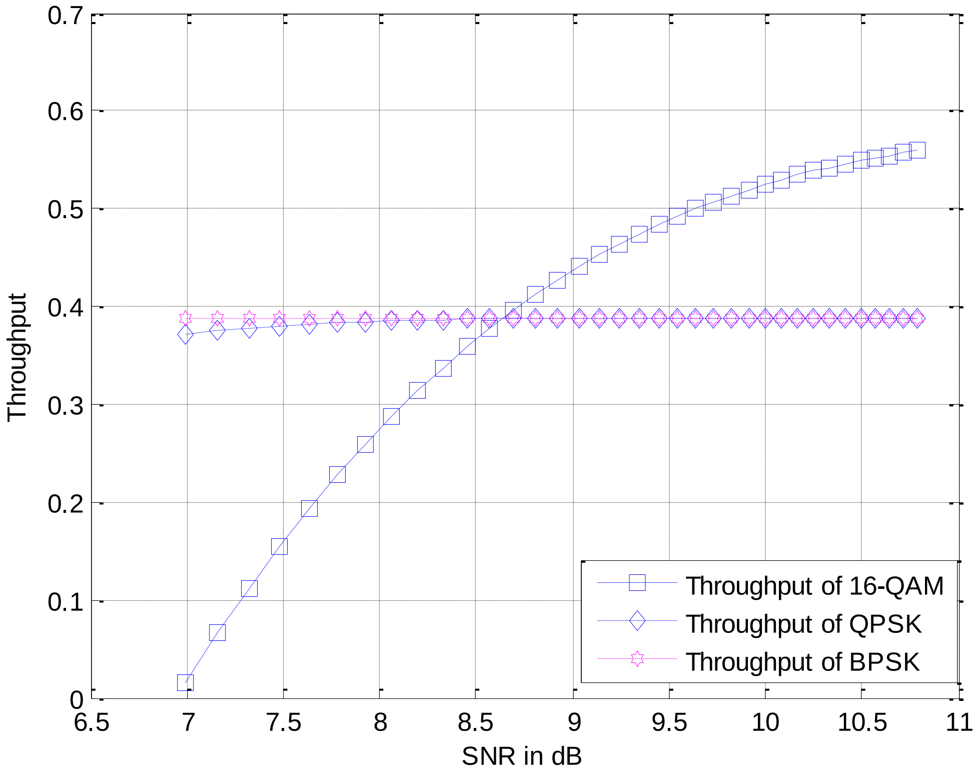


Fig. 4.3: Variation of throughput against SNR for three different modulation schemes

Finally the throughput of the AWGN channel is plotted against the SNR under three different modulation schemes (16 QAM, BPSK and QPSK). Throughputs of BPSK and QPSK are found very close but at lower SNR the throughput of BPSK are found slightly better because of the wider signal space of the constellation diagram. The throughput of 16-QAM is found much smaller compared to the other two modulation schemes because of huge BER at low SNR. The phenomenon can be easily explained from the signal space of 16-QAM. At higher SNR the scenario becomes reversed that is the throughput of 16-QAM is far higher than the case of QPAK and BPSK. At higher SNR the BER of QAM is heavily reduced and conveys four bits per symbol which is twice times higher than the QPSK and four times higher than the BPSK.

CONCLUSION

In this project work we use the expression of probability of bit error under AWGN (Additive White Gaussian Noise); still we have the scope to use the expression of probability of bit error under fading channel, to get the real scenario of the throughput security trade off. Next, we can compare the linear and exponential adversary strength model under different modulation scheme. Finally, we can apply a particular security algorithm (RSA, AES, elliptic curve cryptography etc) or different forward error correction technique (convolutional encoding, linear block code, CRC code etc) on the mathematical model of the project work to make comparison.

REFERENCES

[1] Mohamed A. Haleem, Chetan N. Mathur, R. Chandramouli, and K. P. Subbalakshm, “Opportunistic Encryption: A Trade-Off between Security and Throughput in Wireless Networks,” IEEE Transactions on Dependable and Secure Computing, Oct.-Dec. 2007, Volume:4 , Issue: 4, pp. 313 – 324.

[2] William Stallings. Cryptography and Network Security, Peaterson Education, 2003, pp 27 - 30.

[3] Shafiullah Khan,Jaime Lloret Mauri (eds.). Security for multihop wireless networks. CRC press, 2014, pp 487.

[4] S. Stein, “Fading Channel Issues in System Engineering,” IEEE Journal on Selected Areas in Communications, 1987, vol 5, no. 2, pp. 68-89.

[5] Ezadin Barka, Mohammed Boulmalf, “On the Impact of Security on the Performance of WLAN,” Journal of Communications, June 2007, vol 2, no 4, pp 10-17.

[6] Phongsak, Prasithsangaree and Prashant Krishnamurthy, “Analysis of Trade-off Between Security Strength and Energy Saving in Security Protocols for WLANs,” Telecommunications Program, School of Information Science, University of Pittsburgh, 2004, pp. 5219-5233.

[7] Hanane Fathi, Kazukuni Kobara, Shyam S. Chakraborty, Hideki Imai and Ramjee Prasad, “Impact of Security on Latency in WLAN 802.11b,” Proceeding of IEEE, Globecom 2005, pp. 1752-1756.

[8] Jian Liu, Jian Sun and Shoutao Lv., “A Novel Throughput Optimization Approach in Wireless Systems,” IEEE 12th International Conference on Communication Technology (ICCT), 2010, pp. 1373- 1377.

[9] Paschal A. Ochang, and Phil Irving, “Performance Analysis of Wireless Network Throughput and Security Protocol Integration,” International Journal of Future Generation Communication and Networking,2016, Vol. 9, No. 1, pp. 71-78.

[10] Andrew S. Tanenbaum and David J. Wetherall. Computer Networks (5th Edition), Pearson ,Oct 7, 2010,pp.766-772.

[11] Richard D. Gitlin, Jeremiah F. Hayes, Stephen B. Weinstein. Data Communications Principles, Springer US,1992, pp.305-402.

[12] Simon S. Haykin, Michael Moher. Communication Systems, John Wiley & Sons, 2009, pp.248-337.

[13] Z. Shen, J. G. Andrews, and B. L. Evans, “Short rangewireless channel prediction using local information,” Conf.Record 37th Asilomar Conf. Signals, Systems and Computers, Nov. 2003, Vol.1, pp. 1147- 1151.

[14] Poonam Jindal, Brahmjit Singh, “Study And Performance Evaluation Of Security-Throughput Tradeoff With Link Adaptive Encryption Scheme,” arXiv: 1211.5080, 2012, pp.1-14.

[15] M. Dworkin, “Recommendation for Block Cipher Modes of Operation: Methods and Techniques,” NIST Special Publication, 2001,pp. 800-38A.