Performance Evaluation of 802.11g Architecture Using Security Protocols Based on Index Policy Method

Sagar Kakade, Dr. Rajesh S. Bansode

Abstract— Data security has a major role in the development of communication system as wireless local area networks (WLANs) are beginning to play a much larger role in corporate network environments. Wireless local area networks are very popular for home networking applications, therefore this increase in accessibility has created problems for data security.To deal with these problems stronger security methods such as advanced encryption algorithms and efficient authentication process are used. However, these security methods often hamper network performance. This research examines the effects of Wired Equivalent Privacy (WEP), Data Encryption Standard (DES), Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA) encryption algorithms on packet transmission time, encryption time, computational complexity, and space complexity for 802.11 networks. The work also includes calculating authentication time for Extensible Authentication Protocol (EAP), Challenge-Handshake Authentication Protocol (CHAP), IP Security (IPSec), MAC address authentication and Point to Point Tunneling Protocol (PPTP). Reports reported till date showed the combined effect of encryption and authentication on response time and throughput. Response time increases by 268% and throughput decreases by 73% for 802.1X model. In case of VPN model the researchers observed that there is increase in response time by 130% and decreases in throughput by 50%.The results obtained in this work show significant difference in both the models for packet transmission time, computational complexity, space complexity and encryption time. For lower security levels packet transmission time taken is 17.37secs for 802.1X model while for VPN it is 21.99secs. The packet transmission time taken for higher security levels for 802.1X is 18.42secs whereas for VPN it is 19.63secs. Computational complexity, space complexity and encryption time are 41.16secs, 7853 bytes and 1.26secs repectively in somecases for 802.1X model whereas for VPN it is 78.6secs, 8090 bytes and 1.53secs repectively. 802.1X model is observed to be fastest out of the two methods at all security levels. VPN model proves better for all parameters except for packet transmission time, its performance is not good as compared to 802.1X model. The future scope of this work can be based on researching and implementing other different categories of countermeasures for policy index method and measuring the performance evaluation for each on different hybrid systems namely AES-IPSec, ECC-EAP, ECC-CHAP etc.

Index Terms—802.1X, DES, security levels, security policy index, VPN, WEP, WLAN.

1 Introduction

The 802.11 wireless networks are fast becoming the preferred choice for LAN environments. Given their limited bandwidth (54 Mbps in 802.11g) and the need for security in wireless standards, it is necessary to understand the relative overhead of different security protocols.The MAC sub-layer provides reliable data transmission for the IEEE 802.11 standard similar to a wired network [1].

1.1 IEEE 802.11 standard

IEEE 802.11 was first widely-used wireless local area networking standard and was selected for use in 1997. The standard consists of a medium access control (MAC) sublayer, MAC management protocols and services, and three physical layers (PHYs), as shown in Fig. 1. The three PHYs were an infrared PHY, a frequency hopping spread spectrum (FHSS) radio PHY, and a direct sequence spread spectrum (DSSS) radio PHY. These original PHYs provide data transfer rates of 1 to 2 Mbps. The 1999 revision included two more PHYs, IEEE 802.11a and 802.11b, which would become standards in the industry with data transfer rates of 54 Mbps and 11 Mbps, respectively. The difference between two new PHYs was that IEEE 802.11a operated with an orthogonal frequency division multiplexing (OFDM) signal at Unlicensed National Information Infrastructure (U-NII) bands versus DSSS signal used at 2.4 GHz for IEEE 802.11b. In 2002 the widely used IEEE 802.11g standard was developed as an extension of IEEE 802.11b, providing backwards compatibility [1].

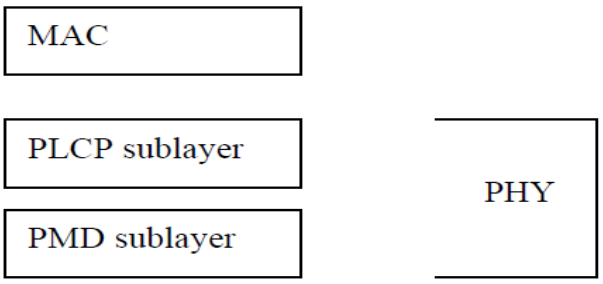


Fig. 1. IEEE 802.11 Layers

The MAC sublayer provides reliable data transmission for IEEE 802.11 standard similar to a wired network. To this extent, the MAC sublayer provides three functions such as a reliable method to transmit data for users, shared access to the

- *Sagar kakade is currently pursuing master's degree program in electronics and telecommunication engineering from T.C.E.T. Mumbai, India. E-mail: sagarkakade7799@gmail.com.*
- *Dr. Rajesh S. Bansode is currently associate professor in Dept. of IT T.C.E.T. Mumbai, India. E-mail: rajesh.bansode1977@gmail.com.*

medium among users, and protection of transmitted data accomplished through encryption. The first function, reliable delivery is completed with a series of two frames. Because the transmission of IEEE 802.11 signals occurs wirelessly and these functions are conducted differently in the MAC sublayer because signals that are transmitted cannot simply be assumed to have been received on a wireless system. The PHY of IEEE 802.11 provides three levels of functionality such as coordination of frame exchanges between MAC and PHY under the control of the physical layer convergence procedure (PLCP) sublayer. The use of signal carrier and spread spectrum modulation is to transmit frames over the radio frequency medium under the control of physical medium dependent (PMD) sublayer that provides carrier sense indication back to the MAC to verify activity on the media [2].

1.2 Authentication and Encryption

The IEEE 802.11 standard has several methods of encryption and authentication that provide varying levels of security for wireless networks [3]. This section provides an overview of those methods.

Authentication provides a method for wireless networks to verify the identity of a user and ensure they are authorized user and can access the network before being connected. This process allows an organization to restrict access of its wireless network to certain individuals just as it would restrict access to its wired network. Without proper authentication a wireless client will not be able to associate with a wireless access point and therefore will be unable to gain access to network resources.

Encryption is a process of shielding transmitted data by changing the structure of data with a known process by one of the following two methods: a) use of a symmetric key paradigm or an asymmetric key paradigm, b) Encryption helps prevent interception of transmitted data for potential malicious use [4].

1.2.1 Authentication

As mentioned previously, a wireless client can gain access to network resources such as an internet connection and must first get associated with a wireless access point. Once this is completed the access point will forward all network information to that client, such as a wired network. Due to this, the process of association ensures that only legitimate clients gain access to the network. This is where authentication is used [4].

There are several authentication methods and protocols that can be implemented within a wireless network. The authentication protocol used for this research are MAC address, PPTP, MD5, CHAP, SHA-1, EAP and IPSec. Some of them are describe in the sections below.

1.2.1.1 EAP

EAP stands for Extensible Authentication Protocol, was first used in the Point-to-Point Protocol (PPP) as a method of establishing connections over dial-up. Since then EAP has been adapted for use in the wireless domain as a method to pass logon credentials between a wireless user and an authentication server. EAP and IEEE 802.1X work together to pass this logon information between the client and authentication server [5].

As previously discussed IEEE 802.1X is a transport medium for EAP frames. When a client connects to a closed port IEEE 802.1X opens that port for transportation of EAP credential frames between the supplicant and authentication server through the authenticator. Since EAP and its various subsets support a variety of authentication methods (certificates, tokens, biometrics, etc.), information can be passed on through the network without requiring any intermediary steps or settings. This is important on a network that may have varying levels of security between clients.

1.2.1.2 IPSec (Internet Protocol Security)

IPSec is a suite of protocols, standards, and algorithms to secure traffic over an untrusted network, such as the Internet. IPSec is supported on both Cisco IOS devices and PIX Firewalls.

IPSec provides four core services:

i. Confidentiality – prevents the theft of data, using encryption.

ii. Integrity – ensures that data is not tampered or altered, using a hashing algorithm.

iii. Authentication – confirms the identity of the host sending data, using pre-shared keys or a Certificate Authority (CA).

iv. Anti-replay – prevents duplication of encrypted packets, by assigning a unique sequencing number.

The IPSec standard is outlined in RFC 2401. IPsec provides encryption and authentication services at the IP (Internet Protocol) level of the network protocol stack. Working at this level, IPsec can protect any traffic carried over IP, unlike other encryption which generally protects only a particular higher-level protocol -PGP for mail, SSH for remote login, SSL for web work, and so on. This approach has both considerable advantages and some limitations. IPsec can be used on any machine which does IP networking. Dedicated IPSec gateway machines can be installed wherever required to protect traffic. IPsec can also run on routers, on firewall machines, on various application servers, and on end-user desktop or laptop machines [6].

Three protocols are used:

i. AH (Authentication Header) provides a packet-level authentication service.

ii. ESP (Encapsulating Security Payload) provides encryption plus authentication.

iii. IKE (Internet Key Exchange) negotiates connection parameters, including keys, for the other two.

1.2.2 Encryption

Encryption provides a method for wireless networks to provide end-to-end security on data streams. IEEE 802.11 networks have various encryption protocols available for use today such as WEP, RSA, and DES etc. Although WEP does not provide the security required by most networks. RSA and DES are quickly becoming the minimum standards to use for data

encryption on wireless networks, it is still in wide use and is examined in this research.

These protocols which rely on different methods to encrypt data with some form of key. This keying process typically introduces a certain amount of overhead into network communications, which is a critical part of this research. As such the manner in which these various protocols encrypt data will be covered. The encryption protocol used in this research are RSA, DES, AES and WEP. WEP is covered in the section below [7].

1.2.2.1 WEP (Wired Equivalent Privacy)

The WEP protocol was originally developed to provide the same level of security as a wired network with three goals in mind: prevent disclosure of packets in transit, prevent modification of those packets and to provide access control to the network. However, after the delivery of WEP algorithm several vulnerabilities were discovered that severely hamper its ability to perform these functions.

WEP keys are created with two lengths: 40 and 104. However, because each WEP key includes a 24-bit initialization vector the total key lengths are 64- and 128-bits, which are the commonly used terms in the industry. The initialization vector (IV) provides added security to data as it changes with each packet [8].

The algorithm used to construct WEP keys is based on the RC4 algorithm developed by RSA Security. This is a priority stream cipher that was intended to be recycled after each key. However, WEP was designed to use the same pre-shared key (up to four different keys) for each packet which creates a huge security concern. To address the problem, the IV was developed to be attached to each WEP key, creating a WEP seed that would be different for every packet [8]. Unfortunately, the IV was not set to be unique and nonrepeating for each packet, which left further vulnerability in the algorithm. The integrity check vector (ICV) at the end of WEP frame is a four-octet linear checksum intended to alert a station when a packet has been modified. This is commonly referred to as CRC-32. If something has been changed within a packet then the checksum will not match.

The paper is divided into six sections were section 2 discusses the work carried out in the related fields of wireless security as literature review, whereas section 3 describes the various techniques and methodologies used in the existing systems. Sections 4 depicts & discusses the experimental results & performance comparison of different index security policies of 802.1X and VPN. The conclusion based on the results achieved is stated in section 5 and future scope in section 6.

2 Literature Review

The whole literature review is focused on the following literature work being done by an array of scholars and researchers in wireless security. As wireless networking has grown in the market place within the past few years there has been an increasing amount of research compiled on them. However, little examination into the impact of security on the performance of those networks has been completed, particularly with the various encryption processes that are becoming the standard for enterprise wireless solutions.

2.1 "An Experimental Study on Wireless Security Protocols over Mobile IP Networks"

Agarwal and Wong [9] examined the security overhead and authentication delays associated with the use of WEP, EAP, and the Internet Protocol Security (IPSec) on a WLAN. The authors analyzed the time delays necessary to authenticate over IEEE 802.1X with varying types of EAP such as Message Digest 5 Algorithm (MD5) and Transport Layer Security (TLS), and its effect on throughput that various security types can cause. As expected, more secure levels require more packet transfers and ultimately more time to complete, with EAP-TLS needing roughly double the packets and time requirement than EAP-MD5. The authors have observed that using small data amounts resulted in no visible differences between encrypted and unencrypted stream throughput. Secondly, the paper addressed how different encryption techniques could be more computationally intensive than others. In their paper they observed how the 3DES encryption in IPSec required more computation power then the RC4 algorithm in WEP.

2.2 "IEEE 802.11 Wireless LAN Security Performance Using Multiple Clients"

This study is extensively to provide information for the research based on Baghaei's work [10]. Baghaei completed a series of experiments on a wireless network with single and multiple client stations, comparing various levels of encryption and authentication. The author used IP Traffic to generate TCP and UDP packet streams to a server from various transmitting stations. Additionally, employed Ethereal to monitor packet arrivals at the server and to help calculate latency and authentication times. To ensure that the network was fully saturated, a traffic bandwidth of 12 Mbps which was sufficiently large to saturate the IEEE 802.11b network was selected. It used four packet sizes were chosen for the experiments, 100, 500, 1000, and 1500 bytes to prevent fragmentation of packets during transmission. The author also completed experiments on an uncongested network with transmission rates lowered to 500 kbps.

The author's results showed staggering overhead associated with these security protocols. It is observed that in uncongested network (traffic rates of 500 kbps) the level 8 security definition resulted in an approximate 35% reduction in throughput for both UDP and TCP traffic. In this experiment, a general downward trend of throughput from security levels 4 through 8, which seemed reasonable as more complex security mechanisms were put in place. However, by increasing the traffic rate to 12 Mbps it was observed that the throughput was reduced by around 86% for TCP and 54% for UDP from security levels 4 through 8 [11].

2.3 "Performing Investigation of Secure 802.11 Wireless LANS: Raising the Security Bar to Which Level?"

Wong [12] provided perhaps the most well prepared study that was found on the subject matter. In addition to using standard TCP and UDP traffic, the author examined specific types of traffic such as HTTP and file transfer protocol (FTP). Wong [12] implemented ten VPN levels of security. This provided for a more in-depth look into overhead associated with layer 3 security mechanisms such as VPNs, but did not expand on previously conducted studies with WEP. With regards to the VPN model, Wong discovered some perplexing outcomes. The throughput levels increase between 17% and 30% when a firewall was present with the scenario. It also compared the IEEE 802.1X model side by side with the VPN model, which generally showed VPN security had a greater effect on throughput and response time than his IEEE 802.1X security levels.

The following general conclusions drawn are:

i. MAC and WEP authentication created no overhead.
ii. Various levels of authentication create different levels of overhead with respect to response times with EAP-TLS having the longest response time.
iii. WEP encryption impact varied and key length only affected response times.
iv. Tunneling with IPSec and PPTP generated large throughput overhead.

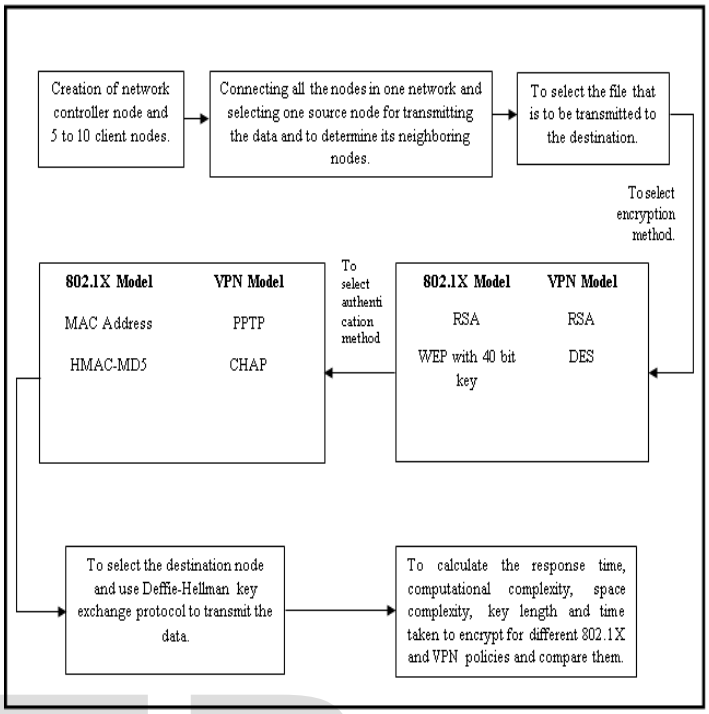
2.4 "Evaluation of Security Architecture for Wireless Local Area Networks by Indexes Based Policy Method: A Noval Approach"

The main evaluation is to analyze effect of TCP and UDP traffic over our WLAN test bed architecture. This paper present a detail study of performance overhead caused by the most widely used security protocols such as WEP, IPSEC VPN and 802.1X. Performance measurement indicates that 802.1X and VPN policy based method can be used based on the service time in future wireless systems [13], while it can simultaneously provide both the necessary flexibility to network operators and a high level of confidence to end users. WEP has minor impact on FTP throughput but decreases HTTP by 7.5%. The analysis shows the combined effect of encryption and authentication FTP response time increases by 268% and throughput decreases by 73%.VPN model and found that there will be increase of response time by 130%, so the throughput decreases by 50% [13].

3 RESEARCH METHODOLOGY

The Methodology proposed in this research work is used to compare security index policies of 802.1X model with VPN model for response time, computational complexity, space complexity, key length and time taken to encrypt in Simulator. Although there are a number of combinations that could be chosen for security configurations utilized for the testing of response time, computational complexity, space complexity, key length and time taken to encrypt. This research focuses on those most likely to be present in a corporate network environment. Proposed system architecture is shown in the

Fig. 2. Proposed system architecture



"Fig. 2" above. The authentication protocols that are examined are MAC address, PPTP, CHAP, HMAC-MD5. However, all levels of encryption, RSA, DES, AES and WEP with 40-bit and 128-bit key are included at some point in the trials.

An overview of the security combinations selected are discussed:

i. Security Level 1 – It entails open association with no encryption on the data flow. This was the base line security scheme used as the starting point for all data comparisons with encryption and authentication.
ii. Security Level 2 – For 802.1X model encryption used is RSA and authentication is completed by MAC address authentication. For VPN model RSA encryption and PPTP authentication were implemented.
iii. Security Level 3 – Open association with a 40-bit WEP key for encryption and HMAC-MD5 authentication for 802.1X model. DES encryption and CHAP (handshake procedure each time the client re-associated with the access point) authentication for VPN model.
iv. Security Level 4 – WEP 40-bit key encryption and SHA-1 authentication for 802.1X model. DES and EAP authentication for VPN model.
v. Security Level 5 - Authentication is completed with EAP and encryption is handled by 128-bit WEP key. AES Encryption and CHAP authentication for VPN model.
vi. Security Level 6 - For 802.1X model HMAC-MD5 authentication and 128-bit WEP key encryption were selected and for VPN model AES encryption with IPsec authentication.

In addition to widespread use of these security setting, it is easy to use measurement campaign. The combination of various security settings provide a broad look into overhead associated with encryption and authentication that allows one to draw accurate conclusions on the effects that encryption and authentication have on network performance.

3.1. Problem Formulation & Implementation

The experiment is simulated with 5 nodes. Initially a Network controller (server) is created with five nodes. Nodes are connected in a mesh network with each other. The further work was done as follows:

i. Selecting a source node and text file to transmit. In this work file size is limited to 10kB.
ii. Selecting the Encryption method from the options for encrypting the file.
iii. On selecting the desired encryption method, time to encrypt and key length is calculated for that specific file.
iv. After Encryption, authentication method was selected for concerned security level.
v. The decryption key was encrypted again using Deffie-Hellman protocol key exchange protocol for secure transfer of file from source to destination.
vi. Random path was generated in the simulation for every file transfer.
vii. On reaching the destination safely computational complexity, space complexity and packet transmission is calculated for security level 2, 3, 4, 5 and 6.

An important part of experiment is to determine the number of trials to utilize. This must balance time feasibility and ensure data accurately represents the system. The tests are completed in simulation software to determine system behaviors. Ultimately, five trials were chosen to complete in each security configuration to obtain suitable means for the final report.

4 Experimental Results

This section is divided into two main sections covering encryption and authentication experiments. However, there is no security mechanism activated for security level 1 in both the models. The main sections cover network configurations for security level 2, 3, 4, 5 and 6. In general each encryption result and authentication result are presented below.

4.1 Computational complexity

In the approach complexity is measured by the quantity of computational resources (time, storage, program, communication) used up by a particular task. Computation theory is basically divided into three parts of different types. First, the exact notions of algorithm, time, storage capacity, etc. must be introduced. For this, different mathematical machine models are required to be defined, the time and storage needs of the computations performed on these need to be clarified (this is generally measured as a function of the size of input). By limiting the available resources, the range of solvable problems gets narrower; this is how the different complexity classes are distinguished. The time taken right from selection of the file to sending it to destination along with encryption and authentication is computational complexity. The time taken to reach the destination minus the time at which the file was selected was calculated as computational complexity [14].

4.2 Space complexity

For calculation of space complexity A Turing machine T is used that is called polynomial, if there is a polynomial f(n) such that time T (n) = O(f(n)). This is equivalent to saying that there is a constant c such that the time demand of T is O(nc). We can define exponential Turing machines similarly (for which the time demand is O(2nc) for some c > 0), and also Turing machines working in polynomial and exponential space. We say that a language has time complexity at most f(n), if it can be decided by a Turing machine with time demand at most f(n). We denote by PTIME, or simply by P, the class of all languages decidable by a polynomial Turing machine. We define similarly when a language has space complexity at most f(n), and also the language classes DSPACE(f(n)) and PSPACE (polynomial space).Space Complexity is the total processing space required by the encryption method and authentication method on the content and the complexity of the content [14].

4.3 Security Level 2

The Security level 2 index based policy of 802.1X consist of RSA encryption and MAC address authentication. For VPN the encryption schemes are RSA and PPTP authentication. With the file size of 1kB transferred from source node 1 to destination node 5 in both the cases, the simulation software supports to calculate time to encrypt, time complexity, space complexity and packet transmission time.

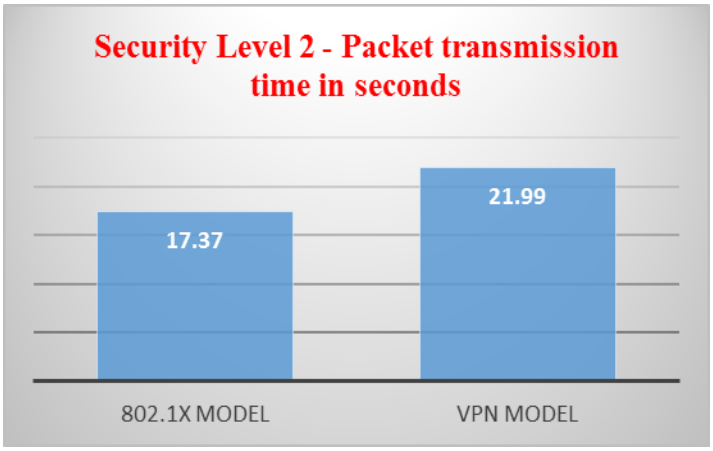


Fig. 3. Packet transmission time for security level 2

The packet transmission time for VPN model requires more time than 802.1X model has shown in the "Fig. 3" above. On comparing both the models it is clear that 802.1X is better than VPN in case of packet transmission time.

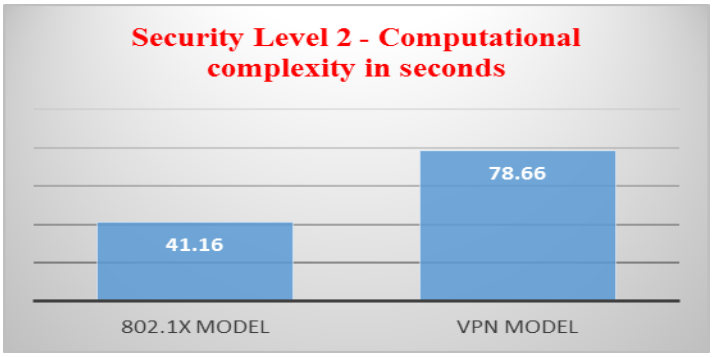


Fig. 4. Computational complexity for security level 2

Computational complexity for 802.1X model is less as compared to VPN model as shown in "Fig. 4". Therefore 802.1X model is good in terms of consuming time but provides less security then VPN model.

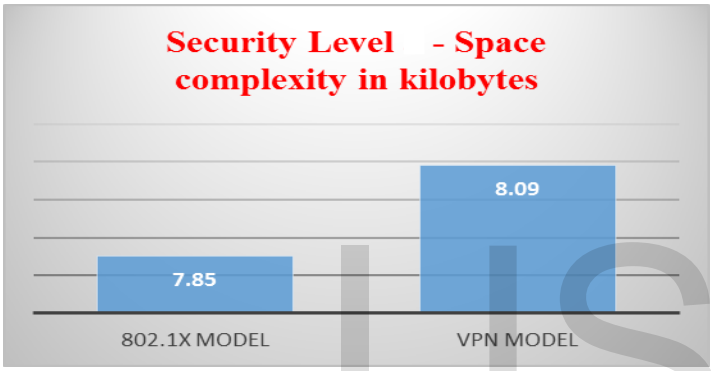


Fig. 5. Space complexity for security level 2

Space complexity for 802.1X is less as compared to VPN model as shown in "Fig. 5". The space complexity result demonstrate that 802.1X model is better than VPN for security level 2.

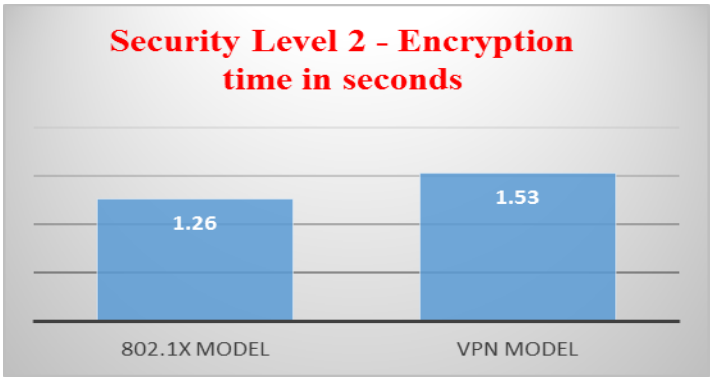


Fig. 6. Encryption time for security level 2

Encryption time required for VPN model is greater than 802.1X model as shown in "Fig. 6". Thus 802.1X is better model interms of encryption time than VPN model. For all the parameter 802.1X performs better than VPN model, thus 802.1X is the fastest in this case.

4.4 Security Level 3

The Security level 3 index based policy of 802.1X consist of WEP 40-bit key encryption and MD5 authentication. For VPN the encryption scheme is DES and CHAP authentication. File size of 1kB is transferred from source node 1 to destination node 5 in both the cases. The simulation software supports to calculate time to encrypt, time complexity, space complexity and packet transmission time.

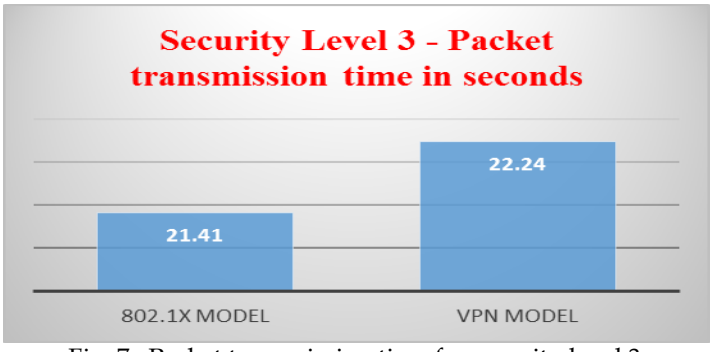


Fig. 7. Packet transmission time for security level 3

From above "Fig. 7" it is observed that VPN model requires more time than 802.1X model and is less efficient than 802.1X model.

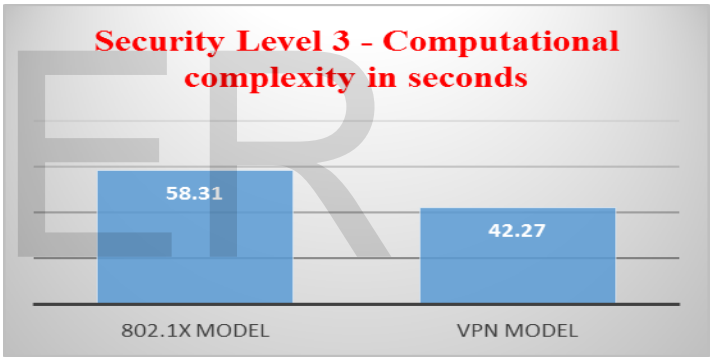


Fig. 8. Computational complexity for security level 3

Compuatational complexity for security level 3 for 802.1X is more as compared to VPN model as shown in "Fig. 8". Thus VPN model proves better than 802.1X.

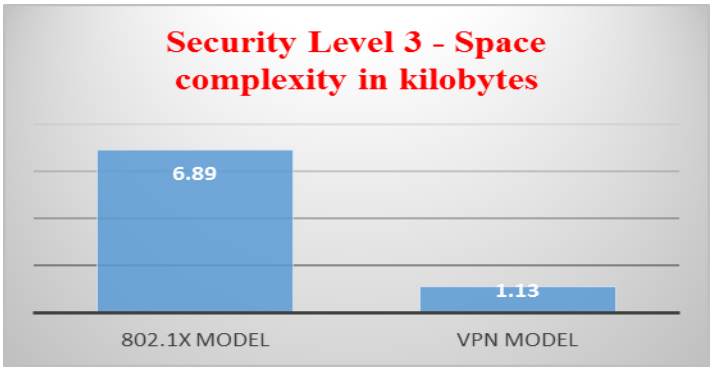


Fig. 9. Space complexity for security level 3

VPN model requires less space in terms of complexity as compared to 802.1X model shown in "Fig. 9" above.

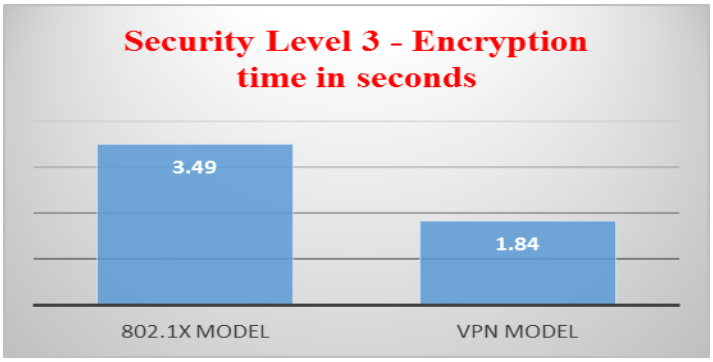


Fig. 10. Encryption time for security level 3

"Fig. 10" shows the encryption time required for security level 3 which depicts that VPN requires less time to encrypt as compared to 802.1X. It can be concluded from security level 3 that VPN is better model than 802.1X model in terms of encryption time, Space complexity and computational complexity.

4.5 Security level 4

Security level 4 index based policy of 802.1X consist of WEP 40-bit key encryption and SHA-1 authentication. For VPN the encryption scheme is DES with EAP authentication. File size of 1kB is transferred from source node 1 to destination node 5 in both the cases. The simulation software supports to calculate time to encrypt, time complexity, space complexity and packet transmission time.

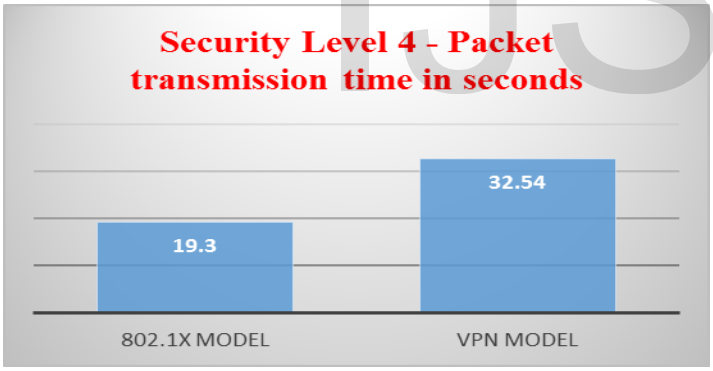


Fig. 11. Packet transmission time for security level 4

Results presented in the above "Fig. 11" show that 802.1X model takes minimum time to transmit a packet as compared to VPN in this case.

The large difference in the result indicate that it take more time for VPN model due to tunneling and overhead caused by DES algorithm, also EAP autentication time required is more in this case.

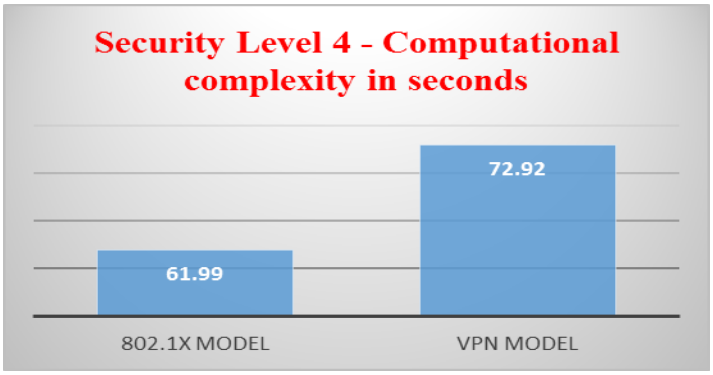


Fig. 12. Computational complexity for security level 4

The "Fig. 12" shows the difference between two models for computational complexity. It clearly states that higher the security higher is the processing time. Computational complexity is high in VPN, so security level of VPN is higher than 802.1X model.

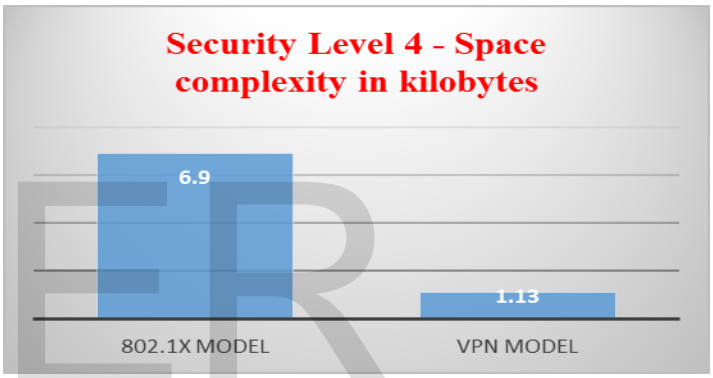


Fig. 13. Space complexity for security level 4

The "Fig. 13" above for space complexity depicts the vast difference in space required for computation for 802.1X model and VPN model. The space complexity is better in 802.1X then VPN model.

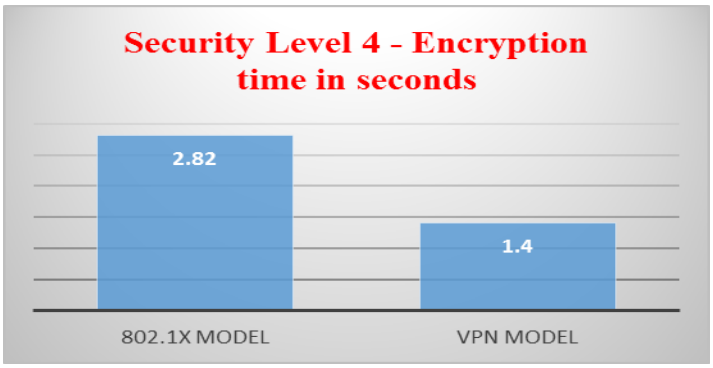


Fig. 14. Encryption time for security level 4

Encryption time for 802.1X model requires more time as compared to VPN model shown in the "Fig. 14". In this case VPN proves to be a better model. In securtiy level 4, 802.1X model performs worst than VPN model in every parameter, thus VPN proves to be better model at this policy index.

4.6 Security level 5

Security level 5 index based policy of 802.1X consist of WEP 128-bit key encryption and EAP authentication. For VPN the encryption scheme is AES with CHAP authentication. File size of 1kB is transferred from source node 1 to destination node 5 in both the cases. The simulation software supports to calculate time to encrypt, time complexity, space complexity and packet transmission time.

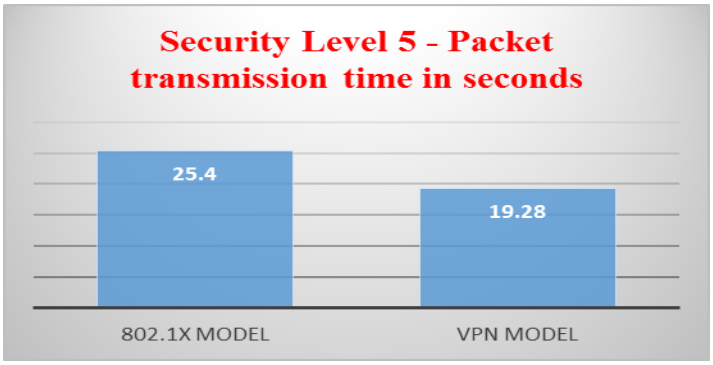


Fig. 15. Packet transmission time for security level 5

The packet transmission time for VPN model requires less time than 802.1X model has shown in the "Fig. 15". On comparing both the models it is clear that VPN is better than 802.1X in case of packet transmission time.

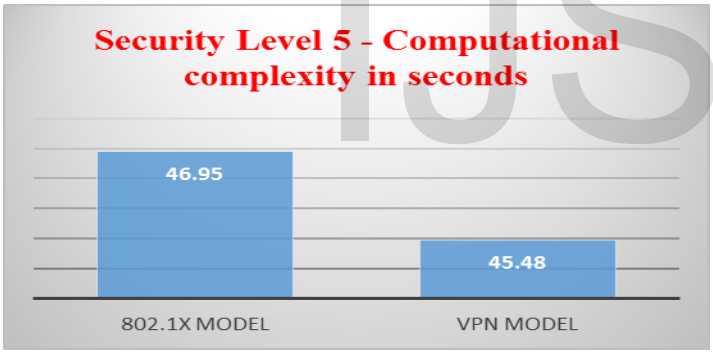


Fig. 16. Computational complexity for security level 5

Compuatational complexity for security level 5 for 802.1X is more as compared to VPN model as shown in "Fig. 16". Thus VPN model proves better than 802.1X.

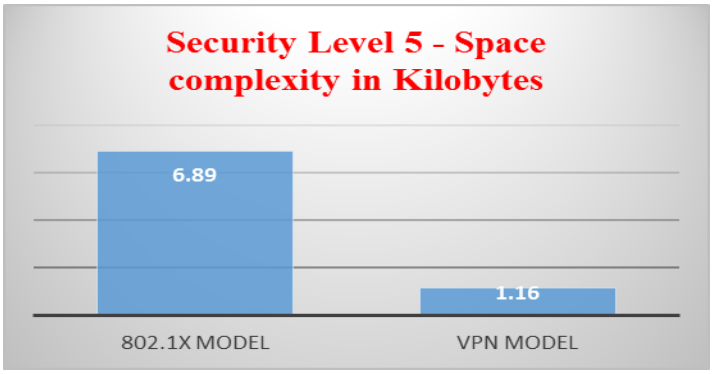


Fig. 17. Space complexity for security level 5

The "Fig. 17" for space complexity depicts the vast difference in space required for computation for 802.1X model and VPN model. VPN proves to be best in this case.

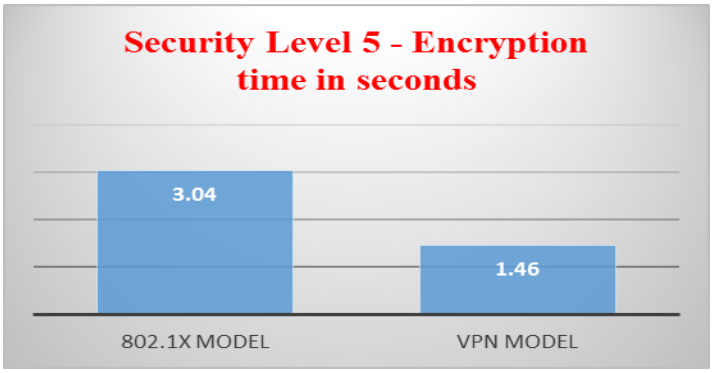


Fig. 18. Encryption time for security level 5

Encryption time for 802.1X model requires more time as compared to VPN model as shown in "Fig. 18". In this case VPN proves to be a better model.

4.7 Security level 6

Security level 6 index based policy of 802.1X consist of WEP 128-bit key encryption and MD5 authentication. For VPN the encryption scheme is AES with IPSec authentication. File size of 1kB is transferred from source node 1 to destination node 5 in both the cases. The simulation software supports to calculate time to encrypt, time complexity, space complexity and packet transmission time.

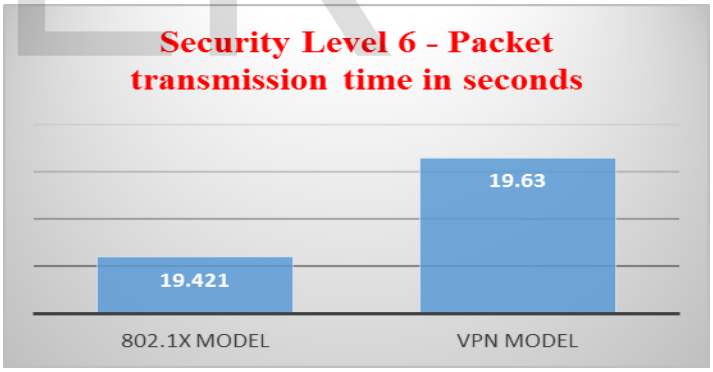


Fig. 19. Packet transmission time for security level 6

The packet transmission time for VPN model requires more time than 802.1X model has shown in the "Fig. 19" above. On comparing both the models it is clear that 802.1X is better than VPN in case of packet transmission time.

The "Fig. 20" shows the difference between two models for computational complexity. It clearly states that higher the security higher is the processing time.VPN model proves to be best model in this case.

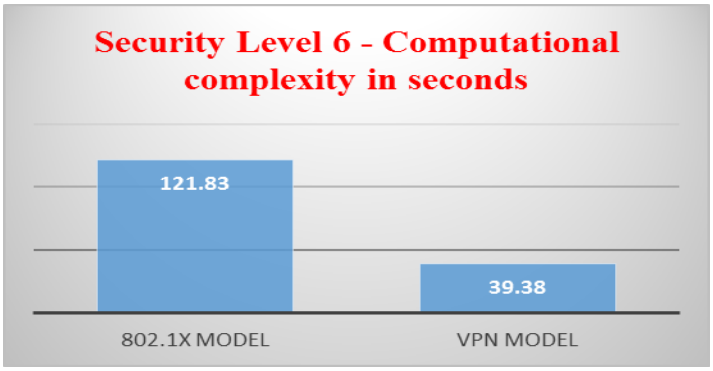


Fig. 20. Computational complexity for security level 6

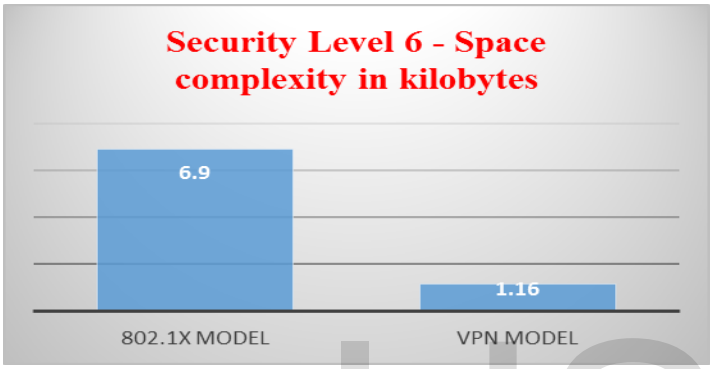


Fig. 21. Space complexity for security level 6

The figure above for space complexity depicts the vast difference in space required for computation for 802.1X model and VPN model.

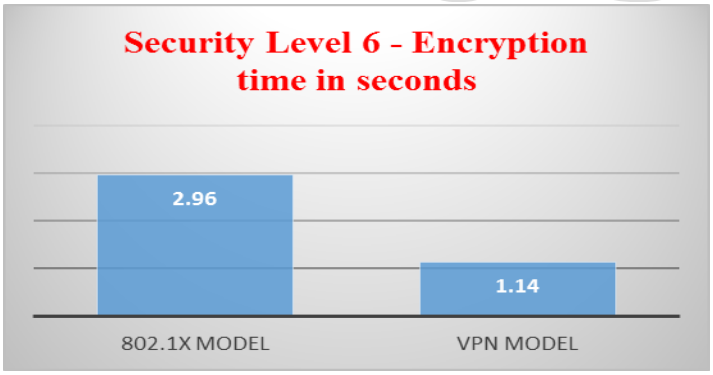


Fig. 22. Encryption for security level 6

Encryption time for 802.1X model requires more time as compared to VPN model as shown in "Fig. 22". In this case VPN proves to be a better model. VPN proves to be best model than 802.1X model for every parameter except for packet transmission time.

The IEEE 802.11g is an interface between the MAC layer and wireless media. In this work the secuirty provided by 802.1X model and VPN model provided authentication at MAC layer and encryption to transmit data safely through wireless medium.

5 Conclusion

This work provide an in-depth look into the effects that encryption and authentication may have on network performance. From the results it is concluded that encryption on today's networks can be implemented efficiently, greatly reducing the amount of bandwidth allocated to encryption processes. As the security level goes on increasing from level 3 to level 6 the response time also increases proportionally, but this method provides flexibility to the user as well as the network engineers to design security level to use for a specific transfer of data. If data security is not so important but good response time is required lower security policies can be configured.

If security is of utmost importance without caring about the delay than one can go for higher security policies such as security level 5 and level 6. Thus is can be observed from the results that higher the security level higher is the computational time and packet transmission time. It can also be observed that authentication using VPN model is better than 802.1X model, whereas encryption for 802.1X model is better than VPN model. The combined effect of encryption and authentication yields good results in VPN than in 802.1X model.

6 Future Scope

There are several areas of potential future work in this area that could be explored. This study attempted to test as many types of common enterprise configurations as possible but left out several that are in use or will continue to grow in the future. For example, EAP-TLS was ignored because of the requirements for client certificates within that particular authentication method. More importantly, the interaction of these other types of authentication with the current encryption schemes could be examined more thoroughly. Although this study attempted to record the results on simulation but the data can help for future work for comparison of security policies.

Acknowledgment

It is a moment of immense satisfaction for me to express my profound gratitude to Dr. Rajesh S. Bansode, whose constant encouragement enabled me to work enthusiastically. I convey my sincere thanks to other faculties for their rigorous brainstorming sessions to shape up this research paper.

References

[1] *A Designer's Companion*, 2nd ed., IEEE Press, New York, NY, 2005.
[2] *Cisco Wireless LAN Security: Expert Guidance for Securing Your 802.11 Networks*, Cisco Press, Indianapolis, IN 2005.
[3] M. j. Mayer, "A survey of security Issues in Multi-cast Communication," *IEEE transactions on Computer Networking*, vol. 4, no. 2, pp 12-23, Nov./Dec 1999.
[4] *Dictionary of Networking*, 3rd ed., SYBEC, Alameda, CA, 1999.
[5] *Certified Wireless Network Administartor*, 3rd ed., McGraw Hill/Osbourne, Emeryville, CA, 2005.
[6] IPSec. (http://www.freeswan.org)
[7] N. Borisov, I. Goldberg, and D. Wanger, "Intercepting mobile com-

munication: The insecurity of 802.11,' in *Proceedings of the Seventh Annual International Conference on Mobile Computing and Networking*, pp. 56-56, Jul 2001.

[8] Jamshaid, Kamran, You, Liyu, Hamza, M. H. "Performance Evaluation of Technologies for Security 802.11 Enterprise Wireless Networks" in *Proceedings of the IASTED International Conference Communications, Network, and Information Security*. New York, NY, December 10-12, 2003.

[9] Wang, Shao-Cheng, Chen, Yi-Ming, Lee, Tsern-Huei, Helmy, Ahmed, "Performance Evaluations for Hybrid IEEE 802.11b and 802.11g Wireless Networks. In *Performance, Computing, and Communications Conference: 24th IEEE International,* pp. 111-118, 7-9 Apr 2005.

[10] Baghaei, Nilufar, "IEEE 802.11 Wireless LAN Security Performance Using Multiple Clients", M.S. thesis, Dept. CS. Eng., Canterbury Univ., Christchurch, New Zealand, 2003.

[11] Kbar, Ghassan, Mansoor, Wathiq. "Testing the Performance of Wireless LAN" in *Asia-Pacific Conference on Communications*, Perth, Australia, pp. 492-496, 3-5 Oct, 2003.

[12] Wong, Jenne, "Performance Investigation of Secure 802.11 Wireless LANs: Raising the Security Bar to Which Level?", M.S. thesis, Dept. CS. Eng., Canterbury Univ., Christchurch, New Zealand, 2003.

[13] D. Nayak, D. B. Phatak, A. Saxena, "Evaluation of Security Architecture for Wireless Local Area Networks by Indexed Based Policy Method: A Novel Approach" *International Journal of Network Security*, vol.7, no.1, pp.1–14, Jul 2008.

[14] *Complexity of Algorithms*, Boston University, Spring 1999.