IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 11, Issue 4, Ver. III (Jul.-Aug .2016), PP 56-65
www.iosrjournals.org

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

Sagar Kakade[1], Dr. Rajesh S. Bansode[2]
[1]*Electronics and Telecommunication, Thakur College of Engineering and Technology*
Mumbai, Maharashtra, India
[2]*Information Technology, Thakur College of Engineering and Technology*
Mumbai, Maharashtra, India

Abstract: *Wireless local area networks (WLANs) are beginning to play a much larger role in corporate network environments. The 802.11g specification is a standard for wireless local area networks (WLANs) that offers transmission over relatively short distances at up to 54 megabits per second (Mbps), compared with the 11 Mbps theoretical maximum with the earlier 802.11b standard. In this paper, focus is on WLAN security technologies designed to improve 802.11 standard by applying security policies. Response time for authentication and encryption of 802.1X model and VPN model is compared. The comparison is done on most widely used security protocols such as WEP, RSA, EAP and DES based on measurement of policy indexing model implementation. The reports reported till date showed 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 found that there is increase in response time by 130% and decrease in throughput by 50%.The calculated results for packet transmission time for security level 2 for 802.1X is 17373 ms while for VPN it is 21996 ms, also for security level 3 it is calculated as 21419 ms for 802.1X and 22243 ms for VPN. The results obtained indicate that VPN policy method take more transmission time as compared to 802.1X policy method, but it provide more security than 802.1X method. The use of different security configuration will provide both the necessary flexibility to network operators and high level of confidence to end users.*

Keywords: *802.1X, DES, security policy index, VPN, WEP*

I. Introduction

IEEE 802.11 was the 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). The three PHYs were an infrared PHY, a frequency hopping spread spectrum (FHSS) radio PHY, and a direct sequence spread spectrum (DSSS) radio PHY. The 1999 revision included two more PHYs, IEEE 802.11a and 802.11b, which became standards in the industry with data transfer rates of 54 Mbps and 11 Mbps, respectively. The difference between the 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 verses the 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].

The MAC sublayer provides reliable data transmission for the IEEE 802.11 standard similar to a wired network. The MAC sublayer provides three functions such as, a reliable method to transmit data for users, shared access to the medium among users, and the protection of transmitted data accomplished through encryption. The first function, reliable delivery, is completed with a series of two frames, as shown in Fig.1. Because the transmission of IEEE 802.11 signals occurs wirelessly these functions must be 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, the coordination of frame exchanges between the MAC and the PHY under the control of the physical layer convergence procedure (PLCP) sublayer, use of signal carrier and spread spectrum modulation to transmit frames over the radio frequency medium under the control of physical medium dependent (PMD) sublayer, and providing carrier sense indication back to the MAC to verify activity on the media [1].

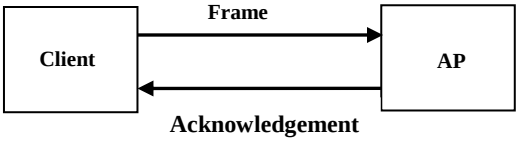

Fig.1. 802.11 Delivery

Authentication provides a method for wireless networks to verify the identity of a user and ensure authorized access to 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 the data with a known process by one of the following two methods: the use of a symmetric key paradigm or an asymmetric key paradigm. Encryption helps prevent interception of transmitted data for potential malicious use [2].

There are several authentication methods and encryption algorithm that can be implemented within a wireless network; however, only certain are of interest in this research. The authentication protocol used for this research is WEP and CHAP. Additionally, the methods of authentication that the research focuses on are 802.1X and Extensible Authentication Protocol (EAP).

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.

II. Literature review

The whole literature review is focused on the following literature work done by 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 [3] examined the security overhead and authentication delays associated with the use of WEP, EAP, and the Internet Protocol Security (IPSec) on a WLAN. They analyzed the time delays necessary to authenticate over IEEE 802.1X with varying types of EAP authentication such Message Digest 5 Algorithm (MD5) and Transport Layer Security (TLS), and the effect on throughput that various security types can cause. As expected, they determined that more secure levels required 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 found that using small data amounts resulted in no visible differences between encrypted and unencrypted stream throughput. Secondly, the paper addressed the different encryption techniques could be more computationally intensive than others. In paper authors observed 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"

Baghaei [4] 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 author chose a traffic bandwidth of 12 Mbps which was sufficiently large to saturate the IEEE 802.11b network. 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 [4].

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 there was 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, the author increased 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 [4].

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

Wong [5] examined specific types of traffic such as HTTP and file transfer protocol (FTP), in addition to standard TCP and UDP traffic. Wong [5] 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 [6]. The author came to the following general conclusions:

i. MAC and WEP authentication created no overhead.
ii. Various levels of authentication created 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 Indexed Based Policy Method: A Novel Approach"

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 [7], 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 analyses shows the combined effect of the 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% [8-9].

III. 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. 3-1 below. The authentication protocols that are examined are MAC address, PPTP, CHAP, HMAC-MD5. However, all levels of encryption, RSA, DES, WEP with 40 bit key are included at some point in the trials.

Below is an overview of the security combinations selected for study:

i. Security Level 1 – This entails open association with no encryption on the data flow. This is 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 MAC address authentication. For VPN model RSA encryption and PPTP authentication were implemented.

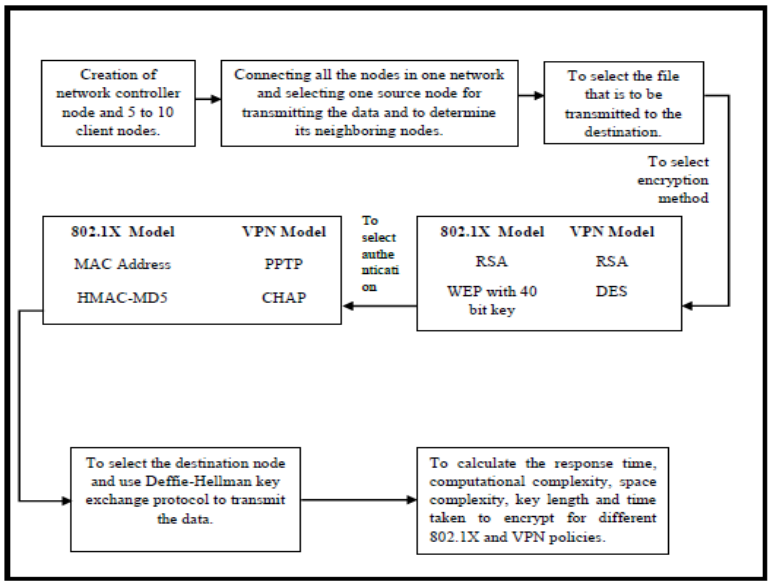

Fig. 3-1. System Architecture

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.

In addition to the widespread use of these security settings, it is easy to use the measurement campaign. The combination of various security settings provided a broad look into overhead associated with encryption and authentication, and allows one to draw accurate conclusions on the effects that encryption and authentication have on network performance [6].

3.1. Problem Formulation & Implementation

This 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 that is to be transmitted. 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 is selected for concerned security level.
v. The decryption key is encrypted again using Deffie-Hellman protocol key exchange protocol for secure transfer of file from source to destination.
vi. Random path is generated in simulation for every file transfer.
vii. On reaching the destination safely computational complexity, space complexity and packet transmission is calculated for security level 2 and security level 3.

An important part of any experiment is determining 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. When the results are presented in next section these averages are the focus of discussion for each security configuration.

IV. Experimental Results

This section is divided into two main sections covering encryption and authentication experiments. Each of these main sections covers the network configurations for security level 2 and security level 3, whereas security level 1 results were observed from pervious works. In general each encryption result and authentication result are presented below.

4.1 Security Level 2 for 802.1X model

The Security level 2 index based policy consist of RSA encryption and MAC address authentication. File size of 1kB is transferred from source node 1 to destination node 5. The simulation software supports to calculate time to encrypt, key length, time complexity, space complexity, packet transmission time. The fig 4-1 below indicates the encryption key generated for security level 2 using RSA algorithm.

Authentication overhead is measured by noting the differences between the first message sent from client and the final accept message sent from the server. This information provides general information about the time necessary for clients to authenticate with a server using different authentication methods. The MAC address authentication is done using hashing algorithm. Authentication for MAC address is shown below in fig 4-2 random signatures are generated for different size text files which provided better authentication and better security.

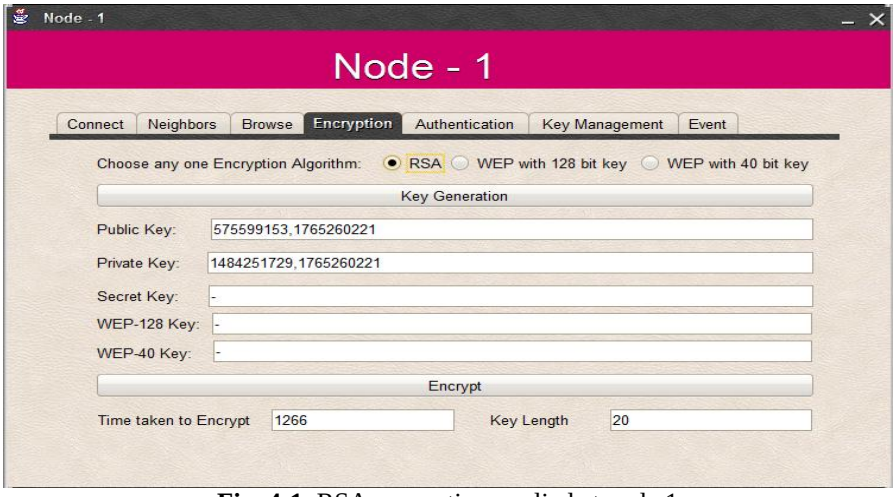

Fig. 4-1. RSA encryption applied at node 1

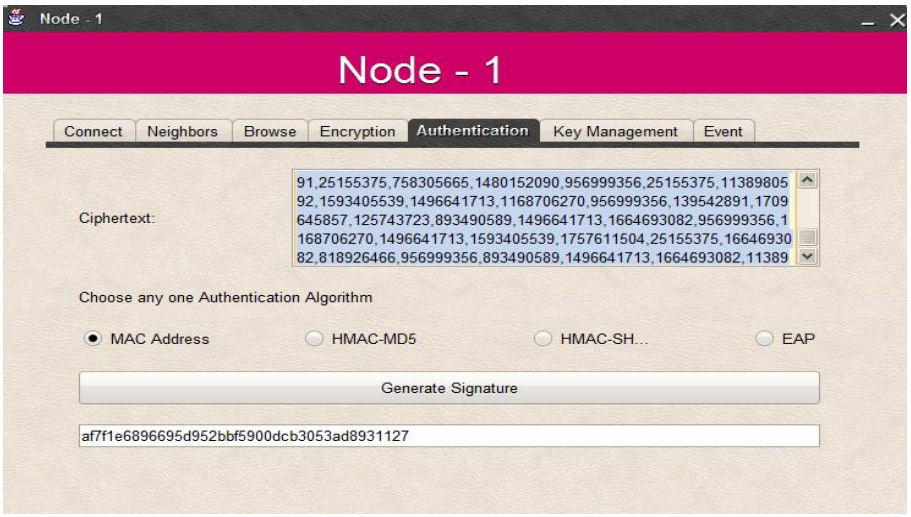

Fig. 4-2. MAC address authentication**.**

4.2 Security Level 2 for VPN model.

The Security level 2 index based policy for VPN consisted of RSA encryption and PPTP authentication.

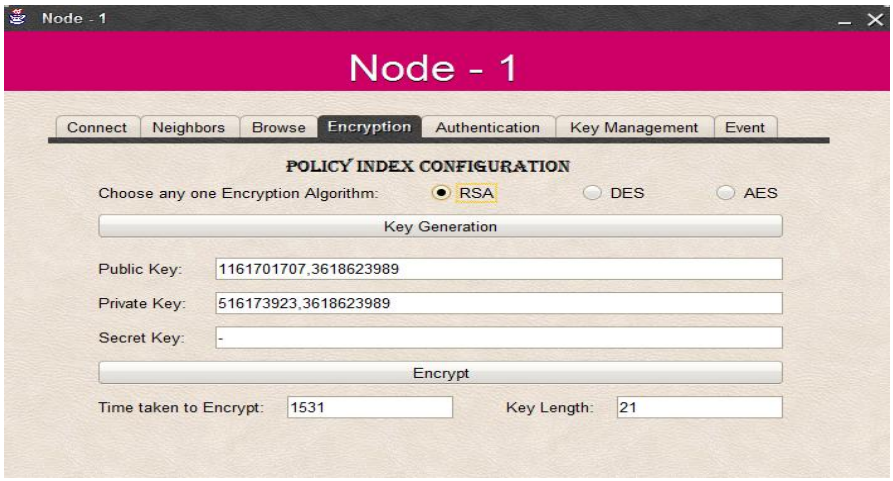

Fig. 4-3. RSA encryption for VPN model for security level 2

File size of 1kB is transferred from source node 1 to destination node 5. Fig. 4-3 above shows RSA encryption for VPN. Authentication for VPN using PPTP is shown in fig. 4-4 below.

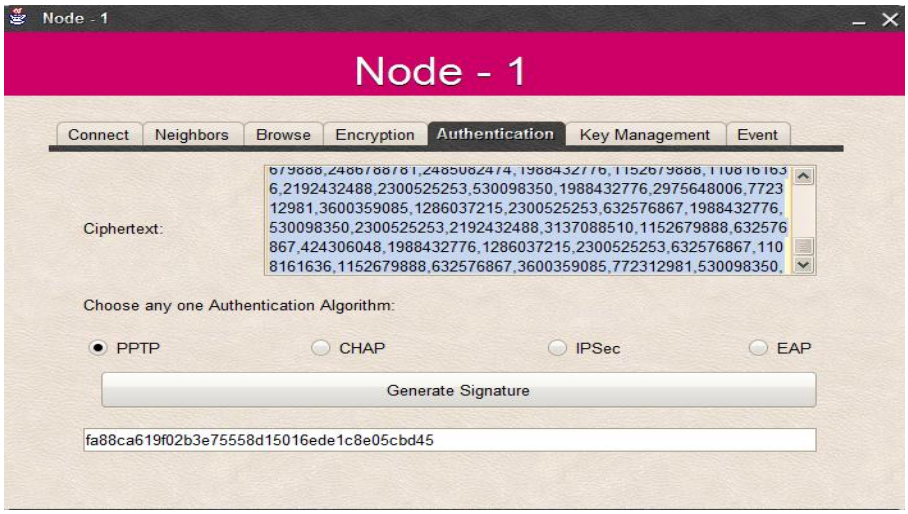

Fig. 4-4. PPTP authentication for VPN model for security level 2

4.3 Security Level 3 for 802.1X model

The Security level 3 index based policy consisted of WEP 40-bit key encryption and HMAC-MD5 authentication method. File size of 1kB is transferred from source node 1 to destination node 4. The encryption with WEP 40-bit key is shown in fig. 4-5 and authentication with HMAC-MD5 in fig. 4-6.

Fig. 4-5. WEP 40-bit key encryption for 802.1X model for security level 3

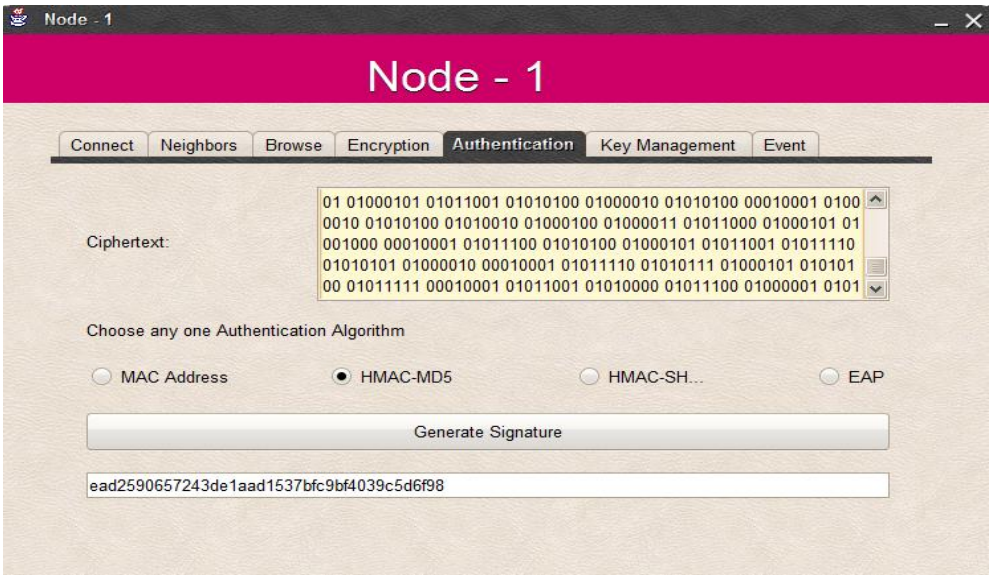

Fig. 4-6. HMAC-MD5 authentication for 802.1X model for security level 3

4.4 Security Level 3 for VPN model

The Security level 3 index based policy consist of DES encryption and CHAP authentication method as shown in fig. 4-7 and fig. 4-8 respectively . File size of 1kb is transferred from source node 1 to destination node 4. The simulator is used to calculate time to encrypt, key length, time complexity, space complexity, packet transmission time. A total of five calculations were conducted corresponding to each of the security configurations utilized. Each experiment had trials covering two different security levels.

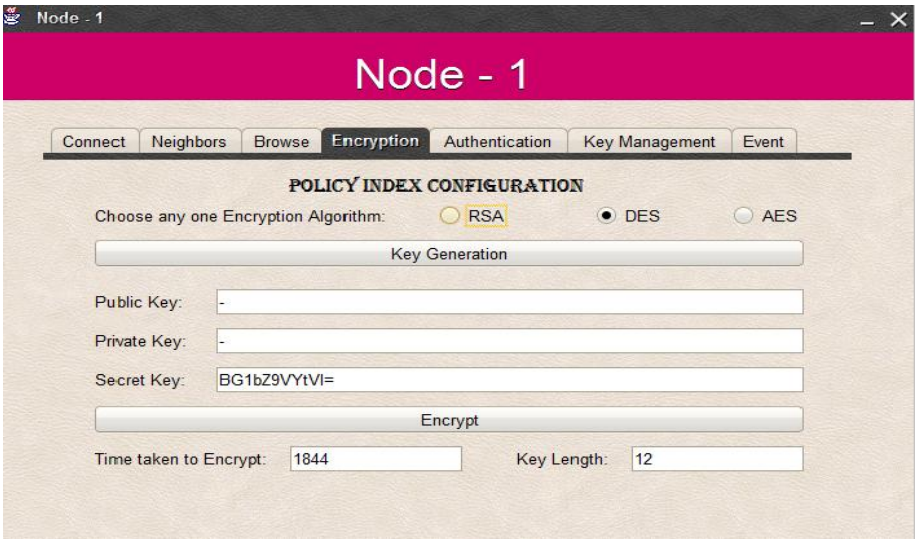

Fig. 4-7. DES encryption for VPN model for security level 3

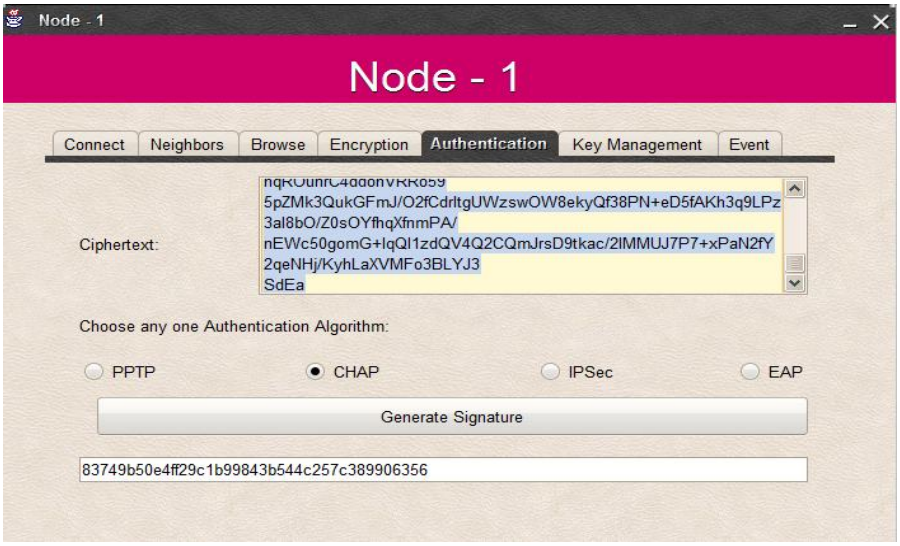

Fig. 4-8. CHAP authentication for VPN model for security level 3

The results of each configuration are presented below:
Table 4-1 given below shows the key length in bits that is generated during experiment for each of security levels for 802.1X model and VPN Model.

Table 4-1. Key length in bits

Security Levels	802.1X Model	VPN Model
Security Level 1	-	-
Security Level 2	20 bits	21 bits
Security Level 3	46 bits	12 bits

Time taken to encrypt is calculated for all the security level. The time to encrypt is the actual time taken by the specific implemented algorithm to encrypt the file before the authentication process. The time to encrypt is shown in Table 4-2 in milliseconds for both the methods. The fig. 4-9 shows the comparison of two policies for encryption. From results it can be seen that as the security level goes on increasing the encryption time also goes on increasing, hence higher the security higher the transmission time.

Table 4-2. Encryption time in milliseconds

Security Levels	Encryption time in milliseconds	
	802.1X Model	VPN Model
Security Level 1	No Security	No Security
Security Level 2	1266	1531
Security Level 3	3493	1844

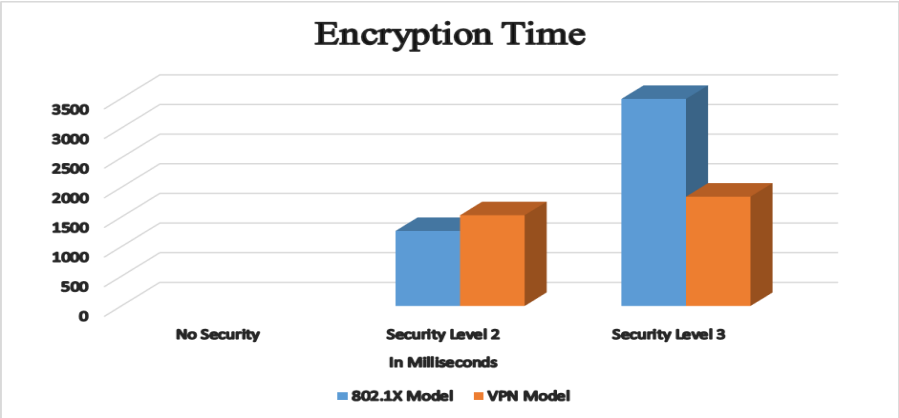

Fig. 4-9. Encryption time in milliseconds

Packet transmission time is the total time required for the file to reach from source to destination.

Table 4-3. Packet transmission time in milliseconds

Security Levels	Packet transmission time in milliseconds	
	802.1X Model	**VPN Model**
Security Level 1	No Security	No Security
Security Level 2	17373	21996
Security Level 3	21419	22243

As soon as the random path is generated the decryption key is generated using diffie-hellman key exchange protocol. The packet is then transmitted to the destination, the time taken from start till end is packet transmission time and the results are shown in Table 4-3, also the fig. 4-10 given below depicts the comparison of the two policies for 802.1X method and VPN method. As security goes on increasing packet transmission time also increases.

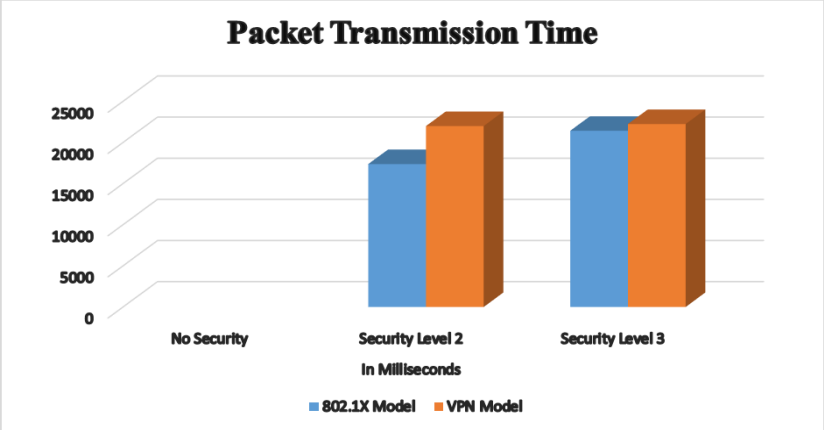

Fig. 4-10. Packet transmission time in milliseconds

4.5 Computational Complexity

In the approach taken by computer science, complexity is measured by the quantity of computational resources (time, storage, program, communication) used up by a particular task. Computation theory can basically be divided into three parts of different character. First, the exact notions of algorithm, time, storage capacity, etc. must be introduced. For this, different mathematical machine models must be defined, and 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 we arrive at different complexity classes [10]. The time taken right from selection of the file to sending it to the destination along with encryption and authentication is computational complexity. The time taken to reach the destination minus the time file was selected is calculated as computational complexity. The fig. 4-11 below shows the comparison of two policies in milliseconds, same is shown in the form of Table 4-4 below.

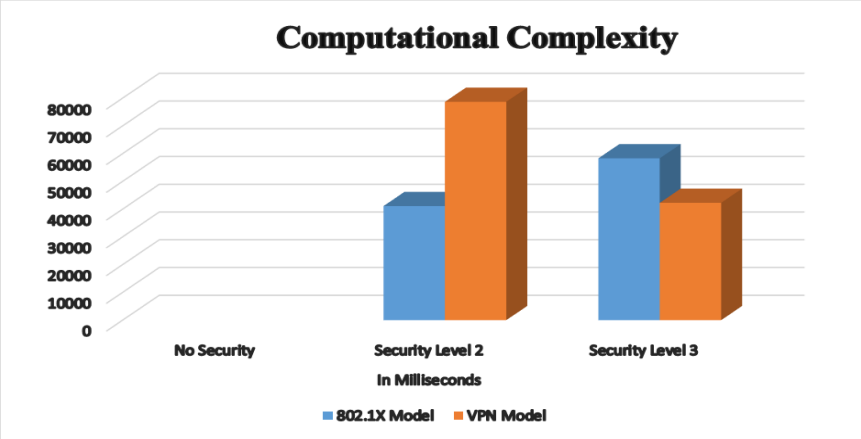

Fig. 4-11. Computational complexity

Table 4-4. Computational complexcity in milliseconds

Security Levels	Computational complexity in milliseconds	
	802.1X Model	VPN Model
Security Level 1	No Security	No Security
Security Level 2	41116	78661
Security Level 3	58315	42277

4.6 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 $O(n^c)$. We can define exponential turing machines similarly (for which the time demand is $O(2n^c)$ 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) [10].Space Complexity is the total processing space required by the encryption method and authentication method on the content and the complexity of the content, it is calculated in bytes, below is the Table 4-5 showing the camparison of space complexity, which is also depicted in the fig. 4-12.

Table 4-5. Space complexity in bytes.

Security Levels	Space complexity in bytes	
	802.1X Model	VPN Model
Security Level 1	No Security	No Security
Security Level 2	7853	8090
Security Level 3	6898	1136

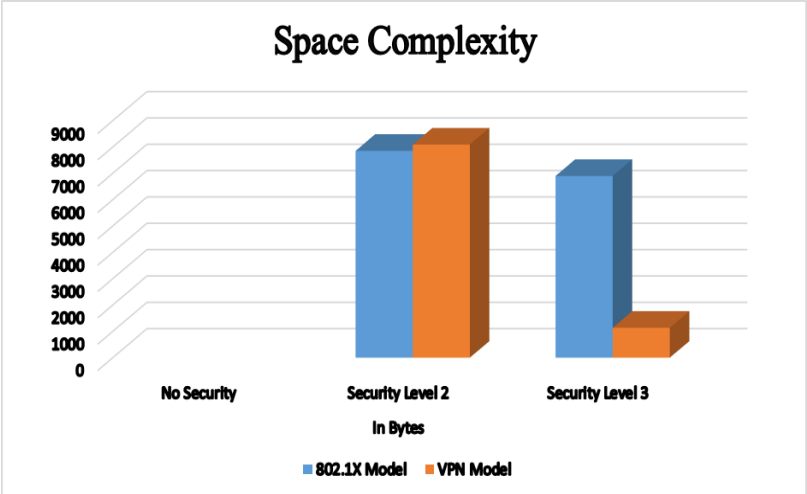

Fig. 4-12. Space complexity in bytes

V. 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 the response time also increases proportionally. 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 the data security is not so important but good response time is required lower policies can be selected. If Security is of utmost importance without caring about the delay than one can chose higher security levels. Thus it 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.

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.

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]. Agarwal, Avesh, K., Wang, Wenye. "Measuring Performance Impact of Security Protocols in Wireless Local Area Networks", Dept. of Elect. and CS Eng., North Carolina State Univ., Raleigh, NC.
[4]. Baghaei, Nilufar. "IEEE 802.11 Wireless LAN Security Performance Using Multiple Clients", Dept. of CS Eng., Canterbury Univ., Christchurch, New Zealand, 2003.
[5]. Wong, 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*, 7-9 April 2005,pp.111-118.
[6]. Wong, Jenne, "Performance Investigation of Secure 802.11 Wireless LANs: Raising the Security Bar to Which Level?", Canterbury Univ., Christchurch, New Zealand, 2003.
[7]. D. Nayak, D. B. Phatak, Ashutosh 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.
[8]. D. Nayak, D. B. Phatak, V. P. Gulati, and N. Rajendran, "Wireless data networks lack inherent security," in *National Workshop on Cryptology*, pp. 67-75, Oct. 2003.
[9]. D. Nayak, D. B. Phatak, V. P. Gulati, and N. Rajendran, "Mobile data Networks security issues and challenges," *in International Conference on Emerging Technology*, pp. 137-148, Dec. 2003.
[10]. *Complexity of Algorithms*, Boston Univ., Spring 1999.