ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2015

An Evaluation of "Security Services" schemes For IEEE 802.11 Wireless LAN's Using Qualnet

Richa Gupta [1], Hamid Ali[2], munendra kumar das[3], Shalini Chaudhary [4]

P.G. Student, Department of Electronics and Communication Engineering, Shobhit University, Meerut, India[1]

Associate Professor, Department of Electronics and Communication Engineering, Shobhit University, Meerut, India[2]

Assistant Professor, Department of Electrical Engineering, Dr. K N Modi Institute of Engineering and Technology, Modinagar, India[3]

P.G. Student, Department of Electronics and Communication Engineering, Shobhit University, Meerut, India[4]

ABSTRACT: In the era of information and communication technology, WLANs are being used for military, multimedia and health application, where high system performance and the ability to stay in link is extremely required. WLAN supports best-effort service at lower investment and cost. Apart from low cost ,IEEE 802.11 technology is relatively easy, quick to install , and operating on a unlicensed frequency of 2.4 GHz which can be built independently by the individual or organization without reliance on operator. With the increasing demand and penetration of wireless services, users now expect good Quality of Services (QoS), in terms of delay; media access delay, throughput, and retransmission attempts. The author has studied the effect on Security by changing number of nodes, changing data rates and changing attacks. The effects of variation of these parameters on Throughput, Average Jitter, Average End to End Delay, Peak Queue Size and Average Queue Length have been studied Throughput of CCMP Security Protocol is more by 13.3% in comparison to WEP Security Protocol. In CCMP Average Jitter and Average End to End Delay are lesser by 7.4% and 10.24% respectively in comparison to WEP Security Protocol. This simply proved that CCMP Security Protocol is provides better security in comparison to WEP Security Protocol and remove the flaws of WEP Security Protocol. Wormhole Attack and Eavesdrop Attack badly affected the performance of IEEE 802.11 WLANs. Throughput in wormhole attack reduces by 17% in comparison to eavesdrop attack. Average Jitter and Average End to End Delay reduces by 14% and 8% respectively in Eavesdrop Attack in comparison to Wormhole Attack.

KEYWORDS: Quality of Service, wireless LANs, performance evaluation, MAC protocol**.**

I. INTRODUCTION

WLAN standard and security services is IEEE 802.11 become top priority in installation of wireless technology-based information infrastructure because of its economic feasibility and high ability over several wireless technologies available today such as microwave, Wi-Fi or IEEE 802.11 and Wi-MAX. Apart from the low cost, IEEE 802.11 technology is relatively easy, quick to install, and operating on an unlicensed frequency of 2.4 GHz which can be built independently by the individual or organization without reliance on operator. A Wireless LAN always uses the electromagnetic waves to transmit the data signals from one end to another end in the network and it is implemented on the physical layer. IEEE 802.11 wireless LAN has two types of network architectures:

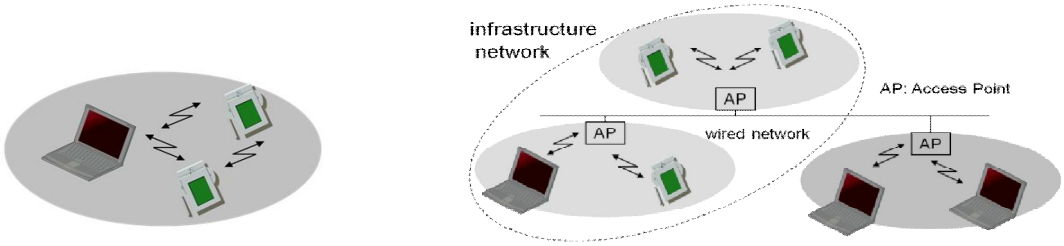
A) Ad-Hoc Network
B) Infrastructure Network

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2015



(a) (b)

Figure 1: a) Ad-Hoc Network b) Infrastructure Network

IEEE group started work on IEEE 802.11 project in year 1997, in order to design a Medium Access Control (MAC) and Physical layer (PHY) which provides benefits to wireless connectivity to fixed stations, portable stations and moving station within the specific boundary of the network. The initial standard includes three Physical layers, FHSS (Frequency Hopping Spread Spectrum), DSSS (Direct Sequence Spread Spectrum) and Infrared. Later on two other transmission technologies were included OFDM (Orthogonal Frequency Division Multiplexing) and HR-DSSS (High Rate Direct Sequence Spread Spectrum).

IEEE802.11 MAC layer consists of Channel Access Mechanism. IEEE802.11 MAC provides two channel access controls, DCF (Distributed Coordination Function) and PCF (Point Coordination Function). PCF provides contention-free channel access and aims at supporting real-time traffic. DCF works based on CSMA/CA (Carrier- sense Multiple Access with Collision Avoidance) with the consideration of the complexity in wireless environment; for example, stations can not listen to the channel for collisions while transmitting.

II. SECURITY IN IEEE 802.11 NETWORKS

The security solutions is a measure of network performance that reflects the network's transmission quality and service availability for IEEE 802.11 standard like WEP, CCMP, etc and which one is considered to be best in which environment.

1. Wired Equivalent Privacy (WEP)

WEP is a first security technique that is used in IEEE 802.11 standards. The main purpose of using the WEP is to provide the security to WLAN like the wired LAN. WEP helps to make the communication secure and provide the secret authentication scheme between AP and the end user which is going to access the WLAN. Basically WEP implemented on initial Wifi networks so that the user can not access the network without the correct key. WEP uses symmetric key encryption that ranges from 64 to 128 bit long encryption key. Usually, the same encrypted key is used for all the nodes in the network and manually forwarded to each node means WEP is unable to provide the key management function. WEP is using the shared key authentication method in which the user needs two things in order to access the WLAN, one is SSID and second is WEP key generated by the AP. The IEEE 802.11 standard defines the three different parameters for the WEP i.e. access control, data privacy and data integrity.

2. CCMP

The CCMP is an encryption algorithm of IEEE 802.11i. CCMP performs in a particular mode of operation that is AES. In other words the mode of operation is known as the algorithm, whose purpose is to change the cipher text to plaintext and vice versa. The main purpose of using the encryption technique is to provide the confidentiality to data and hence it is proved that previous encryption technique is failed to provide the data integrity. In order to provide the integrity to data, a new message authentication code is appended with the original message. The message authentication code is useful for keyed cryptographic function in order to generate the integrity value (ICV).

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2015

In IEEE 802.11i standard is divided the CCMP in to two parts:

i] Counter mode "CTR-Mode". The counter mode is used in AES to encrypt the data.
ii] Cipher block chaining- MAC mode "CBC-MAC Mode". CBC-MAC mode is used to create a MIC code that provides integrity to data.

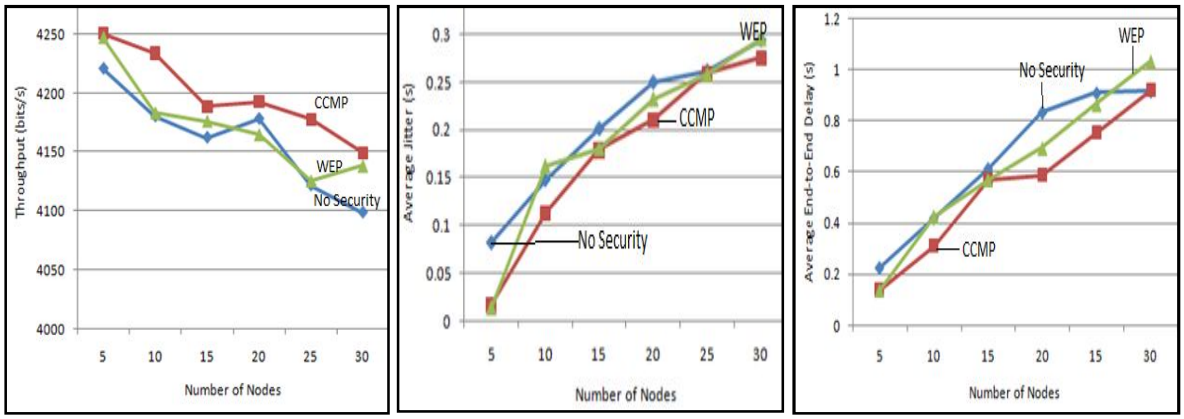
3. Parameters Studied

The following parameters were studied to compare the results obtained to determine the Security of IEEE 802.11 Wireless Local Area networks under WEP and CCMP Security Protocols.
(i) Throughput (bit/sec): The total number of bits (in bits/sec) sent to the higher layer from the MAC layer. The data packets received at the physical layer are sent to the higher layer if they are destined for this station.
(ii) Average Jitter: Jitter is defined as a variation in the Delay of received packets.
(iii) Average End-to-End Delay: It indicates the Length of time taken for a packet to travel from the CBR (Constant Bit Rate) source to the destination. It represents the total Delay between creation and reception of an application packet.

III. SIMULATION SCENARIO

In our work, we use QUALNET 5 to model a WLAN. We have taken three different scenarios to study the performance of WLAN.

Scenario 1: Effect on Security by Changing Number of Nodes



(a) (b) (c)

Figure 2: (a) CBR Server Throughput comparison, (b) Average Jitter comparison , (c) Average End to End Delay comparison for No Security, WEP Security Protocol and CCMP Security Protocol

Analysis of scenario 1 simulation results:

1. The values of CBR Server Throughput for no security, WEP and CCMP are 4160.205, 4172.48 and 4198.82 bits/sec. respectively. As the number of nodes increases the Throughput constantly decreases.
2. Average Jitter for no security, WEP and CCMP are 0.206268, 0.190632 and 0.175432 seconds respectively. As the number of nodes increases the Average Jitter increases.
3. Average End to End Delay for no security, WEP and CCMP are 0.652751, 0.621823 and 0.547728 seconds respectively. As the number of nodes increases the Average End to End Delay constantly increases.

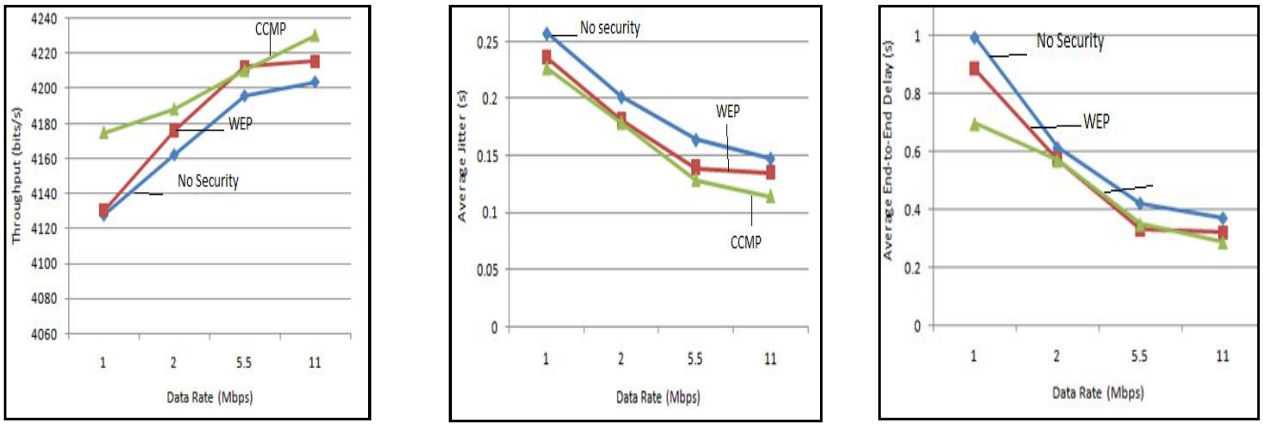
ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2015

Scenario 2: Effect on Security by Changing Data Rates



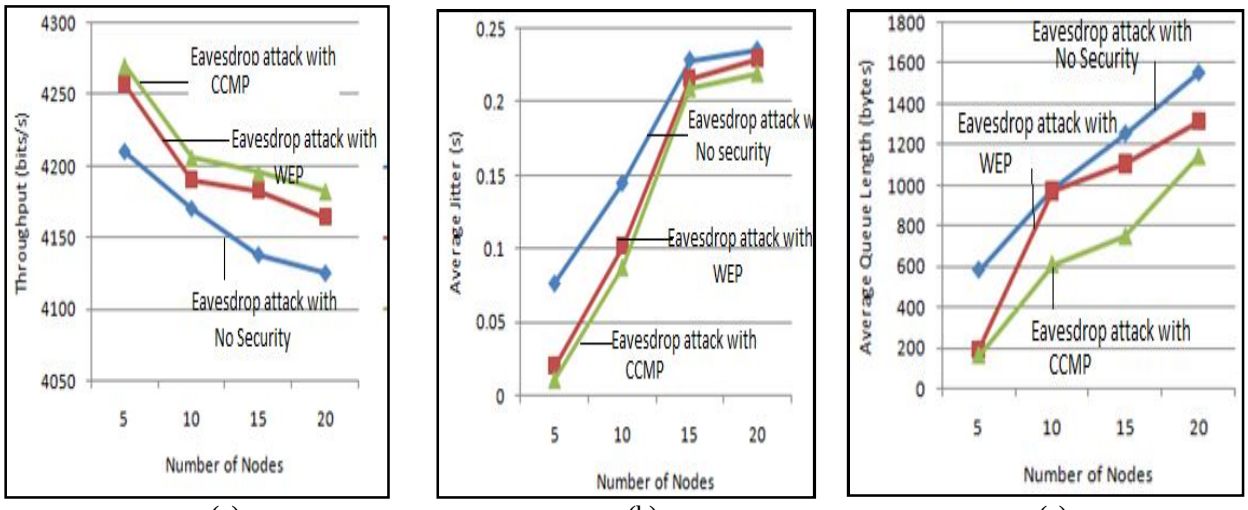
(a) (b) (c)

Figure3 (a) CBR Server Throughput comparison , (b)Average Jitter comparison , (c) Average End to End Delay comparison , for No Security, WEP Security Protocol and CCMP Security Protocol

Analysis of scenario 2 simulation results:

1. CBR Server Throughput for no security, WEP and CCMP are 4168.355, 4180.645 and 4201.09 bits/sec respectively. Throughput is highest for the 11 Mbps and lowest for 2 Mbps.
2. Average Jitter for no security, WEP and CCMP are 0.192469, 0.172761 and 0.162024 seconds respectively. Average Jitter is highest for the 2 Mbps and lowest for 11 Mbps.
3. Average End to End Delay for no security, WEP and CCMP are 0.599576, 0.526785 and 0.475889 seconds respectively. Average End to End Delay is highest for the 2 Mbps and lowest for 11 Mbps.

Scenario 3: Effect of Attacks on Security



(a) (b) (c)

Figure 4: (a) CBR Server Throughput comparison, (b) Average Jitter comparison, (c) Average End to End Delay comparison for No Security, WEP Security Protocol and CCMP Security Protocol

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2015

Analysis of scenario 3 simulation results:

1. CBR Server Throughput for no security, WEP and CCMP in eavesdrop attack are 4161.06, 4198.8 and 4213.3 bits/sec. respectively. The CCMP removes the flaws present in WEP and provides better security to wireless network.
2. Average Jitter value for no security, WEP and CCMP are 0.171716, 0.141712 and 0.131984 seconds respectively. The Average Jitter reduces by 17.48% when WEP security protocol is used in Eavesdrop.
3. Average End to End Delay for no security, WEP and CCMP are 0.559104, 0.453789 and 0.41434 seconds respectively. Average End to End Delay decreases by 8.69% in comparison WEP, When CCMP security protocol is used in Eavesdrop.

IV. CONCLUSION

The findings of the thesis work clearly states that, the implementation of such security mechanisms have a significant impact on the overall network through positively. On the other hand, the implementation of such protocols not only mitigates security related issues, it also increases the overall performance of our IEEE 802.11 Wireless Networks. WEP Security Protocol and CCMP Security protocol which are provision security in IEEE 802.11 networks provide adequate performance to secure IEEE 802.11 Wireless Networks.

Throughput of CCMP Security Protocol is more by 13.3% in comparison to WEP Security Protocol. In CCMP Average Jitter and Average End to End Delay are lesser by 7.4% and 10.24% respectively in comparison to WEP. This simply proved that CCMP is provides better security in comparison to WEP and remove the flaws of WEP.

It is observed that as the number of nodes increases throughput decreases but values of Average Jitter and Average End to End Delay increase. So it can be concluded that it become difficult to provide security to the network as number of nodes increases.

Increasing data rate reduces Average Jitter and Average End to End Delay because it take less time to transmit data from one node to another and increases Throughput at 11 Mbps data also increases about three times in comparison to data rate 1 Mbps. So we can use 11 mbps data rate for better IEEE 802.11 wireless network performance.

Simulation of Wormhole and Eavesdrop attacks proved that attack reduces the performance of network if security measures did not used. Throughput in Wormhole attack reduces by 17% in comparison to Eavesdrop attack. Average Jitter and Average End to End Delay reduces by 14% and 8% respectively in Eavesdrop attack in comparison to Wormhole attack. In this, several methods for improving WLAN performance were investigated. Using QUALNET software tool for network management and capacity planning several network models were created, different scenarios were chosen, simulation were executed and results were viewed and analyzed. We have simulated throughput, Average End to End delay, Average jitter , for no Security, WEP, CCMP service measures for WLAN network.

We have classified over simulation in 3 different scenarios and their conclusion is as follows:

[1]. Throughput of CCMP Security Protocol is more by 13.3% in comparison to WEP Security Protocol.
[2]. In CCMP Average Jitter and Average End to End Delay are lesser by 7.4% and 10.24% respectively in comparison to WEP.
[3]. As the number of nodes increases throughput decreases but values of Average Jitter and Average End to End Delay increase. So it can be concluded that it become difficult to provide security to the network as number of nodes increases.
[4]. Increasing data rate reduces Average Jitter and Average End to End Delay because it take less time to transmit data from one node to another and increases Throughput at 11 Mbps data.

REFERENCES

1. Abdul Qudoos Memon, Ali Hasan Raza and Sadia Iqbal, “WLAN Security”, International Journal of Computer Theory and Engineering, Vol. 1, No. 2, April 2011, pp. 140-145.
2. Nilufar Baghaei and Ray Hunt, “IEEE 802.11 Wireless Lan Security Performance using multiple clients”, IEEE Communications Surveys and Tutorials, Vol. 12, 2004.

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2015

3. Stallings, W., "IEEE 802.11: moving closer to practical wireless LANs", IT Professional. Volume: 3 Issue: 3. Page(s): 17 –23, June 2001.
4. Chye Bin Tay and Norman F. Schneidewind, "Wireless LAN Extension", Journal of Convergence Information Technology, Vol. 5, No. 7, march 2003, pp. 100 -111.
5. QualNet Simulator 5.0, "QualNet 5 users guide scalable network technologies Inc." 2010, pp. 124-128.
6. Timothy X Brown, Jesse E. James and Amita Sethi, "Jamming and Sensing of Encrypted Wireless Ad Hoc Networks", Published at Communications Magazine, IEEE, 2006 pp. 142 - 148.
7. Yang Xiao, Chaitanya Bandela, Xiaojiang (James) Du and Yi Pan, "Security mechanisms, attacks and security enhancements for the IEEE 802.11 WLANs", International journal of Wireless and Mobile Computing, Vol. 1, Nos. 3/4, 2006, pp. 276-288.
8. Marianne Azer, Sherif El-Kassas and Magdy El-Soudani, "A Full Image of the Wormhole Attack Towards Introducing Complex Wormhole Attacks in wireless Ad Hoc Networks", International Journal of Computer Science and Information Security, Vol. 1, No. 1, May 2009.
9. Ali Hamieh and Jalel Ben-Othman, "Detection of Jamming Attacks in Wireless Ad Hoc Networks using Error Distribution", Proceedings of Hotnets-V, 2009.
10. Geethapriya Thamilarasu, Sumita Mishra and Ramalingam Sridhar, "Improving Reliability of Jamming Attack Detection in Ad hoc Networks", Internationa Journal of Communication Networks and Information Security, Vol. 3, No. 1, April 2011, pp. 57-66.
11. G. Jayanthi Lakshmi, S. Babu, B Lakshmana Rao, P Mohan and B Sunil Kumar, "Jamming Attacks Prevention in Wireless Sensor Networks Using Secure Pack Hiding Method", International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 9, September 2013, pp. 3429-3433.
12. Rajpal Singh Khainwar, Mr. Anurag Jain and Mr. Jagdish Prasad Tyagi, "Elimination of Wormhole Attacker Node in MANET Using Performance Evaluation Multipath Algorithm", Network and Complex Systems ISSN 2224- 610X (Paper) ISSN 2225-0603 (Online) Vol.3, No.7, 2013, pp. 22-29.