Impact of Security Algorithms on Various Performance Metrics of Wireless LAN

V. Bhatia, D. Gupta, *Member, IAENG* and H.P. Sinha

***Abstract*— Today is the world of wireless information networks, the popularity of which is increasing day by day. As a result the society has witnessed burgeoning of wireless networks. Wireless LANs are one of the most popular forms of wireless networks. These networks provide an additional feature of maneuverability to their users. However unlike the traditional wired LANs, wireless counterparts are complex in terms of performance and security. Thus with increase in use and deployment of wireless LANs, the need to analyze their performance metrics and security has surfaced in recent years. We have developed simulation scripts for two security algorithms used in WLANs – WEP and WPA, which have been utilized successfully to simulate WLANs, using network simulator software NS2 and studied the effects of these security algorithms on various parameters, viz., end-to-end delay and packet delivery fraction, by implementing these scripts. The results produced by simulation experiments, are used to arrive at succinct conclusion.**

***Index Terms*— end-to-end delay, packet delivery fraction, WEP, WLAN, WPA**

I. Introduction

WITH advancements in technology the society has reached a stage where it cannot limit its mobility while transferring information. Thus gone are the times when only wired form of networks was used. As the society has readily accepted wireless as convenient and practical form of communication, wireless networks have turned out to be one of the recent happenings in the modern world. Wireless LANs are the most popular forms of wireless networks used for communication. The ubiquity of these networks ranges from homes, offices, edifices, cafes, universities and many more. These networks offer number of advantages to their users such as mobility and ease of installation. Inspired by these advantages, there has been a large increase in the number of networks deployed and used. As more and more users have started using these networks, there are number of security issues related to information transfer through this mode. These networks transmit information using radio waves and are not limited by any physical boundaries. This makes a wireless LAN (WLAN) more prone to certain threats and attacks. To introduce security in WLANs, an IEEE 802.11b standard, commonly known as Wired Equivalent Security (WEP), was created. Although WEP was formulated to introduce extra security in wireless LANs, but it proved ineffectual. This was due to various vulnerabilities reported against it that has lead to the amendments in the WEP until another security algorithm known as Wi-Fi Protected Access (WPA) was discovered [1]. WPA was able to restrict number of attacks, however WEP still continued to be used in common household and small office LANs to restrict unintentional thoroughfare. As a result practically both WEP and WPA are used depending upon the level of security desired by the user. Since the field of wireless LAN security is comparatively novel, various performance metrics affected by these security algorithms are still concealed and thus they need to be explored. Foremost performance metrics employed to analyze performance of a WLAN are throughput, packet delivery fraction and end-to-end delay. WEP and WPA have been compared on the basis of throughput [2], [3]. The authors in this paper have tried to simulate the wireless LAN, which make use of WEP or alternatively WPA through simulator software, NS2. These scripts have further been implemented in studying the end-to-end delay and packet delivery fraction for WEP and WPA and have been compared too. This analysis is further extended by varying the size of the network so as to obtain the effects on the two performance metrics in security enabled simulated wireless LAN environment with different number of nodes.

V. Bhatia is a Ph.D. Scholar with the Department of Electronics and Communication Engineering at M.M University, Mullana, INDIA. (phone: +91-9255385355; e-mail: vinay4research@yahoo.com).

D. Gupta is with Department of Electronic Science, University College, Kurukshetra University, Kurukshetra, INDIA. (e-mail: gupty2kuk@yahoo.co.uk).

H. P. Sinha is with the Department of Electronics and Communication Engineering at M.M University, Mullana, INDIA. (e-mail: drhpsinha@gmail.com).

II. Review of Security Algorithms

During 1980's a committee IEEE 802 was involved in the development of wireless LAN standards. However work on wireless LANs started in 1984 with the development of the ISM band for token passing MAC protocol. It was soon realized that this method of token passing would increase wastage of the available spectrum. As a result in 1990, a new working group, IEEE 802.11 was formed by this committee to deal specifically with issues related to WLANS. Since then a number of standards were suggested by the committee to keep pace with increase in variety of bandwidth, range and frequency demands put forward by the society [4]. This section introduces two popular security algorithms, namely WEP and WPA which may be employed to provide security in a wireless LAN.

A. Wired Equivalent Privacy

The WEP was the first encryption protocol, developed in 1997 to be deployed in wireless networks for providing

ISBN: 978-988-19252-8-2
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

authentication and security. WEP as the name suggests was developed to introduce security in wireless LAN which is equivalent to that a wired LAN could possess. IEEE 802.11 defined three goals for enhancing security in a WLAN environment [4]:

• Confidentiality: This is the fundamental goal of WEP as it is necessary to keep intruders away from the secret data.

• Access control: The second goal of the WEP is access control which aims to provide access only to the users who are allowed to do that. It ensures that illegitimate users are not being able to connect to the wireless network.

• Data integrity: This was an added feature of WEP which intends to check whether the received message has some errors during transmission and if yes how can it be corrected. These issues have been taken up by the CRC-32 algorithm which provides integrity check in the WEP.

WEP provides two fold protections to wireless networks as it incorporates secret key for access control and encryption for confidentiality. The secret key is shared between a mobile device and a wireless access point. It comprises of 64 bits with a 24 bit IV (Initialization vector). The key used in WEP is scrambled using a cryptographic function; RC4. RC4 is not particular to WEP but is used frequently in various cryptographic applications. The RC4 algorithm is a two step process consisting of the Key Scheduling Algorithm (KSA) and the Pseudo Random Number Generator (PRGA). Each packet of information is scrambled with a key pattern. The use of Initialization Vector (IV) is a vital feature of WEP. Since the IV keeps on changing, its use helps to produce different ciphertext for same plaintext, which makes prediction of plaintext more difficult during the process of eavesdropping. WEP concatenates the data and IV with the key stream using the exclusive-or (XOR) function. On the other hand the integrity check ensures that the information does not change during transmission. Before a data packet is transmitted, the integrity check (IC) computes a checksum. Then WEP concatenates the data and IC with the keystream using the exclusive-or (XOR) function. WEP is applied to all layers above physical and data link layers for IEEE 802.11b WLANs. [5]. Although WEP was developed to provide security in wireless LANs, it became prey to different types of attacks due certain flaws detected in it [6], [7]. Since an expert hacker is able to play different attacks against WEP, its use became limited to restrict unintentional intrusion only.

B. Wi-Fi Protected Access

As WEP suffered from certain flaws, it became essential to develop another protocol with enhanced capabilities. This ultimately led to discovery of Wi-Fi Protected Access (WPA) by the Wi-Fi Alliance. WPA was discovered as an intermediate solution to various security threats which remained unanswered by WEP, to provide the Wireless users an immediate solution until a secure and stable version got created. The underlying feature of WPA is also same as that of WEP but it differs in its strength to resist various attacks as it uses a stronger encryption process [8]. There are two variants of WPA has two variants: AES and TKIP. WPA uses AES (Advanced Encryption Standards), which is a stronger encryption scheme than RC4 while TKIP-WPA is backward compatible with WEP hardware. Typically Temporal Key Integrity Protocol (TKIP) provides pre-packet key mixing and a message integrity check. TKIP utilizes a longer encryption key than WEP which employed a forty-bit key which is relatively weak even when properly implemented. The 128-bit WEP addressed this short-key problem but it has never been a part of an IEEE standard. Each 802.11 vendor implemented 128-bit WEP on its own, and these unique implementations caused problems for heterogeneous environments in which interoperability of hardware was an issue. By using longer keys and implementation standards, TKIP addresses short-key problem of WEP.

WPA is known to be stronger then WEP as it is effective against many attacks which WEP cannot withstand [8], [9]. It shuts down the network if two packets using the wrong key are sent at any instant of time. Practically when the access point receives these two packets, it assumes the hacker is trying to gain access to the network. Therefore, it shuts-off all connections for some time to avoid the possible compromise of resources on the network. Although this is carried out to provide strength against some wireless attacks, it is used by the attacker to his advantage to bring down the WPA protected wireless LAN. To aggravate the situation, a continuous string of unauthorized data could keep the network from operating indefinitely. In this way the security feature is exploited by the attacker to close down the network. Further modifications were also done to WPA by using CCMP instead of MIC for integrity check and making AES encryption compulsory. This is known as WPA2. WPA is available in two modes, enterprise mode and consumer mode. Enterprise mode uses Remote Authentication Dial In User Service (RADIUS) for authentication while the consumer mode (or personal mode) of WPA uses a combination of pre-shared keys (PSK), TKIP and MIC.

III. Performance Metrics

Performance of a wireless LAN can be analyzed using certain performance metrics [3], [10], [11]. To investigate the details of the wireless LAN subjected to various security algorithms we choose the performance metrics that have been widely used in various other studies on different forms of adhoc networks; the packet delivery fraction [12], [13] and end to end packet delay [14].

A. Packet Delivery Fraction

The packet delivery fraction (PDF) is a measure of loss rate, which shows the maximum throughput the network can support and is an important figure of merit for any Ad-hoc network protocols. This paper measures the packet delivery fraction for a wireless LAN as the dynamic ratio of the packets received by sinks at the destinations over the packets generated from the sources.

PDF = (*data pkt rec*/*data pkt sent*) x 100

Where *data pkt rec* and *data pkt sent* are the number of data packets received and sent by the application, respectively.

ISBN: 978-988-19252-8-2
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

B. *Average End-to-End Delay of Data Packets*

This includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC, and propagation and transfer times. An expression for delay, in IEEE 802.11, has been estimated by comparing its operation to a CSMA system. For this queue at every node is approximated as an M/G/1 queue.

The HOL delay is the delay measured from the instant the packet reaches the head of the queue to the time, the sender knows, the packet is successfully received.

The HOL delay (D) is estimated by the following relation:

$$D = d_s + \sum_{i=1}^{n} d_b^i + \sum_{i=1}^{n} d_r$$

Where d_s is delay caused due to successful transmission of a packet once;

n is any number that is generated randomly;

$\sum_{i=1}^{n} d_b^i$ is the back-off delay at i[th] back-off stage; and

$\sum_{i=1}^{n} d_r$ is the delay caused by retransmissions..

IV. Simulation Parameters and Results

Simulating a wireless LAN implementing WEP and further WPA forms an important part of this research. The simulations of wireless LANs equipped with these security algorithms are done in NS2 software using AWK scripts to extract performance metrics ─ packet delivery fraction and the end-to-end delay. As a part of this work, we have simulated the wireless LANs for different nodes incorporating the two different security algorithms viz, WEP and alternatively WPA which have been discussed in section II. In the first phase of simulation, we have obtained the variation of packet delivery fraction for a standard WEP called WEP-64 for 20, 40 and 60 Nodes. Consequently in the second phase variations end-to-end delay for the same standard is found. Similar variations are obtained for WPA standard too.

A. *Comparison of Packet Delivery Fraction for Different Number of Nodes*

In this section, we have presented the Xgraphs of packet delivery fraction as a function of simulation time (seconds). Fig. 1 shows the variation of packet delivery fraction for WEP-40 and WPA when number of nodes is 20. Fig. 2 shows the packet delivery fraction variation for both the algorithms with number of nodes 40. On the same lines Fig. 3 shows the variation of packet delivery fraction in similar scenario for a 60 nodes in the wireless network. As observed from Fig. 1, Fig. 2 and Fig. 3, the packet delivery fraction is more or less saturated for WEP as well as WPA. However the packet delivery fraction stoops down for WEP as compared to WPA in each case, the difference between both is increasing as the simulation time increases.

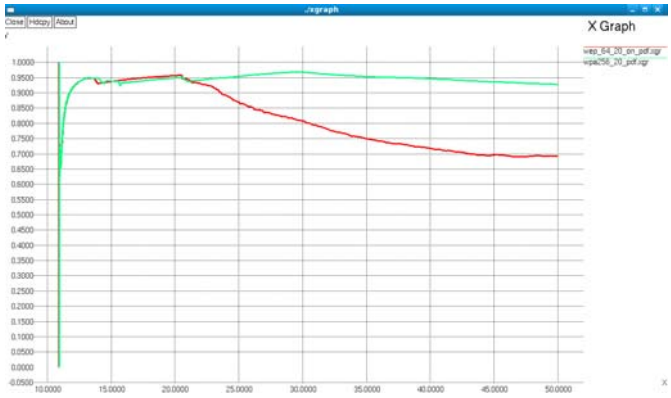

Fig. 1. Comparison of variation in PDF for WEP and WPA for wireless LAN comprising of 20 nodes

B. *Analysis of Packet Delivery Fraction as a Performance Metric*

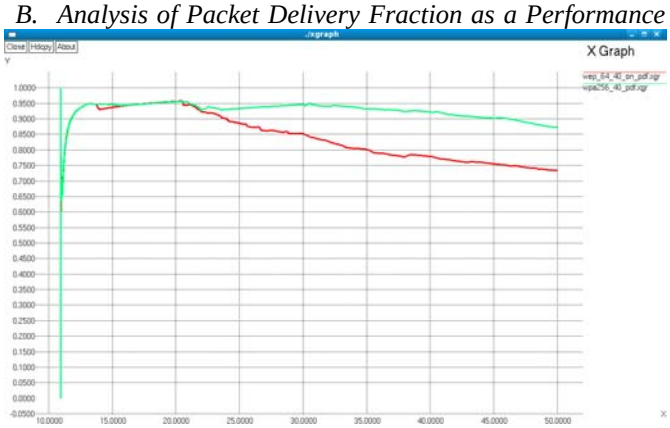

Fig. 2. Comparison of variation in PDF for WEP and WPA for wireless LAN comprising of 40 nodes

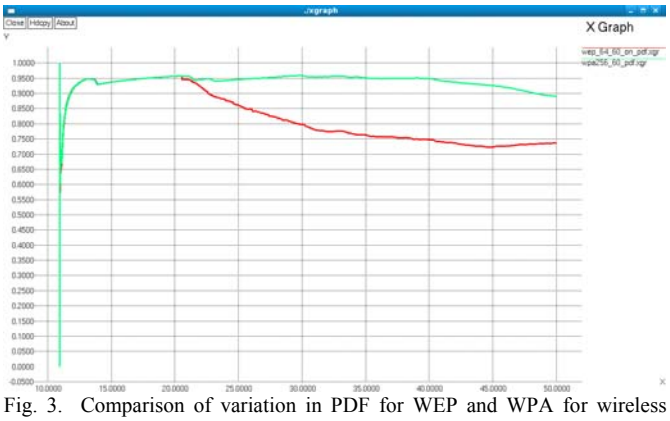

Fig. 3. Comparison of variation in PDF for WEP and WPA for wireless LAN comprising of 60 nodes

The average value of packet delivery fraction for WEP is 0.6919, as compared to 0.9276 when the simulated wireless incorporated WPA for 20 nodes. For a wireless LAN double in terms of number of nodes, the respective values are 0.7342 and 0.8731. For number of nodes increasing to 60, the average packet delivery fraction rises to 0.736 for WEP and 0.8899 for WPA. These observations are plotted in Fig. 4 below:

ISBN: 978-988-19252-8-2
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

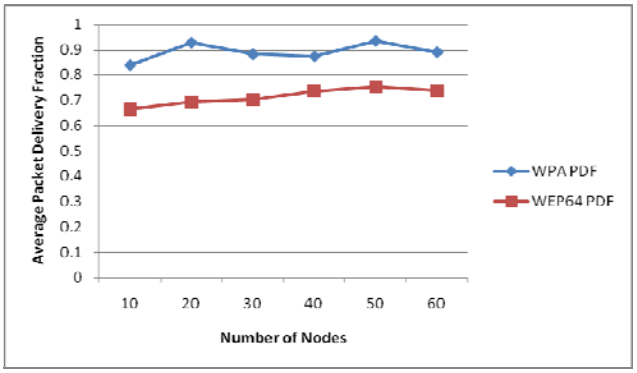

Fig. 4. Analysis chart for average packet delivery fraction for WEP and WPA for different number of nodes

C. *Comparison of End-to-End Delay for Different Number of Nodes*

In this section, we have presented the Xgraphs of end-to-end packet delay (m-sec) variations as a function of simulation time (seconds). Fig. 5 shows the variation of end-to-end packet delay for WEP as well as WPA for 20 nodes in a wireless LAN; Fig. 6 shows the same performance metric variations of WEP and WPA but for 40 nodes in a wireless LAN; while Fig. 7 depicts the variation of end-to-end packet delay in similar scenario for a 60 node wireless LAN.

Fig. 5. Comparison of variation in End to End Delay for WEP and WPA for wireless LAN comprising of 20 nodes

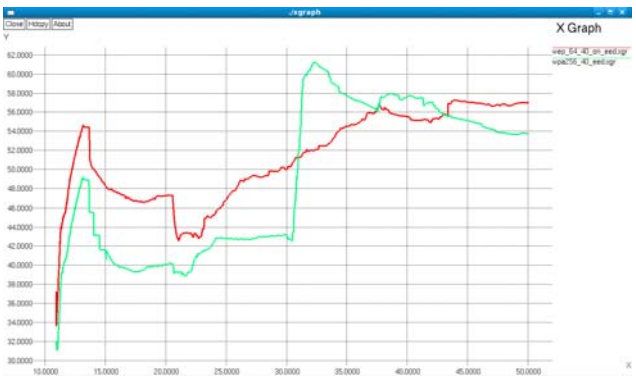

Fig. 6. Comparison of variation in End to End Delay for WEP and WPA for wireless LAN comprising of 40 nodes

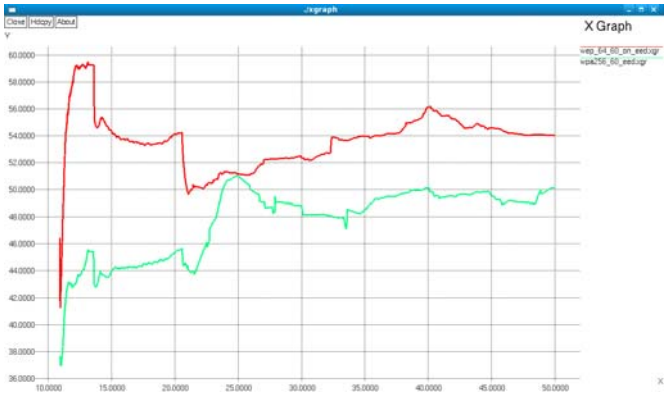

Fig. 7. Comparison of variation in End to End Delay for WEP and WPA for wireless LAN comprising of 60 nodes

End-to-end delay for both security algorithms namely WEP as well as WPA increases stutteringly as observed from Fig. 5, Fig. 6 and Fig. 7.

D. *Analysis of End-to-End Delay as a Performance Metric*

A better insight can be obtained from the average end-to-end delay over the complete simulation. The average value of end-to-end delay for WEP is 40.417386 as compared to 38.413872 when the simulated wireless incorporated WPA for 20 nodes. For a wireless LAN double in terms of number of nodes, the respective values are 57.093845 and 53.762589. For number of nodes increasing to 60, the average end-to-end delay comes out to be 54.016577 for

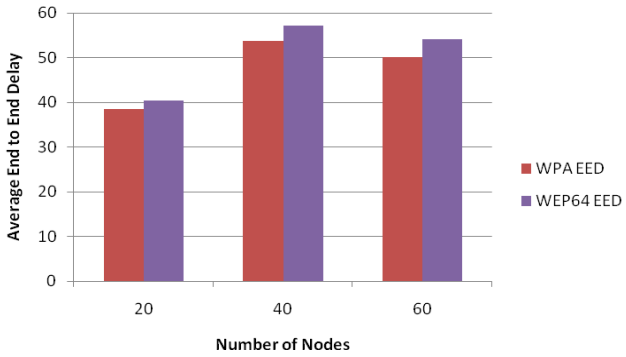

Fig. 8. Analysis chart for average End to End Delay for WEP and WPA for different number of nodes

WEP and 50.143409 for WPA. These observations are plotted in Fig. 8. As depicted from Fig. 8, the average end-to-end delay for WPA is less in all the three cases of simulated WLANs.

V. Conclusion

Analysis done for packet delivery fraction and end-to-end delay revels that WPA offers smaller end-to-end delay as compared to WEP. Moreover it produces a better packet delivery fraction also. Hence WPA wins over WEP in terms of these performance metrics. Thus from the analysis it may be concluded that performance in terms of packet delivery fraction and end-to-end delay is better for WPA, which makes it a better standard to be applied in wireless LAN.

ISBN: 978-988-19252-8-2
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

REFERENCES

[1] "The State of Wi-Fi® Security," *Wi-Fi Alliance*, January, 2012. Available: http://www.wi-fi.org/knowledge-center/white-papers.

[2] V. Bhatia, D. Gupta and H. P. Sinha, "Throughput and Vulnerability Analysis of an IEEE 802.11b Wireless LAN," *International Journal of Computer Applications*, Digital Object Identifier: 10.5120/8182-1509, Volume 52, Number 3, pp. 21-26, 2012.

[3] V. Bhatia, D. Gupta and H.P Sinha, "Implementing comparative analysis of wireless LAN security protocols in NS2," *IASET International Journal of Electronics and Communication Engineering*, to be published.

[4] Wireless LAN medium access control (MAC) and physical layer (PHY) specifications, *IEEE Standard 802.11*, 1999 Edition. Available: http://www.cs.uiuc.edu/homes/haiyun/cs598hl/papers/802.11-1999.pdf [Last accessed 01 March 2013]

[5] F. Haddadi and M. A. Sarram, "Wireless Intrusion Detection System Using a Lightweight Agent", *IEEE Second International Conference on Computer and Network Technology (ICCNT)*, Digital Object Identifier: 10.1109/ICCNT.2010.26, pp. 84-87, 2010.

[6] C. Peikari, and S. Fogie, "Cracking WEP", *Airscanner*, 2003. Sourced: 28 February 2013, http://www.airscanner.com/pubs/wep.pdf

[7] J. Williams, "The IEEE 802.11b security problem", *IEEE Journal IT Professional*, Volume: 3, Issue: 6, pp. 96, 91 – 95, 2001.

[8] Y. Liu, Z. Jin, Y. Wang, "Survey on Security Scheme and Attacking Methods of WPA/WPA2", *IEEE 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM)*, Volume: 3, Issue: 6, Digital Object Identifier: 10.1109/WICOM.2010.5601275, pp. 1- 4, 2010.

[9] V. Bhatia, D. Gupta and H.P Sinha, "Analysis of dictionary attacks on different number of nodes," *Journal of Information Systems and Communications*, ISSN0976-8742, Volume: 3, Issue: 1, pp. 167-169, 2012.

[10] I. Broustis, G. Jakllari, T. Repantis, M. Molle, "A Comprehensive Comparison of Routing Protocols for Large-Scale Wireless MANETs", *3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks*, Volume: 3, Digital Object Identifier: 10.1109/SAHCN.2006.288588, pp. 951 – 956, 2006.

[11] W. Qing-wen, S. Hao-shan, J. Yi, C. Wei, "A Cross-Layer Efficient Routing Protocol for Ad hoc Networks", *Second International Workshop on Education Technology and Computer Science*, Volume: 2, Digital Object Identifier: 10.1109/ETCS.2010.353, pp. 154 – 158, 2010.

[12] R. Khalaf, I. Rubin, "Throughput and Delay Analysis in Single Hop and Multihop", *IEEE 802.11 Networks, 3rd International Conference on Broadband Communications, Networks and Systems*, Digital Object Identifier: 10.1109/BROADNETS.2006.4374367, Page(s): 1 – 9, 2006.

[13] J. Wang, T. Mikami, K. Kanamori, E. Kodama and T. Takada, "An Effective Approach to Improving Packet Delivery Fraction of Ad Hoc Network," *IAENG Proceedings of The International MultiConference of Engineers and Computer Scientists*, vol. 1, pp. 681-686, March 2011. Available: http://iaeng.org/publication/IMECS2011.

[14] G. Epiphaniou, C. Maple, P. Sant, M. Reeve, "Affects of Queuing Mechanisms on RTP Traffic: Comparative Analysis of Jitter, End-to-End Delay and Packet Loss", *International Conference on Availability, Reliability, and Security*, Digital Object Identifier: 10.1109/ARES.2010.67, Page(s): 33 – 40, 2010.

ISBN: 978-988-19252-8-2
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)