Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 12, No.2, December : 2024

SECURITY IMPROVEMENT IN WIRELESS LANS-INFRASTRUCTURE NETWORKS

Mahendra Kumar, Associate Professor, Sant Baba Bhag Singh University,
Khiala, Jalandhar, Punjab-144030, India (E-mail: dei.mahendra@gmail.com)
A. K. Jain, Ex Professor, Instrumentation and Control Engineering Department,
Dr. B R Ambedkar National Institute of Technology Jalandhar, Punjab-144011, India

Abstract: Unlike traditional wired networks, wireless networks do not rely on any fixed infrastructure. Therefore these networks are vulnerable to security attacks. The paper analyzes the security of infrastructure networks based on the RC4 and AEC algorithm in MAC layer. The author has studied the security performance of IEEE 802.11 Wireless LANs (both ad hoc type and infrastructure type) with MAC layer and network layer securities. It was observed that with wormhole attacks, the average throughput and PDR were better with CCMP security as compared to WEP security environments with 5-20 nodes and 50-200 nodes. The average end-to-end delay and jitter were lowest with WEP security as compared to CCMP security environments with 5-20 nodes and 50-200 nodes after wormhole attack.
Keywords: Security, WLAN, WEP, CCMP.

I. INTRODUCTION

Wireless Networks is a data communication system that uses shared radio waves or infrared light to transmit and receive data without wired cables. Wireless Local Area Networks (WLANs) succeeded in providing wireless network access at acceptable data rates. Wireless LAN gives great flexibility and freedom to connect of network or Internet without being physically connected with a cable or modem. Data is transmitted or received via air, walls, ceilings, and even cement structures throughout or between buildings. A variety of wireless technologies have been standardized and commercialized, but no single technology is considered the best because of different coverage and bandwidth limitations. In particular, IEEE 802.11 wireless networking technology has dominated the wireless data-networking segment. This has happened partly due to the timely release of an easily-implemented standard, the low cost of the hardware and high data rates that support current applications (from 1 to 11 Mbps) as well as promising future extensions (possibly exceeding 100 Mbps with 802.11n)[1]. The 802.11 standard introduced the wired equivalent privacy (WEP) protocol in an attempt to bring the security of wireless networks to that of wired ones. The primary goal was to prevent eavesdropping of network traffic. WEP uses the Rivest Cipher 4 (RC4) encryption algorithm to provide confidentiality at the data link layer [2]. In addition to using WEP for privacy, many vendors utilized Access Control Lists (ACLs) based on the Medium Access Control (MAC) address to prevent unauthorized access to the network. The remaining paper is structured as follows. In section II, wireless security protocols are given. In section III, information regarding wireless security criteria is provided, Infrastructure networks seurity with MAC layer security models are discussed in section IV. In section V, information regarding security techniques used in IEEEE 802.11 and a conclusion in section VII.

II. WIRELESS SECURITY PROTOCOLS

A. Wired Equivalent Privacy (WEP)

The 802.11b standard includes a provision for encryption called WEP [9]. Depending on the manufacturer and the model of the NIC card and access point, there are two levels of WEP commonly available. One based on a 40-bit encryption key and 24-bit Initialization Vector (IV), also called 64-bit encryption and generally considered insecure, and a 104-bit key plus the 24-bit IV (so called 128 bit encryption). Figure 1 shows the encryption process in WEP. Two processes are applied to the

plaintext data. One encrypts the plaintext using the RC4 algorithm; the other process protects it against unauthorized data modification using checksum (CRC).

If C1 = P1 ⊕RC4 and C2 = P2 ⊕ RC4

Then

C1 ⊕ C2 = (P1 ⊕ RC4) ⊕ (P2 ⊕ RC4)

= P1 ⊕ P2

Knowledge of this XOR can enable statistical attacks to recover the plaintexts. The statistical attacks become increasingly practical as more cipher texts, that use the same key stream, are known. Once one of the plaintexts becomes known, it is trivial to recover all the others.

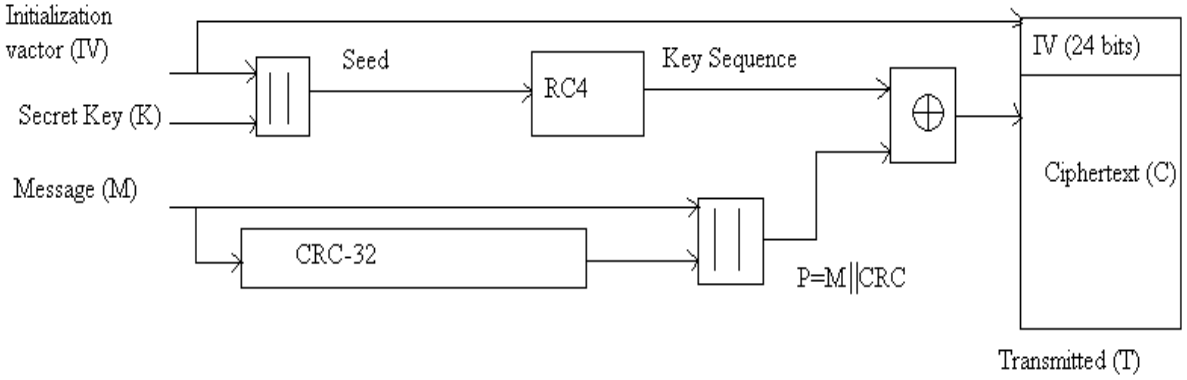

Figure 1: WEP encryption

WEP has defense against this attack. To ensure that a package has not been modified during transition, it used a Cyclic Redundancy Check (CRC) field in the package. The integrity check field is implemented as a CRC-32 checksum, which is part of the encrypted payload of the package. This is because the key sequence is used to protect the integrity check value as well as the data. The receiver has a copy of the same key, and uses it to generate an identical key stream; XORing the key stream with the cipher text yields the original plaintext and the ICV = CRC-32. The decryption is verified by performing the integrity check algorithm, CRC-32, on the recovered plaintext and comparing the output ICV' to the Integrity Check Value (ICV) transmitted with the message as given in Figure 2. If ICV' is not equal to ICV, the received message is tampered, and an error indication is sent to the sending station.

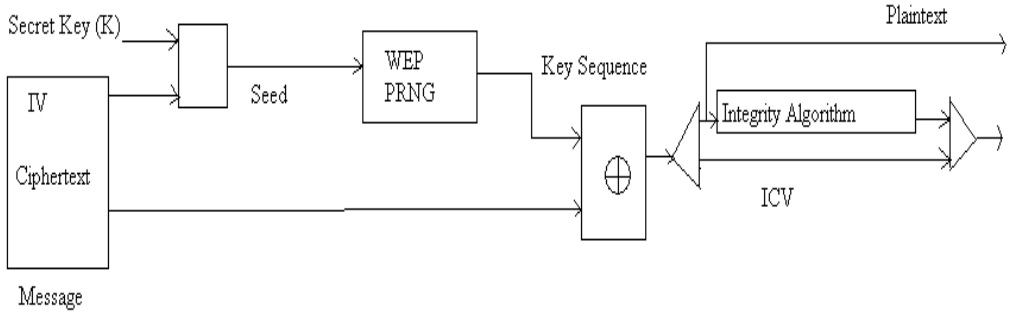

Figure 2: WEP decryption

B. Vulnerabilities in WEP

There has been some interesting work to develop attacks exploiting the vulnerabilities in WEP. It can determine the WEP key in seconds after listening to 100MB-1GB of traffic. And since the current implementation of WEP is based on static keys, eventually it is possible to ferret out the data needed to crack the key. Even though WEP has been shown to be basically insecure with its current implementation of static keys, the real problem is that the majority of access points are being deployed

without WEP even being enabled. That's the equivalent to giving full access to your house to any stranger by keeping your doors open. WEP is vulnerable because of relatively short IVs and keys that remain static. The issues with WEP don't really have much to do with the RC4 encryption algorithm. IEEE 802.11 doesn't provide any functions that support the exchange of keys among stations.

C. IEEE 802.11i

The new security standard, IEEE 802.11i, which was sanctioned in June 2004, fixes all WEP weaknesses. It is divided into three main categories:

1. Temporary Key Integrity Protocol (TKIP) is the data encryption algorithm and provides a short term solution that fixes all WEP weaknesses. TKIP can be used with old 802.11 equipment.
2. Counter Mode with CBC-MAC Protocol (CCMP) [18] is a new protocol that uses AES [9] as its cryptographic algorithm. Since this is more CPU intensive than RC4, new 802.11 hardware may be required. CCMP provides integrity and confidentiality.
3. IEEE 802.1X Port-Based Network Access Control: Either when using TKIP or CCMP, IEEE 802.1X is used for authentication.

D. Wi-Fi Protected Access (WPA)

WPA implements the majority of the IEEE 802.11i standard, and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared. WPA is designed to work with all wireless network interface cards, but not necessarily with first generation wireless access points. WPA is designed for use with an 802.1X authentication server, which distributes different keys to each user; however, it can also be used in a less secure Pre-Shared Key (PSK) mode, where every user is given the same passphrase. One major improvement in WPA over WEP is the Temporal Key Integrity Protocol (TKIP), which dynamically changes keys as the system is used. When combined with the much larger IV, this defeats the well-known key recovery attacks on WEP. In addition to authentication and encryption, WPA also provides vastly improved payload integrity. The Cyclic Redundancy Check (CRC) used in WEP is inherently insecure; it is possible to alter the payload and update the message CRC without knowing the WEP key.

III. SECURITY CRITERIA

In this section, the paper briefly introduces the security criteria used for wireless LAN network.

A. Availability

Availability ensures the survivability of network services despite attacks. Availability does not come to mind as a security concern as quickly as do confidentiality and integrity. But the assurance of availability is very much a security issue. Long-term Denial of Service (DoS) attacks can severely hinder a network's ability to continue. In fact, DoS is often a successful tactic of network services warfare. Moreover, the processes required to prevent or mitigate the effects of loss of availability are very much within the realm of security methodology, because the basic concept of availability assures that authorized persons have uninterrupted access to the information in the system at hand.

B. Integrity

The concept of integrity ensures that the contents of data or correspondences are preserved intact through the transfer from sender to receiver. Integrity embodies the guarantee that a message sent is the message received, that is, it was not altered either intentionally or unintentionally during transmission. Attack on Integrity is usually done in two ways: by the intentional alteration of the data for vandalism or revenge or by the unintentional alteration of the data caused by operator input, computer system, or faulty application errors. The usual mechanism, to ensure integrity of data, is using hash functions and message digestion [10].

C. Confidentiality

Confidentiality means that certain information is only accessible to those who have been authorized to access it. In other words, in order to maintain the confidentiality of some confidential information, we need to keep them secret from all entities that do not have the privilege to access them.

D. Authenticity

Authenticity is essentially assurance that participants in communication are genuine and not impersonators [11]. It is necessary for the communication participants to prove their identities as what they have claimed using some techniques so as to ensure the authenticity. If there is not such an authentication mechanism, the adversary could impersonate a benign node and thus get access to confidential resources, or even propagate some fake messages to disturb the normal network operations.

E. Nonrepudiation

Nonrepudiation ensures that the sender and the receiver of a message cannot disavow that they have ever sent or received such a message. This is useful especially when we need to discriminate if a node with some abnormal behavior is compromised or not: if a node recognizes that the message it has received is erroneous, it can then use the incorrect message as evidence to notify other nodes that the node sending out the improper message should have been compromised.

F. Authorization

Authorization is a process in which an entity is issued a credential, which specifies the privileges and permissions it has and cannot be falsified, by the certificate authority. Authorization is generally used to assign different access rights to different level of users. For instance, the network management function is only accessible by the network administrator. Therefore there should be an authorization process before the network administrator accesses the network management functions.

G. Anonymity

Anonymity means that all the information that can be used to identify the owner or the current user of the node should default be kept private and not be distributed by the node itself or the system software. This criterion is closely related to privacy preserving, in which we should try to protect the privacy of the nodes from arbitrary disclosure to any other entities.

IV. Infrastructure networks seurity with MAC layer security models

This Simulation environment have designed to examine the security parameters of infrastructure less networks with different security models as MAC layer model, Network layer model etc. The setup parameters for Wireless LANs are mention in Table 1.

Table 1: Simulation set up

Scenario Parameters	**Description**
Network type	Wireless LANs
Radio Propagation model	Two ray
Area of network	100m×100m
Number of network node	5, 10, 15, and 20
Data rate	2 Mbps
Simulation time	1800 s
Routing protocol	ANODR, DYMO, LANMAR, FSR and OLSR
MAC layer Model for security	WEP and CCMP
Noise factor	10 dB
Item size	512 bytes
Traffic application	CBR
Application	FTP

A. Performance evolution of Infrastructure networks with CCMP MAC layer security model

Throughput is the measure of the number of packets successfully transmitted to their final destination per unit time. It has observed that CCMP MAC layer security improve the total throughput of infrastructure networks by using OLSR routing protocol with respect to other routing protocols with increased number of network nodes as given in Figure 3. Similarly, we observed that the total throughput in infrastructure networks has decreased by using DYMO, ANODR, FSR, and LANMAR

routing protocols with increasing number of nodes as given Figure 3. Finally, it has observed that CCMP MAC layer security has provided the total throughput of infrastructure networks is highest at five network nodes but lowest at increased twenty network nodes for DYMO, ANODR, FSR, and LANMAR routing protocols.

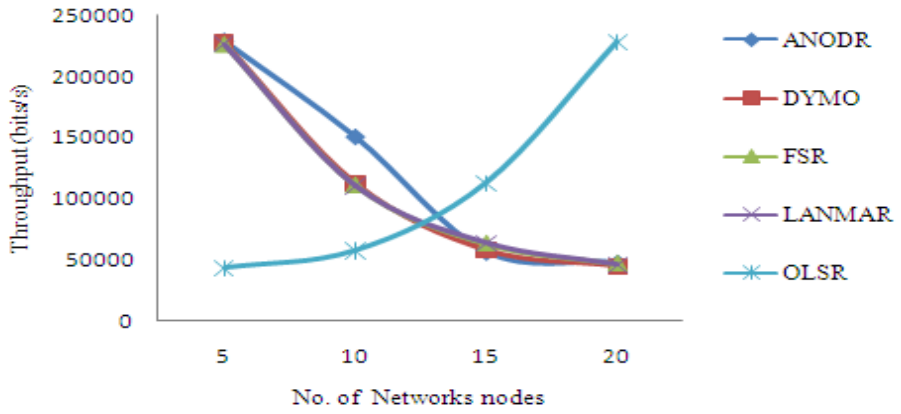

Figure 3: Variation in throughput in infrastructure network with CCMP MAC layer security

Average Jitter is the variation (difference) of the inter-arrival times between the two successive packets received. Figure 4, presents the security performance of infrastructure network with CCMP MAC layer security with various routing protocols, in terms of average jitter through FTP application, when the numbers of network nodes are increased, then average jitter has increased.

However, it has observed that average jitter of Wireless Ad Hoc network with CCMP security has decreased with OLSR routing protocols with increased number of network nodes. In addition, average jitter of infrastructure network has increased with ANODR, DYMO, FSR, and LAMAR routing protocol. At five nodes, it has observed that average jitter is high with OLSR routing protocols. However, at 20- nodes, average jitter variation is low with OLSR routing protocols in infrastructure network but average jitter high with ANODR, DYMO, FSR, and LANMAR routing protocols. The performance of infrastructure network has improved better by using OLSR routing protocol.

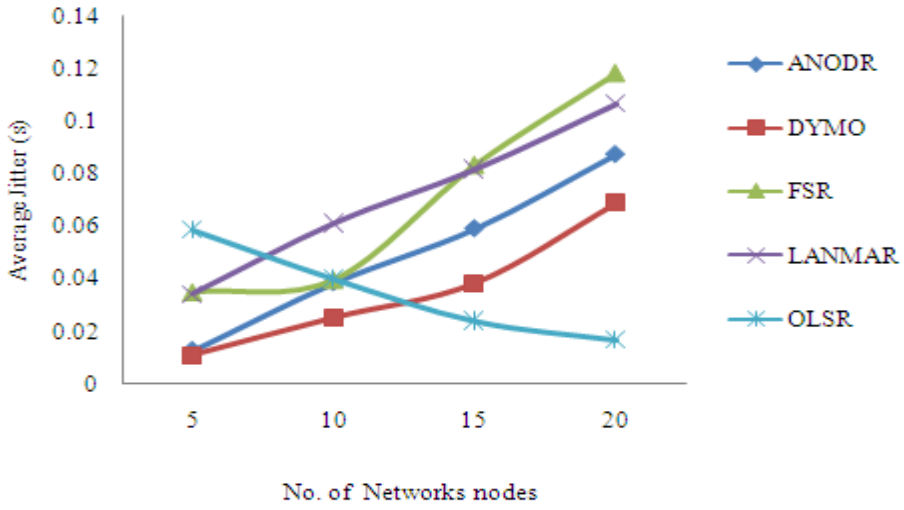

Figure 4: Variation in average jitter in infrastructure network with CCMP MAC layer security

Average end-to-end delay is the variation (difference) of the inter-arrival times between the two successive packets received. Figure 5, presents the security performance of infrastructure network with CCMP MAC layer security with various routing protocols, in terms of average end-to-end delay through FTP application, when the numbers of network nodes are increased, then average end-to-end delay has increased. However, it has observed that average end-to-end delay of infrastructure network

with CCMP security has decreased with OLSR routing protocols with increased number of network nodes. In addition, average end-to-end delay of infrastructure network has increased with ANODR, DYMO, FSR, and LAMAR routing protocol. At five nodes, it has observed that average end-to-end delay is high with OLSR routing protocols. However, at 20- nodes, average end-to-end delay variation is low with OLSR routing protocols in infrastructure network but average end-to-end delay high with ANODR, DYMO, FSR, and LANMAR routing protocols. The performance of infrastructure network has improved better by using OLSR routing protocol.

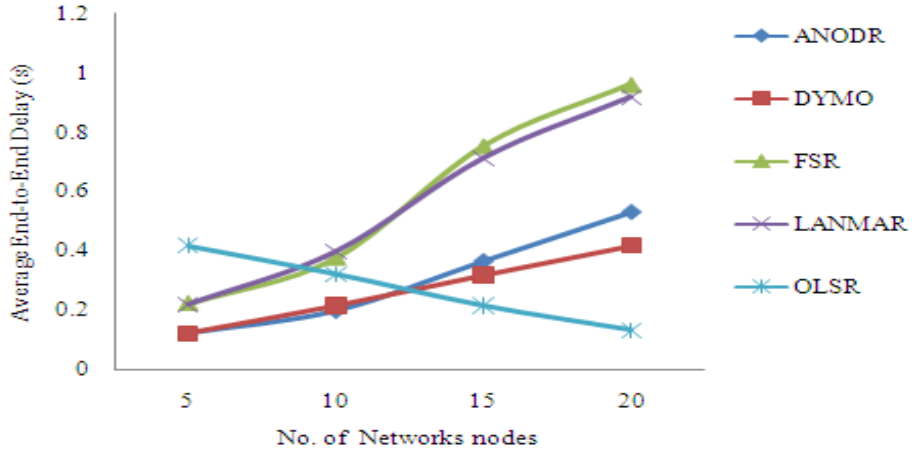

Figure 5: Variation in average end-to-end delay in infrastructure network with CCMP MAC layer security

B. Performance evolution of Infrastructure networks with WEP MAC layer security model

It has observed that WEP MAC layer security improve the total throughput of infrastructure networks by using ANODR routing protocol with respect to other routing protocols with increased number of network nodes as given in Figure 6.

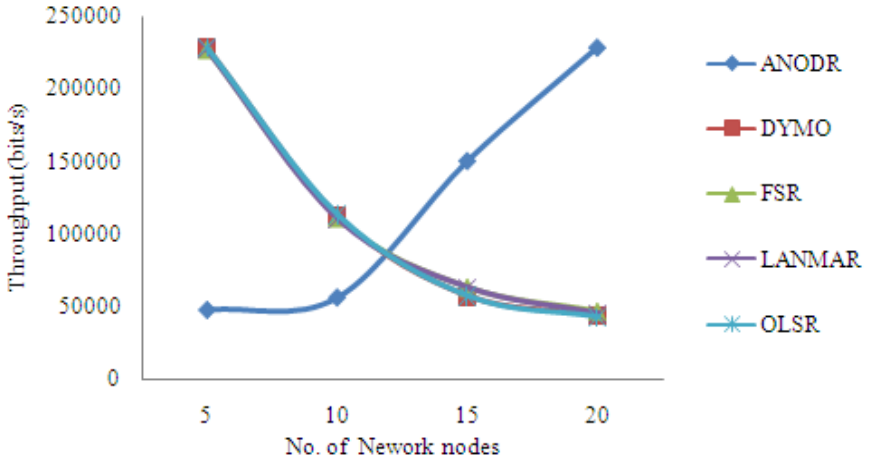

Figure 6: Variation in average throughput in infrastructure network with WEP MAC layer security

Similarly, we observed that the total throughput in infrastructure networks has decreased by using DYMO, FSR, LANMAR, and OLSR routing protocols with increasing number of nodes as given Figure 6. Finally, it has observed that WEP MAC layer security has provided the total throughput of infrastructure networks is highest at five network nodes through DYMO, FSR, LANMAR, and OLSR routing protocols but lowest with ANODR. Similarly, at 20-network nodes, total throughput is highest with ANODR routing protocol.It has observed that WEP MAC layer security improve the average jitter of infrastructure networks by using ANODR routing protocol with respect to other routing protocols with increased number of network nodes as given in Figure 6. Similarly, we observed that the average jitter in infrastructure networks has increased by using DYMO, FSR, LANMAR, and

OLSR routing protocols with increasing number of nodes as given Fig. 6. Finally, we observed that WEP MAC layer security has provided the average jitter of infrastructure networks is lowest at five network nodes through DYMO, FSR, LANMAR, and OLSR routing protocols but highest with ANODR. Similarly, at 20-network nodes, average jitter is lowest with ANODR routing protocol.
Average jitter has defined as a measure of average time taken to transmit each packet of data from source node to destination node. It has observed that WEP MAC layer security improve the average end-to-end delay of infrastructure networks by using ANODR routing protocol with respect to other routing protocols with increased number of network nodes as given in Figure 7. Similarly, we observed that the average jitter in infrastructure networks has increased by using DYMO, FSR, LANMAR, and OLSR routing protocols with increasing number of nodes as given Fig. 8.

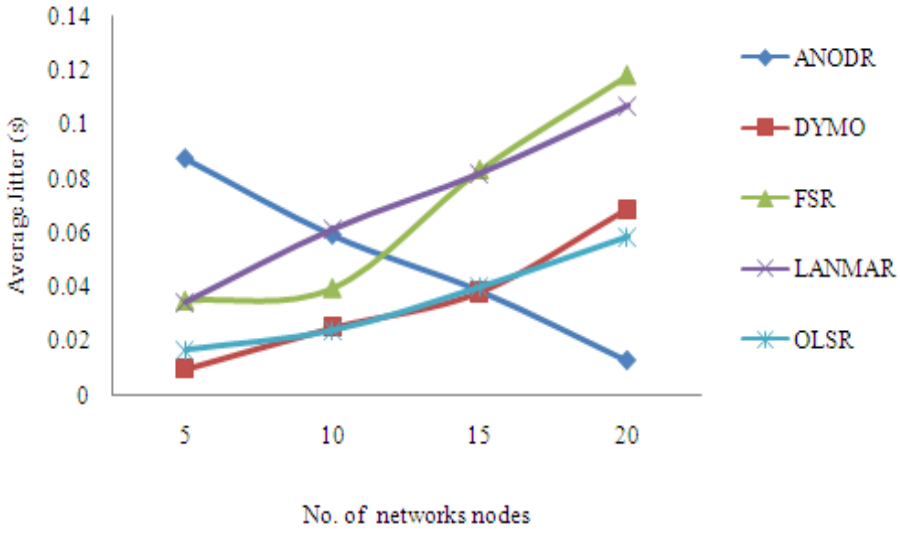

Figure 7: Variation in average jitter in infrastructure network with WEP MAC layer security
Finally in figure 8, it has observed that WEP MAC layer security has provided the average end-to-end delay of infrastructure networks is lowest at five network nodes through DYMO, FSR, LANMAR, and OLSR routing protocols but highest with ANODR. Similarly, at 20-network nodes, average end-to-end delay is lowest with ANODR routing protocol.

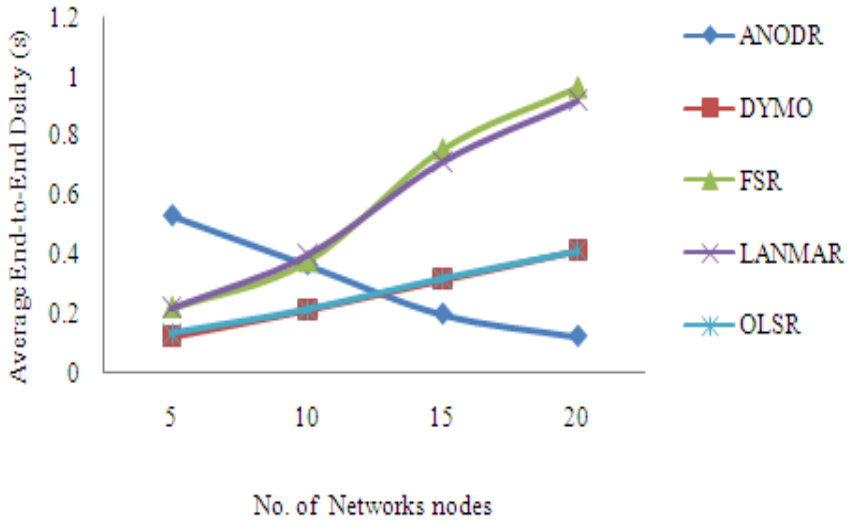

Figure 8: Variation in average end-to-end delay in infrastructure network with WEP MAC layer security

V. CONCLUSION

In this paper authors, study and compare the performance matrices as throughput, average jitter, average end-to-end delay, packet encryption of Wireless Ad Hoc through using MAC layer security. It has observed that CCMP MAC layer security has provided the total throughput of infrastructure networks is highest at five network nodes but lowest at increased twenty network nodes for DYMO, ANODR, FSR, and LANMAR routing protocols. The average jitter of infrastructure network has improved better by using OLSR routing protocol through CCMP MAC layer security. it has observed that average end-to-end delay of infrastructure network with CCMP security has decreased with OLSR routing protocols with increased number of network nodes. In addition, average end-to-end delay of infrastructure network has increased with ANODR, DYMO, FSR, and LAMAR routing protocol. It has observed that WEP MAC layer security has provided the average jitter of infrastructure networks is lowest at five network nodes through DYMO, FSR, LANMAR, and OLSR routing protocols but highest with ANODR. Similarly, at 20-network nodes, average jitter is lowest with ANODR routing protocol. It has observed that WEP MAC layer security has provided the total throughput of infrastructure networks is highest at five network nodes through DYMO, FSR, LANMAR, and OLSR routing protocols but lowest with ANODR. Similarly, at 20-network nodes, total throughput is highest with ANODR routing protocol. it has observed that WEP MAC layer security has provided the average end-to-end delay of infrastructure networks is lowest at five network nodes through DYMO, FSR, LANMAR, and OLSR routing protocols but highest with ANODR. Similarly, at 20-network nodes, average end-to-end delay is lowest with ANODR routing protocol. WEP is only one of many security measures. Although WEP plays an important role in data encryption, the whole network security shouldn't only depend on it. However, in WLAN's application, security is an important aspect that must be considered.

V. REFERENCES

[1] Shin, M.; Ma, J.; Mishra, A.; Arbaugh, W.A., "Wireless network security and interworking", Proceedings of IEEE, Volume 94, Issue 2, pp 455 – 466, February 2006.

[2] Jyh-cheng Chen, Ming-chia Jiang, and Yi-Wen Liu, "Wireless LAN Security and IEEE802.11i", IEEE Wireless Communications, February 2005.

[3] Dell Corporation. "802.11 Wireless Security in Business Networks" September 2001.

[4] N. B. Salem and J-P Hubaux, "Securing Wireless Mesh Networks", in IEEE Wireless Communication, Volume 13, Issue 2, April 2006 pp. 50 - 55.

[5] Arunesh Mishra, Nick L. Petroni, William A. Arbaugh and Timothy Fraser, "Security issues in IEEE 802.11 wireless local area networks: a survey", Wirel. Commun. Mob. Comput., Vol. 4, 2004, pp 821–833.

[6] Yixin Jiang, Chuang Lin, Hao Yin and Zhen Chen, "A mutual authentication and privacy mechanism for WLAN security," WCMC, Vol. 8, 2008, pp101–112

[7] A. Stubble_eld, J. Ioannidis, and A. D. Rubin, "A key Recovery Attack on the 802.11b Wired Equivalent Privacy Protocol (WEP)" ACM Transactions on Information System Security, Vol 7(2), 2004, pp 319-332

[8] Kashif Laeeq, "Security Challenges & Preventions in Wireless Communications", International Journal of Scientific & Engineering Research Volume 2, Issue 5, May-2011

[9] Xinyu Xing; Shakshuki, E.; Benoit, D.; Sheltami, T: "Security Analysis and Authentication Improvement for IEEE 802.11i Specification" IEEE lobal Telecommunications Conference, 2008. IEEE GLOBECOM 2008. pp. 1-5

[10] Binod Vaidya, Sang Duck Lee, Jongan Park: "Evaluation of Secure Multimedia Services over Wireless Access Network", Ubiquitous Multimedia Computing, 2008. UMC '08. International Symposium, May 2008 pp. 181-184

[11] Hassen Redwan and Ki-Hyung Kim: "Survey of Security requirements, Attacks and Network Integration in Wireless Mesh Networks" Frontier of Computer Science and Technology, FCST '08. Japan-China Joint Workshop, 2008 pp. 3-9
[12] Tahir Naeem, Kok-Keong Loo, "Common Security Issues and Challenges in Wireless Sensor Networks and IEEE 802.11 Wireless Mesh Networks," International Journal of Digital Content Technology and its Applications Volume 3, Number 1, March 2009
[13] S. Khan, K-k. Loo, T. Naeem, M.A. Khan, "Denial of service attacks and challenges in broadband wireless network," International Journal of Computer Science and Network Security, Vol. 8, No. 7, pp1-6, July 2008
[14] M. S. Siddiqui, C. S. Hong, "security issues in wireless mesh networks" IEEE International Conference on Multimedia and Ubiquitous Engineering(MUE'07) 2007.
[15] Y. Hu, A. Perrig and D. Johnson, "Wormhole Attacks in Wireless Networks", IEEE Journal on Selected Areas in Communications, Vol. 24, No. 2, February 2006.
[16] U. Baroudi, M.A. Mohiuddin, "Performance analysis of Internet Applications over an adaptive IEEE 802.11 MAC architecture," Journal of the Franklin Institute, Vol.34, 2006, pp 352-360
[17] H. R. Hassan, Y. Challal. "Enhanced WEP: An efficient solution to WEP threats", Proc. WOCN'05, 2005, pp 594-599

Mahendra Kumar was born in Agra, Uttar Pradesh, India on June 6th, 1981. He received B.Tech. Degree in Electronics and Instrumentation Engineering from UPTU, Lucknow in 2005 and M.Tech. Degree in Engineering System from Dayalbagh Education Institute, Dayalbagh, Agra, Utter Pradesh, India in 2007 and received his Ph.D. degree on Wireless Networks from the Dr. B. R. Ambedkar National Institute of Technology, Jalandhar, India in 2016. He has published over thirty-five research papers in national and international journals/conferences. He is presently working as Associate Professor in Deptt. of Electrical Engg., Sant Baba Bhag Singh University, Jalandhar. He has supervised 11 Ph.D. Research Scholars and 07 M.Tech. Students in the area of Wireless Networks. Before joining SBBSU, Jalandhar, He has served as Assistant Professor and Assoc. Prof. at GKU, Bathinda since Aug 2015 to Jun 2023. He has served at IIT Delhi from 2007 to 2009 as JRF. He was lecturer at Deptt. Of Instrumentation and Control Engineering, Dr. B. R. Ambedkar National Institute of Technology, Jalandhar, Punjab, India from July 2009–Dec 2009. His research interests include Quality of Service in wireless networks, medium access protocols for mobile computing, and mesh networks.

A. K. Jain received his B.E and M.E both from IIT, Roorkee, (erstwhile University of Roorkee, Roorkee) India in 1981 and 1987 respectively and received his Ph.D. degree on Quality of Service in High Speed Networks from the Dr. B. R. Ambedkar National Institute of Technology, Jalandhar, India in 2009.He has published over sixty research papers in national and international journals/conferences. He is presently working as Professor and Head in the Department of Instrumentation and Control Engineering, Dr. B. R. Ambedkar National Institute of Technology, Jalandhar, India. He is guiding Ph.D (Four Awarded and two submitted) and M.Tech students in the area of Wireless Networks. Before joining N.I.T, Jalandhar, he has served at TIET Patiala, IET Lucknow, and NIT Hamirpur (Erstwhile REC Hamirpur) in various capacities. His research interests include quality of service in wireless networks, medium access protocols for mobile computing, and mesh networks. Dr. Jain is life member of ISTE India.