CHAPTER 2

LITERATURE STUDY

Wireless LAN technology is among the latest technologies, which no doubt, is shaping the beginning of a new millennium and changing the way information communication is going to happen in the future. Attacks on wireless LAN network and the security issues in these networks have come up in recent years. It is not very primordial, when security algorithms were formed by the IEEE 802.11 working task group in year 1990. Since the problem of security in wireless LAN has surfaced only recently, research in this area is still in its nascence. However, security models and algorithms are under constant development and a lot of work is yet to be carried out like modelling security algorithms, study of various performance metrics for wireless LAN under various constraints with optimal security while pace of data transfer has further to be continuously enhanced.

In this chapter, certain security algorithms, their models and metrics which have been employed for their analysis are discussed. The discussion in this chapter concludes with identification of gaps in the research so far with regard to modelling and simulation of security algorithms; and analyzing them in terms of vulnerability and other performance metrics.
2.1 SECURITY ALGORITHM MODELS

While studying the literature on Wi-Fi communication and its security issues, it was observed that many researches are actively involved in the area of designing wireless security algorithms ranging from description of weakness [64-74] of various security algorithms to even suggesting modifications in them to a certain extent [75-80]. Some emphasis has been laid down on the comparison of security levels of these security algorithms using various types of test beds and practical networks via some of popular wireless devices [67, 81-87].

While going through the literature, especially related to the field of our research topic, it has been observed that structure of Wired Equivalent Privacy (WEP) in sender and receiver side has been covered [64-65, 70] where Lashkari A.H et al have discussed about different versions of it, in addition to some of inherent problems of WEP.

An overview of WEP, its encryption and its decryption process has also been studied through various other research papers [66, 72-73, 76, 88-93]. During the study of these processes several serious security flaws in wireless protocols, stemming from misapplication of cryptographic primitives have evolved. Each of the flaws, its underlying security principle violations, and implemented relative attacks have shown the weakness of WLAN protocols. Besides security flaws in models, an attack test of WEP and an attack algorithm named Predictive Judgment have also been studied [94].

Since weakness of WEP became well-known and various attacks against it were published, enhancements and modifications in WEP were required to be studied. Hence certain modifications in WEP such as e-WEP, d-WEP and d-WPA-PSK have also been studied, which aim to make the existing WEP more secure [77, 95-96]. eWEP aims to resolve WEP flaws without changing the hardware while maintaining interoperability with
original WEP. The d-WEP adopts the frequency of Address Resolution Protocol (ARP) requests to AP as a measure to judge whether an Access Point is attacked and prevents the suspected client to access by dropping any ARP requests from it. On the other hand, the d-WPA-PSK uses a mechanism such that the PSK is regularly replaced to prevent dictionary attacks.

After WEP, the second generation of wireless security protocol usually named as Wi-Fi Protected Access (WPA), has evolved which has been further been studied as well as a small comparison of its structure with the structure of WEP is learnt [64-65, 73, 97]. WPA encapsulation and problems associated with it that happened in the PSK part of its algorithm have also been studied [72]. Agarwal A.K et al have compared the strength of various security protocols and the overheads involved in implementing them [98]. Bohn. S et al. have outlined a general Wi-Fi certification process, categorized necessary test requirements and also discussed development of various security algorithms which have been implemented using Perl language [99]. From some of the papers studied the advantages of WLAN, the major problems, existing security measures, mobility of node, instability of signal and other security aspects have come to picture [67-68, 74].

Even WPA has some flaws which may be exploited. Therefore certain modifications in WPA such as CDM have also been covered during the study [100-101], which attempts to fix a flaw in the disassociation mechanism of the WPA protocol. This helps in restricting the attack that occurs as a result of vulnerability and allows an attacker to shutdown an entire network even for those users that are authorized to use its resources. Algorithms chosen for the CDM scheme are as follows:-

a) SHA-1 DSA: Digital Signature algorithm with SHA family hash function.

b) MD5-RSA: RSA algorithm with MD5 hash function.

c) SHA-1-RSA: RSA with SHA-1 hash function.
MD5-RSA has been found to be the most suitable algorithms for CDM scheme.

*Guelzim, T et al.* have presented yet another scheme to correct the disassociation packet attack flaw, which hackers use to de-authenticate all users in a network [101]. According to them, this scheme relies on the digital signature method. This latter allows the access point to assign management frames with its private key. Mobile users can then verify the signature and accept the packets if the key is valid. Three algorithms which have been compared and studied are: Digital Signature algorithm (DSA), Message-Digest (MD5-RSA) and Secure Hash Algorithm (SHA-1 RSA). After evaluation, it has been observed that DSA is not a very good candidate for this scheme because it introduces a very high latency as well as low throughput. The RSA and MD5 schemes, however, have produced close results and have allowed making this scheme applicable without affecting the latency or the throughput. The scalability of the system in terms of latency, throughput and encryption time by varying the number of wireless nodes from 10 to 100 have further been analyzed. According to them DSA performed worst in all three experiments. Performance of MD5 is as close as SHA1 in terms of latency, but the former scaled better in terms of throughput. On an average, MD5 also produced better results in the encryption time followed by SHA1 and DSA. After studying all the above experiments, it has been observed that MD5-RSA is the most suitable algorithms for scheme like Counter Disassociation Mechanism (CDM). CasperFDR tool and SPL language have also been studied to notice that it can be used to verify the WPA protocol [102]. Security overhead which is defined as “Extra amount of work done with a security scheme enabled, over the work done to push the same data without any security” has been employed to present a performance study of security overheads in 802.11g networks [103].
Both WEP and WPA are popular as security algorithms in wireless networks, which are extensively employed at different places as hotels, cafes and higher educational institutes. Since wireless networks have made their mark in higher educational institutes worldwide, studies of some surveys have also been done [87, 104]. Through the study of literature it has been observed that the current and most widely used wireless standards in tertiary institutions are 802.11b and 802.11g. This has been accounted for because 802.11g can achieve a theoretical data rate of 54 Mbps and is not easily obstructed, since it operates on 2.4 GHz. Moreover it is compatible with the most popular standard, 802.11b. Due to this compatibility it allows a wide range of users with 802.11b equipment to easily connect to 802.11g networks.

Another way of comparing WEP and WPA has been based on operating systems. During my study of literature, the impact of different wireless securities on the network performance for both TCP and UDP have been investigated for different operating systems like Windows XP client, Windows 2000 Server, Windows XP and Windows Vista [81-85, 103, 105, 106]. Ezedin. B et al. have analyzed the effect of encryption techniques like WEP-40 and WEP-104 on throughput in IEEE 802.11g for both TCP and UDP protocols using LanTraffic as network monitoring tool. Narayan. S et al. have evaluated the performance of wireless IEEE802.11n on two operating systems, namely Windows Vista and Windows Server 2008. However Narayan. S et al. in another research have evaluated performance of wireless IEEE802.11n on four operating systems, namely Windows XP, Vista, Server 2008 and Ubuntu [106].

Another technology which has been studied is the peer-to-peer communication, which basically deals with transfer of data wirelessly but through an access point. Peer-to-peer via access point provides better features than traditional peer-to-peer connections (adhoc connections). These
include:  
a) Larger coverage range compared to ad-hoc network which has coverage limitation  
b) Peer-to-peer via access point supports better and consistent security mechanism as the security is controlled via an access point  
c) Peer-to-peer via access point can support more users than traditional ad-hoc connections.

Experiments performed on a wireless test-bed to obtain data, to investigate the effect of different encryption techniques, to investigate the performance and security issues of IEEE 802.11, so as to provide an overview of intrusion, information assurance, and confidentiality risks of utilizing 802.11 wireless network technology have also been studied in this literature study [85,107-109].

Wireless introduces a new aspect in the field of networking that is ‘information assurance’ which is necessary to control administrative traffic of a wireless protocol. Without information assurance of the administrative traffic, adversaries can disrupt, eavesdrop, and replay administrative communications. This potential vulnerability can be used to launch selective Denial of Service (DOS) attacks [110].

Intrusion Detection System (IDS) that works in concurrence with security algorithms forms the next part of literature study. A typical Intrusion Detection System (IDS) scans network traffic and generates an alert when an intrusion has been detected. Some IDS models such as Lightweight Intrusion Management System (LIMS) have been studied for commodity Wi-Fi Networks [111-112]. LIMS includes three major components: a packet collector, an intrusion preemption engine, and an intrusion detection engine. It works in conjunction with current security protocols like WEP and WPA, and does not require any specialized wireless equipment.
Since improvements in technology is a never ending process a third generation of wireless security protocol commonly known as WPA2 or IEEE 802.11i has also evolved, which has been studied through research papers. A theoretical comparison among various wireless security protocols and impact of WPA2 security-bandwidth trade-off for IPv4 and IPv6 has been covered [66, 113-115]. It has been found that for both IPv4 and IPv6 implementing security can adversely impact the bandwidth in IEEE 802.11 environments.

2.2 PERFORMANCE METRICS MODELS

To study and analyze performance of wireless LANs some metrics are required. Several performance metrics have been studied, some of which deal specifically with wireless LAN networks [86,116-123] and others with another types of wireless networks [124-132]. In ad hoc networks, performance objectives are often in contention with each other. Indeed, due to the transmission errors incurred over wireless channels, it is difficult to achieve a high rate of transmission in conjunction with reliable delivery of data and low latency. In order to obtain favourable throughput and delay performances, the system may choose to compromise on its reliability and have nodes forcibly dropping a small fraction of packets [133]. Therefore for such networks number of performance metrics need to be employed to analyze the performance. Several performance metrics have been studied and three of them, viz. throughput, PDF and end-to-end delay have been chosen in this piece of research work to analyze wireless LANs enabled with different security algorithms:-

2.2.1. Throughput

Various research papers studied are focused on modelling the throughput and evaluation of performance of the network in its terms [86,133-137], which is defined as the average rate of successful data packets delivered over a communication channel and is usually measured in bits per
second. The effective throughput of a random network can be modelled as a random variable and its expected value may be computed using Monte-Carlo methods [137].

Throughput as a performance metric has been found to be employable for Mobile Ad Hoc Network (MANET), comparison of Link State, AODV and DSR protocols, characterization of tradeoffs and measurement of public wireless LAN (PWLAN) traffic statistics [133-135]. Throughput has been employed as a performance metric not only in wireless LANs but other forms of wireless networks also [112].

Throughput is defined as the average number of packets successfully delivered (to the destination) in unit time, along a typical flow in the network.

Analytical model to provide estimates for throughput in single hop and multihop IEEE 802.11 networks have been studied in literature [138-139]. The models focus on delivering accurate estimates for MAC-layer throughput for both single hop and multihop networks under all loading conditions using a regenerative approach to calculate the throughput.

Average user throughput has been used as a performance metric and is defined as the total number of bits successfully transmitted for each user divided by the total service time [140]. The service time includes both queuing and transmission delays, i.e., it is the time between message arrival and when the last bit of the message is successfully received. Two algorithms namely network-assisted least-interference-based dynamic packet assignment (NA-LI-DPA) and network-assisted dynamic packet assignment for optimizing the throughput have been studied.

During the study of literature, related to throughput, it is observed that it is used as a measure to improve network congestion control mechanism by finding means to increase it, video transmission over third generation (3G)
wireless network, impact of interference, Distributed Coordination Function (DCF) of 802.11 networks and analysis on various routing protocols viz., AODV, DSR, and DSDV, employed in wireless networks [112,141-145].

There are some other performance metrics also which have a good correlation to the throughput. One of them is the number of conflicting pairs, which has been used in the client-assisted minimum conflict pairs scheme [142]. The asymptotic throughput capacity of large mobile wireless ad hoc networks has also been analyzed [146].

Throughput analysis of an Enhanced Distributed Channel Access (EDCA) WLAN using a control theoretic approach has also been studied, which adapts the Contention Window (CW) to the conditions of the WLAN, based on an analytical model of its operation, and it is fully compliant with the 802.11e standard [147]. Performance study of the Distributed Coordination Function (DCF) of 802.11 networks considering erroneous channel is done [143-144].

Various protocols like AODV, DSR, DSDV, Reference Point Group Mobility model (RPGM) based AODV and Enhanced-AODV (E-AODV) have been found and studied which are implemented using simulation software such as NS-2 to address various problems in MANETs by throughput calculations or graphical plots[137, 145,148].

2.2.2. Packet Delivery Fraction

The ratio of the data packets delivered to the destinations to those generated by the CBR sources is known as packet delivery fraction. While going through a study of various performance metrics in literature, packet delivery fraction has been found to be used in various research studies to analyze one or the other form of wireless networks. Packet delivery fraction as a performance metric has been studied for various applications and research areas [89, 135, 137, 145, 148-167].
Several protocols proposed for different wireless scenarios such as Enhanced-AODV (E-AODV), Reliable-AODV, load-balancing AODV LB-AODV, Cross-Layer Efficient Routing Protocol (CLERP) are studied where packet delivery fraction has emerged as an important performance metric which could be employed in our research to analyse the WLANs enabled with different security algorithms [148-152].

Compared to the omni-directional scheme E-AODV uses minimum number of control packets and with lower broadcast redundancy. E-AODV has been found to have more bandwidth and higher energy efficiency. Another protocol known as Reliable-AODV makes use of two levels of threshold for node’s Battery Power as well as Received Signal Power, so as to maximize the probability of finding a backup route before the active route breakage. A protocol called LB-AODV, which incorporates the concept of Reliable-AODV load-balancing (LB) has been covered. CLERP adopts cross-layer design to establish backup route to reduce the packet losses when link breaks occur. To decrease the unnecessary overhead of hello packets, adaptive links connectivity is employed, which uses adjusting rate of sending hello packets.

During the course of study of literature on performance metrics various routing problems in MANETS covering PDF as a performance metric are studied [153-156, 167]. MANET is a system of wireless mobile nodes dynamically self-organizing in arbitrary and temporary network topologies. Frequent topology changes caused by node mobility make raising the packet delivery fraction in a MANET a challenging problem. A number of heuristics for enhancements of the performance of Ad hoc On-demand Distance Vector (AODV) routing protocol for mobile ad hoc networks are investigated. These heuristics have been implemented with AODV protocol proposal, and simulated using simulator software such as the ns-2 simulator or Glomosim simulator [134, 145, 151, 154-155, 162-165]. Majumder, K et al. have used a simulation model based on NS-2 for the purpose for
comparison between Ad hoc On Demand Distance Vector Routing (AODV) and Dynamic Source Routing (DSR) protocols in the hybrid networking environment [164]. Majumder. K et al. have also used this performance differential to carry out another simulation based performance analysis of the other two prominent routing protocols: Destination Sequenced Distance Vector Routing (DSDV) and Dynamic Source Routing (DSR) protocols in the hybrid networking environment using NS-2. History-Based Adaptive Backoff (HBAB) MAC Protocol, using PDF as a performance metric is studied [159, 161].

Packet delivery fraction along with energy spent by the network can be employed as a figure of merit to evaluate the performance of some protocols [135, 158-159].

2.2.3. End-to-End Delay

Another performance metric which has surfaced as relevant from the study of literature is the end-to-end delay. This metric is used in various wireless applications; for example, vehicular ad hoc network (VANET), analysis of videoconferencing, analysis of LEO Satellite Networks, MANETS [89, 133-134, 149, 167-170] etc. Average end to end delay refers to the time taken for a packet to be transmitted across a network from source to destination. This is greatly dependent upon the routing protocol and also on the number of nodes involved in the application [148]. Srinivasa. S et al. has defined the mean end-to-end delay, as the average number of time slots it takes for the packet at the head of the source model to successfully hop to the destination [133].

End-to-end delay as a performance index has been studied in various areas of research such as vehicular ad hoc network (VANET), Ad Hoc On-Demand Distance Vector (AODV), DSR routing protocol, HBAB MAC Protocol, multicast extension of IEEE 802.11 protocol, Temporally-Ordered

A Vehicular Ad Hoc Network (VANET) is a wireless technology that is used in moving vehicles where the vehicles are treated as wireless nodes in a network and form a mobile network. The multihop packet delivery delay in a low density vehicular ad hoc network (VANET) is studied in the literature so as to explore end-to-end delay as a performance metric. Here a disrupted vehicle-to-infrastructure communication scenario, where end-to-end path is unlikely to exist between a vehicle and the nearest road side unit are covered [168]. This study has helped in investigating the effect of the vehicle density, transmission range, and speed difference between vehicles on the end-to-end packet delivery delay.

Another application area of end-to-end delay as a performance metric is Ad hoc On-Demand Distance Vector (AODV). AODV is a routing protocol for mobile ad hoc networks (MANETs) and other wireless ad hoc networks. It has been studied to be a reactive routing protocol i.e it establishes a route to a destination only on demand. End-to-end delay as a performance index is studied in various types of analysis of these protocols and networks [148, 151-152, 155-156, 160, 162, 164, 169]. Jain. S et al. have developed a multicast extension of IEEE 802.11 protocol and evaluated its performance using ns-2 simulator [151].

End-to-end delay is employed to analyze (WiMAX) technology also. Through the study, it has been observed that comparison of the performance of various routing protocols such as AODV, DSR, and DSDV for mobile WiMAX environment may be done using end-to-end delay. The performance matrix may include packet delivery fraction, throughput, and number of packet dropped in addition to end-to-end delay. These performance metrics may be simulated using simulation software such as NS-2 [145].
This performance metric has been used in proposing some protocols like History-Based Adaptive Backoff (HBAB) MAC protocol too [159, 161]. Another scheme (Reliable-AODV) proposed by Kumar. G et al. has also been studied for which end-to-end delay for data packets is measured [149]. Gupta, N et al. have considered MANETs for their research and deliberated on different routing protocols which are widely used in it [167]. A Mobile ad hoc network (MANET) is a self-configuring network of mobile devices connected by wireless links. The communication in ad hoc network is uncertain because established route could be broken anytime. There may be a lot of delay between active route breakage & backup route discovery, causing the loss of a lot of data packets. Thus end-to-end delay may be used in these networks too [134].

Behaviour of the Ad Hoc On-Demand Distance Vector (AODV) routing protocol in situations of link failures due to the mobility of nodes in wireless ad hoc networks has been studied [169]. Here, AODV performance is compared when the failure repair happens locally from the node, before the link breaks to the case where the repair is performed from the source node using four different metrics; one of them being the packet delivery delay. It has been observed that AODV scales very well in terms of end-to-end delay [151]. The simulation results of CLERP introduced demonstrate improvement in the performance of route discovery frequency, end-to-end delay, packet delivery fraction and routing load compared to AODV [152]. A scheme to solve the problem of re-initialisation of route discovery process has been proposed by Wang Qing-wen et al, which suggests that each source node maintains an alternative route to the specified destination node [155]. Simulation results in this research have been observed and found that this modification has the capability to reduce the average end to end delay.
2.2.4. Other performance metrics

As per the literature study, throughput, packet delivery fraction and end-to-end delay are found to be important performance metrics which have been extensively used. However, during the study it has been observed that there are still many metrics, which may be used for analyzing the performance of a wireless network [137, 145, 152-153, 156-160, 162, 164, 177-178].

Fading in wireless networks is one of such metrics which, may be used as a performance metric [177-178]. Normalized routing load is still another performance metric used to study the behaviour of mobile Ad-hoc network routing protocols [137, 152-153, 156-157, 160, 162, 164].

Energy spent by the network has also been studied as a performance measure [158]. Here Malaguti et al, have presented a simulation study of the performance of two multicast routing protocols. As performance metric energy is considered by Bertocchi. F et al [135]. Srinivasa. S et al. have utilized the end-to-end reliability and defined it as the fraction of packets generated at the source that are eventually successfully delivered [133]. It has been denoted by $R$ and by definition, $0 \leq R \leq 1$. Number of dropped packet and network lifetime are other performance metrics studied as part of literature study [145, 159].

2.3 SOFTWARE CHOSEN FOR ANALYSIS

The field of wireless networks depends on the use of certain software for its analysis and research. A number of software may be employed for performance evaluation and analysis [179]. During the course of literature study some indications on appropriate software for carrying out our research were found.
NS-2 has been studied as a tool for analysis of various schemes and comparison between different existing protocols [100, 136, 145, 148, 151, 153, 160, 162, 165, 179, 180-184].

It has been utilised to fix a flaw in the disassociation mechanism of the WPA protocol, to present an analysis on different routing protocols employed in wireless networks and to present observations regarding the behaviour of these protocols [100, 145, 148, 151, 153, 160, 164, 184]. Majumder, K et al. have carried out a simulation based performance analysis of DSDV and DSR protocols in the hybrid networking environment using NS-2 [160, 164].

NS-2 is utilised in a security scheme, CDM which, attempts to fix a flaw in the disassociation mechanism of the WPA protocol [100]. Enhanced-AODV (E-AODV) protocol has been covered during the literature study, which addresses the problem in MANETs and uses Network Simulator-2 (NS-2) [148]. NS-2 has been used to present an analysis on routing protocols like AODV, DSR, and DSDV employed in these wireless networks [145].

NS-2 network simulator has been used to first implement an evolving graph based routing protocol, and then to use it as a benchmark while comparing, some popular ad hoc routing protocols viz. AODV, DSR, OLSR and DSDV [180]. The development process models implemented in Network Simulator for point multi point topologies, design of beyond 3G networks, set of libraries written for NS-2 called Multi InteRfAce Cross Layer Extension (MIRACLE) have also been covered [181-182]. Underwater networking and its protocol design has also been studied [183]. The tool used for the design and testing of this protocol is also Network Simulator. Harris A. F et al present the design and implementation of a interface and a channel model for underwater acoustic networks in the ns2 network simulator.
Other that this, several other areas of networking have been studied, such as, the IEEE 1609.4 Standard for Wireless Access in Vehicular Environments (WAVE) that has been utilized to enhance the performance of vehicular networks with multi-channel operations. In this study implementation of the IEEE 1609.4 protocol and an evaluation study of 1609.4-based VANETs is done using the ns2 simulator [136].

Wireless networking applications in real-time control systems have also been studied [125]. In this study two applications for Wireless Networked Control Systems (WiNCS) are covered and comparison of various performance criteria, both from networking as well as control point of view are observed. For this purpose, an emulation tool called PiccSIM, abbreviated from Platform for integrated communications and control design, simulation, implementation and modelling, has been employed. PiccSIM is a design and evaluation platform for networked control systems, where different networks can be emulated using the real-time extension of Network Simulator. Use of various other software such as QualNet, Glomosim, LanTraffic etc. have also been studied, typically in the research area of wireless protocols but their use was limited for certain applications only [151].

Qualnet also been used along with NS-2 to carry out the simulations, which are utilized to present observations regarding the behaviour of protocols used in large-scale mobile ad hoc networks (MANETs) [151]. A simulation experiment has also been studied which is performed by using Glomosim simulator to study the effects of three types of attacks, viz; Routing Table Poisoning Attack, Routing Loop Attack and Misrouting Attack on AODV protocol [134]. LanTraffic as network monitoring tool has been studied which may be utilized to analyze the effect of encryption techniques (WEP-40 and WEP-104) on throughput in IEEE 802.11g for TCP and UDP protocols [85].
2.4 IDENTIFICATION OF RESEARCH GAPS

Through a detailed and extensive study of literature it has been observed that performance metrics like throughput, packet delivery fraction and end-to-end delay have been employed extensively for analysing various research work. This forms the basis of utilizing them on security enabled wireless LANs so that their performance can be judged based on these metrics. Some research papers have analysed these algorithms but they are based on a test bed, where number of nodes are very limited. Again simulators like NS-2 or Qualnet have been employed for routing solutions or algorithmic improvements; and the same may be utilised for simulating a wireless LAN with a reasonable number of nodes which have some security algorithms employed in them. This would provide an altogether complete view of the wireless security of modern network. Identifying these research gaps we present simulation of a wireless LAN with WEP and alternatively WPA implemented in it and measuring throughput, packet delivery fraction and end-to-end delay in these wireless LAN along with number of comparisons and analysis in subsequent chapters.