CHAPTER-1

INTRODUCTION

This chapter provides the motivation behind the research work, background knowledge, previously reported work related to the intrusion detection and a comprehensive review of the outstanding vulnerabilities and attacks in Wireless Local Area Networks (WLAN). The need, objectives, research methodology and scheme of the study have also been described.

1.1 Motivation

In today’s broadcasting environment, the computation of the data through Wireless Local Area Networks (WLAN) networks is more prone to attacks when it is compared with wired networks [8, 11]. This is mainly due to wired networks are properly secured through protected cables where as wireless signals are transmitted in open air. Wireless Local Area Networks are widely operable in any kind of circumstances due to its availability, flexibility and mobility. It also makes us more economical due to its easy configurability by which we can cover a larger span of transmission availability by limiting the additional wired networking infrastructure. Though we have many subsequent features of having a WLAN with its mobility and freedom that comes with it but it is exposed to vulnerabilities and attacks. The part of success behind the popularity of WLANs
is due to the availability of the 802.11 standard from IEEE. The standard specifies operation of WLANs in three ways as shown in the figure1.1:

i. **Infrastructure Mode**: Every WLAN workstation (WS) communicates to any machine through an access point (AP). The machine can be in the same WLAN or connected to the outside world through the AP.

ii. **Ad Hoc Network Mode**: Every WS talks to another WS directly.

iii. **Mixed Network Mode**: Every WS can work in the above two modes simultaneously. This is also called the Extended Basic Service Set (EBSS)

![Figure 1.1: Types of Wireless LAN](image-url)
The WLAN security risk analysis and risk management should be in a position to confront these types of security risks and assails since they are imperative in organizational business plan.

The current scenarios in wireless technology offer inadequate level of security standards where one couldn’t really rely on them. Most of the attacks that are encountered in wireless environment are to be enhanced with some more important steps to eradicate these attacks. The radio frequency communication is major temperament of wireless environment, which makes the possibility of some unpreventable attacks like denial of service which is mainly caused due to radio interference [24].

1.2 Background

802.11’s security problems are well known, and the threat of war driving is well publicized [12]. However so far, no known studies have been conducted to assess the risk faced by organizations and the full extent of unauthorized use of wireless LANs. This study seeks to investigate intrusion detection in the Wireless LAN. Wireless LAN standards offer very unsatisfactory level of security and one could not truly trust them. When using products based on these standards the security issues must be taken care in the upper layers [57]. Some commonly used attacks are more stressed in wireless environment and some additional effort should be used to prevent those [82]. The nature of the radio communication makes it practically impossible to prevent some attacks, like denial of service using radio interference. When the wireless networks are used in strategic applications, like manufacturing or
hospitals, the possibility of this kind of attack should be taken into account with a great care [25, 49]. This study seeks to investigate intrusion detection in the WLAN, to maintain the confidentiality, integrity and availability of data transmitted on a LAN.

The main considerable difference between wired and wireless transmission is that the Wireless LAN is not having a predetermined infrastructure and later can be operated in disconnected mode [9, 33]. Due to these main differences, the intrusion detection techniques became very complex to apply for the Wireless networks. Even the present network based Intrusion Detection System (IDS) are not able to detect some of the attacks. This results in complexity to find out and to distinguish false alarms from the intrusions.

Manifestly, there are number of solutions provided by the network security and management for securing WLAN by incorporating many features in intrusion detection system. Even though, there is no perfect and absolute solution to the network security due to limitations and issues that confine the necessity of the existing Intrusion Detection System (IDS). Some of the preceding attacks are not yet detected due to some limitations of the IDS and different new types of attacks came into existence. The capability of the existing IDS is very less to detect these new types of attacks, which are absolutely more vulnerable when compare to the previous attacks. Though IDS have some accomplishments in identifying some specific attacks, the care should be taken for the efficient detection of all attacks.
The distinctive susceptibilities of LAN (802.11x) networks make attack a very possible one. It is highly improbable to physically protect the wireless networks as in the case of wired networks. The source of attacks in opposition to a wireless network can be from the next office, the parking lot of the building, across the street, or possibly several miles away, i.e. the attack can be carried out from anyplace. In order to establish the apt defense strategy it is vital to realize the facts of different attacks in opposition to the wireless infrastructure. The execution of several attacks which are not predominantly treacherous can be performed with ease. However, the execution of certain attacks that have destructive effects can be seriously complicated. The risk involved in wireless security is high as compared to wired LAN security [57].

There are many threats to wireless local area networks (WLANs) and they are potentially disturbing. A WLAN can be affected by the security issues which are ranging from misconfigured wireless access points (WAPs) to session hijacking to Denial of Service (DOS). Wireless networks are not only vulnerable to TCP/IP based attacks which are related to wired networks but they are also focused on the particular threats in the wide array of 802.11. WLANs should use a security solution which includes an intrusion detection system (IDS) which helps to assist in the defense and detection of these possible threats [20]. Even organizations without a WLAN should consider an IDS solution because they may be dangerous due to wireless threats. Wireless local area networks are focused to a variety of threats. The Wired Equivalent Privacy (WEP), which is the standard 802.11-encryption method, is weaker.
By introducing a misbehaving wireless application protocol (WAP) into the WLAN coverage area, the hackers can attack a WLAN and collect the sensitive data. As several wireless clients are connected simply to the WAP with the best signal strength the misbehaving WAP can be designed to look like an actual WAP. Also the users can be “tricked” to associate with the misbehaving WAP accidentally. All the communications can be observed by the hacker through the misbehaving WAP, when a user is associated. Misbehaving WAPs can also be introduced by the users besides the hackers. WLANs can be highly attractive to the users when low cost and easy implementation is combined with the flexibility of the wireless network communications. The users can create a backdoor into the network, subverting all the hardwired security solutions and give the network open to the hackers by installing a WAP on a recognized LAN.

WLAN can be made fatal owing to fact that Networks using 802.11 are susceptible to numerous denials of service (DoS) attacks. Wireless communications stumbling upon physical objects are naturally susceptible to signal degradation. In addition, hackers can overflow WAPs with associating requests and bring about malicious DoS attacks, hence forcing them to reboot. Besides, they can deny service to a wireless client by employing the rogue WAP to send repeated de-authenticate requests.

There are various other WLAN threats existing and the identification of further susceptibilities is being carried out at an escalating speed [74]. The reality of the threats, their ability to create broad destruction and their rising familiarity with increase in fame of the 802.11 technology is a fact. The identification of the threats
to a WLAN can be complicated in the absence of a detection mechanism. A network may not be sufficiently secure in opposition to the threats facing it, when the awareness of the threats is absent. It is only possible to appropriately equip the WLAN with the essential security measures when the threats to the network are recognized.

1.3. Intrusion Detection

Intrusion detection systems (IDSs) collect and scrutinize the data to recognize computer system and network intrusions and mishandlings [7, 112]. The conventional IDSs have been designed for wired systems and networks to identify intrusions and mishandling. Of late, wireless networks have been concentrated for employing the IDSs constructed [35]. Monitoring and analyzing user and system activities, recognizing patterns of known attacks, identifying abnormal network activity, and detecting policy violations for WLANs are the functions of these wireless IDSs. Wireless IDSs collect all local wireless transmissions and rely either on predefined signatures [113] or on anomalies in the traffic [27] to produce alerts. A Wireless IDS has further employment necessities and certain distinctive features definite to WLAN intrusion and misuse detection when compared with standard, wired IDS. A wireless IDS assists to implement policy in addition to identifying attackers. There are several security-related issues in WLANs, however, a lot of the security flaws can be dealt with [27, 113].

Centralized wireless IDS and decentralized wireless IDS are the two kinds of wireless IDSs [27, 34]. The former is generally a mixture of individual sensors
collecting and forwarding all 802.11 data to a central management system where the storing and processing of the wireless IDS data is performed, whereas, one or more devices that execute both the data gathering and processing/reporting functions of the IDS are typically comprised in the latter. The cost and management concerns restrict the decentralized method to be appropriate for smaller (1-2 WAP) WLANs.

Moreover, the detection of numerous attacks can be performed with the assistance of a wireless IDS. A Wirelesses IDS can perceive many of the standard wireless attacks and identify rogue WAPS [71], recognize non-encrypted 802.11 traffic and assist to cut off an attacker's physical location. There are several advantages of a wireless IDS, however there are some disadvantages also, which must be considered before using such system. Wireless intrusion detection is a new technology. We should be careful before applying any new technology to an operational network. Since, it is new technology there may be some faults or weakness which could possibly reduce the WLAN security. Wireless IDS technology develops quickly and this warning will not act as prevention in the future. A potential turn-off to wireless IDS solution may be cost. This cost grows with the combination of the WLAN size to be monitored, due to the requirement for a large number of sensors. Hence, larger the WLAN size, more is the cost of IDS usage [14, 37].

1.4. Attacks in Wireless LAN

The wireless nature of WLAN opened the door for the intruders and attacks that can come from any direction. WLAN traffic travels over radio waves that cannot be constrained by the walls of the building, which made intruders and hackers
access the network potentially from the parking lot or across the street. In this section the most frequently occurring attacks are briefly explained, e.g. active attacks, passive attacks, layered based attacks, denial-of-source attacks and also some possible countermeasures presented [12, 14, 26].

The attacks may be classified on the basis of followings

- **Attacks based on Behavior:** The attacks in WLAN based on behavior are mainly classified into two main categories [12]. They are active and passive attacks that are dangerous.

- **Attacks based on Routing:** Attacks against the routing message can be classified into Masquerading, Eavesdropping and Modification.

- **Attacks based on different layer:** Security threats in physical layer, Security threats in Link layer, Security threats in Network Layer, Security threats in Transport layer and Security threats in application layer.

1.4.1 Attacks based on Behavior

**1.4.1.1 Active attack:** An intrusion into a computer network, attempts to delete or modify the data stored on the computers, form a part of the network is one of the most serious forms of attack. Since, many companies operations critically depend on data. In these types of attacks the entity that is attacked gets alert of when attacked. That is the interruption from the attacker is of such kind that he gets aware of the attack, hence called active attack. In other words, the attacks in WLAN are said to be active attacks if the intruder or the hacker able to access the network and making
some modifications to the information such as resources or messages that are transmitted through this network. These types of attacks are detectable but sometimes they are not preventable. As the intruder gains information from the passive attack, there is possibility of an active attack against the network (Welch, 2003). There is lot of possibilities for the intruders to launch the active attacks in wireless networks. Under the active attacks, denial of service attacks (DoS), unauthorized access, spoofing, flooding attacks and theft of devices are the common attacks [86].

1.4.1.1i. Denial of Service (DoS) Attacks: A denial of service (DoS) attack is one where the authorized users cannot use services, as the intruder attends to compose the network not capable to serve. Wireless networks are vulnerable to a denial-of-service attack that is not viable against their wired networks. Because these signal travels through air rather than cables, as wireless networks are very free in accordance with the RF signals either deliberate or accidental. There is a chance of accidental interference in some cases such as when a cordless telephone is operating in the same radio band and in physical proximity to the wireless node. Sometimes, there is a chance of the interference with one wireless network with the other which is close to it that makes the service unusable

1.4.1.1ii. Replay attack: The integrity of the information of the network or the integrity of the specific session is mainly aimed by the intruder comes under replay attack. With the help of the authorizations of the target, the reply attacks occur by gaining the access to the network, but the actual session or the sessions that are attacked are not distorted or interfered with in anyway. Any how this is not the
practical attack or real time attack because the intruder has to access the network after the original sessions. In a replay attack, the attacker captures the authentication of a session or sessions. The attacker then either replays the authenticated session at a later time or uses multiple sessions to synthesize the authentication part of a session. The authentication of a session or sessions is captured by the attacker or the intruder. The intruder may either replay the authenticated session afterwards or the authentication sessions are synthesized to several sessions. Since the session valid, the intruder interacts with the network without being confidentiality to any used authentication. The attacker can still be able to control WLAN by specific modifying parts of the packets to get the required outcome without the WLAN employs encryption [85].

1.4.1.1iii. Unauthorized access: In this type of attack, the attackers mainly aim at a particular user by gaining unauthorized access to the entire network. This attack depends on network security architecture. In some security architectures, if the attackers access the wireless network, then he or she also gets access to the wired network while in some security architectures, the access control which is usually implemented using the access control list (ACL) controls the wired components. Anyhow by spoofing the victim’s MAC address, the access control rights can be bypassed. Masquerading is quite similar to the spoofing. This attack mainly tries to accessing the services or privileges for which the attacker is not authorized to access.

1.4.1.1iv. Rouge access points: In order to provide convenience to their authorized users, these rouge access points are come into existence which can be a thought of sub-divisions of access points. The rouge access points has very minimal or no
security which becomes a major point for the attackers to attack. Even if the user uses a WEP, the attacker can attack and exploit the algorithm by using various methods [84]. The attacker or the intruder can have a chance to setup a rouge access point to gain future access to the network or even to obtain user a/c information. Generally the attackers try to fraudulent rouge access point for the respective AP to get hold of people’s user name and password. Rouges access points a vital role in mounting a MITM attack

1.4.1.1v. Man in the middle attack: Man in the middle attack is an indirect viewpoint of attacking data confidentiality. The organizations might have employed security measure such as virtual private network.

1.4.1.1vi. Session hijacking: The session hijacking in basically done by obtained by MAC address of the access point (AP). The victim is authenticated by the AP and attacker impersonates as the AP by using its MAC address and gains control over the session. This attack happens in real time and also compromises the integrity aspect. Further information in

1.4.1.2. Passive Attack: The passive attack is an intrusion into a computer network which reads the data passing through some of the transmission lines without modifying it. In this type of attacks, the entity that is attacked is uninformed of the attack; (example the attacker is just trying to observer you). In other words, when an attacker or an intruder listens to or eavesdrops on network traffic, then there is occurrence of passive attack. Network monitor in Microsoft products or TCP dump in Linux-based products, or Air snort is the common available tools for the intruders to
capture network traffic using a wireless adaptor that maintain promiscuous mode. These attacks are not malevolent in nature. The attack called as war driving is the most famous attack done by the intruders. The intruders mainly try to detect the access point of the Wireless network. But looking for and detecting wireless traffic is perhaps not illegal even though but there are certain claims that are opposed and often made. Any one can use the frequencies, if the wireless communication takes place on unlicensed public frequencies, where there is a chance of more passive attacks that becomes more difficult. Passive attacks are by their very nature difficult to detect. If a person logs into an authorized MAC address acquiring an IP address, then an administrator using dynamic host configuration protocol (DHCP) can may or may not notify [73]. But there are several limited legal responses, if a wardriving is actively attempting to crack any encryption used on the network or otherwise interfering or analyzing wireless traffic with malicious intent then he or she should be susceptible to being charged with a data-related crime depending upon the place and the country in which the activity took place. There are two types of passive attacks that came into existence. They are passive eavesdropping and traffic analysis. The below is the study of the passive attacks.

1.4.1.2i. Traffic analysis: Footprinting is the first step for any type of attacking and the wireless footprinting is carried out by traffic analysis. In traffic analysis, the attacker determines the load on the communication medium by the recognizing the number of packet transmitted and the size of the packets, the source and destination address of the packets and the types of packets. Before mounting an attack the attacker have to obtain sufficient information about the network [76]. The assumption
is that payload of the packets is encrypted and the attacker cannot decrypt the payload which makes the attacker to see only the header and any trailer information visible to the attacker. But here the attacker uses a wireless card operating in immoral mode and software to count the number and size of the packets being transmitted [8].

1.4.1.2ii. Passive Eavesdropping: In this attack the attacker passively monitors the wireless session and the payload. If the payload is encrypted, this includes breaking the encryption to read the plaintext. The only precondition is that the attacker has access to the transmission. As described in the previous section, a directional antenna can detect 802.11 transmissions under the right conditions miles away [38]. Therefore, this is an attack that cannot easily be stopped by using physical security measures. One would believe that wireless network users would configure their wireless access points to include some form of encryption; however, studies have shown that less than half of the wireless access points in use even have the vulnerable 802.11 wireless security standard, the wired equivalent privacy (WEP) protocol, properly configured and running. The attacker can gain two types of information from passive eavesdropping. The attacker can read the data transmitted in the session and can also gather information indirectly by examining the packets in the session, specifically their source, destination, size, number, and time of transmission. The impact of this type of attack is that not only is the privacy of the information compromised, but the information gleaned is an important precondition for other, more damaging attacks.

1.4.2 ATTACKS AGAINST ROUTING MESSAGES
Routing is one of the most vital mechanisms in the ad hoc networks. Improper and insecure routing mechanisms will not only degrade the performance of the ad hoc networks, but will also render such networks vulnerable to many security attacks. In this work, attacks against routing messages are classified based on the classification suggested by Stallings [88]. In such classification, information or messages could be deviated from the normal operation flow using Masquerading, eavesdropping, modification, interception, and interruption or fabrication attacks. In a more rigorous case, attackers also might use any combination of these attacks to disrupt the normal information flow. Attacks against the routing message can be classified into Masquerading, Eavesdropping and Modification [88].

1.4.2.1 Masquerading: The ability of an unauthorized third party to masquerade as a legitimate user of a wireless network can range from being a very simple to complex undertaking, with the degree of complexity based upon the security in effect. If the victim’s WLAN does not employ any security it becomes a relatively simple process for an unauthorized third party to determine the SSID in use by an access point and gain access to victim’s network. If the WEP is enabled gaining access to victim’s network becomes more difficult, but not impossible due to the weaknesses of the WEP.

1.4.2.2 Eavesdropping: In a wireless network, eavesdropping is easy because wireless communications are not easily confined to a physical area. A nearby attacker can receive the radio waves on the wireless network without any substantial effort or equipment. All frames sent across the wireless medium can be examined in real time or stored for later examination. Although, the transmission distance in wireless LANs
is normally limited to hundreds of meters, this limitation is based upon the use of small antennas built into PC cards and other factors used to create wireless network interface cards.

1.4.2.3 Modification: A data modification attack results from the fact that the integrity check value (ICV) used by WLANs is a Cyclic Redundancy Check-32 (CRC). The CRC-32 is linear with respect to a bit flipping process. This means that flipping bit \( n \) in the message results in a deterministic set of bits in the CRC that must be flipped to produce a correct checksum on the modified message. Because flipping bits carry through after the decryption, this allows the attacker to flip arbitrary bits in an encrypted message and correctly adjust the checksum so that the resulting message appears valid.

1.4.3 ATTACKS BASED ON DIFFERENT LAYER

The layer based classification of WLAN attacks is mainly based upon the attacks on TCP/IP protocol layers that are used in WLAN communication. The layer based classification is mainly based on physical layer, network layer, link layer, Transport layer and application layer [98].

1.4.3.1. Security attacks in physical layer

The most common physical layer attacks in WLAN are eavesdropping, interference, denial-of-service and jamming. The common radio signal in WLAN is easy to jam or intercept. Moreover an attacker can overhear or disrupt the service of wireless network physically. An attacker with sufficient transmission power and knowledge
of the physical and medium access control layer mechanisms can gain access to the wireless medium.

1.4.3.2. Security attacks in Link layer

Many attacks can be launched in link layer by disrupting the cooperation of the protocols of this layer. Wireless medium access control (MAC) protocols have to coordinate the transmission of the nodes on the common communication or transmission medium. The IEEE 802.11 MAC protocol uses distributed contention resolution mechanisms which are based on two different coordination functions. One is Distributed Coordination Function (DCF) which is fully distributed access protocol and the other is a centralized access protocol called Point Coordination Function (PCF). For resolving channel contention among the multiple wireless hosts, DCF uses a carrier sense multiple access with collision avoidance (CSMA/CA) mechanism [99].

1.4.3.2i. Threats in IEEE 802.11 MAC: The IEEE 802.11 MAC is vulnerable to DoS attacks. To launch the DoS attack, the attacker may exploit the binary exponential back off scheme. For example, the attacker may corrupt frames easily by adding some bits or ignoring the ongoing transmission. Among the contending nodes, the binary exponential scheme favors the last winner which leads to capture effect. Capture effect means that nodes which are heavily loaded tend to capture the channel by sending data continuously, thereby resulting lightly loaded neighbors to back off endlessly. Malicious nodes may take the advantage of this capture effect vulnerability. Moreover, it can cause a chain reaction in the upper level protocols
using back off scheme, like TCP window management. Another vulnerability to DoS attacks is exposed in IEEE 802.11 MAC through NAV (Network Allocation Vector) field carried in the RTS/CTS (Ready to Send/Clear to Send) frames [87]. During the RTS/CTS handshake, a small RTS frame including the time needed to complete the CTS, data and ACK frames is sent by the sender. All the neighbors of the sender and receiver update their NAV field according to the time that they overheard for transmission duration. The attacker in the local neighborhood is also aware of the duration of the ongoing transmission and he/she may transmit a few bits within this period to incur bit errors in a victim’s link layer frame via wireless interference.

1.4.3.2ii. Reduction of Quality (RoQ) Attack: By the high rate or high volume, the typical DDoS flooding attacks are characterized. An alternative of distributed denial of services (DDoS) attacks has been identified recently which is too complex to detect which are called as shrew attacks or Reduction-of-Quality (RoQ) attacks. Instead of refusing the clients from the services completely, these RoQ attacks throttle the TCP throughput heavily and reduce the QoS to end systems gradually [33,43]. The transients of systems adaptive behavior is targeted by the RoQ attacks instead of limiting its steady-state capacity. The RoQ attacks can use source and destination IP address spoofing, and they do not have distinct periodicity, and may not filter the attack packets precisely. In order to escape from being caught by the traceback techniques, RoQ attacks often launch attacks through multiple zombies and spoof header packet information. But, it is important to control the frequency domain characteristics of attacking flows. In order to throttle the TCP flows efficiently, the
attacking period has to be close to the Retransmission Time Out (RTO). Using traffic spectrum, the energy distribution pattern will give up such malicious flow detection mechanisms even if the source IP addresses are carried in packet header are falsified [39]. By the high rate or high volume, the typical DDoS flooding attacks are characterized. An alternative of DDoS attacks has been identified recently which is too complex to detect which are called as shrew attacks or Reduction-of-Quality (RoQ) attacks. Instead of refusing the clients from the services completely, these RoQ attacks throttle the TCP throughput heavily and reduce the QoS to end systems gradually [80]. The transients of systems adaptive behavior is targeted by the RoQ attacks instead of limiting its steady-state capacity. The RoQ attacks can use source and destination IP address spoofing, and they do not have distinct periodicity, and may not filter the attack packets precisely. In order to escape from being caught by the traceback techniques, RoQ attacks often launch attacks through multiple zombies and spoof header packet information. But, it is important to control the frequency domain characteristics of attacking flows. In order to throttle the TCP flows efficiently, the attacking period has to be close to the Retransmission Time Out (RTO). Using traffic spectrum, the energy distribution pattern will give up such malicious flow detection mechanisms even if the source IP addresses are carried in packet header are falsified [80, 93].

1.4.3.3. Security attacks in Network Layer

A number of attacks in network layer have been identified and studied in the literature. An attacker can absorb network traffic, inject themselves in the path sandwiched between the source and destination, and control the network traffic flow.
The main attacks in network layer are Routing Protocols, On-Demand, Table-driven, Routing Table Overflow Attack and Wormhole Attack etc.

1.4.3.4 Security threats in Transport layer

The SYN flooding attack is also DoS attack and Session Hijacking attacks that are performed by creating a large number of half-opened TCP connections with a target node is a major attack in the transport layer. TCP connection between two communicating parties is established through completing three way handshakes. The sender sends a SYN message to the receiver with a randomly generated ISN (Initial Sequence Number). The receiver also generates another ISN and sends a SYN message including the ISN as an acknowledgement of the received SYN message. The sender sends acknowledgement to the receiver. In this way the connection is established between two communicating parties using TCP three way handshakes. During SYN flooding attack, a malicious node sends a large amount of SYN packets to the target node, spoofing the return address of the SYN packets. Session hijacking is a critical error and gives a malicious node the opportunity of behaving as a legitimate system. All the communications are authenticated only at the beginning of session setup.

1.4.3.5 Security attacks in application layer

There are two major attacks in the application layer i.e the Malicious Code Attacks and the Repudiation attacks. The various malicious codes such as virus, worm, spywares and Trojan horse attack both operating systems and user applications that cause the computer system and network to slow down or even damaged. An attacker can
produce this type of attacks in WLAN and can seek their desire information [91]. In Repudiation attacks the solution that taken to solve authentication or non-repudiation attacks in network layer or in transport layer is not enough. Because, repudiation refers to a denial of participation in the communication. Example of repudiation attack on a commercial system: a selfish person could deny conducting an operation on a credit card purchase or deny any on-line transaction.

In the study of various attacks in wireless local area networks and their classification are useful as the most of these types of attack can be handle with moderate efficiency. The security administrator can analyze these and understand the risks involved and hence implement a wireless network that can counter the active and passive attacks against WLAN .In this study we revealed that there is a countermeasure of the different attacks are there but there is recently one attacks in the MAC layer that is an alternative of DDoS attacks called shrew attacks or Reduction-of-Quality (RoQ) has been identified in this study which is very much difficult to detect. The RoQ attacks can use source and destination IP address spoofing, and they do not have distinct periodicity, and may not filter the attack packets precisely.

1.5 Vulnerabilities in Wireless Local Area Networks (WLAN)

Along with all the vulnerabilities widespread to wired networks [72], wireless LANs introduces a new sequence of threats. Most of the vulnerabilities (as shown in figure 1.2) in wireless environment are same as in a wired network; additional vulnerabilities are quite distinctive in nature than others. Vulnerabilities occur because data in wireless local area networks is transmitted with the help of radio waves, that can be
caught and translated, and the data is generally sent as clear text, that is, with no encryption [84,85]. The most significant and important vulnerabilities are access control vulnerabilities, authentication vulnerabilities, WEP vulnerabilities, WPA/WPA2 vulnerabilities, system network management protocol [79]. The fundamental IEEE 802.3 Ethernet protocol that underlies the 802.11 standards does a logical task of making sure that data integrity will be achieved using a 4-byte Cyclic Redundancy Check (CRC) computed over the data [10, 33].

**Figure 1.2: Critical Vulnerabilities in Wireless Local Area Networks**

1.5. i. **Access Control Vulnerabilities:** Vulnerability tests are carried out to identify vulnerabilities whereas penetration tests are used to check how the access control mechanisms are overpowered and illegal access is achieved. Also the systems can be closed or congested with malevolent data by means of techniques such as DoS
attacks, till right to use is deprived for genuine users. The 802.11 standard does not sufficiently address access control. The features of MAC address access control list (ACL) offer incomplete forms of access control. The SSID is used for recognizing the network and not as a security measure. Unluckily and only due to chance, the use of a SSID is often incorrectly recognized as a password protection. The SSID contained in the bonfire frame is always sent in plaintext, independent of the deployment of the WEP option. A few wireless client, either malicious or not, can listen for this bonfire to obtain the SSID and find a way around this low level access control. A number of 802.11 vendors offer a MAC address ACL feature that provides minimal access control by restraining access to just authorized wireless cards. Unluckily, the packets containing the MAC addresses are transferred in clear text and the entries on the ACL can be effortlessly acquired through traffic monitoring. The unauthorized users can spoof these MAC addresses and attempt to gain access to the AP. In the majority of the time, the AP has the factory configuration for the administrator username and password. At the time, the unauthorized user has accessed the AP, the configuration of the AP can be changed.

1.5. ii. Authentication Mechanism Vulnerabilities: The authentication mechanism defined in the 802.11 is used to bring the wireless link up to the assumed physical standards of a wired link. There are vulnerabilities present in both the design and the implementation of the service.

1.5. iii. 802.1X/EAP (Extensible Authentication Protocol) Vulnerabilities: Initially introduced in WPA, the 802.1X framework has the potential to significantly improve the authentication capabilities of 802.11 wireless networks. Sarcastically, the
authentication protocol specified by 802.1X is vulnerable to attack chiefly due to its incapability to authenticate its own messages. Due to this fault, EAP messages can be forged in a man-in-the-middle scenario, potentially permitting an attacker to bypass an authentication mechanism or to hijack an 802.11 session [69].

1.5. iv. WEP (Wired Equivalent Protocol) Vulnerabilities: The weakest aspect of the system is the distributed shared key. With the use of static shared keys, distributed among all the clients in the form of “passwords,” the number of users knowing these keys will grow as the network gets bigger which creates the following problems: Public or shared key amongst a lot of people does not remain secret for a long time; When the shares key is distributed manually it can be time consuming, particularly in a huge environment with lots of users.

1.5. v. WPA/WPA2 (Wireless Protected Access) Vulnerabilities: The WPA and WPA2 have introduced procedures intended to address the major vulnerabilities of WEP, nevertheless a few new vulnerabilities were introduced and several vulnerabilities remain, particularly in WPA because of the requirement for backwards compatibility, and short compute requirements. Even though 802.1X authentication support was made obligatory in WPA/WPA2, its use requires an exterior authentication server and therefore the user is given an option to use an easy pre-shared key mechanism like WEP. Unluckily, as with WEP, the pre-shared key authentication mechanism for both WPA and WPA2 is susceptible to key management issues: it is almost impossible to maintain a single shared key secret among a large community, and re-keying and distributing new keys for a huge community is equally complicated[33].
1.6 Need of the Study

In today’s broadcasting environment, the commutation of the data through Wireless Local Area Networks (WLAN) networks is more prone to attacks, when it is compared with wired networks. WLAN networks are widely operable in any kind of circumstances due to its availability, flexibility and mobility. Though, we have many subsequent features of having a WLAN with its mobility and freedom that comes with it but it is exposed to malevolent attacks. The current scenarios in wireless technology offer inadequate level of security standards where one couldn’t really rely on them. Most of the attacks detection techniques that are encountered in wireless environment are to be enhanced with some more important steps to eradicate these attacks. The radio frequency communication is major temperament of wireless environment, which makes a possibility of some unpreventable attacks. In the literature number of techniques had been developed for different types of attacks, but the effective detection of these attacks are remain open problem. So there is a need of study to design a new efficient technique to detect the intrusions in wireless networks.

1.7 Scope

All the work in this thesis is based on the IEEE 802.11 infrastructure WLAN. The research is specially focused on to study different security problems or flaws in wireless networks and to detect some of these attacks using intrusion detection techniques. It is known that wireless networks are prone to more attacks than wired networks because there is no need of any physical access to wireless networks. The sole focus of this thesis is on Intrusion Detection Techniques for wireless Local Area
Networks (WLAN). The work presented in this thesis is not based on statistical or mathematical modeling; this work is on the basis of Network Simulator 2 (NS2).

1.8 Research Aims

The security problems of Wireless Local Area Networks (WLAN) are well known, and the threat of war driving is well publicized. However so far, no known studies have been conducted to assess the risk faced by organizations and the full extent of unauthorized use of wireless LANs. This study seeks to investigate intrusion detection in the Wireless LAN to maintain the confidentiality, integrity and availability of data transmitted on a LAN. The purpose of the study is to scrutinize the security problems or flaws in wireless networks and to detect some of these attacks using an intrusion detection technique. The research work start with the study of some of the vulnerabilities and possible attacks on wireless networks and to determine the efficiency of the intrusion detection system detecting these attacks.

The followings are the major objective of our study

i. To study various vulnerabilities and attacks on Wireless Local Area Networks (WLAN) and their detection using the Intrusion detection System (IDS).

ii. To study some of the existing security methods used for WLAN and explore the possibility of improvements in the same.

iii. To analyze various techniques based on misuse detection or anomaly based detection for securing wireless LAN.
iv. To study, number of commercial available Intrusion detection tools that are capable of monitoring wireless traffic.

v. Finally, overall objective is to develop a new efficient technique for monitoring, detecting and responding to the various security breaches to the WLAN

1.9 Research Methodology

- A comprehensive literature survey has been conducted to understand the strength and weaknesses of the existing intrusion detection techniques and tools. The study led to the design and development of three new techniques (namely Cross Layer Based, MAC Layer Based and Distributed techniques) that attains low misdetection ratio and false positive rate while increasing the packet delivery ratio.

- The techniques have been implemented in NS2 simulator on Fedora platform.

- In order to reach the conclusion, the performance of the proposed techniques has been compared with the existing techniques.

1.10 Thesis Structure

This thesis is divided into six major chapters, which are structured around the aims of the research.

The first chapter presents the Motivation, Background, objectives and a comprehensive review of the outstanding vulnerabilities and attacks in WLAN. The classification of wireless local area network attacks are proposed based on the imperative parameters.
Chapter 2 presents the literature survey. It includes the review of different intrusion detection tools and techniques by taking the vital research parameters. This is useful for developing new intrusion detection techniques for WLAN.

Chapter 3 presents the Design of Cross Layer Based Intrusion Detection Technique for WLAN. In this technique a combined weight value is computed from the Received signal strength (RSS) and Time taken for RTS-CTS handshake between sender and receiver (TT). Since it is not possible for an attacker to assume the RSS exactly for a sender by a receiver, it is an useful measure for intrusion detection.

Chapter 4 presents the Design and Development of MAC layer based defense architecture for RoQ attacks in WLAN. A defense scheme is proposed that includes the detection and response stages.

Chapter 5 presents the Design of Distributed Technique for Detecting the Wormhole attacks in WLAN.

Chapter 6 summarizes this work by discussing the contributions of the proposals and drawing the conclusions. The scope for future research is also outlined.

1.11 Limitations of the study

- The thrust of the study is on the Intrusion Detection Techniques for IEEE 802.11 Wireless LAN. The Mobile Ad-hoc Networks (MANET) have not been taken into the purview.
- This research focuses attention on detection of specific attacks rather than on a general method that tries to detect all the attacks.
1.12 Chapter Summary

This chapter describes why and how the present study was designed and conducted. The various types of attacks and vulnerabilities were studied. The focus of this research is to develop efficient intrusion detection technique for WLAN that attains effective detection. The need, aims, scope, research methodology and chapter scheme of the study have also been described.

In the next chapter, an endeavour has been made to examine the different intrusion detection tools and techniques through the review of relevant literature available on the subject.

----------------------