CHAPTER 1
INTRODUCTION

1.1 Wireless Technology

Wireless technologies enable one or more devices to communicate without physical connections. Wireless technologies use radio frequency transmissions as the means for transmitting data, whereas wired technologies use cables. Wireless networks are frequently categorized into three groups based on their coverage range: Wireless Wide Area Networks (WWAN), Wireless Local Area Networks (WLAN), and Wireless Personal Area Networks (WPAN). WLAN is a data transmission system designed to provide location-independent network access between computing devices by using radio waves rather than a cable infrastructure.

The following Figure 1-1 shows various types of network available.

![Wireless and Wired Access Networks Diagram]

Figure 1-1 Types of Networks
1.2 Wireless Local Area Networks (WLAN)

Wireless local area networks are groups of wireless networking nodes within a limited geographic area, such as an office building or campus, that are capable of radio communication. WLANs are usually implemented as extensions to existing wired Local Area Networks (LAN) to provide enhanced user mobility and network access. Today, WLAN technology is experiencing tremendous growth. The key reason for this growth is the increased bandwidth made possible by the IEEE 802.11 standard [4].

WLANs allow greater flexibility and portability than the traditional wired LAN. Unlike a traditional LAN, which requires a wire to connect a user’s computer to the network, a WLAN connects computers and other components to the network using an Access Point (AP) device. An access point communicates with devices equipped with wireless network adaptors; it connects to a wired Ethernet LAN via an RJ-45 port. Access point devices typically have coverage areas of up to 300 feet (approximately 100 meters). This coverage area is called a cell or range. Users move freely within the cell with their laptop or other network device. Access point cells can be linked together to allow users to even “roam” within a building or between buildings. Station (STA) is a wireless endpoint device. Typical examples of STAs are laptop computers, Personal Digital Assistant (PDAs), mobile telephones, wireless headphones, microphones, remote controls, cordless computer keyboards and mice and other consumer electronic devices with IEEE 802.11 capabilities [20].
1.3 Wireless Networking Principles

Wireless networking refers to the transmission of signals, which are transmitted and received via antennae through a wireless medium such as air or space instead of through a physical cable. But nowadays the term wireless networking generally refers to Wireless Local Area Networks (WLANs). Using electromagnetic waves, WLANs transmit and receive data over air minimizing the need for wired connections. Since there is no physical connection involved so the data communication is done via electromagnetic airwaves (radio and infrared). Radio waves are often referred to as radio carriers because they simply perform the function of delivering energy to a remote receiver [23]. The data being transmitted is superimposed on the radio carrier so that it can be accurately extracted at the receiving end. This is generically referred to as modulation of the carrier by the information being transmitted. Once data is modulated onto the radio carrier, the radio signal occupies more than a single frequency, since the frequency or bit rate of the modulating information adds to the carrier. As the communications are being done through radio waves, there is a very good chance that multiple radio carriers can exist in the same space at the same time. It is possible to avoid the radio carriers from interfering with each other if the radio waves are transmitted on different radio frequencies. To extract data, a radio receiver selects one radio frequency while rejecting all other radio signals on different frequencies.

An access point that acts as a transmitter/receiver (transceiver) device connects to the wired network from a fixed location using standard Ethernet cable. At minimum, the access point receives, buffers, and transmits data between the WLAN and the wired network infrastructure.
A single access point can support a small group of users and can function within a range of less than one hundred to several hundred feet.

Figure 1-2  Classifications of Wireless LANs

From Figure 1-2, it’s quite evident that modes of communication within wireless networks can be classified under either radio wave or infrared technology. There are various technologies to choose from to carry data when designing a wireless network.
1.4 Radio Transmission Technology

Radio transmissions use radio frequencies (RF) to transmit information. There are many different radio frequency ranges in the electromagnetic spectrum that are assigned to different services. From 800 MHz to 2.5 GHz, range of the electromagnetic spectrum, is used for various services such as digital cordless phones, pagers, personal digital assistants, laptops and personal computer memory card international association (PCMCIA), and so on. There are four predominantly used technologies to transmit data using radio frequencies [34][40]. They are Narrow band technology, Spread spectrum technology, Frequency-hopping spread spectrum technology, Direct-sequence spread spectrum technology.

Narrowband Technology: In this technology, the data is transmitted directly on a center frequency, much like a radio broadcast, so the transmitter and receiver must be tuned to the same bandwidth. Narrowband radio keeps the radio signal frequency as narrow as possible just to pass the information. Interception can be avoided by carefully coordinating different users on different channel frequencies. Like the signals from radio and TV stations, narrowband signals are subject to interference from signal reflections. This interference is caused when signals reflected off walls and other objects arrive at different intervals. Such interferences make communication unreliable. Unlike the human eye, communications equipment is not sophisticated or intelligent enough to discern the difference between reflections and the real transmission. In order for the narrowband technology to work properly a clear channel for communications has to be ensured. This can be achieved by carefully
allocating each available frequency band to make sure that no nearby networks share the same frequency [53].

*Spread Spectrum Technology:* Spread spectrum simply means that data is sent over a number of discrete frequencies available for use at any time in the specified range. There are two different implementations for spread spectrum technology. Spread spectrum technology is most widely used data communication system in wireless LANs. This technique has been designed to increase the efficiency in bandwidth even though there are some tradeoff’s associated with it. The frequency range for transmission using spread spectrum technology is 902Mhz to 928Mhz, which has been set-aside for wireless data communications. Even though the bandwidth consumed with spread spectrum technology is more than in case of narrowband transmission, it produces a signal that is, in effect, louder and thus easier to detect. Using spread spectrum technology it is highly unlikely that one spread spectrum network user will interfere with another. The original Institute of Electrical and Electronics Engineers wireless-ethernet specification, known as IEEE 802.11, designated two kinds of spread spectrum frequencies for communicating between devices: frequency hopping and direct sequence.

*Frequency-Hopping Spread Spectrum Technology:* In this method of communication, short burst of data is sent and then frequencies are shifted and then another short burst is transmitted. It uses a narrowband carrier than changes frequency in a pattern known to both transmitter and receiver. The frequencies are synchronized in a fashion such that a single logical channel is maintained. The devices that are communicating using frequency-hopping technique agree on which frequencies to hop to, and use each frequency for a brief period of time before interfering with each
other. In frequency-hopping, the data is generally sent on just two to four frequencies simultaneously, they use 1 MHz or less of the available bandwidth. Because they use any given frequency for such short time they are less prone to interference. Frequency- Hopping based devices are easier and cheaper than devices using infrared.

*Direct-Sequence Spread Spectrum Technology:* Using this technology, Communication is done by splitting each byte of data into several parts and sending them concurrently on different frequencies. Direct-sequence spread spectrum generates a redundant bit pattern for each bit to be transmitted. Direct-sequence unlike frequency hopping uses a lot of available bandwidth, about 22 MHz. The transmissions in sequence-sharing are suitable for bandwidth sharing because they offer an improved signal-to-noise ratio compared with narrowband transmissions. Even if some of the bits are lost during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission. Direct-sequence spread spectrum is capable of much greater speed than frequency-hopping.

### 1.5 Wireless Devices

A station, or client, is typically a laptop or notebook personal computer (PC) with a wireless Network Interface Card (NIC). A WLAN client may also be a desktop or handheld device (e.g., PDA, or custom device such as a barcode scanner). Wireless laptops and notebooks—“wireless enabled”—are identical to laptops and notebooks except that they use wireless NICs to connect to access points in the network. The wireless NIC is commonly inserted in the client's Personal Computer Memory Card International Association (PCMCIA) slot or Universal
Serial Bus (USB) port. The NICs use radio signals to establish connections to the WLAN [68].

A wide range of devices use wireless technologies, with handheld devices being the most prevalent form today. The most commonly used wireless handheld devices are laptop computers, text messaging devices, Personal Digital Assistants (PDA), and smart phones [48].

1.6 Benefits

WLANs offer four primary benefits:

- **User Mobility**—Users can access files, network resources, and the Internet without having to physically connect to the network with wires. Users can be mobile yet retain high-speed, real-time access to the enterprise LAN.

- **Rapid Installation**—The time required for installation is reduced because network connections can be made without moving or adding wires, or pulling them through walls or ceilings, or making modifications to the infrastructure cable plant. For example, WLANs are often cited as making LAN installations possible in buildings that are subject to historic preservation rules.

- **Flexibility**—Enterprises can also enjoy the flexibility of installing and taking down WLANs in locations as necessary. Users can quickly install a small WLAN for temporary needs such as a conference, trade show, or standards meeting.
• **Scalability**—WLAN network topologies can easily be configured to meet specific application and installation needs and to scale from small peer-to-peer networks to very large enterprise networks that enable roaming over a broad area.

1.7 WLAN Advantages

• Mobility that improves productivity with real-time access to information, regardless of user location, for faster and more efficient decision-making.

• Cost-effective network setup for hard-to-wire locations such as older buildings and solid-wall structures.

• Reduced cost of installation in dynamic environments requiring frequent modifications and WLANs liberate users from dependence on hard-wired access to the network backbone, giving them anytime, anywhere network access. This freedom to roam offers numerous user benefits for a variety of work environments, such as:
  
  o Immediate bedside access to patient information for doctors and hospital staff.
  
  o Easy, real-time network access for on-site consultants or auditors.
o Improved database access for roving supervisors such as production line managers, warehouse auditors, or construction engineers.

o Simplified network configuration with minimal involvement for temporary setups such as trade shows or conference rooms.

o Faster access to customer information for service vendors and retailers, resulting in better service and improved customer satisfaction.

o Real-time access to study group meetings and research links for students.

1.8 IEEE 802.11 Basics

The IEEE initiated the IEEE 802.11 project in 1990 with the objective to “develop a Medium Access Control (MAC) and Physical Layer (PHY) specification for wireless connectivity for fixed, portable, and moving stations within an area.”. In 1997, IEEE first approved the IEEE 802.11 international interoperability standard for WLANs. The IEEE 802.11 standard supports three transmission methods, including radio transmission within the 2.4 GHz ISM band [39]. In 1999, IEEE ratified two amendments to the IEEE 802.11 standard—IEEE 802.11a and IEEE 802.11b—that define radio transmission methods and modulation techniques.
WLAN equipment based on IEEE 802.11b quickly became the dominant wireless technology. IEEE 802.11b equipment transmits in the 2.4 GHz band, offering data rates of up to 11 Mbps. IEEE 802.11b was intended to provide performance, throughput, and security features comparable to wired LANs. IEEE 802.11a operates in the 5 GHz Unlicensed National Information Infrastructure (UNII) frequency band, delivering data rates up to 54 Mbps. In 2003, IEEE released the IEEE 802.11g amendment, which specifies a radio transmission method that also uses the 2.4 GHz Industrial, Scientific and Medical (ISM) band and can support data rates of up to 54 Mbps. In addition, IEEE 802.11g-compliant products are backward compatible with IEEE 802.11b-compliant products. With 802.11b, WLANs will be able to achieve wireless performance and throughput comparable to wired Ethernet. Outside of the standards bodies, wireless industry leaders have united to form the Wireless Ethernet Compatibility Alliance (WECA). WECA’s mission is to certify cross-vendor interoperability and compatibility of IEEE 802.11b wireless networking products and to promote that standard for the enterprise, the small business, and the home. Members include WLAN semiconductor manufacturers, WLAN providers, computer system vendors, and software makers—such as 3Com, Aironet, Apple, Breezeecom, Cabletron, Compaq, Dell, Fujitsu, IBM, Intersil, Lucent Technologies, No Wires Needed, Nokia, Samsung, Symbol Technologies, Wayport, and Zoom [1].

1.9 Frequency and Data Rates

IEEE developed the 802.11 standards to provide wireless networking technology like the wired Ethernet that has been available for many years. The IEEE 802.11a standard is the most widely adopted
member of the 802.11 WLAN family. It operates in the licensed 5 GHz band using Orthogonal Frequency Division Multiple Access (OFDM) technology. The popular 802.11b standard operates in the unlicensed 2.4 GHz–2.5 GHz Industrial, Scientific, and Medical (ISM) frequency band using a direct sequence spread-spectrum technology. The ISM band has become popular for wireless communications because it is available worldwide. The 802.11b WLAN technology permits transmission speeds of up to 11 Mbps. This makes it considerably faster than the original IEEE 802.11 standard (that sends data at up to 2 Mbps) and slightly faster than standard Ethernet [16].

1.10 WLAN Topology

IEEE 802.11 defines two pieces of equipment, a wireless station (STA), which is usually a PC equipped with a wireless Network Interface Card (NIC), and an Access Point (AP), which acts as a bridge between the wireless and wired networks. An access point usually consists of a radio, a wired network interface (e.g., 802.3), and bridging software conforming to the 802.1d bridging standard. The access point acts as the base station for the wireless network, aggregating access for multiple wireless stations onto the wired network[55].

The 802.11 standard defines two modes: infrastructure mode and ad hoc mode. In infrastructure mode, the wireless network consists of at least one Access Point (AP) connected to the wired network infrastructure and a set of wireless end stations (STA). This configuration is called a Basic Service Set (BSS) as shown in Figure 1-3. An Extended Service Set (ESS) is a set of two or more BSSs forming a single subnetwork. Since most corporate WLANs require access to the wired LAN for
services (file servers, printers, Internet links), they will operate in infrastructure mode.

![Diagram of an Infrastructure WLAN]

**Figure 1-3 An Infrastructure WLAN**

Infrastructure mode assumes the presence of one or more APs bridging the wireless media to the wired media. The AP handles station authentication and association to the wireless network. Multiple APs connected by a Distribution System (DS) can extend the range of the wireless network to a much larger area than can be covered by any one AP. In typical installations, the DS is simply the existing IP network infrastructure.
**Ad hoc mode** (also called peer-to-peer mode or an Independent Basic Service Set, or IBSS) is simply a set of 802.11 wireless stations that communicate directly with one another without using an access point or any connection to a wired network [12][22].

Figure 1-4  An Ad Hoc Network

An ad hoc network is usually one that exists for a limited time between two or more wireless devices that is not connected through an Access Point (AP) to a wired network as shown in Figure 1-4. For example, two laptop users wishing to share files could set up an ad hoc network using 802.11 compatible NICs and share files over the Wireless Medium (WM) without need for external media (e.g., floppy disks, flash cards)[11]. This mode is useful for quickly and easily setting up a wireless network anywhere, such as a hotel room, convention center, or airport, or where access to the wired network is barred (such as for consultants at a client
One of the key advantages of ad hoc WLANs is that theoretically they can be formed anytime and anywhere, allowing multiple users to create wireless connections cheaply, quickly, and easily with minimal hardware and user maintenance. In practice, a number of different types of ad hoc networks are possible, and the IEEE 802.11 specification allows many of them. An ad hoc network can be created for various reasons, such as supporting file sharing activities between two client devices. However, client devices operating solely in ad hoc mode cannot communicate with external wireless networks. A further complication is that an ad hoc network can interfere with the operation of an AP-based infrastructure mode network that exists within the same wireless space [67].

The use of multiple APs connected to a single DS allows for the creation of wireless networks of arbitrary size and complexity. In the IEEE 802.11 specification, a multi-BSS network is referred to as an Extended Service Set (ESS)[5]. Figure 1-5 conceptually depicts a network with both wired and wireless capabilities, similar to what would generally be deployed in an enterprise environment. It shows three APs with corresponding BSSs, which comprise an ESS. The ESS is attached to the wired enterprise network or DS, which, in turn, is connected to the Internet and other outside networks [3]. This architecture could permit various STAs, such as laptop computers and PDAs, to access network resources and the Internet. In addition, the use of an ESS provides the opportunity for IEEE 802.11 WLAN STAs to roam between APs while maintaining network connectivity.
1.11 WLAN Standards

In 1997, the LAN Standards Committee of the IEEE Computer Society, published 802.11, the first internationally sanctioned standard for wireless LANs [27]. The 1999 edition of the 802.11 standard defined the Physical Layer (PHY) and the Medium Access Control layer (MAC) for WLANs. It defined PHYs for 1 and 2 Mb/s data rates in the unlicensed 2.4-GHz radio frequency (RF) band. The 802.11 standard has specified the PHYs shown in Table 1-1.
<table>
<thead>
<tr>
<th>IEEE 802.11 Specifications</th>
<th>Maximum data rate</th>
<th>RF</th>
<th>Functional Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11</td>
<td>2 Mbps</td>
<td>2.4 GHz (ISM)</td>
<td>Legacy technology that is minimally used</td>
</tr>
<tr>
<td>802.11a</td>
<td>54 Mbps</td>
<td>5 GHz (UNII)</td>
<td>Not compatible with IEEE 802.11b or IEEE 802.11g. Provides better than 10Base-T Ethernet speeds</td>
</tr>
<tr>
<td>802.11b</td>
<td>11 Mbps</td>
<td>2.4 GHz (ISM)</td>
<td>Equipment based on IEEE 802.11b has been the dominant WLAN technology. Provides close to 10Base-T Ethernet speeds. Is generally combined with IEEE 802.11g as product offerings as IEEE 802.11b/g</td>
</tr>
<tr>
<td>802.11g</td>
<td>54 Mbps</td>
<td>2.4 GHz (ISM)</td>
<td>Backward compatible with IEEE 802.11b. Provides better than 10Base-T Ethernet speeds. Supported by most current WLAN products</td>
</tr>
<tr>
<td>802.11n</td>
<td>300 Mbps</td>
<td>2.4 GHz (ISM), 5 GHz (UNII)</td>
<td>Backward compatible with IEEE 802.11a/b/g. Provides better than 10Base-T Ethernet speeds</td>
</tr>
</tbody>
</table>

Table 1-1 Comparison of 802.11 PHYs.

1.12 ISO OSI Reference Model For WLAN

The Physical Layer defines how data is transmitted over the physical medium. The IEEE assigned 802.11 two transmission methods for radio frequency (RF) and one for Infrared. The two RF methods are Frequency Hopping Spread-Spectrum (FHSS) and Direct Sequence
Spread-Spectrum (DSSS). These transmission methods operate within the Industrial, Scientific, and Medical band (ISM) 2.4 GHz band for unlicensed usage.

Figure 1-6 shows a graphical representation of how the IEEE 802.11 protocol layers map to the OSI seven layer model. As with traditional wired Ethernet networks based on the IEEE 802.3 standard, the Data Link Layer is subdivided into the Logical Link Control (LLC) and Media Access Control (MAC) sub layers. An existing IEEE 802 series protocol, 802.2, was adopted for use with WLAN networks for the LLC layer. A new MAC sub layer for 802.11 was then developed, based on Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) channel access methods [17]. The 802.11 MAC serves as a single, common interface to the Physical Layer (PHY) protocols below it [65][15].

The PHY layer is responsible for the actual Radio Frequency (RF) transmission and defines the frequencies and the modulation methods used. It is worth noting that the very first PHY developed, the original 802.11 PHY, suffered from low throughput and interoperability problems and was not widely adopted. Subsequent PHY standards (802.11a/b/g) based on better modulation techniques and higher throughput were developed to address the problem and are now in wide use. Although the initial problems with the original 802.11 Physical Layer specification delayed the wide-spread adoption of WLANs, it did spur the creation of the Wireless Ethernet Compatibility Alliance (WECA), an industry group devoted to the certification of 802.11 products for standards compliance and interoperability with other WLAN products. WECA brands compliant WLAN products with the “Wi-Fi” (for Wireless
*Fidelity* label, so WLAN networks are often referred to as **Wi-Fi** networks [9].

![OSI/ISO Network Model for WLAN](image)

The Data Link layer is made up of two sub-layers, as shown in the Figure 1-7, the Media Access Control (MAC) layer and the Logical Link Control (LLC) layer [28]. The Data Link layer determines how transmitted data is packaged, addressed and managed within the network. The LLC layer uses the identical 48-bit addressing found in other 802 LAN networks like Ethernet where the MAC layer uses a unique mechanism called Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA). This mechanism is similar to the Carrier Sense Multiple Access/Collision Detect (CSMA/CD) used in Ethernet, with a few major
differences [25]. While the 802.3 Ethernet MAC is essentially Carrier Sense Multiple Access/Collision Detection (CSMA/CD), the 802.11 MAC is Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA).

The reason for this difference is that there is no practical way to both transmit and receive at the same time on the wireless medium. Opposed to Ethernet, which sends out a signal until a collision is detected before a resend, CSMA/CA senses the airwaves for activity and sends out a signal when the airwaves are free[64][75]. If the sender detects conflicting signals, it will wait for a random period before retrying. This technique is called "listening before talking" (LBT).

1.13 WLAN Security

Security technologies should be implemented to solve the authentication problem and to preserve the privacy and integrity of data transmitted on air. WLAN standards cannot provide end-to-end security because they are only used for the wireless link between the AP and STA as shown in Figure 1-7.
The requirements of wireless security can fall into two categories.

1. Encryption and Data Privacy – The aim of encryption is to provide a mechanism to provide data privacy and integrity. The data should not be decrypted by any unauthorized means. All transmitted packets should be originated from the senders. The security mechanism should enforce the integrity of data under any circumstances.

2. Authentication and Access Control – Authentication should be mutual, enabling wireless device clients and access points to authenticate each other. A framework should be introduced in order to facilitate the transmission of authentication messages between clients, access points.
and authentication servers. From the perspectives of access points, a mechanism should be introduced to validate client credentials in order to grant right level of access to the requested clients [8][29].

### 1.14 Threats and Vulnerabilities

Figure 1-8 provides a general taxonomy of security attacks to help organizations and users understand some of the attacks against WLANs.

Network security attacks are typically divided into *passive* and *active* attacks. These two broad classes are then subdivided into other types of attacks [30][61].
1.14.1 **Passive Attack**—An attack in which an unauthorized party gains access to an asset and does not modify its content (i.e., eavesdropping). Passive attacks can be either eavesdropping or traffic analysis (sometimes called traffic flow analysis). These two passive attacks are described below.

**Eavesdropping**—The attacker monitors transmissions for message content. An example of this attack is a person listening into the transmissions on a LAN between two workstations or tuning into transmissions between a wireless handset and a base station.

**Traffic analysis**—The attacker, in a more subtle way, gains intelligence by monitoring the transmissions for patterns of communication. A considerable amount of information is contained in the flow of messages between communicating parties.

1.14.2 **Active Attack**—An attack whereby an unauthorized party makes modifications to a message, data stream, or file. It is possible to detect this type of attack but it may not be preventable. Active attacks may take the form of one of four types: Masquerading, Replay, Message modification, and Denial-Of-Service (DoS). These attacks are defined below.

**Masquerading**—The attacker impersonates an authorized user and thereby gains certain unauthorized privileges.

**Replay**—The attacker monitors transmissions (passive attack) and retransmits messages as the legitimate user.
**Message modification**—The attacker alters a legitimate message by deleting, adding to, changing, or reordering it.

**Denial-of-service**—The attacker prevents or prohibits the normal use or management of communications facilities.

The risks associated with 802.11 are the result of one or more of these attacks. The consequences of these attacks include, but are not limited to, loss of proprietary information, legal and recovery costs, tarnished image, and loss of network service[47]. As the number of organizations that deploy wireless networks continues to grow, it becomes even more important to understand the types of vulnerabilities and threats facing legacy IEEE 802.11 WLANs and implement appropriate security measures. Some of the vulnerabilities that are described are inherent in the legacy IEEE 802.11 WLAN standard, while others are relevant to WLANs or wireless networking in general.

### 1.14.3 Loss of Confidentiality

Because of the broadcast and radio nature of wireless technology, ensuring confidentiality is significantly more difficult in a wireless network than a wired network. Traditional wired networks provide inherent security through the use of a physical medium to which an attacker needs to gain access. Wireless networks propagate signals into space, making traditional physical security countermeasures less effective and access to the network much easier, increasing the importance of adequate confidentiality on wireless networks.
Passive eavesdropping on legacy IEEE 802.11 WLAN communications may cause significant risk to an organization. An adversary can scan RF signals and capture data traversing the wireless medium. Sensitive information, including proprietary information, network IDs and passwords, and configuration data, are some examples of data that may be captured. In addition, attackers with high-gain antennas can capture data from wireless networks beyond a network’s normal operating range, again making confidentiality a critical security measure.

Eavesdropping performed with a wireless network analyzer tool or sniffer is particularly easy for legacy IEEE 802.11 WLANs. Sniffers can take advantage of flaws in the key-scheduling algorithm that was provided for the implementation of RC4 used by WEP. To exploit these weaknesses, the sniffer passively monitors the WLAN and computes the encryption keys after a variable number of packets have been sniffed. On a highly saturated network, collecting the amount of data required to compute the WEP keys only takes several hours; if traffic volume is low, it may take up to one day. For example, a busy AP that is transmitting 3,000 bytes at 11 Mbps will exhaust the 24-bit IV space after approximately 10 hours. Once the attacker recovers two cipher texts that have used the same IV, both data integrity and confidentiality may be easily compromised.

Another risk to WLANs is loss of confidentiality through simple eavesdropping on broadcast traffic. Ethernet hubs generally broadcast network traffic to all physical interfaces and connected devices, which leaves the broadcasted traffic vulnerable to unauthorized monitoring. For example, an AP connected to a port on an Ethernet hub that is broadcasting data traffic would broadcast all of the data traffic it received
on its wired interface over its wireless interface. The use of the Ethernet hub infrastructure increases the risk that the AP may be broadcasting proprietary or sensitive data that was transmitted through the hub. Switches alleviate this concern by providing dedicated channels between communication devices [41].

A malicious or irresponsible user could surreptitiously physically insert a rogue AP into a closet, under a conference room table, or in any other hidden area within a building. The rogue AP could then be used to allow unauthorized individuals to gain access to an enterprise network. As long as its location is in close proximity to the users of the WLAN, and it is configured to appear as a legitimate AP to wireless clients, the rogue AP may successfully convince wireless clients of its legitimacy and cause wireless clients to connect and transmit traffic to the rogue AP.

In this scenario, an attacker can easily capture all of the data transmitted through the rogue AP, bypassing all wireless protocol confidentiality. It is also important to note that not all rogue APs are deployed by malicious users. In many cases, rogue APs are deployed by users who want to take advantage of wireless technology without the approval of the IT department. These APs are often deployed without proper security configurations and pose significant security risks.

1.14.4 Loss of Integrity

Data integrity issues in wireless networks are similar to those in wired networks. Because organizations frequently implement wireless and wired communications without adequate cryptographic protection of data, integrity can be difficult to achieve. For example, an attacker can
compromise data integrity by deleting or modifying the data in an email via the wireless system. This can be detrimental to an organization if important email is widely distributed among email recipients. Because the security features of the legacy IEEE 802.11 standard do not provide strong message integrity, other kinds of active attacks that compromise system integrity are possible.

1.14.5 Loss of Availability

A denial of WLAN availability often involves some form of DoS attack, such as jamming or flooding. Jamming occurs when an RF signal emitted from a wireless device overwhelms other wireless devices and signals, causing a loss of communications. Jamming may be caused deliberately by a malicious user or caused inadvertently by emissions from other legitimate devices operating within unlicensed spectrum, such as a cordless telephone or microwave oven. Flooding attacks are initiated using software designed to transmit a large number of packets to an AP or other wireless device, causing the device to be overwhelmed by packets and cease normal operation. Flooding can cause a WLAN to degrade to an unacceptable performance level or even fail completely. Jamming and flooding threats are difficult to counter in any radio-based communications, and the legacy IEEE 802.11 standard does not provide any defense against them.

IEEE 802.11 management frames provide another vector for DoS attacks against WLANs. Management frames govern the process of associating and disassociating APs and STAs from a WLAN. By design, the IEEE 802.11 standard does not provide protection against these attacks. If an adversary forges a disassociation frame and sends it to an AP or STA, the targeted device will grant the request and close its
communications association. Another type of attack, known as an association attack, targets an AP’s association table, which monitors the state of STAs associated with the AP. An association attack typically floods this table with false requests until the AP no longer allows legitimate associations. More advanced association attacks can force STAs to connect to false APs where the victim is subject to a variety of malicious attacks.

Users can also cause a loss of unavailability by unintentionally monopolizing the capacity of a WLAN, such as downloading large files, effectively denying other users access to the network [44][51].

1.15 WLAN Security attacks

Broadly, security concerns in the WLAN world are classified into physical and logical. There are many security threats and attacks that can damage the security of WLANs. Those attacks can be classified into logical attacks and physical attacks.

1.15.1 Logical Attacks

MAC Address Spoofing: MAC addresses are sent in the clear when a communication between STAs and AP takes place. A way to secure access to APs and hence to the network is done to deny other users from listening to the communication. Integrity means preserving the accurateness and the correctness of information transmitted between STAs and AP. Any security solution should achieve these three goals together. The security and management problem become huge as more APs are installed in the network. So there is a need to centralize and manage security issues in small WLANs as well as large ones and a need
to develop techniques to counter security threats. As WLANs applications like wireless Internet and wireless e-commerce spread very fast, there is a need to assure the security of such applications.

**Attacks on WEP:** Wired Equivalent Privacy (WEP) is a security protocol based on encryption algorithm called "RC4" that aims to provide security to the WLAN similar to the security provided in the wired LAN. WEP has many drawbacks like the usage of small Initialization Vector (IV) and short RC4 encryption key as well as using XOR operation to cipher the key with the plain text to generate cipher text [71]. Sending the MAC addresses and the IV in the clear in addition to the frequent use of a single IV and the fact that secret keys are actually shared between communications parties are WEPs major security problems.

**Denial of Service attack:** Denial of Service attacks or DoS is a serious threat on both wired and wireless networks. This attack aims to disable the availability of the network and the services it provides. In WLANs, DoS is conducted in several ways like interfering the frequency spectrum by external RF sources hence denying access to the WLAN or, in best cases, granting access with lower data rates[72].

**Man-in-the-middle attack:** This is a famous attack in both wired and wireless networks. An illicit STA intercepts the communication between legitimate STAs and the AP. The illegal STA fools the AP and pretends to be a legitimate STA; on the other hand, it also fools the other end STA and pretends to be trusted AP. The Figure 1-9 shows Man-in-Middle attack.
Figure 1-9 Representation of Man-in-Middle attack

**Bad network design:** WLANs function as an extension to the wired LAN hence the security of the LAN depends highly on the security of the WLAN. The vulnerability of WLANs means that the wired LAN is directly on risk. A proper WLAN design should be implemented by trying to separate the WLAN from the wired LAN by placing the WLAN in the Demilitarized Zone (DMZ) with firewalls, switches and any additional access control technology to limit the access to the WLAN. Also dedicating specific subnets for WLAN than the once used for wired LAN could help in limiting security breaches. Careful wired and wireless LAN network design plays important role to secure access to the WLAN.

**Default AP configurations:** Most APs are shipped with minimum or no security configuration by default. This is true because shipping them with all security features enabled will make usage and operation difficult for normal users. The aim of AP suppliers is to deliver high data rate, out of the box installation APs without sincere commitment to security. Network security administrators should configure these AP according to the organizations security policy. Some of the default unsecured setting in
APs shipped today are default passwords which happens to be weak or blank[70].

SSID: Service Set Identifier (SSID) is the name given to a certain WLAN and it is announced by the AP, the knowledge of SSID is important and works like the first security defense. Unfortunately, by default, some APs disable SSID request which means users can access the WLAN without proving the knowledge of SSID. On the other hand, some APs don't disable SSID request, in fact the SSID request is enabled but the SSID name itself is broadcasted in the air. This is another security problem because it advertises the existence of the WLAN. SSID requests should be enabled and SSID names shouldn't be broadcasted so users have to prove the knowledge of WLAN's SSID prior establishing communication.

1.15.2 Physical attacks

Rogue Access Points: In normal situations, AP authenticates STAs to grant access to the WLAN. The AP is never asked for authentication, if the AP is installed without IT center's awareness. These APs are called "Rogue APs" and they form a security hole in the network. An attacker can install a Rogue AP with security features disabled causing a mass security threat. There is a need for mutual authentication between STAs and APs to ensure that both parties are legitimate. Network security administrators can discover Rogue APs by using wireless analyzing tools to search and audit the network.

Physical placement of APs: The installation location of APs is another security issue because placing APs inappropriately will expose it to physical attacks. Attackers can easily reset the APs once found causing
the AP to switch to its default settings which is totally insecure. It is very important for network security administrators to carefully choose appropriate places to mount APs [38][43].

**AP's coverage:** The main difference between WLANs and wired/fixed LANs is that WLANs relies on Radio Frequency (RF) signals as a communication medium. The signals broadcasted by the AP can propagate outside the perimeter of a room or a building, where an AP is placed, allowing users who are not physically in the building to gain access to the network. Attackers use special equipments and sniffing tools to find available WLANs and eavesdrop live communications while driving a car or roaming around. Because RF signals obey no boundaries, attackers outside a building can receive such signals and launch attacks on the WLAN. This kind of attack is called "war driving". Publicly available tools are used for war driving like Net Stumbler. Hobbyists also chalk buildings to indicate that signals are broadcasted from the building and the WLAN can be easily accessed. This marking is called "war chalking". In War chalking, information about the speed of the connection and whether the authentication scheme used is open or shared keys are mentioned in the form of special codes agreed upon between war-chalkers [46][54].

### 1.16 PROBLEM SPECIFICATION

As the number of organizations that deploy wireless networks continues to grow, it becomes even more important to understand the types of vulnerabilities and threats facing legacy IEEE 802.11 WLANs and implement appropriate security measures. To access a WLAN in a shared key authentication scheme, both mobile station and AP should have the
correct shared secret key; this key is used to encrypt confidential information. 40-bit key is the default key size shipped with WLAN products. An Initialization Vector (IV), typically 24-bit, is being reused multiple numbers of times. So wireless network system needs efficient mechanism to provide fresh encryption and integrity keys, undoing the threat of attacks stemming from key reuse.

1.17 OBJECTIVE OF THE THESIS

The IEEE 802.11 standard has several methods of encryption and authentication that provide varying levels of security for wireless networks. Authentication provides a method for wireless networks to verify the identity of a user and ensure they are authorized access to the network before being connected. Without proper authentication a wireless client will not be able to associate with a wireless access point and therefore will be unable to gain access to network resources.

The Wired Equivalent privacy (WEP) protocol is used in 802.11-based WLANs. It is used to secure communications between APs and wireless Stations(STAs) and to provide secured authentication schemes. The aim was to provide security to the WLAN similar to the security provided in the wired LAN. It is based on a stream cipher encryption algorithm RC4. WEP is used to control access to the WLAN and to encrypt confidential information.

To access a WLAN in a shared key authentication scheme, both STA and AP should have the correct shared secret key; this key is used to encrypt confidential information. The length of this key is 40-bits; this is
a very short key length. The main drawback of WEP is the use of this 40-bit key even though RC4 encryption algorithm can support up to 104 bit key but 40-bit key is the default key size shipped with WLAN products. Another problem with WEP is the use of a short Initialization Vector (IV), typically 24-bit, and it is being reused multiple numbers of times. The WEP encryption key, also called as key stream, is generated from the concatenation of the short shared secret 40-bits key and 24-bit IV. The 64-bit WEP encryption key stream and the 40-bit shared secret keys are the secret elements in the security system. Due to the short shared key length (40-bits), the frequent reuse of this key, short IV length, and again the frequent reuse of IV value, the generated WEP encryption key stream repeats itself after a period of time which means that the cipher text generated by this key stream is easily breakable.

The IEEE 802.11 specification does not, unfortunately, identify any means for key management. Therefore, generating, distributing, storing, loading, escrowing, archiving, auditing, and destroying the material is left to those deploying WLANs. Key management is not properly specified in 802.11 specifications. As a result, many vulnerabilities could be introduced into the WLAN environment. These vulnerabilities include WEP keys that are non-unique, never changing, factory-defaults, or weak keys (all zeros, all ones, based on easily guessed passwords, or other similar trivial patterns).

Key management was not part of the original 802.11 specification. If an enterprise recognizes the need to change keys often and to make them random, the task is formidable in a large WLAN environment. For example, a large campus may have as many as 15,000 APs. Generating,
distributing, loading, and managing keys for an environment of this size is a significant challenge.

In WEP, there is no solid key distribution policy and a single key is reused frequently. Moreover, if every station uses the same key, a large amount of traffic may be rapidly available to an eavesdropper for analytic attacks. This problem will not only make the AP vulnerable to attacks but it will make all other APs and STAs vulnerable as well. Even worse, key distribution is static by default which means all STAs have to have the key entered manually and when the key compromised, all STAs have to revoke it and use a new key. Generally, WEP lacks key management and distribution system.

Temporal Key Integrity Protocol (TKIP) is developed to address the vulnerabilities associated with WEP and developed to provide backwards compatibility with WEP to prevent the need to replace all hardware that only supported WEP. TKIP supports a re keying mechanism, to provide fresh encryption and integrity keys, undoing the threat of attacks stemming from key reuse. It creates a new key for each packet significantly reducing the possibility of guessing a key.

This research’s main objective is to enhance key mixing mechanisms in TKIP through transmission rate from Physical Layer Convergence Protocol (PLCP) to generate various pattern of key streams in order to avoid key reuse which is vital security flaw amongst various security flaws.
1.18 RESEARCH CONTRIBUTION

Millions of WEP-based devices, have already shipped and deployed. It is also not cheaper to replace the hardware as an entire unit. This implies that WEP patches operating on already-deployed 802.11 hardware will, of necessity, rely entirely on software upgrade. The main role of proposed mechanism is:

“Signal field (Transmission Bit rate) from Physical Layer Convergence Protocol (PLCP) frame of physical Layer is assigned to IV field of TKIP frame of Data Link Layer” during the time of encryption which enhances

a) rekeying mechanism, to provide fresh encryption and integrity keys, undoing the threat of attacks stemming from key reuse.

b) per-packet key mixing function, to de-correlate the public IVs from weak keys.

This proposed methodology is developed to provide backward compatibility with WEP to prevent the need to replace all hardware.

1.19 ORGANIZATION OF THE THESIS

The chapters of the thesis are organized as follows:

The Chapter 1 introduces WLAN, security, threats, vulnerabilities, and objectives of the Thesis. The Chapter 2 describes previous work on various security flaws, frame of Physical Layer. The Chapter 3
explains proposed methodology and its architectural model for enhancement to TKIP key mixing through Transmission rate from PLCP. Chapter 4 outlines Implementation Methods. Chapter 5 shows pattern of various key streams generated and analysis of Key streams. Chapter 6 contains the conclusion of the thesis. Chapter 7 indicates future work and enhancement. Annexure for specification of NETGEAR WG 102 PROSAFE 802.11 WIRELESS ACCESS POINT and glossary of terms is appended.

1.20 SUMMARY

This chapter focuses on various security threats and vulnerabilities in wireless local area environment and describes role of this thesis.