**Available Online at www.ijcsmc.com**

**International Journal of Computer Science and Mobile Computing**

**A Monthly Journal of Computer Science and Information Technology**

**ISSN 2320–088X**

*IJCSMC, Vol. 3, Issue. 1, January 2014, pg.53 – 68*

**SURVEY ARTICLE**

# A SURVEY OF WIRELESS NETWORK SECURITY

**S. Gopalakrishnan**
Assistant Professor, Department of ECE, PSNA college of Engineering and Technology, Dindigul, Tamil Nadu, India
lapog.gopal@gmail.com

## ABSTRACT

Wireless networking is inherently insecure. From jamming to eavesdropping, from man-in the middle to spoofing, there are a variety of attack methods that can be used against the users of wireless networks. Modern wireless data networks use a variety of cryptographic techniques such as encryption and authentication to provide barriers to such infiltrations. However, much of the commonly used security precautions are woefully inadequate. They seem to detract the casual sniffer, but are unable to stop the powerful adversary. In this article, we look into the technology and the security schemes in IEEE 802.11, cellular and Bluetooth wireless transport protocols. We conclude that the only reliable security measure for such networks is one hat is based on application level security such as using a VPN.The wireless communication technology also acquires various types of security threats. This paper discusses a wide variety of attacks in WSN and their classification mechanisms and different securities available to handle them including the challenges faced.

Keywords- Wireless Sensor Network; Security Goal; Security Attacks; Defensive mechanisms; Challenges

## INTRODUCTION

Wireless technologies, in the simplest sense, enable one or more devices to communicate without physical connections without requiring network or peripheral cabling. Wireless technologies use radio frequency transmissions as the means for transmitting data, whereas wired technologies use cables. Wireless technologies range from complex systems, such as Wireless Local Area Networks (WLAN) and cell phones to simple devices such as wireless headphones, microphones, and other devices that do not process or store information. They also include infrared (IR) devices such as remote controls, some cordless computer keyboards and mice, and wireless hi-fi stereo headsets, all of which require a direct line of sight between the transmitter and the receiver to close the link.

## WIRELESS NETWORKS

Wireless networks serve as the transport mechanism between devices and among devices and the traditional wired networks (enterprise networks and the Internet). Wireless networks are many and diverse but are frequently categorized into three groups based on their coverage range: Wireless Wide Area Networks (WWAN), WLANs, and Wireless Personal Area Networks (WPAN). WWAN includes wide coverage area technologies such as 2G cellular, Cellular Digital Packet Data (CDPD) and Global System for Mobile Communications (GSM), and Mobitex. WLAN, representing wireless local area networks, includes 802.11, HiperLAN, and several others. WPAN represents wireless personal area network technologies such as Bluetooth and IR. All of these technologies are “tether less”—they receive and transmit information using electromagnetic (EM) waves. Wireless technologies use wavelengths ranging from the radio frequency (RF) band up to and above the IR band. The frequencies in the RF band cover a significant portion of the EM radiation spectrum, extending from 9 kilohertz (kHz), the lowest allocated wireless communications frequency, to thousands of gigahertz (GHz). As the frequency is increased beyond the RF spectrum, EM energy moves into the IR and then the visible spectrum. Wireless networks allow devices to be moved about with varying degrees of freedom and still maintain communication with each other. They also offer greater flexibility than cabled networks and significantly reduce the time and resources needed to set up new networks and allow for ad hoc networks to be easily created, modified or torn down. There are many forms of wireless networks. One way of categorizing wireless networks is to consider the relative range and complexity of each type of network. For example:

**WIRELESS PERSONAL AREA NETWORK (WPAN) –** a small-scale wireless network that requires little or no infrastructure and operates within a short range. A WPAN is typically used by a few devices in a single room instead of connecting the devices with cables. Examples include print services or enabling a wireless keyboard or mouse to communicate with a computer.

**WIRELESS LOCAL AREA NETWORKS (WLANS)** are groups of wireless networking nodes within a limited geographic area, such as an office building or campus, that are capable of radio communications. WLANs are usually implemented as extensions to existing wired local area networks to provide enhanced user mobility.

**WIRELESS METROPOLITAN AREA NETWORKS (WMANS)** can provide connectivity to users located in multiple facilities generally within a few miles of each other. Many WMAN implementations provide wireless broadband access to customers in metropolitan areas.

**WIRELESS WIDE AREA NETWORKS (WWANS)** connect individuals and devices over large geographic areas. WWANs are typically used for mobile voice and data communications, as well as satellite communications.

**WIRELESS LAN:**

WLANs allow greater flexibility and portability than do traditional wired local area networks (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 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.

**AD HOC NETWORKS:**

Ad hoc networks such as Bluetooth are networks designed to dynamically connect remote devices such as cell phones, laptops, and PDAs. These networks are termed "ad hoc" because of their shifting network topologies. Whereas WLANs use a fixed network infrastructure, ad hoc networks maintain random network configurations, relying on a master-slave system connected by wireless links to enable devices to communicate. In a Bluetooth network, the master of the piconet controls the changing network topologies of these networks. It also controls the flow of data between devices that are capable of supporting direct links to each other. As devices move about in an unpredictable fashion, these networks must be reconfigured on the fly to handle the dynamic topology. The routing that protocol Bluetooth employs allows the master to establish and maintain these shifting networks.

**LAYERED SECURITY FOR WIRELESS NETWORKS:**

A layered approach to wireless security can provide a high degree of protection and leverage existing network security investments. The layered approach consists of the following four levels: [1]

- Wireless deployment and policy
- Wireless access control
- Perimeter security
- Application security

When implemented, as discussed below, the layered approach can make a WLAN more secure than a typical wired network by centralizing points of access, implementing manageable device-level security and governing internal access with firewall-level

policies. Security professionals speak in terms of work factor, which is an important concept when implementing layered security. A network with a high work factor is difficult to break into, while a network with a low work factor can be compromised more easily. If hackers determine that the network has a high work factor, which is inherent in the layered approach, they will soon move on to those that are less secure.

**LEVEL1-WIRELESS DEPLOYMENT AND POLICY**

Best practices for wireless deployment and policy are:

Deploy the minimum number of WAPs needed for adequate Coverage. Set WAP broadcast power to the lowest practical level.

- Verify broadcast coverage in and around facility.

Maintain policies for:

- Installation of WAPs
- NIC operational mode
- WLAN user-group access, including employees, visitors
- Contractors

The physical deployment of wireless networking devices is the foundation on which a secure environment is created. The basic rule of thumb maintains that one does not over design the wireless network. The goal is to avoid broadcasting where it is not necessary. When designing the network, consider who is accessing the WLAN, where they are located and what the minimum coverage requirements are. Using common sense is also helpful. For example, four WAPs should not be installed in a space where one would suffice or in areas that do not need access to the network, such as the building entrance waiting room. More is not necessarily better. Wireless NICs can be set to one of two operational modes—infrastructure mode, which allows the NIC to communicate only with a WAP, and ad hoc mode, which allows the NIC to communicate with any wireless device, such as other NICs. A policy should exist requiring NICs to operate in infrastructure mode only. Devices in *ad hoc* mode can be readily exploited by hackers.

**LEVEL 2—WIRELESS ACCESS CONTROL**

Best practices for wireless access control include:

- Configure the WEP for the highest level of encryption.
- Change the SSID regularly, where practical.
- Do not broadcast the SSID.
- Verify the media access control (MAC) address upon device connection.
- Maintain and enforce access policies for unauthorized/unrecognized devices.

In practice, access control has two components: device access control and user authentication (personnel access control). Level two is concerned with device access, while user authentication is addressed in level three, perimeter security. It is crucial that the security measures, such as WEP and SSID that are built into wireless network devices are properly configured and managed. The WAP must be configured not to Broadcast the SSID, and the SSID should be changed regularly, if practical. Also, the WEP should be set to the highest level of encryption (typically 128- or 256-bit encryption), and the pass

phrase should be changed regularly, which may or may not be practical depending on the size of the network.

**LEVEL 3-PERIMETER SECURITY**

Best practices for perimeter security include:

- Install an intrusion prevention system (IPS) and wireless firewall on WLAN.
- Encrypt WLAN traffic using a virtual private network (VPN).
- Direct all traffic through the VPN server and configure clients appropriately.
- Maintain and enforce VPN routing and access policies.
- Maintain and enforce access policies for user authentication (i.e, username/password).

VPN technology provides a method for securing traffic that moves across entrusted network segments, such as the Internet or the WLAN. A VPN is essentially an extension of a private network that encompasses encapsulated, encrypted and authenticated connections. VPN encryption algorithms are Complex and extremely difficult to compromise. VPN connections should be required for all WLAN traffic. Implementing VPN for a wireless network entails deploying a VPN server on the network and configuring all WLAN clients to communicate through a VPN tunnel terminated on this server.

**LEVEL-4-APPLICATION SECURITY**

Best practices for application security include:

- Implement an application-level user authentication system.
- Maintain and enforce permissions and password policies.
- Install vendor patches as they become available.

Activating basic security measures at the application level on the network is a recommended best practice, irrespective of the wired/wireless nature of connectivity. Protecting network applications, such as Windows NT, People soft and other enterprise systems, with rigorous password policies and Permissions provide one final hurdle that hackers must overcome to gain access to the proprietary information. It is imperative to install application patches as they are released. Patches frequently address known security vulnerabilities. Most network breaches exploit such vulnerabilities and are the primary reason signature-based IPSs are an indispensable component of a comprehensive network security program.

**IEEE 802.11 STANDARD OR WIRED EQUIVALENT PRIVACY (WEP)**

The 802.11 standard provides a number of options for authentication. Here we discuss the two that provide the most protection from unauthorized users.

## CLOSED SYSTEM AUTHENTICATION (SERVICE SET IDENTIFIER (SSID))

This is the most basic security authentication mechanism for 802.11 networks. The SSID can be used as a shared secret; however, as a security mechanism it is virtually worthless. In its most secure configuration the access point will not respond to probe requests. This gives the illusion of maintaining the SSID as a shared secret. In reality, the SSID is transmitted unencrypted. An attacker can use passive eavesdropping to discover the SSID, or if she is impatient, she can use an active attack. To actively attack a WLAN using SSID as a shared secret the attacker sends a forged disassociates message to the target and then eavesdrops as the target automatically begins to reassociate with an authentication transaction. There is some indication that some administrators have used this in an attempt to restrict unauthorized users but it is only effective against the most unskilled attacker.

## MEDIA ACCESS CARD (MAC) ACCESS LIST

Access Points can be programmed to allow access to the WLAN by MAC address. This security mechanism is designed to deny access to all clients except those explicitly authorized to use the WLAN. The effort required to implement and maintain access lists is large. This mechanism does not scale well and is only useful for small WLANs. Access Lists can easily be defeated by an attacker with minimal tools. It provides no protection from the insider, who is an authorized user of the network. An outsider who obtains a wireless network access card (WNIC) that is authorized entry into the WLAN is effectively an insider. An outsider can also sniff the traffic between the AP and the client collecting a valid MAC address. She can then craft packets with a forged MAC address for easy access to the WLAN. Although not a scalable security measure, this mechanism will stop an attacker without any specialized attack tools. It effectively raises the bar, albeit only a small amount, and therefore meets the Blazing Saddles Principle described earlier.

## SHARED RC4 KEY AUTHENTICATION

WEP's implementation of shared RC4 Authentication does not offer a high degree of security. Defeating WEP authentication has been published by both Borisov et. al. and Arbaugh et al. An attacker that intercepts a single authentication sequence can then authenticate into the WLAN at will using this key. Many WLANs employ a single key for all users. Regardless, WEP only allows for four total keys, making this vulnerability serious.

## IEEE 802.11 STANDARDS OR WEP.

WEP is a layer 2 encryption scheme based on the RC4 stream cipher. It relies on a secret key that is shared by the client and server. WEP uses a non cryptographic checksum of the plaintext to insure integrity. The plaintext and the checksum are encrypted using an initialization vector, the secret key and the RC4 algorithm. The initialization vector and the encrypted payload are then sent to the recipient. WEP 40 bit key size can be attacked by brute force. The 104 bit keys are not currently vulnerable to brute force attacks but regardless of key size WEP is vulnerable to both passive and active eavesdropping. WEP

encryption can be defeated passively when the key stream is reused. Because the WEP initialization Vector (IV) is only 24 bits, reuse can occur quite frequently even in a well implemented version of WEP.

## WIRELESS NETWORK COMPONENTS AND ARCHITECTURAL MODELS

IEEE 802.11 has two fundamental architectural components, as follows:

**STATION (STA).** A STA is a wireless endpoint device, also called a client device. STAs enable end users to gain access and utilize resources provided by wireless networks. Examples include laptop computers, personal digital assistants, mobile phones and other consumer electronic devices with IEEE 802.11 capabilities.

**ACCESS POINT (AP).** An AP logically connects STAs with a distribution system (DS), which is typically an organization's wired network. APs can also logically connect wireless STA with each other without accessing a distribution system. Wireless APs provide users with a mobile capability by allowing users to freely move within an APs coverage area while maintaining connectivity between the user's client device and the AP. APs can also be linked together using wired infrastructure to allow users to "roam" between APs within a building or campus. The IEEE 802.11 standard also defines the following two WLAN design structures or configurations, as follows:

**AD HOC MODE.** The ad hoc mode does not use APs. Ad hoc mode is sometimes referred to as infrastructure less because only peer-to-peer STAs are involved in the communications. This mode of operation is possible when two or more STAs are able to communicate directly to one another. Examples are laptops, mobile phones, PDAs, printers and scanners being able to communicate with each other without an AP. One of the key advantages of ad hoc WLANs is that theoretically they can be formed any time and anywhere, allowing multiple users to create wireless connections cheaply, quickly, and easily with minimal hardware and user maintenance. However, an ad hoc WLAN cannot communicate with external 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.

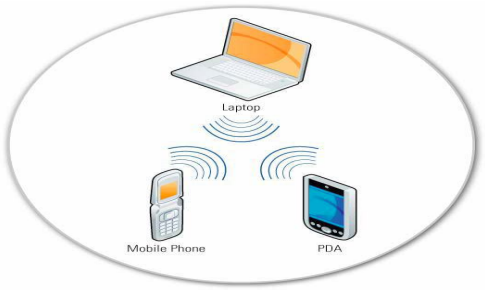



Figure-1:IEEE 802.11 Ad Hoc Mode Architecture

**INFRASTRUCTURE MODE.** In infrastructure mode,[2] an AP logically connects STAs to each other or to a distribution system (DS), which is typically an organization's wired network. The DS is the means by which STAs can communicate with the organization's wired LANs and external networks such as the Internet. Infrastructure mode is the most commonly used mode for WLANs. [2]

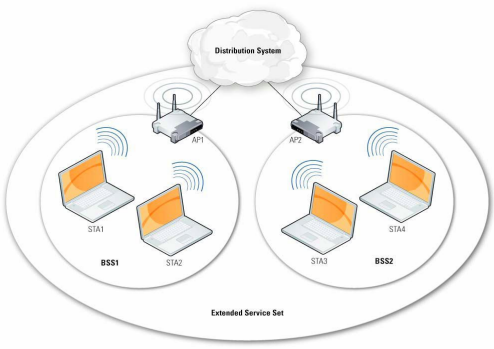



Figure-2:IEEE 802.11 Infrastructure Mode.

**802.11 ARCHITECTURE**

The IEEE 802.11 standard permits devices to establish either peer-to-peer (P2P) networks or networks based on fixed access points (AP) with which mobile nodes can communicate. Hence, the standard defines two basic network topologies: the infrastructure network and the ad hoc network. The infrastructure network is meant to extend the range of the wired LAN to wireless cells. A laptop or other mobile device may move from cell to cell (from AP to AP) while maintaining access to the resources of the LAN. A cell is the area covered by an AP and is called a "basic service set" (BSS). The collection of all cells of an infrastructure network is called an extended service set (ESS). This first topology is useful for providing wireless coverage of building or campus areas. By deploying multiple APs with overlapping coverage areas, organizations can achieve broad network coverage. WLAN technology can be used to replace wired LANs totally and to extend LAN infrastructure. A WLAN environment has wireless client stations that use radio modems to communicate to an AP. The client stations are generally equipped with a wireless network interface card (NIC) that consists of the radio transceiver and the logic to interact with the client machine and software. An AP comprises essentially a radio transceiver on one side and a bridge to the wired backbone on the other. The AP, a stationary device that is part of the wired infrastructure, is analogous to a cell-site (base station) in cellular communications. All communications between the client stations and between clients and the wired network go through the AP. The basic topology of a WLAN is depicted in Figure

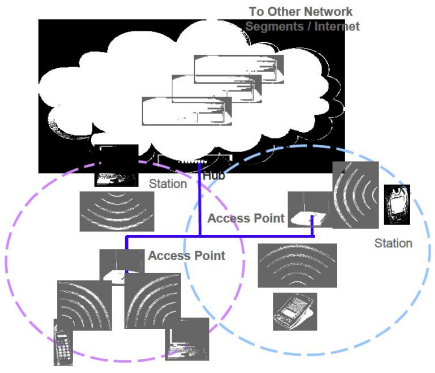



Figure-3: Fundamental 802.11 Wireless LAN Topology

Although most WLANs operate in the "infrastructure" mode and architecture described above, another topology is also possible. This second topology, the ad hoc network, is meant to easily interconnect mobile devices that are in the same area (e.g., in the same room). In this architecture, client stations are grouped into a single geographic area and can be Internet-worked without access to the wired LAN (infrastructure network). The interconnected devices in the ad hoc mode are referred to as an independent basic service set (IBSS). The ad hoc topology is depicted in Figure.

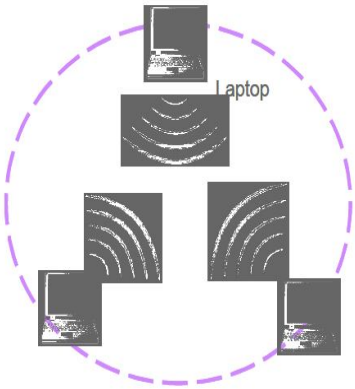



Figure-4:IEEE 802.11 Wireless LAN Ad Hoc Topology

The ad hoc configuration is similar to a peer-to-peer office network in which no node is required to function as a server. As an ad hoc WLAN, laptops, desktops and other 802.11 devices can share files without the use of an AP.

**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.

Because of these fundamental benefits, the WLAN market has been increasing steadily over the past several years, and WLANs are still gaining in popularity. WLANs are now becoming a viable alternative to traditional wired solutions. For example, hospitals, universities, airports, hotels, and retail shops are already using wireless technologies to conduct their daily business operations.

## SECURITY OF 802.11 WIRELESS LANS

This section discusses the built-in security features of 802.11. It provides an overview of the inherent security features to better illustrate its limitations and provide a motivation for some of the recommendations for enhanced security. The IEEE 802.11 specification identified several services to provide a secure operating environment. The security services are provided largely by the Wired Equivalent Privacy (WEP) protocol to protect link-level data during wireless transmission between clients and access points. WEP does not provide end-to-end security, but only for the wireless portion of the connection as shown in Figure.

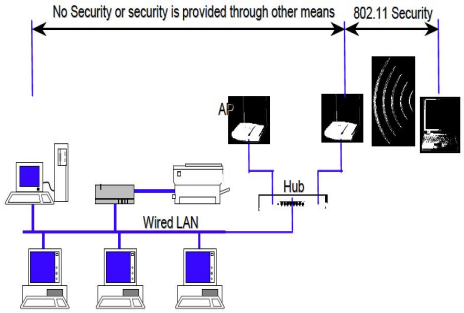



Figure 5: Wireless Security of 802.11 in Typical Network

## SECURITY FEATURES OF 802.11 WIRELESS LANS PER THE STANDARD

The three basic security services defined by IEEE for the WLAN environment are as follows:

**AUTHENTICATION**-A primary goal of WEP was to provide a security service to verify the identity of communicating client stations. This provides access control to the network by denying access to client stations that cannot authenticate properly.

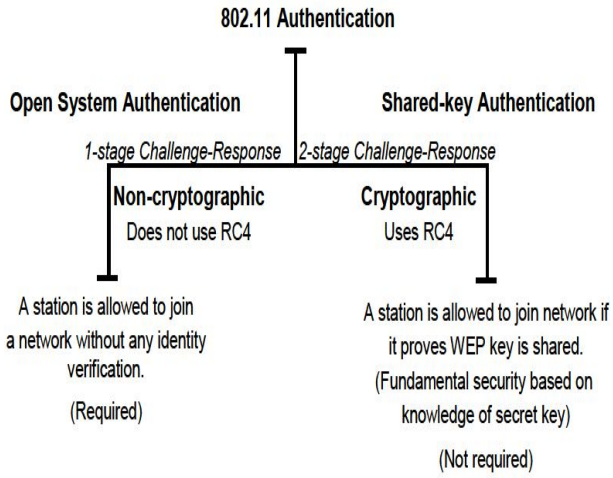
**CONFIDENTIALITY**-Confidentiality, or privacy, was a second goal of WEP. It was developed to provide "privacy achieved by a wired network." The intent was to prevent information compromise from casual eavesdropping (passive attack).

**INTEGRITY**-Another goal of WEP was a security service developed to ensure that messages are not modified in transit between the wireless clients and the access point in an active attack. It is important to note that the standard did not address other security services such as audit, authorization, and non repudiation. The security services offered by 802.11 are described in greater detail below.

## AUTHENTICATION

The IEEE 802.11 specification defines two means to "validate" wireless users attempting to gain access to a wired network: open-system authentication and shared-key authentication. One means, shared-key authentication, is based on cryptography, and the other is not. The open-system authentication technique is not truly authentication; the access point accepts the mobile station without verifying the identity of the station. It should be noted also that the authentication is only one-way: only the mobile station is authenticated. The mobile station must trust that it is communicating to a real AP.




## TAXONOMY OF 802.11 AUTHENTICATION TECHNIQUES

With Open System authentication, a client is authenticated if it simply responds with a MAC address during the two-message exchange with an access point. During the exchange, the client is not truly validated but simply responds with the correct fields in the message exchange. Obviously, with out cryptographic validatedation, open-system authentication is highly vulnerable to attack and practically invites unauthorized access. Open-system authentication is the only required form of authentication by the 802.11 specification.[3]

Shared key authentication is a cryptographic technique for authentication. It is a simple "challenge response" scheme based on whether a client has knowledge of a shared secret. In this scheme, as depicted conceptually in Figure, a random challenge is generated by the access point and sent to the wireless client. The client, using a cryptographic key that is shared with the AP, encrypts the challenge (or "nonce," as it is called in security vernacular) and returns the result to the AP. The AP decrypts the result computed by the client and allows access only if the decrypted value is the same as the random challenge transmitted. The algorithm used in the cryptographic computation and for the generation of the 128-bit challenge text is the RC4 stream cipher developed by Ron Rivest of MIT. It should be noted that the authentication method just described is a rudimentary cryptographic technique, and it does not provide mutual authentication. That is, the client does not authenticate the AP, and therefore there is no assurance that a client is communicating with a legitimate AP and wireless network. It is also worth noting that simple unilateral challenge-response schemes have long been known to be weak. They suffer from numerous attacks including the infamous "man-in-the-middle" attack. Lastly, the IEEE 802.11 specification does not require shared-key authentication.

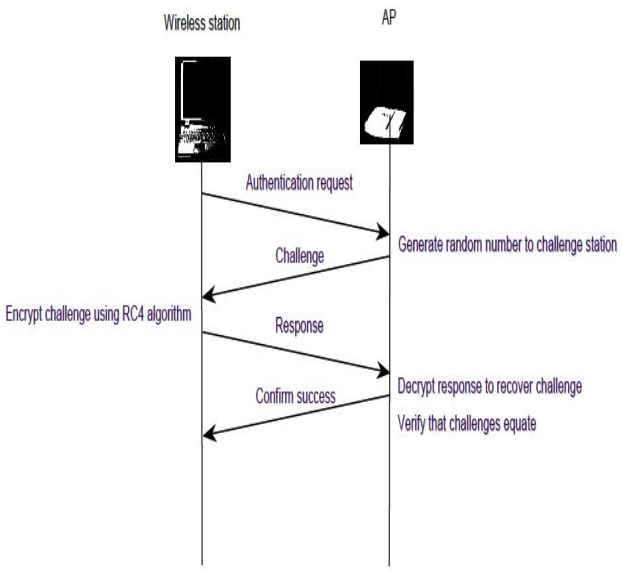



Figure-6:Shared-Key Authentication Message Flow.

**PRIVACY**

The 802.11 standard supports privacy (confidentiality) through the use of cryptographic techniques for the wireless interface. The WEP cryptographic technique for confidentiality also uses the RC4 symmetric key, stream cipher algorithm to generate a pseudo-random data sequence. This "key stream" is simply added modulo 2 (exclusive-OR-ed) to the data to be transmitted. Through the WEP technique, data can be protected from disclosure during transmission over the wireless link. WEP is applied to all data above the 802.11 WLAN layers to protect traffic such as Transmission Control Protocol/Internet Protocol (TCP/IP), Internet Packet Exchange (IPX), and Hyper Text Transfer Protocol (HTTP).The WEP privacy is illustrated conceptually in Figure7.

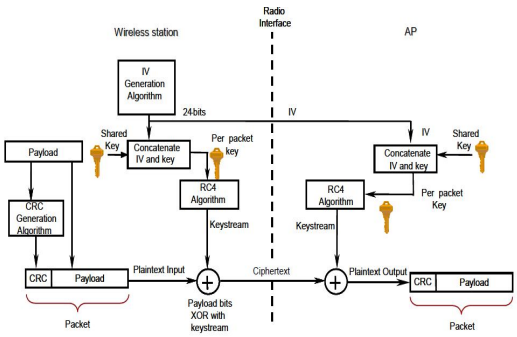



Figure-7:WEP Privacy Using RC4 Algorithm

**INTEGRITY**

The IEEE 802.11 specification also outlines a means to provide data integrity for messages transmitted between wireless clients and access points. This security service was designed to reject any messages that had been changed by an active adversary "in the middle." This technique uses a simple encrypted Cyclic Redundancy Check (CRC) approach. As depicted in the diagram above, a CRC-32, or frame check sequence, is

computed on each payload prior to transmission. The integrity-sealed packet is then encrypted using the RC4 key stream to provide the cipher-text message. On the receiving end, decryption is performed and the CRC is recomputed on the message that is received. The CRC computed at the receiving end is compared with the one computed with the original message. If the CRCs do not equal, that is, "received in error," this would indicate an integrity violation (an active message spoofer), and the packet would be discarded. As with the privacy service, unfortunately, the 802.11 integrity is vulnerable to certain attacks regardless of key size. In summary, the fundamental flaw in the WEP integrity scheme is that the simple CRC is not a "cryptographically secure" mechanism such as a hash or message authentication code.

**SECURITY REQUIREMENTS AND THREATS**

The 802.11 WLAN or WiFi industry is burgeoning and currently has significant momentum. [4], All indications suggest that in the coming years numerous organizations will deploy 802.11 WLAN technology.. There have been numerous published reports and papers describing attacks on 802.11 wireless networks that expose organizations to security risks. This subsection will briefly cover the risks to security i.e., attacks on confidentiality, integrity, and network availability.

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

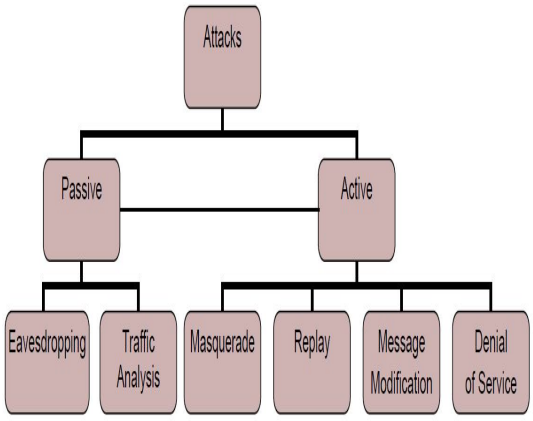



Figure-8: A General Taxonomy Of Security Attacks

**PASSIVE ATTACK** - An attack in which an unauthorized party gains access to an asset and does not modify its content.

**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.

**ACTIVE ATTACK -** An attack whereby an unauthorized party makes modifications to a message, data stream, or file. It is possible for these attacks to be detected but they may not always be preventable. Active attacks may take the form of one of four types (or combination thereof) listed below.

**MASQUERADING -** The attacker impersonates an authorized user and thereby gains certain unauthorised 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 communication facilities.

**LOSS OF CONFIDENTIALITY**

Confidentiality is the property with which information is not made available or disclosed to unauthorized individuals, entities, or processes. This is, in general, a fundamental security requirement for most organizations. [5],Due to the broadcast and radio nature of wireless technology, confidentiality is a more difficult security requirement to meet in a wireless network. WLANs risk loss of confidentiality following an active attack as well. Sniffing software as described above can obtain user names and passwords (as well as any other data traversing the network) as they are sent over a wireless connection. An adversary may be able to masquerade as a legitimate user and gain access to the wired network from an AP. Once "on the network," the intruder can scan the network using purchased or publicly and readily available tools. The malicious eavesdropper then uses the user name, password, and IP address information to gain access to network resources and sensitive corporate data.

**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. A hacker, for example, can compromise data integrity by deleting or modifying the data in an e-mail from an account on the wireless system. This can be detrimental to an organization if important e-mail is widely distributed among e-mail recipients. Because the existing security features of the 802.11 standard do not provide for strong message integrity, other kinds of active attacks that compromise system integrity are possible. As discussed before, the WEP based integrity mechanism is simply a linear CRC. Message modification attacks are possible when cryptographic checking mechanisms such as message authentication codes and hashes are not used.[6]

**LOSS OF NETWORK AVAILABILITY**

A denial of network availability involves some form of DoS attack, such as jamming. Jamming occurs when a malicious user deliberately emanates a signal from a wireless

device in order to overwhelm legitimate wireless signals. Jamming may also be inadvertently caused by cordless phone or microwave oven emissions. Jamming results in a breakdown in communications because legitimate wireless signals are unable to communicate on the network. Nonmalicious users can also cause a DoS. As a result, agency security policies should limit the types and amounts of data that users are able to download on wireless networks.

## COUNTERMEASURES

Organizations can mitigate risks to WLANs by applying countermeasures to address specific threats and vulnerabilities. Countermeasures at the management, operational and technical levels can be effective in reducing the risks commonly associated with WLANs.

## MANAGEMENT COUNTERMEASURES:

In light of the security issues, any deployment of wireless technology on an agency's computing network must be subject to usual risk management processes and underpinned by a sound business case as to why this technology should be used [7].The cornerstone of an effective WLAN security strategy involves documenting, deploying and enforcing WLAN security policies and practices. Organizations should ensure that all critical personnel are properly trained on the use of wireless technology. Network administrators need to be fully aware of the security risks that WLANs and wireless devices pose. They must work to ensure security policy compliance and to know what steps to take in the event of an attack. Finally, the most important countermeasure is trained and aware users.

## OPERATIONAL COUNTERMEASURES:

Physical security is a fundamental step for ensuring that only authorized users have access to wireless equipment. Physical security combines such measures as access controls, personnel identification, and external boundary protection. As with facilities housing wired networks, facilities providing wireless network connectivity need physical access controls. It is important to consider the range of each AP that will be deployed as part of a WLAN environment. [8] Design for security: when placing wireless APs for strategic coverage, consider signal bleed into uncontrolled areas where transmissions may be intercepted. If the range extends beyond the physical boundaries of the building's walls, the extension creates security vulnerability.

## TECHNICAL COUNTERMEASURES:

Technical countermeasures involve the use of hardware and software solutions to help secure the wireless environment. Software countermeasures include proper Access Point configurations (i.e. the operational and security settings on an AP), software patches and upgrades, authentication, intrusion detection systems, personal firewalls for wireless devices, and encryption.[9] Hardware solutions include smart cards, virtual private networks (VPNs), public key infrastructure (PKI), a separate switching infrastructure for the wireless network (separating it from a wired network), and biometrics. It should be noted that hardware solutions, which generally have software components, are listed simply as hardware solutions.[10].

## CONCLUSION

Wireless networking provides numerous opportunities to increase productivity and cut costs. It also alters an organization's overall computer security risk profile. Although it is impossible to totally eliminate all risks associated with wireless networking, it is possible to achieve a reasonable level of overall security by adopting a systematic approach to assessing and managing risk. This paper discussed the threats and vulnerabilities associated with each of the three basic technology components of wireless networks (clients, access points, and the transmission medium) and described various commonly available countermeasures that could be used to mitigate those risks. A combined effort of users, employers and system administrators is required in order to fight against such malicious activities. Appropriate countermeasures in every form can help the organization minimize the risk of illegal penetration. Up to date tools, constant monitoring, proper management and appropriate countermeasures are the ultimate weapons to fight against wireless security attacks.

## References

[1] Mitchell Ashley , "A Guide to Wireless Network Security" Information systems Control Journal ,Volume 3,2004.

[2] Karen Scarfone, Derric Dicoi, " Wireless Network Security for IEEE 802.11a/b/g,Bluetooth(DRAFT)",NISTPublication-800-48.Augest 2007.

[3] Tom karygiannis, Les Owens, "Wireless Network Security for IEEE 802.11a/b/g,Bluetooth(DRAFT)",NISTPublication-800-48.November 2002

[4] Ahmed M. Al Naamany , Ali Al Shidhani, Hadj Bourdoucen, "IEEE 802.11 Wireless LAN Security Overview", IJCSNS International Journal of Computer Science and Network Security, VOL.6 No.5B, May 2006.

[5] Omar Cheikhrouhou & Maryline Laurent & Amin Ben Abdallah & Maher Ben Jemaa, "An EAP-EHash authentication method adapted to resource constrained terminals", Institute TELECOM and Springer-Verlag.Hal-00506549,Version 1-28 July 2010

[6] "Applied Cryptographhy" By Bruse Schneier.

[7]"AdvancedComputing Applications,Data bases and Networks" By Shahin Ara Begum,Prodipto Das.

[8] John Vollbrech, Robert Moskowitz, "Wireless LAN Access Control and Authentication" Interlink networks-2002.

[9] "Cryptography and Network Security" By William Stallings

[10]http://www.practicallynetworked.com/support/mixed_wep.htm

## Author Biography:

**GOPALAKRISHNAN S** was born in Tamil Nadu, India, in 1985. He received the B.E. degree in Electronics and Communication Engineering from PET Engineering College affiliated to Anna University Chennai and the M.E. degree in Embedded System Technologies from SA Engineering College affiliated to Anna University Chennai, India in 2011. He is currently pursuing the Ph.D. degree from the Department of Information Communication Engineering Anna University, Chennai. He is working as a Assistant Professor in PSNA College of Engineering and Technology, Dindigul, TamilNadu, India. His research interests include computer vision and computer Networks.