Volume 8, No. 4, May 2017 (Special Issue)
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
REVIEW ARTICLE
Available Online at www.ijarcs.info

Wireless Network Components &Security Protocol

Er. Gurpinder Singh[1]
Ph.D Scholar
Sant Baba Bhag Singh University[1]
Jalandhar, Punjab, India[1]
Sirhind007@gmail.com[1]

Parminderpal[2]
M.Tech. Scholar
Sant Baba Bhag Singh University[2]
Jalandhar, Punjab, India[2]
parminder_mahey@yahoo.com[2]

***Abstract:-*Wireless networks are a general term to refer to various types of networks that communicate without the need of wire lines. Wireless networks can be broadly categorized into two classes based on the structures of the networks: wireless ad-hoc networks and cellular networks. The need for security on any network is apparent. Wireless network/Internet access technology is being increasingly installed in both office and public environment. Wireless network provide many advantages but it also joined with new security threads and alters the organization's overall information security risk profile when considering a network with a Wireless Access Point, or WAP", available, new security concerns come into play. Because wireless is broadcast in nature, anyone within range of a wireless card can intercept the packets being sent out without interrupting the flow of data between wireless card and base station. We present a structure to help managers understand and assess the various threats associated with the use of wireless Network. We also discuss various solutions for countering the threats.**

Keywords: Wireless Network, Data Flow control, Wireless Ad-hoc network, cellular Network, WAP.

I. INTRODUCTION

A wireless network is a flexible data communications system, which uses wireless media such as radio frequency technology to transmit and receive data over the air, minimizing the need for wired connections. Wireless networks are used to augment rather than replace wired networks and are most commonly used to provide last few stages of connectivity between a mobile user and a wired network. A wireless local area network (WLAN) is a flexible data communications system that can use microwave, infrared or radio frequency technology to transmit and receive the signal the medium is air. 802.11 were first WLAN stranded which was implemented in 1997.It is based on radio frequency (technology) and the operating frequency was 2.4 GHz and has a maximum throughput of 1 to 2 Mbps. And later on 802.11b was introduce and have the same operating frequency as in 802.11,but with a maximum speed of 11 Mbps.while 5GHz 802.11a wireless, for an added price, can provide up to 54 Mbps, more than enough to take full advantage of a cable modem or DSL connection.More often than not, the small-network wireless user will utilize only.
whatever security features are broadcasted on the box of the wireless equipment's purchased. Because it is part of the 802.11 specification, a security feature known as Wired Equivalent Privacy (WEP), is available with most base stations sold today. An encrypted key is associated with each network; anyone who wants to use the network must have that key. Many people depend on WEP to prevent their packets from being inhaled and to avoid outsiders from joining their network without their permission.WLAN has been widely used in many sectors ranging from corporate, education, finance, healthcare, retail, manufacturing, and warehousing. According to a study by the Gartner Group, approximately 50 percent of company laptops around the world will be equipped for WLAN. It has increasingly becoming an important technology to satisfy the needs for installation flexibility, mobility, reduced costofownership, and scalability.

A. ADVANTAGE

a) *Mobility***:** provide mobile users with access to real-time information so that they can roam around in the network without getting disconnected from the network

b) *Installation speed and simplicity:* installing a wireless system can be fast and easy and can eliminate the need to pull cable through walls and ceilings.

c) *Reach of the network:* the network can be extended to places which cannot be wired

d) *More Flexibility: wireless* networks offer more flexibility and adapt easily to changes in the configuration of the network.

e) *Reduced cost of ownership:* while the initial investment required for wireless network hardware can be higher than the cost of wired network hardware, overall installation expenses and life-cycle costs can be significantly lower in dynamic environments.

f) *Scalability:* wireless systems can be configured in a variety of topologies to meet the needs of specific applications and installations. Configurations can be easily changed and range from peer-to-peer networks suitable for a small number of users to large

CONFERENCE PAPERS
National Conference on Emerging Trends on Engineering & Technology (ETET-2017)
On 21st April 2017
University Inst. of Engg. & Tech. & University Inst. of Computer, SBBS University, Punjab (India)

infrastructure networks that enable roaming over a broad area.

II. COMPONENTS

Components of a traditional WLAN network include APs; network interface cards (NICs) or client adapters, bridges, repeaters, and antennae. Additionally, an authentication, authorization, and accounting (AAA) server (specifically a Remote Address Dial-In User Service [RADIUS] server), network management server (NMS), and "wireless-aware" switches and routers are considered as part of an enterprise WLAN network.

802.11 Wireless LAN Components

- Stations
- Wireless APs
- Ports

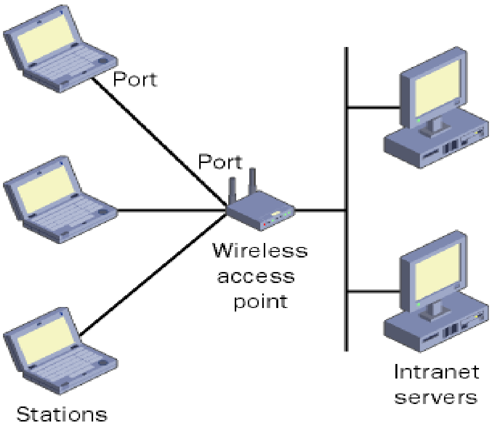

Figure 1. Wireless Components

a) *Network Interface Card (NICs)*

A major part of a wireless LAN includes a NIC that operates within the computer device and provides wireless connectivity. A wireless LAN NIC, sometimes referred to as a radio card, often implements the 802.11 standard.

Figure 2 Network Interface Card (NIC)

b) Access Points

An access point contains a radio card that communicates with individual user devices on the wireless LAN, as well as a wired NIC that interfaces to a distribution system, such as Ethernet.

Figure 3. Access Point (AP)

c) Routers

By definition, a router transfers packets between networks. The router chooses the next best link to send packets on to get closer to the destination. Routers use Internet Protocol (IP) packet headers and routing tables, Routers implement the Network Address Translation (NAT) protocol that enables multiple network devices to share a single IP address provided by an Internet service provider (ISP). Figure 1.3 illustrates this concept. Routers also implement Dynamic Host Configuration Protocol (DHCP) services for all devices. DHCP assigns private IP addresses to devices. Together, NAT and DHCP make it possible for several network devices, such as PCs, laptops, and printers to share a common Internet IP address.

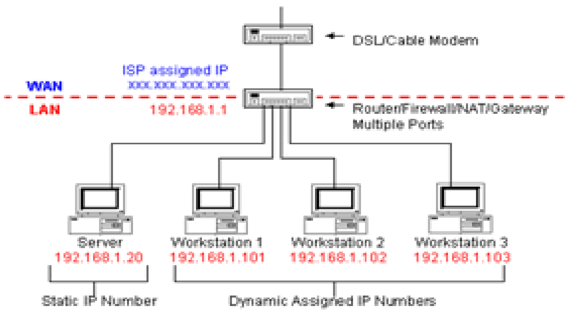

Figure 4.NAT and DHCP Are Essential Protocols That Routers Implement

WLAN PERFORMANCE

Much the same way a cordless phone works better when it is close to its base, wirelessly networked computers function best when located relatively close together and in open sight of each other. The level of performance of an 802.11 WLAN is dependent on a number of important environmental and product-specific factors:

- Distance between WLAN devices (AP and NICs)
- Transmission power levels
- Building and home materials
- Radio frequency interference
- Signal propagation
- Antenna type and location

Depending on environmental specifics, automatic downshifting by the access point or client allows compatibility adjustment to prevailing radio frequency conditions. At any one moment, an 802.11b network can be running at 11 Mbps, 5.5 Mbps, 2 Mbps, or 1 Mbps 22 Mbps wireless networking products). And depending on where each wireless device is in a home or office, each of those devices can be transmitting at any one of these speeds. Typically, the software applications that ship with an 802.11 NIC adapter are capable of reporting current connection speeds and also allow users to perform site surveys for the best location of an access point. The diagram below shows how distance and building materials can impact the performance of an 802.11 network.

III. CLASSIFICATION OF WIRELESS NETWORK

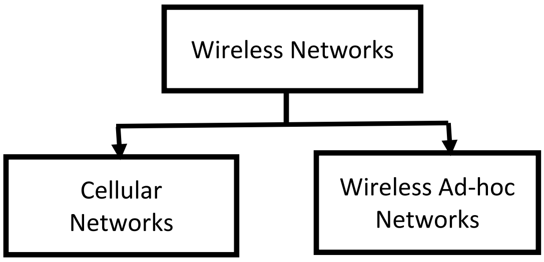

Figure 5 Classification of Wireless network

A. CELLULAR NETWORK

A cellular network a wireless network distributed over land areas known as cells, each served by at least one fixed-location transceiver, known as a cell site or base station. All cellular phone networks worldwide use a portion of the radio frequency spectrum designated as ultra-high frequency, or "UHF", for the transmission and reception of their signals. This enables a large number of devices like mobile phones, pagers, etc to communicate with each other.

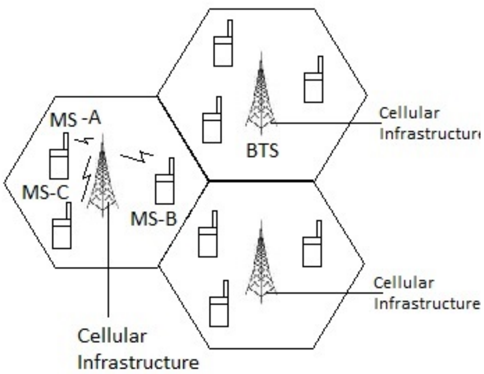

Figure 6 Cellular network

B. Wireless Ad-hoc Network

Wireless ad hoc networks are distributed networks that work without fixed infrastructures and in which each network node is willing to forward network packets for other network nodes. Today many portable devices, such as laptop, mobile phones, PDAs and mp3 players, for use in professional and personal lives. For the most part, these devices are used separately and their applications do not interact. Imagine, however, if they could interact directly they share documents, business cards would automatically find their way into the address catalogue on a laptop and the number catalogue on a cell phone, their laptops could remain online, likewise, incoming email could now be diverted to their PDAs, finally, as they enter the office, all communication could automatically be routed through the wireless network.

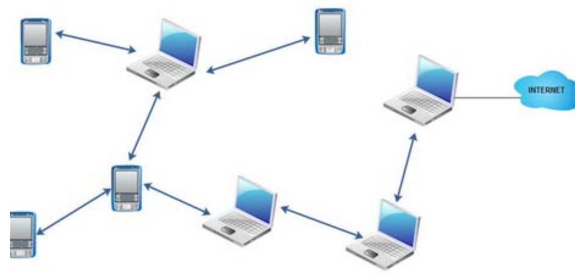

Figure 7. Ad-hoc network

A wireless ad hoc network is a decentralized type of wireless network.,[1][2] The network is ad hoc because it does not rely on a pre-existing infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. Instead, each node participates in routing by forwarding data for other nodes, so the determination of which nodes forward data is made dynamically on the basis of network connectivity. In addition to the classic routing, ad hoc networks can use flooding for forwarding data. An ad hoc network typically refers to any set of networks where all devices have equal status on a network and are free to associate with any other ad hoc network device in link range. Ad hoc network often refers to a mode of operation of IEEE 802.11 wireless networks.

IV. SECURITY PROTOCOLS

IEEE 802.11 standard [1] was defined Wired Equivalent Privacy (WEP). WEP is designed to protect linkage-level data for wireless transmission by providing secrecy, access control, and data integrity, to provide secure communication between the device and an access point (AP) wireless LAN

A. WEP

Initially, WEP (Wired Equivalent Privacy) was the only link-level security option defined in the 802.11 standard based on shared key secrets and the RC4 stream cipher. WAP was basically developed for protection of the confidentiality and integrity of the wireless network traffic.

For security proposed, WEP uses encryption in two operations i.e. produces a checksum of the data, and then it encrypts the plaintext and the checksum using RC4 [2].

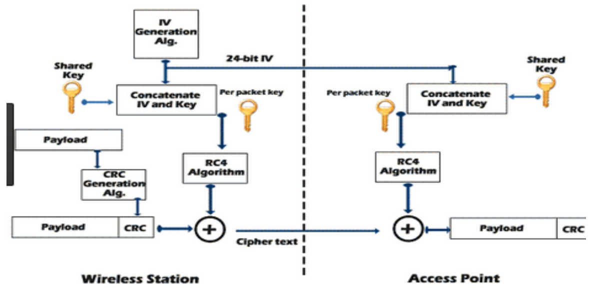

Figure 1.7 WEP encryption and decryption

WEP uses the RC4 stream cipher with a 64 or 128 bits key to provide data packet encryption. In addition, WEP can be used as a access control method, because once WEP is active, the Access Point will just start communication with nodes that have the same shared secret key, refusing the others.

B. WEP authentication methods

WEP specifies two types of authentication: Open System and Shared Key. "Open System" means no authentication. Any station can attempt to communicate. Shared Key authentication requires four steps:

- The initiating station sends an authentication request to the receiving station, which in most cases will be an AP.
- The AP sends back a clear text challenge message.
- The station uses RC4 to encrypt the message and send it back to the AP.
- The AP decrypts the message. If it matches the message sent, the requesting station has been configured with the correct key, proving that it is authorized to use the network.

The two stations are then free to exchange messages, each encrypting and decrypting using RC4 and the same key used in the authentication process.

C. RC4 operation

The sending station combines the configured master key with a 24-bit initialization vector (IV) to create a 64-bit key. The IV strengthens encryption by causing successive packets to be encrypted with different keys, making it more difficult for a hacker to determine the configured key.The method depends on the implementation. Some stations use a random-number generator to generate an IV for each packet, and some start at zero and increment. The IV is sent to the receiving station in clear text in each packet. A checksum of each packet's contents is calculated using the CRC-32 algorithm and appended to the end of the packet. The combined key, along with the text to be encrypted, is input to RC4.

- The bytes in the combined key are scrambled by the key-scheduling algorithm.
- The scrambled key is then fed to a pseudo-random generator function that uses the scrambled key to output a key byte for each byte of the packet to be encrypted.
- Each byte of the encrypted message is created by an exclusive or (XOR) of the message byte and the key byte.
- The checksum is encrypted and added at the end of the encrypted text.

The receiving station uses the configured master key and the received clear text IV to decrypt the packet text and checksum. It then calculates the checksum over the packet text. If the received checksum and calculated checksum match, the packet contents have not been altered in transit.

D. WPA and WPA 2

Wi-Fi Protected Access (WPA) is specified by the IEEE 802.11i standard. The standard is aimed at providing a stronger security compared to WEP and is expected to tackle most of the weakness found in WEP [3-4]WPAWi-Fi Protected Access was the Wi-Fi Alliance's direct response and replacement to the increasingly apparent vulnerabilities of the WEP standard. The Wi-Fi Alliance intended WPA as an intermediate measure to take the place of WEP pending the availability of the full IEEE 802.11i standard. The most common WPA configuration is WPA-PSK (Pre-Shared Key). The keys used by WPA are 256 bit, a significant increase over the 64-bit and 128-bit keys used in the WEP system. The WPA protocol works in a similar way to WEP. WPA mandates the use of theRC4stream cipher with a 128bit key and a 48 bit initialization vector (IV), compared with the 40 bit key and the 24 bit IV in WEP.WPA uses the Extensible Authentication Protocol (EAP) framework [5] to conduct authentication. When a user (supplicant) tries to connect to a network, an authenticator will send a request to the user asking the user to authenticate herself using a specific type of authentication mechanism. The user will respond with corresponding authentication information. The authenticator relies on an authentication server to make the decision regarding the user's authentication

E. WPA2

WPA2 is not separate from WPA like TKIP is required; Advanced Encryption Standard (AES) is optional. The basic idea is to provide backward compatibility for WPA on the same hardware designed for WEP and TKIP can be implemented on the same hardware but AES cannot be implemented on this hardware. AES is also known as block cipher, which can be implemented on a fixed size of data units. AES accepts key sizes of 128 bits, 196 bits, and 256 bits. One of the most significant changes between WPA and WPA2 was the mandatory use of AES algorithms and the introduction of CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol) as a replacement for TKIP (still preserved in WPA2 as a fallback system and for interoperability with WPA). Opportunely, the same susceptibility that is the biggest hole in the WPA armor, the attack vector through the Wi-Fi Protected Setup (WPS), remains in modern WPA2-capable access points.WPA2 allows the caching of a Pair-wise Master Key (PMK), this key is used in access point(AP) and a wireless customer for session creation. Thus a wireless customer can reconnect a recently connected the same access point without having to authenticate.WPA2 enables a wireless customer to authenticate itself to a wireless access point that it is moving to while the wireless customer maintains its connection to the existing access point. It is used by the customer to from one access point to another, and it is especially useful for timing-sensitive applications.

V. CONCLUSION

It is important that organizations more frequently assess risks and test and evaluate system security controls when wireless networks (technologies) are installed. In this paper, we discussed the 802.11 Wireless Network security protocols and mechanism that we can find in any 802.11 device. All the feature 802.11 devices are effective but some of them are easy to by- pass. SSID hiding and MAC access control can be used from to block attacker, but cannot be trusted as security measure.

WEP protocol was designed to protect 802.11 wireless technologies; it has limitations that cannot provide trusted security levels.

REFERENCES

[1] L. M. S. C. of the IEEE Computer Society. Wireless LAN medium access control (MAC) and physical layer (PHY) specifications, technical report, IEEE Standard 802.11, 1999 ed., 1999.

[2] R.L. Rivest, The RC4 encryption algorithm, RSA Data Security, Inc., March 1992 technical report.

[3] W.A. Arbaugh, An inductive chosen plaintext attack against WEP/WEP2, IEEE Document 802.11-01/230, May 2001.

[4] N. Borisov, I. Goldberg, D. Wagner, Intercepting Mobile Communications: The Insecurity of 802.11, MobiCom 2001.

[5] Aboba, L. Blunk, J. Vollbrecht, J. Carlson, E.H. Levkowetz, Extensible Authentication Protocol (EAP), request for comment, Network Working Group, 2004.

[6] Stubblefield, A; et al. (2004) ‘A Key Recovery Attack on the 802.11b Wired Equivalent Privacy Protocol(WEP)’ in ACM Transactions on Information and System Security, Vol. 7, No. 2, May 2004, pg 319–332.

[7] DESIDOC Bulletin of Information Technology , Vol. 25, No.1, January 2005, pp. 13-18© 2005, DESIDOC.

[8] URL: http://en.wikipedia.org/wiki/WEP