ISSN:0975-9646

Survey on Different Types of Attacks and Counter Measures in Wireless Networks

N. Vijaya gopal, Dr.V.Srikanth, M. Mohan Chandra
Department of CSE,KL University,India.

***ABSTRACT*—Communications in wireless networks has been facilitating numerous emerging applications that require packet delivery from one or more senders to multiple receivers. Communications are sensitive to various kinds of attacks due to insecure wireless channels. Communications in wireless networks remains a challenging and Internal or external issues. In this paper we have introduce types of attacks and counter measures. Wireless networks are used in many commercial and military applications to bring event driven and real time data. Research in network security has produced several security solutions. It has been observed that packet delivery ratio decreases when we increase number of nodes while energy and latency increases**.

***Keywords*—wireless networks, attacks, counter measures, packets.**

I. INTRODUCTION

Wireless Networks constituting large number of nodes are becoming to solve the many challenging commercial, domestic and military applications. Wireless Networks gather and distribute data from the fields where common networks are unreachable for various environmental and strategic reasons.

Wireless networking has important as one of the most promising concept for auto-configurable and self-organizing wireless networking to provide adaptive and flexible wireless connectivity to mobile users. This concept can be used for very different wireless access technologies such as wireless local area network (WLAN), wireless metropolitan area network (WMAN), and wireless personal area network (WPAN) technologies.

Due to the computation and power limitations wireless networks are more vulnerable to security threats. Security does not come free, adding heavy security measures in terms of computation power, limitation in memory poses and energy significant challenges in designing a light weight security solution against attacks on wireless networks.

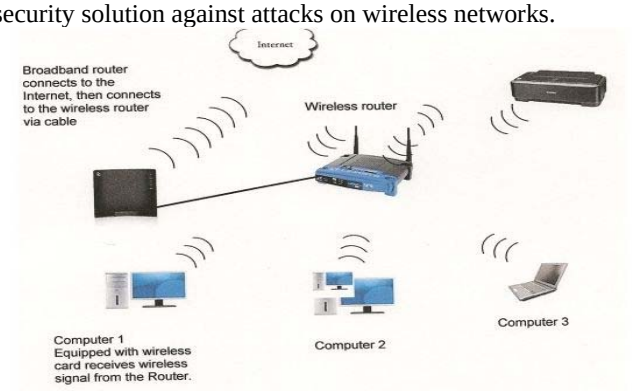

Fig: Diagram Of Wireless Network.

II. WIRELESS LAN OVERVIEW

In this section, we give a brief overview of wireless LAN (WLAN) while emphasizing the features that help an attacker. We assume that the reader is familiar with the TCP/IP suite.

IEEE 802.11 refers to a family of specifications developed by the IEEE for over-the-air interface between a wireless client and an AP or between two wireless clients. To be called 802.11 devices, they must conform to the Medium Access Control (MAC) and Physical Layer specifications. The IEEE 802.11 standard covers the Physical (Layer 1) and Data Link (Layer 2) layers of the OSI Model.

A. Stations and Access Points

A wireless network interface card (adapter) is a device, called a station, providing the network physical layer over a radio link to another station. An access point (AP) is a station that provides frame distribution service to stations associated with it. The AP itself is typically connected by wire to a LAN.

The station and AP each contain a network interface that has a Media Access Control (MAC) address, just as wired network cards do. This address is a world-wide-unique 48-bit number, assigned to it at the time of manufacture. The 48-bit address is often represented as a string of six octets separated by colons or hyphens While the MAC address as assigned by the manufacturer is printed on the device, the address can be changed in software.

Each AP has a 0 to 32 byte long Service Set Identifier (SSID) that is also commonly called a network name. The SSID is used to segment the airwaves for usage. If two wireless networks are physically close, the SSIDs label the respective networks, and allow the components of one network to ignore those of the other. SSIDs can also be mapped to virtual LANs thus, some APs support multiple SSIDs. Unlike fully qualified host names SSIDs are not registered, and it is possible that two unrelated networks use the same SSID.

B. Channels

The stations communicate with each other using radio frequencies between 2.4 GHz and 2.5 GHz. Neighboring channels are only 5 MHz apart. Two wireless networks using neighboring channels may interfere with each other.

C. WEP

Wired Equivalent Privacy (WEP) is a shared-secret key encryption system used to encrypt packets transmitted between a station and an AP. The WEP algorithm is intended to protect wireless communication from eavesdropping. A secondary function of WEP is to prevent unauthorized access to a wireless network. WEP encrypts the payload of data packets. Management and control frames are always

transmitted in the clear. WEP uses the RC4 encryption algorithm. The shared-secret key is either 40 or 104 bits long. The key is chosen by the system administrator. This key must be shared among all the stations and the AP using mechanisms that are not specified in the IEEE 802.11.

D. Infrastructure and Ad Hoc Modes

A wireless network operates in one of two modes. In the ad hoc mode, each station is a peer to the other stations and communicates directly with other stations within the network. No AP is involved. All stations can send Beacon and Probe frames. The ad hoc mode stations form an Independent Basic Service Set (IBSS).

A station in the infrastructure mode communicates only with an AP. Basic Service Set (BSS) is a set of stations that are logically associated with each other and controlled by a single AP. Together they operate as a fully connected wireless network. The BSSID is a 48-bit number of the same format as a MAC address. This field uniquely identifies each BSS. The value of this field is the MAC address of the AP.

E. Frames

Both the station and AP radiate and gather 802.11 frames as needed. The format of frames is illustrated below. Most of the frames contain IP packets. The other frames are for the management and control of the wireless connection .

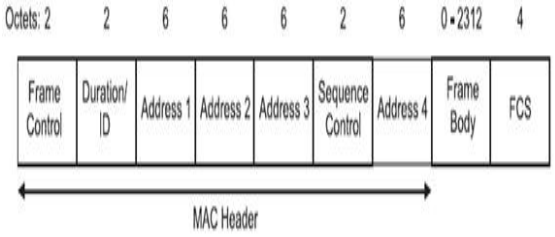

Fig 2: An IE802.11 Frame

There are three classes of frames. The management frames establish and maintain communications. These are of Association request, Association response, Re-association request, Re-association response, Probe request, Probe response, Beacon, Announcement traffic indication message, Disassociation, Authentication, De-authentication types. The SSID is part of several of the management frames. Management messages are always sent in the clear, even when link encryption (WEP or WPA) is used, so the SSID is visible to anyone who can intercept these frames. The control frames help in the delivery of data.

F. Authentication

Authentication is the process of proving identity of a station to another station or AP. In the open system authentication, all stations are authenticated without any checking. A station A sends an Authentication management frame that contains the identity of A, to station B. Station B replies with a frame that indicates recognition, addressed to A. In the closed network architecture, the stations must know the SSID of the AP in order to connect to the AP. The shared key authentication uses a standard challenge and response along with a shared secret key.

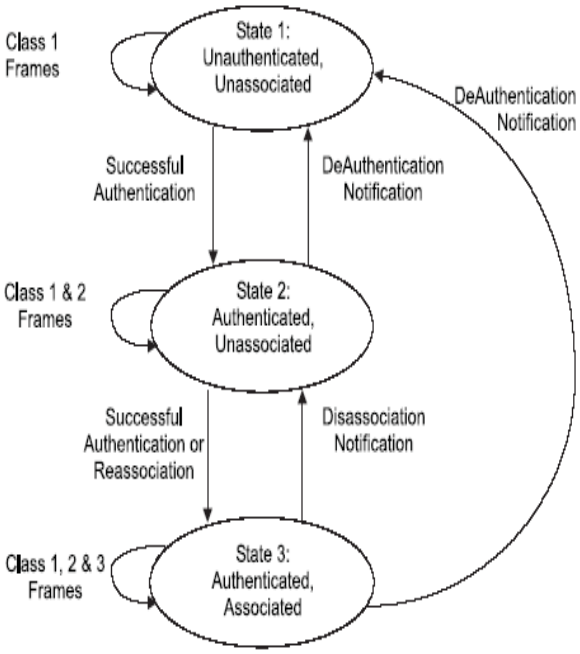

Fig 3: States and Services

G. Association

Data can be exchanged between the station and AP only after a station is associated with an AP in the infrastructure mode or with another station in the ad hoc mode. All the APs transmit Beacon frames a few times each second that contain the SSID, time, capabilities, supported rates, and other information. Stations can chose to associate with an AP based on the signal strength etc. of each AP. Stations can have a null SSID that is considered to match all SSIDs.

The association is a two-step process. A station that is currently unauthenticated and unassociated listens for Beacon frames. The station selects a BSS to join. The station and the AP mutually authenticate themselves by exchanging Authentication management frames. The client is now authenticated, but unassociated. In the second step, the station sends an Association Request frame, to which the AP responds with an Association Response frame that includes an Association ID to the station. The station is now authenticated and associated.

III. Different Types Of Wireless Attacks

A. Denial of service Attack:

A Denial-of-Service attack (DoS) occurs when an attacker continually bombards a targeted AP (Access Point) or network with bogus requests, premature successful connection messages, failure messages, and/or other commands. These cause legitimate users to not be able to get on the network and may even cause the network to crash. These attacks rely on the abuse of protocols such as the Extensible Authentication Protocol (EAP).

The DoS attack in itself does little to expose organizational data to a malicious attacker, since the interruption of the network prevents the flow of data and actually indirectly

protects data by preventing it from being transmitted. The usual reason for performing a DoS attack is to observe the recovery of the wireless network, during which all of the initial handshake codes are re-transmitted by all devices, providing an opportunity for the malicious attacker to record these codes and use various "cracking" tools to analyze security weaknesses and exploit them to gain unauthorized access to the system. This works best on weakly encrypted systems such as WEP, where there are a number of tools available which can launch a dictionary style attack of "possibly accepted" security keys based on the "model" security key captured during the network recovery.

B. Jamming Attack:

Since RF (radio frequency) is essentially an open medium, jamming can be a huge problem for wireless networks. Jamming is one of many exploits used compromise the wireless environment. It works by denying service to authorized users as legitimate traffic is jammed by the overwhelming frequencies of illegitimate traffic. A knowledgeable attacker with the right tools can easily jam the 2.4 GHz frequency in a way that drops the signal to a level where the wireless network can no longer function. The complexity of jamming is the fact that it may not be caused intentionally, as other forms of wireless technology are relying on the 2.4 GHz frequency as well. Some widely used consumer products include cordless phones, Bluetooth-enabled devices and baby monitors, all capable of disrupting the signal of a wireless network and faltering traffic.

C. Man In The Middle Attack:

The man-in-the-middle attack in cryptography and computer security is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.

The attacker must be able to intercept all messages going between the two victims and inject new ones, which is straight forward in many circumstances.

D. Interception Attack:

The wireless network used a username and password to allow access to the local network, the attacker can use a Wireless Sniffer for an attack. An attacker can sniff and capture legitimate traffic. Many of the tools that accomplish this are based on capturing the first part of connection session, where the data would typically include the username and password. With this, the intruder can then be disguised as that user by using this captured information.

Wireless sniffing requires the attacker to be within the range of the wireless traffic. This is usually around 300 feet range, but wireless equipment continues to strengthen their signals, pushing the wireless signal further out. On the surface this seems to be a beneficial feature for the user because the user can then access the network or surf the web at a further location from the base-station, but in actuality it creates a greater risk for the user because it allows intruders to attack at a further location as well. If an attacker can sniff the wireless traffic, it is possible to inject false traffic into the connection. The attacker can then hijack the victim's session by issuing commands on behalf of the user.

E. RAP Attack:

RAP (Rogue Access Points) have become a huge issue in wireless security. A Rogue Access Point is one connected to a network without authorization from an administrator. With low end access points steadily decreasing in price and increasing in availability, RAPs have become much more common. Additionally, many of these access points contain features that make them nearly invisible when coupled with legitimate networks, doing a fine job to conceal their presence. Rogues Access Points are often created by employees looking for additional freedom in the work environment. Many employees simply bring in their access points from home and plug them right into their work stations and the company LAN without consent from administrators. These type of RAPs are potentially dangerous as many people who create them are not aware of the security issues associated with a wireless network.

F. Ad Hoc Associations Attack:

Ad hoc mode allows computers to communicate in a peer-to-peer fashion. An example would be of two people wanting to share a file, but could not come up with a USB flash drive or writable CD between them. So they just set up their computers to use ad hoc networking and move the file from one computer to a shared folder on the other computer. The availability of USB flash drives these days usually trumps this process as setting up an ad hoc network can be an involved and time consuming process. This is a good thing, as can be seen in Mr. Hiner’s post. Still, even just having ad hoc association enabled on a computer is inviting any computer similarly configured and within range to associate, including people who wish to do harm.

G. MAC Spoofing Attack:

MAC spoofing attacks are attacks launched by clients on a Layer 2 network. Attackers spoof their MAC address to perform a man-in-the-middle (MiTM) attack. In one common attack, the attacker pretends to be the default gateway and sends out a gratuitous Address Resolution Protocol (ARP) to the network so that users send their traffic through the attacker rather than the default gateway. The attacker then forwards user traffic to the real default gateway. An attacker on a fast enough host can capture and forward packets so that victims do not notice any change in their network access. Many tools available for download from the Internet, such as Ettercap, can accomplish such a task, and preventing such attacks is quite problematic.

H. Evil Twin:

Evil twin is a term for a rogue Wi-Fi access point that appears to be a legitimate one offered on the premises, but actually has been set up by a hacker to eavesdrop on wireless communications among Internet surfers.

Evil twin is the wireless version of the phishing scam. An attacker fools wireless users into connecting a laptop or mobile phone to a tainted hotspot by posing as a legitimate provider.

Wireless devices link to the Internet via "hotspots" – nearby connection points that they lock on to. But these hotspots can act like an open door to thieves. Anyone with suitable equipment can locate a hotspot and take its place, substituting their own "evil twin".
This type of evil twin attack may be used by a hacker to steal the passwords of unsuspecting users by either snooping the communication link or by phishing, which involves setting up a fraudulent Web site and luring people there.

IV. WIRELESS ATTACKS COUNTER MEASURES:

The following are the counter measures for different types of attacks i.e. how these attacks are being attacked due to the lack of following reasons.

- recognize features of the primary modes used for cellular communication
- recognize features of the RF technologies for 2.4 Ghz wireless LANs
- identify the components of Bluetooth security algorithms
- sequence the steps of the association process
- recognize how wireless systems work
- recognize features of the WEP authentication methods
- identify the vulnerabilities of WEP
- recognize how wireless networks are vulnerable to DoS attacks
- recognize how the broadcast bubble makes wireless networks vulnerable to eavesdropping
- recognize common wireless hacking tools
- recognize how to increase the security of wireless LANs
- recognize how wireless security protocols work and how to defend a wireless network

V. CONCLUSION:

Our work describes about wireless networks and how the data has been shared among different destinations, and shown how the attackers are being attacked in between the data transfer and related counter measures have been discussed to reduce the attacks.

REFERENCES

[1] AusCERT. AA-2004.02 - denial of service vulnerability in IEEE 802.11 wireless devices. http://www.auscert.org
[2] R. Bruno, M. Conti, and E. Gregori, IEEE 802.11 Optimal Performances: RTS/CTS Mechanism vs. Basic Access, PIMRC, 2002
[3] B. Dahill et al., “A Secure Protocol for Ad Hoc Networks,“ IEEE ICNP, 2002.
[4] X. Gu and R. Hunt, “Wireless LAN Attacks and Vulnerabilities” In the Proceeding of IASTED Networks and Communication Systems, April 2005.