A Critical Study on Wireless Network Attacks for Preventing Channel Congestion

N.Lakshmi Haritha [#1], M.Ashok[*2]

[#1] *Student: M.Tech 2nd Year CSE Dept.*
Mother Theresa Educational Society Group Of Instuttions
Nunna,Vijayawada,India
** Faculty*
Cse Dept.
Mother Theresa Educational Society Group Of Instuttions
Nunna,Vijayawada,India

***Abstract*— The Wireless communication has been favoured by many promising applications that require packet delivery from one or more senders to multiple receivers. Notifications are sensitive to various types of attacks because the channels are unsecured in wireless. The wireless communication has a number of difficult issues. In this article we present the types of attacks and countermeasures and address the problem of channel congestion of interference in wireless networks. In these attacks, the opponent is active only for a short period of time, selectively posts of great importance. We illustrate the advantages of channel blockade in terms of degradation of network performance. Wireless networks are used in many commercial and military applications to bring data based on real-time events. Research in network security has produced several security solutions. And 'it is observed that the rate of delivery of packets decreases as the number of nodes increases.**

***Keywords*—wirelesscommunication; Reciever;Attacks,congestion**

I. *Introduction*

Wireless networks rely on the continuous availability of the wireless medium to interconnect the participating nodes. However, the open nature of this medium makes it vulnerable to multiple security threats. Anyone with a transceiver can spy wireless transmissions, inject false messages, or jam legitimate ones. While listening and message injection can be prevented by cryptographic means of interference attacks are much more difficult to counter. It has been shown to update serious denial of service attacks (DoS) attacks against wireless networks. In the simplest form of push, the adversary interferes with the reception of messages by transmitting a jamming signal continuously, or several short interfering pulses. First, the adversary must spend a significant amount of energy to the frequency bands of interest jam. Second, the continued presence of unusually high levels of interference makes such attacks easy to detect. Conventional anti-jamming techniques rely heavily on spread spectrum (SS) communications or some form of lock avoidance (eg, frequency hopping or withdrawals slow spatial retreats). The wireless network is important as one of the most promising concepts for self-configuration and self-organizing wireless network to provide adaptable and flexible wireless connectivity for mobile users.

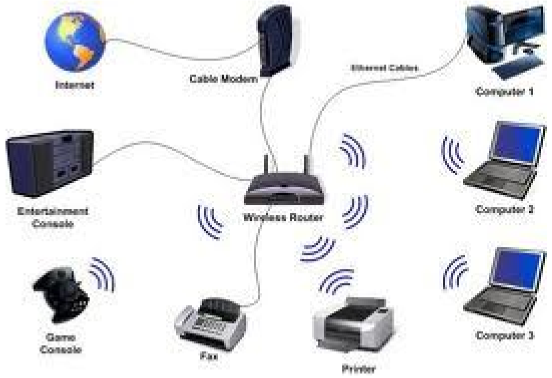

Fig 1: Outline for Wireless LAN Network

II. *Wireless LAN Overview*

In this section, we give a brief overview of wireless LAN (WLAN), emphasizing the characteristics 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 access point(AP) or between two wireless clients. To call 802.11, must be that of medium access control (MAC) and physical layer specifications. The IEEE 802.11 standard covers (Layer 1) physical and data link (Layer 2) of the OSI model layers.

A. *stations and access points*

A card wireless network interface (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 distribution service to stations associated frame. The AP itself is typically connected to a LAN cable. AP station and each contains a network interface that has an address of medium access control (MAC) and wired network cards do. This address is a 48-bit worldwide-unique, assigned to him at the time of manufacture. The 48-bit address is often represented as a string of six octets separated by colons or dashes, 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 bytes long Service Set Identifier (SSID), which 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 SSID label the respective networks, and allow the network components to ignore the other. SSID can also be assigned to Virtual LANs therefore some APs support multiple SSIDs. Unlike the fully qualified host names are not registered SSID, and it is possible that two separate networks use the same SSID.

B. *Channels*

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

C. *WEP*

Wired Equivalent Privacy (WEP) is a system of shared secret-key encryption is used to encrypt packets transmitted between a station and an access point. The WEP algorithm is intended to protect wireless communication from intruders. A secondary function of WEP is to prevent unauthorized access to a wireless network. WEP encrypts the payload of the 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 stations and the AP through 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 ad hoc mode, each station is a point to the other stations and communicates directly with other stations in the network. AP is not involved. All stations can send Beacon and Probe frames. The ad hoc mode stations form an Independent Basic Service Set (IBSS).A station on the infrastructure mode only communicates with an AP. Basic Service Set (BSS) is a set of stations that are logically associated with each other and controlled by a single access point. Together, they operate as a fully connected wireless network. The BSSID is a 48-bit 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. *Marcos*

Both the station and collect and radiate 802.11 AP frames as necessary. The frame format is illustrated below. Most frames containing IP packets. The other pictures are for management and control of the wireless connection. There are three kinds of frames.

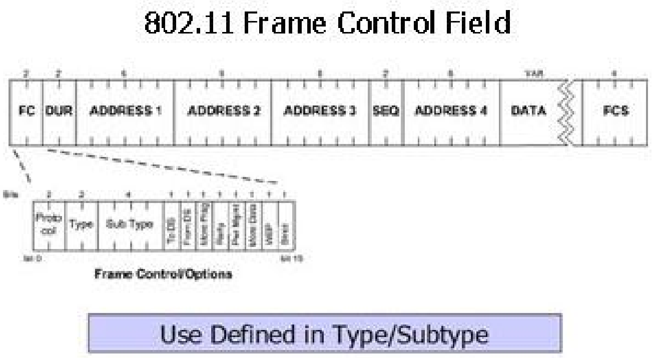

Fig 2:Frame Format of IP Packet

It is the request of the Association, the Association's response, the request for re-association, reassociation response, probe request, probe response, Beacon, Traffic Indication Message Announcement, disassociation, authentication, De-authentication types. The SSID is part of several management frameworks. Management messages are sent always safe, even when using link encryption (WEP or WPA), so that the SSID is visible to anyone who can intercept these frames. Control frames assist in the delivery of data.

F. *Authentication*

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

III. Different types of wireless attacks

A. *Denial of Service Attack:*

A denial of service attack (DoS) occurs when an attacker continually bombards a specific access point (AP) or network with bogus requests, premature successful connection messages, error messages and / or other commands. These legitimate users because of not being able to get on the net and can even cause the network to crash. These attacks are based on the abuse of protocols such as Extensible Authentication Protocol (EAP).The DoS attack itself does little to expose data to a malicious attacker organization since the network interruption prevents the flow of data and, indeed avoiding indirectly protects data to be transmitted. The most common reason for a DoS attack is to observe the recovery of the wireless network, during which all initial recognition codes are relayed by all devices, providing an opportunity for a malicious attacker to register these codes and the use of various cracking "" The tools to analyze and exploit security weaknesses to gain unauthorized access to the system. This works best in systems weak WEP encryption, where there are a number of tools available that can launch attack style security keys "possibly accepted" based on the security key "model" captured in the recovery dictionary network.

B. Jamming Attack:

Since RF (radio frequency) is essentially an open environment, jam can be a big problem for wireless networks. Interference is one of many exploits used to compromise the wireless environment. Its action is to deny service to authorized users and that legitimate traffic is jammed by the overwhelming frequency of illegitimate traffic. An attacker with knowledge of the right tools can easily interfere with the frequency of 2.4 GHz in a way that reduces the signal to a level that can no longer operate the wireless network. Jam complexity is the fact that there may be caused intentionally, as other forms of wireless technology based on the 2.4 GHz frequency, and. Some consumer products used include cordless phones, Bluetooth devices and baby monitors, all capable of interrupting the signal from a wireless network and halting traffic.

C. Man in the Middle Attack:

The attack man-in-the-middle in cryptography and computer security is a form of active listening 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 through a company 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 straightforward in many circumstances.

D. Interception of Attack:

The wireless network uses a user name and password to allow access to the local network, the attacker can use a wireless sniffer attack. An attacker can track and capture legitimate traffic. Many of the tools that accomplish this are based on capture of the first part of the connection session, where data usually include the user name and password. With this, the intruder can then be disguised as that user by using this captured information. Wireless Inhalation requires the attacker is within range of the wireless traffic. This is usually about 300 feet away, but the team continues to strengthen its signal wireless, wireless signal pushing further. At first glance this appears to be a beneficial feature for the user, since the user can access the network or surf the web in a location away from the base station, but actually creates a greater risk to the user, and that allows intruders to attack in an even more too. If an attacker can intercept wireless traffic, it is possible to inject false traffic on the connection. The attacker can hijack the victim's session by issuing orders on behalf of the user.

E. Rap Attack:

RAP (access points) have become a major problem in wireless security. A rogue access point is one connected to a network without authorization from an administrator. With access points constantly low end lower prices and increased availability, the NAPs have become much more common. Furthermore, many of these access points contain features that make them almost invisible when combined with legitimate networks, doing a good job of hiding their presence. Rogues access points are often created by employees for greater freedom in the workplace. Many employees simply bring their points of access from home and plug them right into their jobs and the company LAN without the consent of the directors. Such regional action are potentially dangerous because many people who create them are not aware of the security issues associated with a wireless network.

F. Attack Ad Hoc Associations:

Ad hoc mode allows computers to communicate peer-to-peer. An example would be two people who want to share a file, but could not come to a USB flash drive or a recordable CD between them. So just configure their computers to use ad hoc networks and move the file from one computer to a shared folder on the other computer. The availability of USB flash drives these days usually exceeds this process as the creation of an ad hoc network can be a complicated and time consuming. This is a good thing, as you can see in the post of Mr. Hiner. But even just having ad hoc association enabled on a computer is inviting any computer configured similarly and within the range of association, including people who want to do harm.

G. MAC Spoofing attack:

MAC spoofing attacks are attacks by clients in a Layer 2 network. Attackers spoof MAC address for an in-the-middle-man attack (MITM). In a common attack, the attacker poses as the default gateway and sends a gratuitous Address Resolution Protocol (ARP) to the network for users to send their traffic through the attacker instead of the default gateway. The attacker forwards the user traffic to the actual default gateway. An attacker on a fast enough machine can capture and send packets to victims see no change in their access to the network. Many of the tools available for download from the Internet, such as Ettercap, can fulfill this task, and prevention of this type of attack is quite problematic.

H. Evil Twin:

Evil Twin is a term for an access point Wi-Fi for criminal purposes appears to be a legitimate in the building, but in reality has been created by a hacker to eavesdrop on wireless communications among Internet .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 supplier. Devices wireless Internet link through "hot spots" - nearby connection points that enclose. But these hotspots can act as an open door for thieves. Anyone with suitable equipment can locate an access point and take his place, replacing its "evil twin". This kind of evil twin attack can be used by a hacker to steal passwords from unsuspecting users, either sniffing the communication link or phishing, which involves creating a fake website and attract people there.

IV. Wireless Attacks Counter Measures:

The following are the response measures for different types of attacks that is how these attacks are under attack due to the lack of following reasons.

1. Recognize the characteristics of the primary modes used for cellular communication
2. Recognize the characteristics of RF technology 2.4GHz wireless LAN
3. Identify the components of the Bluetooth security algorithms
4. Identify the Sequence of steps of the association process
5. Recognize the characteristics of WEP authentication methods
6. Identify the vulnerabilities of WEP
7. Recognize how wireless networks are vulnerable to denial of service attacks
8. Recognize how the bubble emission makes wireless networks vulnerable to espionage
9. Recognize the common wireless hacking tools

V. Channel Congestion Attacks

We give a brief description of these anti-jamming approaches.

A. *The information replication control:* An intuitive approach to combating channel interference is repeated multiple control information dissemination channels. In this case, an insider with limited hardware resources can not jam all emissions at the same time. Moreover, if the node has only partial knowledge of the locations of the transmission channels, privileged information may address only a subset of channels known to it. Due to the limited number of channels available, this system provides protection against a small number of colluding attackers.

B. *PN code assignment unique:* An alternative method for neutralizing channel congestion attack is dynamically vary the location of the broadcast channel on the basis of the physical location of the communication nodes. [7] The main motivation of this architecture is that any issue is inherently limited to the communication range of the transmitting station. Thus, for the broadcasts intended for the receivers in different collision domains, there is no particular advantage in using the same broadcast channel, different from the design simplicity. Allocating different broadcast channels to different regions of the network leads to a partitioning of the network inherent in groups.

C. *Elimination of secrets:* the interference targeted attacks can be countered insider secrets to avoid the first. In the design proposed in [9], a transmitter randomly selects a PN code from a public codebook. To recover a transmitted packet, receivers must record the transmitted signal and decoding attempt using each PN code in the codebook

D. *Jamming attacks Countering selective data* An intuitive solution to prevent packet classification is to encrypt the packets transmitted with a secret key. In this case, the entire packet, including its header, must be encrypted. While a shared key enough to protect the point-to-point communications, for the broadcast packets, this key must be shared by all intended recipients. Therefore, this key is also known that one inner jaw. In symmetric encryption schemes based on block encryption, receiving a cipher text block is sufficient to obtain the corresponding plaintext block, if one knows the decryption key. Therefore, encryption alone does not prevent insiders from classify packets issued. To avoid classification, a package must remain hidden until transmitted in its entirety. One possible way to temporarily hide the packet transmitted is the use of commitment schemes. In a commitment scheme, the transmitting node hides the package by spreading a compromised version of it. Package content cannot be inferred by receiving the commitment (hiding property). After the transmission is completed, the node releases a value-commitment, revealing the original package

E. *Congestion identification Dropper:*

Current methods to detect misbehavior such as self-organizing systems WMN can be classified into Reputation systems [2], the credit-based systems , and recognition systems [1]. Reputation systems: Reputation systems identified misbehaving nodes based on reputation metrics per node, calculated on the basis of interactions with each node peers.

Various schemes have been proposed for the management of handling of information. Node can flood warnings throughout the network, if it detects misbehaving node. Alternatively, the information can be provided on-demand, after a request from a particular node has been received. In the latter scenario, floods of the application are necessary to discover nodes that have second-hand information. Both methods consume considerable bandwidth resources because the underlying flood operations for the dissemination and collection of second-hand information. Computer robust reputation metrics is equally important for the identification of packet droppers. The simple aggregate statistics have proved vulnerable to false accusations of collusion malicious nodes, and sudden changes in behavior patterns. For example, a misbehaving node can exhibit a long history of good behavior in order to build a reputation metric before begins to misbehave. These cases are handled by assigning greater weight to recent behavioral observations and / or the adoption of additive-increase multiplicative decrease algorithms for updating the reputation metrics. A key challenge for any metric calculation algorithm is the selective nature of packet droppers. When a very small fraction of the packets are dropped, the indicators do not take into account the type of package are required to have high rates of misdetection. Dropping the selectivity can be detected with the use of storage-efficient reports (For example, on the basis of Bloom filters) by bundle conduct node. Based on these reports, it is possible to perform multiple tests to identify malicious selective drop patterns. These patterns are likely to have some structure compared to deterministic packet losses due to congestion or bad channel quality.

F. ACK based systems: schemes based on different techniques in hearing collection method behavioral observations firsthand. Intermediate nodes (More than one hop away) are responsible for acknowledging receipt of messages to multiple nodes upstream jumps [10]. These systems are suitable for the faithful retransmission control unicast traffic, at the expense communication overload for transmitting an additional ACKs assembly. However, the ACK-based schemes are not used to identify emission insiders selectively dropping packets. Such packages are maintained generally unacknowledged in wireless networks, to avoid ACK implosion situation. Moreover, a small set of colluding nodes can ACKs still provide authentic previous nodes while dropping packets.

CONCLUSION

WMNs are prone to various external and internal security threats. While most external attacks can be mitigated with a combination of cryptographic mechanisms and robust communication techniques, internal attacks are much harder to counter because the adversary is aware of the network security and its protocols. Channel congestion attack is a challenging problem. Current solutions attempt to eliminate the use of these attacks for protecting broadcast communications.

References

[1] I.F. Akyildiz, X. Wang, and W. Wang. Wireless mesh networks: a survey. Computer Networks, 47(4):445–487, 2005.

[2] EEE P802.11s/D1.01 standard. At https: //mentor.ieee.org/802.11/dcn/07/11-07-0335-00-000s -tgs-redline-between-draft-d1-00-and-d1-01.pdf, 2007.

[3] Alejandro Proano and Loukas Lazos. Selective jamming attacks in wireless networks. In Proceedings of the IEEE International Conference on Communications (ICC), 2010.

[4] T.X. Brown, J.E. James, and A. Sethi. Jamming and sensing of encrypted wireless ad hoc networks. In Proceedings of the 7th ACM International Symposium on Mobile ad hoc networking and computing, 2006.

[5] J. So and N.H. Vaidya. Multi-channel MAC for ad hoc networks: handling multi-channel hidden terminals using a single transceiver. In Proceedings of the ACM MobiHoc Conference, pages 222–233, 2004.

[6] P. Tague, M. Li, and R. Poovendran. Probabilistic mitigation of control channel jamming via random key distribution. In Proceedings of the International Symposium in Personal, Indoor and Mobile Radio Communications (PIMRC), pages 1–5, 2007.

[7] L. Lazos, S. Liu, and M. Krunz. Mitigating control-channel jamming attacks in multi-channel ad hoc networks. In Proceedings of the Second ACM Conference on Wireless Network Security (WiSec), pages 169–180, 2009.

[8] Jerry Chiang and Yih-Chun Hu. Cross-layer jamming detection and mitigation in wireless broadcast networks. In Proceedings of the ACM MobiCom Conference, pages 346–349, 2007.

[9] Christina Popper, Mario Strasser, and Srdjan Capkun. Jamming- ´ resistant broadcast communication without shared keys. In Proceedings of the USENIX Security Symposium, 2009.

[10] K. Liu, J. Deng, P.K. Varshney, and K. Balakrishnan. An acknowledgment-based approach for the detection of routing misbehavior in MANETs. IEEE Transactions on Mobile Computing, 6(5):536–550, 2007.