Jamming Attacks in Wireless Networks

S.Praveen Kumar, *S.Swapna*

Aurora's Technological and Research Institute, JNTUH Hyderabad, Andhra Pradesh, pin code-500035, India

Summary
The commodity of the medium in wireless networks makes it easy for an adversary to launch a Wireless Denial of Service (WDoS) attack. A jammer can continually transmit a radio signal in order to block any access to the medium by legitimate wireless nodes. Jamming techniques can vary, from simple ones based on the continual transmission of interference signals, to more sophisticated that rely on exploiting the protocol used for communication among wireless devices. We illustrate various techniques that where introduced in order to detect the presence of an adversary node as well as the mechanisms proposed for protecting the network from such attacks.

Keywords
Wireless DOS, Jamming, Security in Wireless Local Area Network.

1. Introduction

Jamming is a special kind of DoS attack and it is specific kind of wireless networks. Jamming occurs when Radio Frequencies interfere with the operation of the wireless network. In some cases, the jamming is not malicious and is caused by the presence of other devices, such as cordless phones, that operate in the same frequency as the wireless network. In a case like this, the administrator should implement policies regarding the use of these devices, such a banning the use of Bluetooth devices, or choose wireless hardware that uses different frequencies. Intentional and malicious jamming occurs when an attacker analyzes the Spectrum being used by wireless networks and then transmits a powerful signal to interfere with communication on the discovered frequencies. Fortunately, this kind of attack is not very common because of the expense of acquiring hardware capable of launching jamming attacks. This jamming a network represents a kind of pyrrhic victory for the attacker—a lot of time and effort expending merely to disable communications for a while. Many metropolitan areas deploy public WMANs for people to use freely. Moreover, the prevalence of WLANs as the basic edge access solution to the Internet is rapidly becoming the reality. However, wireless
Networks are accompanied with an important security flaw; they are much easier to attack than any wired network [1] Denial-of-service (DoS) attacks against such networks may permit real-world damage to the healthy and safety of people. Without proper security mechanisms, networks will be confined to limited, controlled environments, negating much of the promise they hold. The limited ability of individual sensor nodes to thwart failure or attack makes ensuring network availability more difficult. [2].
Wireless signal jamming are used to interfere with wireless local area networks (WLAN); and it is a type of Denial of service (DoS) attack. The Wireless Signal Jamming Device is used to stop transmission temporarily or turn off the power during the usage of units. These include Radios, Televisions, Microwaves, or any unit that receives electrical signals for operation. These are more advanced and more expensive version used to jam satellite communications. A jamming device transmits the radio frequencies in the cell phone, disrupting the communication between the phone and the cell-phone base station in the tower. These Wireless signal jammers are most often used to interfere with the wireless local area networks (WLAN), and this jamming is a type of denial of service (DoS) attack. Jamming is the radiation of electromagnetic energy in a communication channel which reduces the effective use of the electromagnetic spectrum for legitimate communication. Jamming results in a loss of link reliability, increased energy consumption, extended packet delays and disruption of end-to-end routes [5].

2. Managing the Denial of Service Attacks

- Design business for survivability. To have business continuity provisions in place.
- Design network for survivability. To take steps that help to ensure that critical services continue in spite of attacks or failures and you should be a good network citizen so that Your potential to be attacked depends on the security of other sites and vice versa.
- And make your network is directly proportional to the extent that other Internet users, including home users, adhere to good practices. Conversely, the threat that your network represents to others is directly proportional to the extent that your organization adheres to good practices. [3]

Attacks can be managed and which is of two ways:
1. Make target of that attack.
2. Make abused to amplify the attack on the networks.
If you do not take a specific action on the Denial of Service (DOS) the attacks can do a serious damage to your network services or as an entire institution in that your network. To

Manuscript received October 5, 2013
Manuscript revised October 20, 2013

prevent the network from such attacks you should turn off the broadcast on all router ports or you should take the measures to assure your network cannot be abused in this manner. Adversaries may easily observe communications between wireless devices, and just as easily launch simple denial of service attacks against wireless networks by injecting false messages. By doing so, he either prevents users from being able to commence with legitimate MAC operations, or introduces packet collisions that force repeated back offs, or even jams transmissions. [4] So for these we are using MAC and PHY layer security threat in the wireless network with the help of the MAC address we are going to attack the server the client request is blocked by the server the denial of service is protected by the network in the wireless computers. Nowadays in Internet the Denial of service attacks (DoS attacks) are some of the hardest security problems.

3. Background on MAC Protocol

Each network adapter should have a unique MAC address (Media Access Control. It consists a series of twelve letters and numbers that functions at the most basic level so your router can communicate with your device. With MAC address filtering, each device that attempts to connect to the network must match its MAC address to a list you define in the router's administration tool. Wireless networks are less secure than wired ones. So the wireless security is the prevention of unauthorized access or it damages to computers using wireless networks.

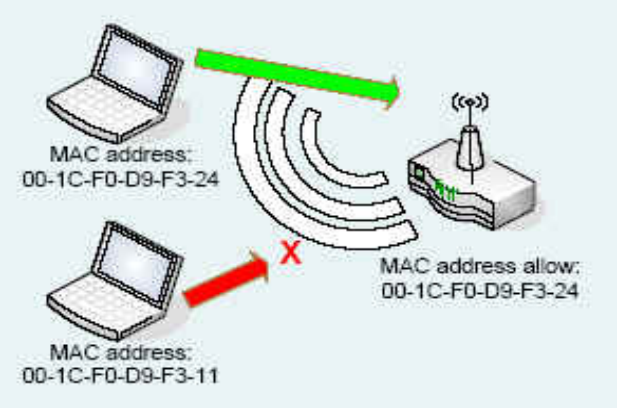

Fig shows MAC address Filter:

With the deployment of wireless networks in business environments, organizations are working to implement security mechanisms that are equivalent to those of wire-based LANs. An additional component of this security requirement is the need to restrict unauthorized users and allow the wireless network to authorized users or (valid users). Physical access to the WLAN is different than access to a wired LAN. Existing wired network have access points, typically RJ45 connectors, located inside buildings which may be secured from unauthorized access through the use of such devices as keys and/or badges. A user must gain physical access to the building to plug a client computer into a network jack. Once the device is authenticated then the user of the device can be authenticated. At this point the user may desire a secure channel for communication [6]. With the help of these MAC we can not provide the network for unauthorized person. Access points and routers they keep track of the MAC addresses of all devices which are connected to them. Then the administrator restricts the network to allow connections from those MAC addresses that you specify. That means outsiders people makes very difficult to access your network. Make sure that you use this option to specify only those MAC addresses that are allowed to access the network.

4. Threats in Wireless Networks

The following steps which involves the ways of maintaining the secure wireless networks and associated devices.

1. We should maintain a full understanding of the topology of the wireless network.
2. Frequently we should Create a data backups
3. We should apply the patches in security enhancements.
4. Labeling and keeping inventories of the fielded wireless and handheld devices are necessary.
5. We should define standard security settings for access points.

Now a day's Wireless technology are changing rapidly. New products and features are being introduced continuously. So, for these we should provide security in the Wireless Networks. These WLANs are flexible and portable than the traditional wired local area networks (LAN) these LAN, requires a wire to connect a user's computer to the network, this WLAN connects to computers and other components to the network using an access point device. The access point communicates with devices with the help of wireless network adaptors (WNA). These (WNA) connects to a wired Ethernet LAN via a RJ-45 port typically these access point's coverage area is approximately 100 meters. The coverage area is nothing but 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. [7].

Wireless technologies uses radio frequencies signal transmissions for transmitting data, whereas wired technologies use cables. Malicious hackers are general individuals from outside of an agency or organization such hackers may gain access to the wireless network access

point by eavesdropping on wireless device communications. Malicious code involves viruses, worms, Trojan horses, logic bombs, or other unwanted software that is designed to damage the files in the computer. An attacker can apply the jamming in several ways. We should apply local device protection jamming attack on wireless communication.

5. Packet Sending and Receiving

With the help of these packets the data is transferred through the network. Data can be divided into *packets*

- Data routes across the Internet can be *Switched* to avoid congestion
- Entire mechanism is handled by the TCP/IP protocols.

The receiving mechanism, or protocols, that are used to encode the packet ensures safe transit, and provides a way of reconstructing the data when it reaches its destination. The protocols used on the Internet are referred to as Transmission Control Protocol. These TCP/IP labels the each packet with the unique IP address of another computer. The packets are sent from one "router" to the "another router" so that each router reads the IP address of that packet and decide the path. Thus the packet is transferred on the desired path. Transmissions of the packets at the head of the queue can eventually *expire* and the packets themselves get discarded. [1] Our technique exploits an intrinsic characteristic of the wireless medium: since the power of the jamming signal degrades with distance, farther transmitters do not sense strong jamming signals. In addition, the SNR requirement at such transceivers is often satisfied. This cannot be concealed by the attacker [8] The attacker choose to expose their identities by using a small number of IP addresses or risk being quickly detected by using randomly spoofed IP addresses. The evaluation results show that *Source IP address Monitoring (SIM) [9]*. *S*ome network services are available to any system that is attached to the network and that is capable of sending and receiving packets. This is certainly true of the lowest-level service of packet delivery, in which the only barrier to sending packets is obtaining a network connection. [10] In other cases, the legitimate provision of some network services might require authorization dependent on authentication using an Internet Protocol address, password, or cryptographic credential. This type of authentication is normally performed in applications at the highest layer of the network, and the packets are still delivered by the network even if the authorization fails.

5.1 Packet Send Ratio (PSR): [1, 4]

The ratio of packets that are successfully sent out by a legitimate traffic source compared to the number of packets it intends to send out at the MAC layer. Suppose *A* has a packet to send. Many wireless networks employ some form of carrier-sensing multiple access control before transmission may be performed.

For example, in the MAC protocol employed by Mica2, the channel must be sensed as being in an idle state for at least some random amount of time before A can send out a packet. Further, different MAC protocols have different definitions on an idle channel. Some simply compare the signal strength measured with a fixed threshold, while others may adapt the threshold based on the noise level on the channel. A radio interference attack may cause the channel to be sensed as busy, causing *A*'s transmission to be delayed. If too many packets are buffered in the MAC layer, the newly arrived packets will be dropped. It is also possible that a packet stays in the MAC layer for too long, resulting in a timeout and packets being discarded. If *A* intends to send out *n* messages, but only *m* of them go through, the **PSR is *m/n***. The PSR can be easily measured by a wireless device by keeping track of the number of packets it intends to send and the number of packets that is successfully sent out. [1] and [4].

5.2 Packet Delivery Ratio (PDR) [1, 4]

The ratio of packets that are successfully delivered to a destination compared to the number of packets that have been sent out by the sender. Even after the packet is sent out by *A*, *B* may not be able to decode it correctly, due to the interference introduced by *X*. Such a scenario is an unsuccessful delivery. The PDR may be measured at the receiver *B* by calculating the ratio of the number of packets that pass the CRC check with respect to the number of packets received. PDR may also be calculated at the sender *A* by having *B* send back an acknowledge packet. In either case, if no packets are received, the PDR is defined to be 0. [1] and [4].

6 Conclusion

Wireless networks use free space as medium with Radio frequency Signal to connect sending and receiving devices. Securing the Dos attacks depends on the whole internet community. Protection to your computer from malware that could be used in these attacks. The Security against DOS is an ongoing race between the hacker experts. So in this paper we are using the proposed system for providing the security. Unfortunately, there is no such thing as secure data on a computer these days. Hacking attempts and other exploits are increasingly on the rise, causing a direct threat to your personal data. In order to secure your confidential files and folders, you should configure them with password protection or go one step further with encryption. By doing so, you can limit the chances of someone breaking into the system and viewing or stealing your sensitive data.

Reference

[1] Konstantinos Pelechrinis, Marios Iliofotou and Srikanth V. Krishnamurthy "Denial of Service attacks in Wireless Networks: The case of Jammers" in IEEE Communications Surveys & Tutorials, VOL. 13, NO. 2, SECOND QUARTER 2011.

[2] Anthony D. Wood and John A. Stankovic. Denial of service in sensor networks. IEEE Computer, 35(10):54.62, October 2002

[3] Computer Emergency Response Team. CERT Advisory CA-2000-01 "Managing the Threat of Denial-of-Service Attacks, v10.0, October 2001.

[4] W. Xu, W. Trappe, Y. Zhang, and T. Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In ACM MobiHoc, 2005.

[5] Miroslav Pajic and Rahul Mangharam "Anti-Jamming for Embedded Wireless Networks" Department of Electrical and Systems Engineering University of Pennsylvania

[6] Robert J. Boncella(2002). Wireless Security: Communications of the Association for Information Systems (Volume 9, 2002) 269-282

[7] Tom Karygiannis and Les Owens (2002). Wireless Network Security 802.11, Bluetooth and Handheld Devices.

[8] K. Pelechrinis, I. Koutsopoulos, I. Broustis and S.V. Krishnamurthy,"Lightweight jammer localization in wireless networks: System design and implementation," Globecom, 2009.

[9] Tao Peng ,Christopher Leckie ,Kotagiri Ramamohanarao "Detecting Distributed Denial of Service Attacks Using Source IP Address Monitoring" ARC Special Research Center for Ultra-Broadband Information Networks Department of Electrical and Electronic Engineering The University of Melbourne, Victoria 3010, Australia.

[10] Clay Shields. What do we mean by network denial of service? In Proceedings of the 2002 IEEE Workshop on Information Assurance and Security, June 2002.

S. Praveen Kumar is pursuing M.Tech in Web Technologies from Aurora's Technological and Research Institute, JNTUH, A.P, INDIA. His research areas include image processing, and computer networks.

S. Swapna received her M.Sc. Computer Science in 2007 from Reddy women's College Narayanguda and M.Tech in Web Technologies from Aurora's Technological and Research Institute, JNTUH, A.P, INDIA. Her area of expertise includes Operating system, Web Security and Database and Management System (DBMS), image processing. She is working as Assistant Professor in department of Information Technology at Aurora's Technological and Research Institute, Hyderabad