Study on Jammers and Defense Strategies in Wireless Networks

E.Sasikala
Assistant Professor, KSR College of Engineering

N. Rengarajan, PhD.
Professor & Principal, KSR College of Engineering

ABSTRACT

Wireless networks overcame the limitations of the traditional approaches in the implementation of the wired networks. The number of nodes can be easily extended and provided with then the services of the networks. Amenities of the private networks are risked by the invaders and their activities to disclose the confidential contents. These invaders established a standard mode of attacking by jamming the services upon described functions. The jammers would key in attack packets to the networks claiming to be a reasonable request to block the services of the intended users. Ultimately, the network would continue answering the meaningless queries of the attackers thereby avoiding or making the users to wait indefinitely. Increase in the attacks would degrade the services and standards of the wireless networks. Denial of Service (DoS) attacks involves mechanisms to flood the medium of data transfer with futile packets, or to alter the contents of the significant information of the packets. Denial of Service attacks has extended their area of attacks to pretense their identity and revises the contents of the message packets to pose a threat to the networks. Mechanisms that have been proposed to detect and mitigate the effects of those jammers are examined in this study.

Index Terms: Jamming, detection mechanisms, wireless networks, network security

1.INTRODUCTION

Networks have been implemented to share the services to a number of users of the same characteristics. The central repository acts as the source for the demanding users irrespective of the number and on possessing the right authentication. Every node in the network has been provided with a constant established link via cables. These links also limited the entry of the attacker into the network. The network administrator is the only member to authenticate and allow access to the new users, possessing the central control over the available users in the networks.

Discussing this strategy makes it solid that the extendibility is limited to a level and cost constraints over the implementations are considerably higher. Efficiency of the networks is based on the security and other safety measures included for protecting the users and their sessions. The wireless networks era simplified the methodologies for implementing a large network over different geographical locations still possessing a central control and resources repository for numerous users. Internet services are the best example of such a network providing services to limitless users simultaneously and accurately. Individual organizations with branches over different nations can be ascertained with much easier methodologies and low cost. Wireless networks eliminated the impractical connectivity and made the unpredicted channels for communication to be possible. These wireless networks have been preferred in most applications nowadays.

But the major factor to be considered in these networks is whether it contains equal security options as the traditional approaches. The wireless networks have defined easier protocols to enter and obtain access to the services of the networks [1][4]. This applies to the unauthorized users too. Members or Nodes other than the network administrator authorizes are attackers of the network. The attackers intend to fixate their connection with the network and disturb the efficiency of the network. Attackers originate their attacks in the form of requests to obtain a service or a connection establishment.

The attackers are named to be the Jammers, as the name suggests, the allocated bandwidth for communication is subjected to illegitimate data transfer. The bandwidth permits the attack packets which in turn deny service for the intended users [3][5]. Jammers were initially blocking the bandwidth allocated. In recent past, jammers are capable of attacking the individual packets after analyzing the type of packets and their information on the source and destination addresses, the length of the packets, the information on the path selected for the data transfer.

2.A DISCUSSION ON THE JAMMERS

Unauthorized users try to misuse the services and block the authorized from getting their intended service. These attackers continuously forward uncontrolled number of requests at the same time and preventing the network to concentrate on the prescribed function. The prescribed function is the response to the request of the intended user. Different requests of varying issues would distract the network and confuse the network on the priority on tasks leading to a sudden death of the system.

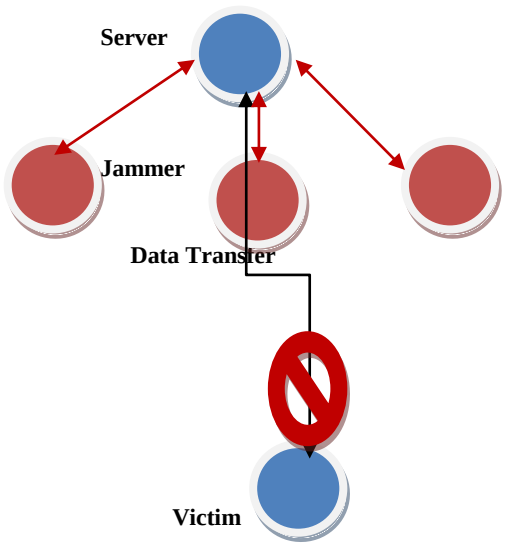

Figure 1: Forwarded Attack Packets from Jammers to block the service of Intended User

Jammers [6]were devices to transmit a high power signal of the same frequency as the original radio signal. The transmission and reception of the radio signals requires high power transreceivers at both the ends. The original signal of each radio would select the particular frequency for transmission. The antenna would focus over a specific direction and starts its transmission. The receiver at the other end would need to be tuned to the same frequency for reception of the original signal. Slight variations would introduce noise and other interfering signals along with the right signal. Jammers, the attackers in the meanwhile would select the same frequency and transmit a high power signal in the medium. The receivers end will be able to receive the high power attack signal instead of original signal. These jammers were implemented in war fields to prevent the opponent nation from misleading the people about false information.

The same conceptual model was proposed in the wireless networks, to block the medium with packets of data and control messages with no meaning. The server would be fooled or not care about the verification of the origin of those packets. Doubting the uncontrolled flow of packets in these mediums then initiates a defensive strategy. Jammers in wireless networks have to be more responsive over the sensing of the type of packets being transmitted in the medium to produce an equivalent attack to avoid detection. The type of packets may be of control, data, or any request messages to establish connection and their responses. Alterations in the information content of the messages would greatly affect the sensitivity of the messages. Jamming activities are based on the level of alterations in the content.

3.JAMMING ACTIVITIES

The jamming[3] can be mere flooding of the packets into the medium or try accessing the network by impersonating as a legitimate user. The network maintains a log on the authorized users with the details on the Access points, IP addresses and the location based definitions. The server considers a table named as Access Identification (AID) to record the permitted users of the network. Jammers have evolved to obtain access from the network by impersonating as an original user. The major defect of the wireless framework is the unwrapped architecture, which eliminates the need for checking the frame authentication and the physical boundary (location) of the requesting node. The node may forward a request from any location and can obtain service. The jammer is also capable of faking the identity of a particular user and transfer packets on his/her behalf.

The other modes of attacks are to drain the resources of the network medium or the node. The medium is of limited bandwidth which can be easily misused by fake data transfer of the attackers. Intended for the better availability of resources to limitless users, little care has been taken on the authenticating protocols. This facilitated the number of users to enter, access and exit the network. Simplifying the entry procedure encouraged many attackers to misbehave and jam the services to the other users. The jamming nodes are either internal or external to the network. External and internal users have distinguished characteristics. The jammers have a specifying mode of attack and they are discussed as follows.

4.TARGETS OF JAMMING ATTACKS

Flooding the packets into the medium comprised of mechanisms to increase the flow of packets than the permitted levels of flow to exhaust the medium. This type of attack[5] would have a clear pattern and possess a same origin in most cases. Flooding attacks are easier to be detected and thus the path can be blocked as the remedy. This mode of attack does not need much effort as the packets do not have any order or characteristics and thus forwarded to a specific targeted address of the victim. ICMP, SYNC floods are the examples of this type of jamming attacks.

Jammers also impose attack on the different contents of the message packets. The data packets transferred would be comprised of route requests and route responses of different nodes[5][7]. The nodes need to request a server for establishing a connection and the server responds with a yes or no message. Jammers blocking the route requests and responses would eliminate the connectivity and further communication. If there is no connection established then the nodes cannot obtain services from the server. If the either messages are not responded, the node remains waiting for the responses indefinitely. The Clear To Send (CTS) and Request To Send (RTS) messages are transferred between the source and destination for seeking permission to forward a message. Considering the necessity of this pair message is absolute for communication. Either of this message is enough to be blocked for jamming the entire activities of the network. Without the request, there is no CTS message and after a request made, there should be a CTS response.

The above mentioned jammers need a proper analysis on the type of the packets transmitted. There are other jammers which block only the narrowband signal. These signals blocking jammers are devices which are transmitting signals of the source frequency. The equivalent energy signal jams the medium which denies the service for the legitimate users. Signal jammers are not energy efficient as they operate on the limited battery backup and drain as soon as they emit the signal continuously.

Jammers originate the disassociation and deauthentication attacks for affecting the Authenticity of the nodes. Every node needs to be associated to a network after being authenticated by the network administrator. In this type of jamming attacks, the attacker would act as the authenticated user and break the authorization. The network would disassociate the node from its service list and denies its further requests. Deauthentication of node is far more serious than the disassociation attack. The node is removed from the authorized list of nodes and thus the node should renew the whole process to obtain the service again.

The interesting type of jammers is when the attacker raises attacks being internal to the network. Being a part of the network, the already authenticated user would be aware of all the protocols and other frameworks of the network. With enough knowledge on the internal architecture, the adversary is capable of proposing a more serious attack than the external attackers. These jammers concentrate on the messages of high importance such as messages on TCP protocols. The external jammers would possess a pattern of attack such as the source of attack, the type of packets and mitigating them would be considerably easier. In case of an internal attacker, the jammer will not be active for a long time to evade detection and be careful enough about the defensive mechanisms present in the network. These internal jammers are of the greedy nature with the intention of obtaining the exclusive services all the time they need. Otherwise they seek revenge over the grudges held on the organization for some reasons.

The above sections stated the types of jammers and their mode of attacks over the services and resources of the

network. The following section discusses over the countermeasures available.

5.COUNTERMEASURES OF JAMMING

There have been several measures proposed as the remedy for the jamming attacks [7][9][10]. Each measure tried, introduced a new type of attack. The basic countermeasure is to limit the bandwidth and mark their boundaries[16]. This method prevents the entry of the attackers from remote locations. Constraints on the boundaries would eliminate distant and anonymous attacks.

The details on the traffic flow at normal levels, at a congested rate (peak hours) are recorded for periodic monitoring of the traffic flow in the medium. On proved that the normal levels are exceeded then there has been an attack and the defensive strategies implemented are activated [14] [15]. The monitoring also records the information of the sessions of every user, their location and the data transfer.

The implemented defensive and preventive mechanisms are helpful in identifying the attack, controlling the jamming attacks and a few of them tries to trace the source of the attackers to their locality.

6.CONCLUSION

This paper discusses the origin of the jammers, how they are initiated, and the functions of a jammer. The jammers need to be eradicated to improve the efficiency and security of the wireless network. The compatibility and usability enhanced the jammers intrusion. Controls and additional conditions on the framework of the wireless networks could possibly mitigate the jamming attacks. Since every attack is unique, a general strategy cannot be designed to solve all modes of attacks. Hence a solution which is the ultimate and fruitful for major attacks needs to be framed and implemented.

7.REFERENCES

[1] C. Schleher, Electronic Warfare in the Information Age. Artech House,1999.

[2] R. Mallik, R. Scholtz, and G. Papavassilopoulos, “Analysis of an on-off jamming situation as a dynamic game," IEEE Trans.Commun., vol. 48,no. 8, pp. 1360-1373, Aug. 2000.

[3] D. Wood and J. A. Stankovic, “Denial of service in sensor networks,"IEEE Comput., vol. 35, no. 10, pp. 54-62, 2002.

[4] R. Negi and A. Perrig, “Jamming analysis of MAC protocols," Carnegie Mellon technical memo, 2003.

[5] J. Bellardo and S. Savage, “802.11 denial-of-service attacks: real vulnerabilities and practical solutions," in Proc. USENIX Security Symp., pp. 15-28, 2003.

[6] Wood, J. Stankovic, and S. Son. “JAM: a jammed-area mapping service for sensor networks," in Proc. IEEE Real-Time Syst. Symp., pp.286-297, 2003.

[7] G. Noubir and G. Lin, “Low-power DoS attacks in data wireless LANs and countermeasures," SIGMOBILE Mob. Comput. Commun. Rev., vol. 7, no. 3, pp. 29-30, 2003.

[8] J. M. McCune, E. Shi, A. Perrig, andM. K. Reiter, “Detection of denialof-message attacks on sensor network broadcasts," in Proc. IEEE Symp.Security Privacy, 2005.

[9] W. Xu et al., “The feasibility of launching and detecting jamming attacks in wireless networks," in Proc. ACM Int’l. Symp. Mobile Ad Hoc Netw. Comput., 2005, pp. 46-57.

[10] M. Li, I. Koutsopoulos, and R. Poovendran, “Optimal jamming attacks and network defense policies in wireless networks," in Proc IEEE INFOCOM, May 2007.

[11] Q.Huang, H.Kobayashi, and B.Liu. “Modeling of distributed denialof service attacks in wireless networks,” in IEEE Pacific Rim Conf.Commun., Computers and Signal Process., vol. 1, pp. 113-127, 2003

[12] L.Sherriff, “Virus launches DDoS for mobile phones,” [Online]. Available:

http://www.theregister.co.uk/content/l/12394.html

[13] M. Acharya and D. Thuente, “Intelligent jamming attacks, counterattacks and (counter)2 attacks in 802.11b wireless networks,” in Proc.OPNETWORK-2005 Conf., Washington DC, USA, Aug. 2005.

[14] Y.Zhang, W.Lee, and Y.-A.Huang, “Intrusion Detection Techniques for Mobile Wireless Networks,” in ACM J. Wireless Net., vol. 9, no. 5, Sept.2003, pp. 545-56.

[15] A.B.Smith, “An examination of an intrusion detection architecture for wireless ad hoc networks,” in 5th National. Colloq. Inf. Syst. Sec.Education, May 2001.

[16] O.Kachirski and R.Guha, “Intrusion detection using mobile agents inwireless ad hoc networks,” in Knowledge Media Net., Proc. IEEE Wksp.,July 10-12, 2002, pp. 153-58.

[17] W.Xu et al, “Channel surfing and spatial retreats: Defenses against wireless denial of service,” in Proc. 2004 ACM Wksp. Wireless Security,2004, pp.80-89.

[18] V. Navda, A. Bohra, S. Ganguly, and D. Rubenstein, “Using channel hopping to increase 802.11 resilience to jamming attacks,” in IEEE iNFOCOM, Mini-Conf., 2007.