ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, No 5, May 2013

Mitigating Denial of Service Attacks in Wireless Networks

S. Raja Ratna, CSE Department, Francis Xavier Engineering College, Tirunelveli
R. Ravi, Professor, CSE Department, Francis Xavier Engineering College, Tirunelveli
Dr. Beulah Shekhar, Department of Criminology and Criminal Justice, MS University, Tirunelveli

Abstract - **The open nature of the wireless media becomes a root cause for denial of service attack. Denial of Service (DOS) can be different types and disrupt multiple layers. The idea here is to prevent the cyberspace from DOS attack. Zombie is a computer that has been compromised by the hackers for performing malicious activities. Group of zombie computers involved in jamming activities is called botnets. Denial of Service attack either injects malicious packet or drops legitimate packets from the network. The objective of DOS attack is to prevent the receiver from reception of legitimate data and to get control over the entire network. This paper proposes a survey on three types of DOS attack such as selective forwarding attack, pollution attack and jamming attack and its detection techniques.**

Index terms - **Compromise, Cyberspace, DOS, Jamming**

1. INTRODUCTION

Wireless networks are more borne to intentional or unintentional attacks than the wired based networks. The wireless medium allows for radio interference attacks that target communications. The simplest form of such attacks is denial of service attack which can block any current legitimate communication. Communication in wireless network takes place in air medium [2]. Due to the severe security attacks in the wireless media, the network faces various difficulties. Prevention of DOS attack in cyberspace has become a very serious problem in network security.

Cyberspace refers to global network of computers, it is an imaginary, virtual reality where computers communicate and internet activities takes place. In cyberspace the threat will be virtual but the consequences will be real [8]. Hence cyberspace requires prevention from jamming attack while allowing the legitimate users accessing the wireless communication safely. Zombie is a computer connected to the internet that has been compromised by the hackers for sending various attack. Group of zombie computers involved in jamming activities is called botnets. In traditional communication systems, the aim of jammer is to disallow the reception of communications to the receiver using as little power as possible.

A Denial of Service (DOS) prevents the legitimate users from using a specified network resource such as a website, computer system, etc. The Distributed Denial of Service (DDoS) attack is a coordinated attack that is launched indirectly through many compromised computing systems. The Denial of Service attack either drops the packet or injects malicious data into the network. The goal of this attack is to prevent the receiver receiving legitimate data.

If the attacker uses an attack from single host it is called DOS attack [2], whereas in DDOS the attacker uses multiple host simultaneously to launch attack against remote host. It is better to prevent the data from attacking rather than to get cured after attacking. The attacker just flood the network with useless packets to keep the server busy with unwanted traffic or cause congestion so that the server cannot handle legitimate packets or not able to receive packets [15]. The outcomes of attacks are as follows:

1. Large number of illegitimate packets that take too many resources from the network.
2. Making the receiver not able to handle the legitimate data.
3. Causing the system to break down.

In this article we survey the issues related to different types of Denial of service attack by considering both the attack and defend sides of the problem. We present different attack strategies related to wireless network. This paper explains three different types of denial of service attack and the techniques used to detect the attack.

i) Selective forwarding attack
ii) Pollution attack
iii) Jamming attack

In selective jamming attack, the forwarding node receives all the packets but forwards only a portion of it. Pollution attack means injection corrupted packets into the network. Jamming attack tends to block the communication channel.

The remainder of the paper is organized as follows: In Section 2, we analyze selective forwarding attack and its channel aware detection scheme. In Section 3, we discuss about pollution attack related DOS issues and its

code guard detection scheme. Section 4, explains how honey node is used as a scheme for detecting jamming attack. In section 5, we conclude.

2. SELECTIVE FORWARDING ATTACK

In selective forwarding attack / selective dropping attack, the misbehaving router accepts all the packets but refuses to forward all; it forwards only a portion of it while dropping the remaining. But many times, the packet loss may be due to normal collision or bad quantity of the channel. Hence a special detection technique is needed to identify selective forwarding behavior from normal collision losses [9].

In this type of attack, the compromised node delay the route discovery process as well as prevent the router to find [6] any new route for transmission but it forces the router to choose inefficient alternative path. Channel aware detection (CAD) algorithm is used to detect the selective forwarding attack.

CAD Algorithm:

Step 1:

X(i-1) is the upstream node, X(i+1) is the downstream node. Each node X(i) calculate the number of previous hop (upstream) and number of next hop (downstream).

Step 2:

Each node checks for downstream traffic monitoring and upstream traffic monitoring by checking whether there is any dropping of packets.

Step 3:

Measure the loss rate between current node and previous node.

Step 4:

Misbehavior is detected by comparing the measured loss rate with detection threshold.

Step 5:

Two operations are performed when the router sends data to downstream

i) Maintain the acknowledge send by upstream node.
ii) Observe the downstream traffic to find whether the packet is forwarded or dropped.

3. POLLUTION ATTACK

The adversaries inject corrupted packet into the network, it is known as pollution attack. Pollution attack can be of plain packet pollution attack or coded packet pollution attack i.e., the corrupted packets can be either plain packet or coded packet [3]. The packet send by the source is known as plain packet. Coded packet is obtained by performing bitwise XOR operation on a set of plain packets.

Corrupted plain packet and corrupted coded packet are the two types of corrupted packets. A packet is labeled as plain packet, but is different from the original packet sent by the source, it is known as corrupted plain packet. A packet is labeled as coded packet (XORing of plain packet), but is different from the original coded packet, it is known as corrupted coded packet.

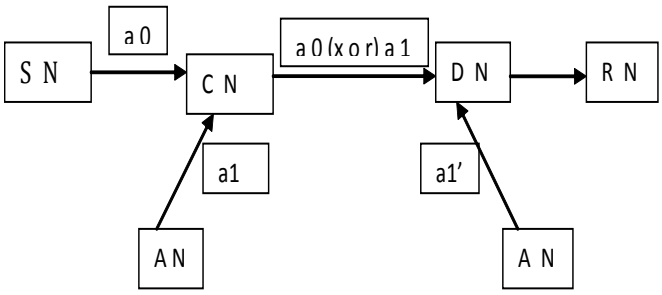

Fig. 1. Plain Packet Pollution attack

The Fig. 1 explains about the plain packet pollution attack, where SN – Source Node, CN – Coding Node, DN – Decoding Node, AN – Attacker Node, RN – Receiver Node. The two attacker node send corrupted packet a1 and a1' to node CN and node DN. The node CN codes the packet a0 with packet a1 (XORing each bit) and sends X= a0(XOR)a1 to node DN. Then node DN decodes the packet X with the packet a1' and it will get a corrupted packet which is send to the receiver node.

In case of corrupted plain packet pollution attack, the adversary either modifies the plain packet send by the source or inject corrupted plain packet into the original plain packet. Packet injection by adversary is traditional one, whereas in this case corrupted packet is injected. A Code Guard technique is used to identify pollution attack [14].

Code Guard:

Code Guard uses digital signature to identify pollution attack. Three types of nodes are considered source node, forwarding node and encoding/decoding node.

Step 1:

The source node signed each plain packet it creates and the coded packet is also signed by the node that created it. After signing, the packets are forwarded to the next hop node.

Step 2:

The forwarding node after receiving the plain or coded packet, it verifies the packet signature. If matches, the node forward the packet to the next hop without any change, if not the packet is dropped and a bad notification link message is send to the source node.

Step 3:
The encoding/decoding node does the same as forwarding node but send pollution notification message to the source node. The encoding / decoding node is also a forwarding node.

Step 4:
As soon as the source receives the pollution notification, it finds the corrupted bit by comparing it with the originally sent signed plain packet.

Step 5:
The source starts a bit-level trace back procedure to identify the history of corrupted bit.

Step 6:
The process finishes when the attacker node is identified.

4. JAMMING ATTACK

Jamming attack refers to blocking the communication channel with the aim of preventing the flow of any information through the channel. This attack comes under Denial-of-Service (DOS) attacks [8], and is one of the most dangerous forms of attacks in wireless networks. Normally wireless networks are classified into wireless infrastructure-based networks and infrastructure-less networks. Here infrastructure-less network is considered with base station and mobile nodes. Mobile nodes are connected through base station. Jamming attack is detected using honey nodes. Honey node is a node present in the network which can easily senses the presence of jammer and inform the base station about the situation. When the base station is informed about the presence of attacker, it immediately changes the frequency of operation dynamically.

Using honey nodes

Honey node is a node used as a detection strategy for defending against jamming attack [7]. The network consists of base station, mobile nodes, honey node and jammer node. The honey node is present in the base station and acts as a secondary interface to communicate with the mobile nodes. It guards the frequency of operation [4]. Honey nodes get the information about the attacker by attracting the jammers. When honey node is attacked, it does not affect other different nodes because other nodes are operating in different frequency.

As soon as the honey nodes detect an attack it immediately informs the base station. The base station informs the associated nodes to change the frequency of operation. When the mobile nodes do not respond to any information send by the base station, it is detected that the mobile node is under attack. The algorithm works well for both base station and mobile node. When the mobile node detects an attack, using pseudo random channel sequence it changes the frequency of operation.

Algorithm:

Step 1: Scan the current channel to detect the presence of jammer.

Step 2: If honey node detects the attack.

2.1: It immediately informs the base station.

2.2: It continues to communicate with jammer to waste the jammer time.

2.3: The base station informs the associated mobile nodes to change the channel of operation.

2.4: The mobile node gets the next channel using pseudo random sequence.

Step 3: If base station detects the attack

3.1: Inform the honey node about attack.

3.2: Send information to associated nodes.

3.3: If the nodes send respond to the base station, then the base station issues a frequency.

3.4: If any node does not respond, the base station broadcast frequency change command and change frequency of operation.

Step 4: If mobile node detects attack

4.1: Wait to receive information from base station.

4.2: If information not received within the time limit, choose the next channel using pseudo random sequence.

5. CONCLUSION

We have addressed jammer as an internal threat model which knows about network secrets and protocols used. This paper shows four different types of denial of service attacks and its detection strategy. In conclusion, we can say that the field of anti-jamming detection is by now mature and well-developed. Then a question arises, why our data's are jammed and could not be protected. The answer is that we do not protect against jamming in all the available ways. In other words, one point, which should always be remembered by end users, is that the anti-jamming technologies should be not only designed and developed, but also deployed and used.

REFERENCES

[1] T. Dempsey, G. Sahin, Y. Morton, and C. Hopper, "Intelligent Sensing and Classification in Ad Hoc Networks: A Case Study," IEEE Aerospace and Electronic Systems Magazine, vol. 24, no. 8, pp. 23-30, Aug. 2009.

[2] B. Thapa, G. Noubir, R. Rajaramanand, and B. Sheng, "On the Robustness of IEEE802.11 Rate Adaptation Algorithms against Smart Jamming,"

Proc. ACM Conf. Wireless Network Security (WiSec), 2011.

[3] Jing Dong, Reza curtmola, Cristina Nita-Rotaru and David K.Y.Yau, "Pollution attacks and defenses in wireless interflow nwetwork coding systems", IEEE transactions on dependable and secure computing, vol. 9, no. 5, September

[4] M. Wilhelm, I. Martinovic, J. Schmitt, and V. Lenders, "Reactive Jamming in Wireless Networks: How Realistic Is the Threat," Proc. ACM Conf. Wireless Network Security (WiSec), 2011.

[5] X. Liu, G. Noubir, and R. Sundaram, "Spread: Foiling Smart Jammers Using Multi-Layer Agility," Proc. IEEE INFOCOM, pp. 2536-2540, 2007.

[6] B. Greenstein, D. Mccoy, J. Pang, T. Kohno, S. Seshan, and D. Wetherall, "Improving Wireless Privacy with an Identifier- Free Link Layer Protocol," Proc. Int'l Conf. Mobile Systems, Applications, and Services (MobiSys), 2008.

[7] Sudip Misra, Sanjay K. Dhurandher, Avanish Rayankula and Deepansh Agrawal, "Using honey nodes for defense against jamming attacks in wireless infrastructure-based networks", computers and electrical engineering, may 2009

[8] T.X. Brown, J.E. James, and A. Sethi, "Jamming and Sensing of Encrypted Wireless Ad Hoc Networks," Proc. ACM Int'l Symp. Mobile Ad Hoc Networking and Computing (MobiHoc), pp. 120-130, 2006.

[9] Devu Manikantan Shila, Yu cheng, and Tricha Anjali, "Mitigating selective forwarding attacks with a channel-aware approach in WMNs",IEEE transactions on wireless communications, vol. 9, no. 5 , may 2010.

[10] Konstantinos Pelechrinis, Mario Illiofotou and Srikanth V. Krishnamurthy, "Denial of service attacks in wireless networks: The case of jammers", IEEE communications survey & tutorials, vol. 13, no. 2, second quarter.

[11] G.Noubir and G.Lin ,Low –power DoS attacks in data wireless LAN's and countermeasures , ACM SIGMOBILE Mobile Computing and Communications review,7(3):29, 30,2003.

[12] O.Goldreich, Foundations of Cryptography: Basic applications, Cambridge University Press, 2004.

[13] I.Venkata Saj Manoj ,"*Cryptography and Steganography*", International Journal of Computer Applications (0095 – 8887), Volume 1-No.

[14] G.Lin and G.Noubir . On link layer Denial of service in data wireless LANs. Wireless communications and MobileComputing, 5(3):273-284, May 2004.