Defeating DOS Attacks in Wireless Networks in Presence of Jammers

Kaushal Patel[1], Prof. D. N. Dakhane[2], Prof. Ravindra L. Pardhi [3]
Dept of IT[1], Associate Professor in Dept of IT[2], Assistant Professor in Dept of IT[3], Sipna COET,Amravati [1, 2, 3]
Email: kaushalpatel15@gmail.com.[1],dmdakhane@sipnaengg.ac.in[2],rlpardhi@sipnaengg.ac.in[3]

Abstract- The commodity of the medium in wireless networks makes it easy for an adversary to launch a Wireless Denial of Service (WDoS) attack. All current research work demonstrates that such attacks can easily be accomplished. For example 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. In this survey we present a detailed reference to all jamming attacks been recorded in literature since now. In addition, we illustrate various techniques that were introduced in order to detect the presence of an adversary node as well as the mechanisms proposed for protecting the network from such attack.

Index Terms- ***DoS; DDoS; DDRS.***

1. INTRODUCTION

Security is one of the critical attributes of any communication network. Various attacks have been reported over the last many years. Most of them, however, target wired networks. Wireless networks have only recently been gaining widespread deployment. At the present time, with the advances in technology, wireless networks are becoming more affordable and easier to build. 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.[3]
The shared and easy to access medium is undoubtedly the biggest advantage of wireless networks, while at the same time is its Achilles' heel. In particular, it makes it extremely easy for an adversary to launch an attack. The goal of traditional DoS attacks is to overflow user and kernel domain buffers. However, such "brute-force" jamming techniques, which mainly exploit PHY and MAC layer vulnerabilities, can be detected easily. Jammers have responded by employing more intelligent ways to accomplish jamming task in order to evade detection.[7]

1.1. *DoS*

As DoS attacks become one of the most threatening security issues, the need to detect this type of attack is increasing. DoS is not just a "game" played for fun by some attackers, it has become an effective weapon for cyber war or for so called "hacktivist" groups. In general, detection is required before the spread of a

DoS attack. DoS detection is often part of a wider intrusion detection system (IDS). An IDS is best defined as software or hardware used to detect unauthorized traffic or activities that are against the allowed policy of a given network. Intrusion detection is not a new research field, with one of the earliest published IDS papers in 1980 by Anderson in 1987, Denning provided a structure for researchers working on IDS.[1]IDS can be classified based on the serving component (the audit source location) as either host-based, network-based or a combination of both. In a host-based IDS the audit information, such as application and operating system log files, are monitored while the network traffic is monitored in a network-based IDS. The host-based is usually located in a single host while the network-based system is usually located on machine separate from the hosts that it protects. Hybrid intrusion detection systems combine both the network and host-based systems. The rest of this paper is organized as follows.[8]

1.2. *IDS Overview*

Network-based IDS (NIDS) usually detects attacks such as worms, scans, DoS attacks, and other types of attacks. In the following, a general overview of the IDSs will be presented. Then, more precisely DoS detection techniques will be reviewed. Network IDSs are generally categorized based on the detection method as one of two types: signature-based or anomaly-based detection. Signature-based, also known as rule- or misuse-based, detects an attack by comparing well-known attack signatures, or patterns, with the monitored traffic. A match generates an alarm for a potential attack. This type has fast detection time, detects most known attacks, and, generally has a low false positive rate, it does not signal an alarm for legitimate traffic. On the other hand, an anomaly-based IDS, also known as behavior-based, operates by comparing the network traffic behavior against previous "normal" traffic behavior. Any deviation in the comparison is considered to be a sign of an attack. The system acquires a normal traffic profile, usually through training, and monitors the traffic for any differences with the normal profile. The normal traffic behavior is classified into two types:

standard and trained. The standard is based on standard protocols and rules such as TCP handshaking connection set up and how the attacker could perform a half connection attack. The trained traffic is used to determine a threshold value for future detection.[5] There are many network anomaly-based systems and interested readers can refer to. Anomaly detection can detect unknown attacks; however, it generally produces higher false positive rates than signature-based systems. In practice, systems may combine both signature and anomaly-based techniques. In general, anomaly-based intrusion detection systems operate in three phases: parameterization, training, and detection. In parameterization, the parameters of the system are defined. The model of the normal behavior of the traffic will be built in the training phase. In the detection phase, the traffic behavior is compared against that in the training phase. If the comparison exceeds a threshold value a detection alarm is triggered.[4]

1.3. *Objective*

- Detecting jammers
- Reduce the effect of DOS attack
- Improve wireless communication

We describe some of the most harmful attacks that can be launched by a jammer. We develop such as one system, to show the effect of the dos attack. In our proposed system, the normal client and server process is initially depicted, then the attack is launched manually to show how the dos attack affect the normal client/server process.

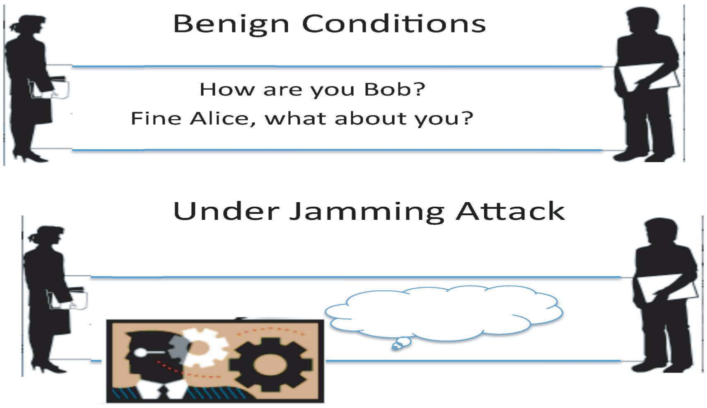

Fig.1 Jamming Entity Representation

First, we start by formally defining jammers. We will adopt the definition given by Xu : “We define a jammer to be an entity who is purposefully trying to interfere with the physical transmission and reception of wireless communications”. A pictorial representation of the jammer is given in Figure 1.Before describing the various jamming models, it is important to refer to some criteria and metrics that are used to characterize the attack model.[3]

2. JAMMERS

2.1. *Constant jammer*

All the time emits radio signals at the wireless medium. The signals that he/she emits are totally random. They don’t follow any underlying MAC protocol and are just random bits. The goal of this type of jammer is either for a legitimate user to sense all the time the channel busy and as a result the sender will never get access to the channel to send data or to pose interference to a node that has send out data and as a result to corrupt the packets sent out. Similar in some way to the constant jammer is the deceptive jammer. Its similarity lays in the fact that deceptive jammer also sends out constantly bits, however this time the bits are not random.[8]

2.2. *Deceptive jammer*

Continually injects regular packets to the channel without any gap between the transmissions. This has as a result a legitimate user to believe that there is an legitimate transmission going on and as a result this node will remain at the receive state even if it has data to send out. One problem that the previously described jammers can face is this of energy failure. They emit signals to the wireless medium all the time so their life time is restricted.[8]

2.3. *Random jammer*

Jams for tj seconds and sleeps for ts seconds. At the jamming period the jammer can follow any of the models that we have described since now or any of the models that we will describe in following sections. By changing tj and ts we can achieve different levels of effectiveness and power saving. Jamming models are mentioned and can be found with more details at target mostly at the transmission of a packet. They try to avoid the transmission of a packet from the sender. [8]

2.4. *Reactive jammer*

On the other hand a jammer can target the reception of the packet. So a reactive jammer is sensing the channel all the time and when he/she senses a packet to be sent, transmits a radio signal in order to cause collision and as a result corruption of the data that the packet transfers.[8]

3. Implement Methodology.

3.1. *Jamming Efficiency Criteria*

Following list of widely used jamming efficiency criteria:

- Energy efficiency
- Probability of detection
- Level of DoS
- Strength against physical layer techniques such as FHSS,DSSS, CDMA.

An ideal jamming attack should have high energy efficiency (i.e., consume low power), low probability of detection (preferably close to 0), achieve high levels of DoS (i.e., disrupt communications to the desired (or maximum possible) extent) and be resistant to PHY layer anti-jamming techniques (i.e., do not allow signal processing techniques to overcome the attack). Often, the criteria of interest are jamming scenario dependent. In other words, the jamming scenario dictates the most suitable criteria for use. For example, when malicious nodes have limited energy resources, energy efficiency will be their prime goal. Of course, in all cases jammers may attempt to be effective in as many of the aforementioned criteria as possible. As a simple example, in order to maintain a low probability of detection, the jammer can adopt techniques that are consistent with MAC layer behaviors. More details on jamming techniques will be provided in the following sections.[8]

3.2. *Jamming Efficiency Metrics*

In order to quantify the extent to which the jammer satisfies the above criteria, we need to define metrics that capture the jammer's behavior. For describing these metrics, we will use simple scenarios with one transmitter (*Tx*) and one receiver(*Rx*).Introduce the following two, widely used, metrics (PSR and PDR).

3.2.1. Packet Send Ratio (PSR):Let's assume that the MAC layer of *Tx* has n packets for transmission. Due to jamming interference, only m (n ≥ m) of these packets can eventually be transmitted. PSR is then defined to be:

$$\mathrm{PSR} = \frac{\mathrm{m}}{\mathrm{n}} = \frac{\text{Packet Sent}}{\text{Packets Intended To Be Sent}} \dots (1)$$

PSR is an easily computed measure which intuitively captures the effectiveness of the jammer towards a transmitter employing carrier sensing as its medium access policy. The jamming signals can render the medium busy due to carrier sensing and as a result the transmission queues of *Tx* will get filled up quickly. Packets arriving at a full queue will be dropped. Moreover, depending on the semantics of the MAC protocol employed, transmissions for packets at the head of the queue can eventually expire and the packets themselves get discarded. The PSR metric can quantify such jamming effects.[1]

3.2.2 Packet Delivery Ratio (PDR)

Let's suppose that Rx receives m packets sent out from *Tx*. However, from these m packets only q were successfully delivered to the higher layers of *Rx*. A successful reception means that the packet successfully passed the CRC (Cyclic Redundancy Codes) check. In contrast to PSR, PDR captures the effectiveness of the jamming attack towards *Rx*. The PDR is defined as follows (note that if *m*= 0then PDR is defined to be zero):

$$\mathrm{PDR} = \frac{\mathrm{q}}{\mathrm{m}} = \frac{\text{Packets That Pass The CRC}}{\text{Packets Received}} \dots (2)$$

3.2.3. Jamming-to-Signal Ratio

Traditionally, jamming strength (mostly referring to PHY layer jamming) is measured by the jamming-to-signal ratio given by the following equation.[1]

$$\frac{J}{R} = \frac{P_j G_{jr} G_{rj} R_{tr}^2 L_r B_r}{P_t G_{tr} G_{rt} R_{tj}^2 L_j B_j} \dots (3)$$

Where the subscript j we refer to the jammer, with r to the receiver and with t to the transmitter. *Px* is the transmission power of node *x*, *Gxy* is the antenna gain from node *x* to *y*, *Rxy* is the distance between nodes *x* and *y*, *Lr* is the communication link's signal loss, *Lj* is the jamming signal loss and *Bx* is node's *x* bandwidth.

3.2.4. Connectivity index

The presence of jammers in an Adhoc wireless network can hurt connectivity (i.e., disrupt the existence of routes between all wireless nodes in the network).To capture the effect of jamming on the connectivity of a wireless ad hoc network, Noubiret al. introduce the connectivity index.

Let *G* = *(V,E)* be the directed connectivity graph representing the multi-hop ad hoc network after removing the jammed links. Let *G*= (*V*,*E*) be the transitive closure of *G*. The connectivity index of *G* is defined to be:

$$\text{Connectivity Index} = \frac{|E^{'}|}{\frac{|V|(|V|-1)}{2}} \cdots (4)$$

From the definition of the transitive closure, E contains all the pair of nodes of the graph for which, there are exists a path that connects them. The connectivity index is simply the ratio of the number of such pairs to the number of all possible pairs of nodes in the network. As a result, a connected graph has a connectivity index of 1, while a graph partitioned in two connected graphs of equal size, has a connectivity index 0.5.[5]

3.4. *Dynamic Detecting & Recovery System (DDRS) algorithm*

- Detect the number of packets coming from a particular source to a particular destination
- Keep a track on the number of packets
- If the number of packets given to a particular destination by a particular source exceed a particular threshold then discard the packets from that particular connection
- Repeat this for all the nodes in the network.
- Jammers would be avoided because any connection which is used by a jammer would pass and waste lot of packets at runtime.[2]

3.5. DDoS attacks detection algorithm:

1. Set the sampling frequency as *f*, the sampling period as *T*, and the grouping thresholds as GT_T and GT_S.
2. In the router after aggregation of traffic, sampling the network flows come from the upstream routers.
3. Calculate the numbers of packet which has various recognizable characteristics (such as the source IP address or the packet's size, etc.) in each sampling time interval.
4. Calculate in parallel the probability distributions of the sampled network flows.
5. Calculate in parallel the values of the total variation and the similarity coefficient among each of the pair.
6. If the value of the total variation of any two distributions is more than the lower bound of the grouping threshold GT_T (1.1045) and the value of the similarity coefficient is less than the upper bound of GT_S (0.7220), then the system detected the DDoS attacks from Flash crowds, and begins to raise alarms and discard attack packets.
7. If the value of total variation is located in the grouping threshold GT_T (the lower bound: 0.5921, and the upper bound: 1.1045) and the value of the similarity coefficient is located in GT_S (the lower bound: 0.7220, and the upper bound: 0.8708), then the system detected the DDoS attacks from Normal network flow, and begins to raise alarms and discard attack packets.
8. If the value of the total variation of any two distributions is less than the upper bound of the grouping threshold GT_T (0.5921) and the value of the similarity coefficient is more than the lower bound of GT_S (0.8708), then the system detected the Flash crowds from Normal network flow, and begins to raise alarms.
9. Otherwise the router forwards the packets to the destination or the downstream routers.
10. Return to step 2.[8]

4. RESULTS.

This snapshots shows the exact functioning of the system at respective time and gives the information about system

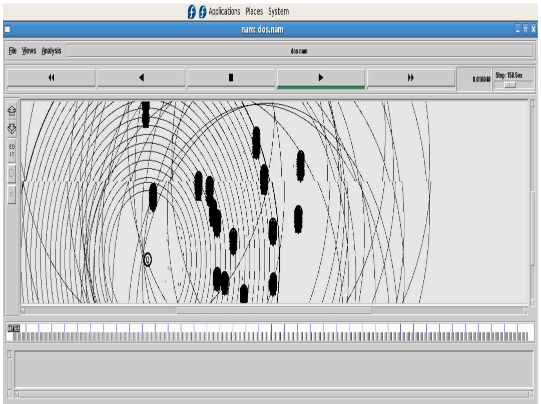

Fig.2. Basic functioning of system at time T1

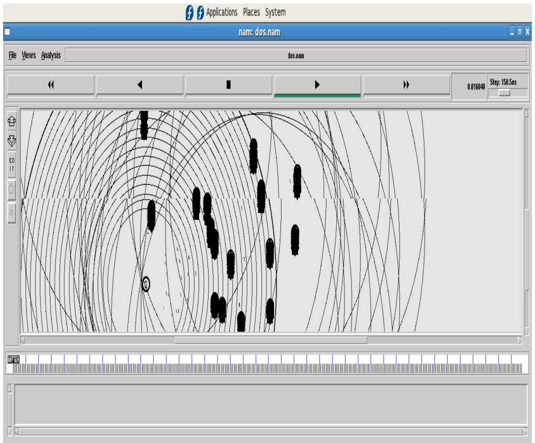

Fig.3. Basic functioning of system at time T2

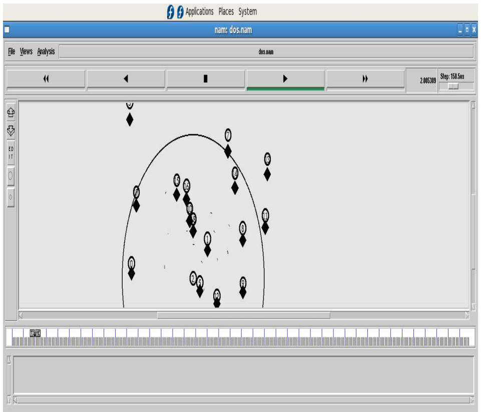

Fig.4. Basic functioning of system at time T3

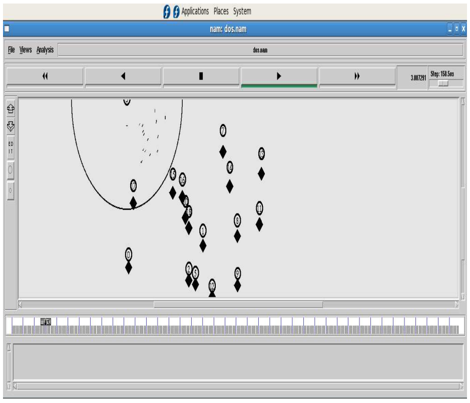

Fig.5. Basic functioning of system at time T1

4.1. *Delay Variation*

We use amount of delay in packets receving to detect DDoS attack traffic. Delay over time would have limited variation if the traffic keeps its behavior over time (i.e. attack-free situation); while an introduction of attack traffic in the network would elicit significant delay variation in short time period. Our experimental results with typical Internet traffic trace show that delay variance changes when traffic behaviors affected by DDoS attack In contrast, normal traffic exhibits a remarkably stationary delay.

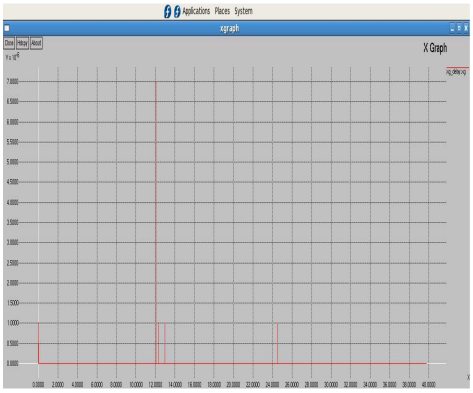

Fig.6. Delay variation

4.2. *Energy Variation*

We utilize energy distribution based on wavelet analysis to detect DDoS attack traffic. Energy distribution over time would have limited variation if the traffic keeps its behavior over time (i.e. attack-free situation); while an introduction of attack traffic in the network would elicit significant energy distribution deviation in short time period. Our experimental results with typical Internet traffic trace show that energy distribution variance changes markedly causing a "spike" when traffic behaviors affected by DDoS attack In contrast, normal traffic exhibits a remarkably stationary energy distribution. In addition, this spike in energy distribution variance can be captured in early stage of attack, for ahead of congestion build-up, making it an effective attack detection.

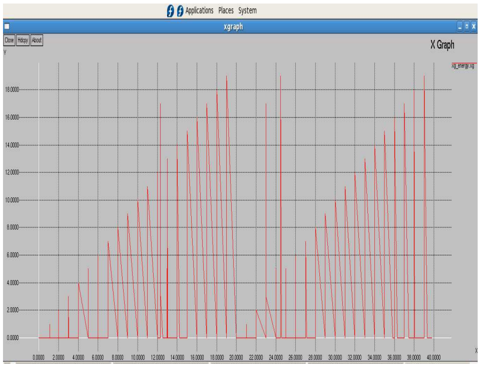

Fig.7. Energy Variation

4.3. *Throughput variation*

We use throughput to detect DDoS attack traffic. Throughput would have limited variation if the traffic keeps its behavior over time (i.e. attack-free situation); while an introduction of attack traffic in the network would elicit significant throughput variation in short time period. Our experimental results with typical Internet traffic trace show that throughput variance changes when traffic behaviors affected by DDoS attack In contrast, normal traffic exhibits a remarkably stationary throughput variation.

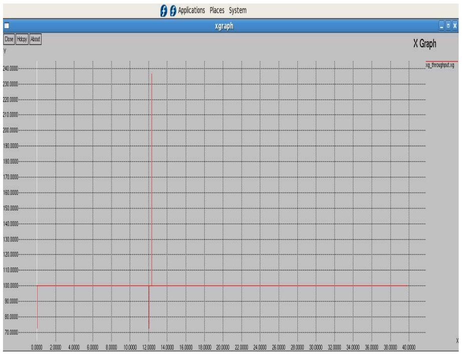

Fig.8. Throughput Variation

4.4. *Text output*

Here text output gives the detail of functioning of system that gives information about which node affect by jammer and which packet will not be sent. It also gives information about source address and destination address details of attack also mention here.

```
Under Jammers, Flash DDOS Detected, so the packet would not be sent
Source Address:6, Dest Address:8
Under Jammers, Flash DDOS Detected, so the packet would not be sent
Source Address:17, Dest Address:8
Under Jammers, Flash DDOS Detected, so the packet would not be sent
Source Address:0, Dest Address:8
Under Jammers, Flash DDOS Detected, so the packet would not be sent
Source Address:3, Dest Address:8
Under Jammers, Flash DDOS Detected, so the packet would not be sent
Source Address:9, Dest Address:9
Under Jammers, Flash DDOS Detected, so the packet would not be sent
Source Address:12, Dest Address:9
Under Jammers, Flash DDOS Detected, so the packet would not be sent
Source Address:4, Dest Address:9
Under Jammers, Flash DDOS Detected, so the packet would not be sent
Source Address:8, Dest Address:9
No DDOS found, so processing the packet
Node-Number of Packets
0000-0
0001-2
0002-11
0003-11
0004-2
0005-4
0006-6
0007-11
0008-11
0009-11
0010-11
0011-0
0012-0
0013-0
0014-0
0015-0
0016-0
0017-0
0018-0
0019-0
```

5. CONCLUSION AND FUTURE WORK

Here in DDRS algorithm for improving th effect of DoS attack in case of jammers. Other prevention schemes require properties that might not be applicable in realistic scenarios. Given the already widespread deployment of wireless systems, solutions that require large scale changes(and cannot be applied for example through a software patch) are unrealistic. DoS is one of the main security threats in the Internet. Defending against DoS becomes a necessary step that must be considered by the companies and ISPs. IDS are used to detect different types of intruders including DoS/DDoS attacks. By using hybrid probability metrics to detect DDoS attacks and through experiment and simulation gives that the proposed metric can not only detect DDoS attacks from the normal flows, but also can recover from DoS attack.

REFERENCES

[1] A. Wood and J. Stankovic, “Denial of service in sensor networks,” IEEEComp., vol. 35, no. 10, Oct. 2002, pp. 5462.

[2] Ke Li, Wanlei Zhou, Ping Li, Jing Hai and Jianwen Liu “Denial of Service Attacks in Wireless Networks:The Case of Jammers” School of Engineering and Information Technology Deakin University

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

[4] S.Bhargava and D.P.Agrawal, “Security enhancements in AODV protocol for wireless ad hoc networks,” in VTC 2001 Fall, vol. 4, Oct. 7-11,2001.

[5] T.X.Brown, J.E.James, and A.Sethi, “Jamming and sensing of encrypted wireless ad hoc networks,” in MobiHoc06, 22-25 May, Florence, Italy.

[6] W. Xu, K. Ma, W. Trappe, and Y. Zhang, “Jamming sensor networks:Attacks and defense strategies,” in IEEE Netw., May/June 2006

[7] Y.Zhang and W.Lee, “Intrusion detection in wireless ad hoc networks,” in ACM MobiCom 00, Boston, MA.

[8] 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.