

# Distributed Denial-of-Services Attack detection in IEEE 802.11i Wireless LAN

Chandrakala\*, DeshlahraAmritanjali\*\*, V.V.S.Sriram\*\*\*

Birla Institute of Technology (Deemed University), Mesra, Ranchi

\* kaladeshlahra@gmail.com, \*\* amritanjali@indiainfo.com, \*\*\*sriram@bitmesra.ac.in

*Abstract: The IEEE 802.11i is one of the much popular wireless local area network standards that is being widely deployed. Much research has been done on the IEEE 802.11 wireless network standard and the standard is known for its insecurity. Several reports have addressed the 802.11-based network vulnerabilities mainly for its lack of security mechanisms for Internet. This paper is based on enhancing the security mechanisms for a specific Internet attack called the Denial-of-Service attack. The attack prevents or prohibits the normal use or management of communications facilities. A Denial-of-service attack may occur if the attacker generates a lot of traffic on the network, which may block the server for hours or by attacking the resource itself. Another form of Denial-of-Service attack is the use of a strong radio signal. This denies legitimate users from accessing a resource. This paper discusses a new approach to the prevention and protection from Denial-of-Service attack and also considers Denial-of-Service attack in distributed environment.*

Keywords: IEEE 802.11i, Wireless Local Area Network, Denial-of-Service Attack (DDoS).

## I. INTRODUCTION

*Overview of wireless Local Area Network:*

Wireless LAN technology is the fastest growing segment of the communication market. According to Gartner Research, worldwide shipment of WLAN units will grow at an annual rate of 42% through 2007. Frost & Sullivan predicted a 125% growth in India in 2003 followed by a compounded annual growth rate of 48.6% until 2009. While wireless LAN connectivity has transported us to the frontiers of phenomenal productivity, it comes along with the resident Achilles heel grim security vulnerabilities the bane of WLAN as we see it today. A plethora of reports have been published describing attacks on 802.11 wireless networks. Malicious attackers are able to passively eavesdrop or analyze traffic; even actively subvert WLAN security by replaying, inserting or modifying messages; masquerading or launching denial-of-service attacks.

### A. 802.11 SECURITY MECHANISMS:

To protect wireless networks, the 802.11 standard provides three security mechanisms Service Set Identifier (SSID), Media Access Control (MAC) address filtering, and Wired Equivalent Privacy (WEP). Each Access Point (AP) is programmed with an SSID that corresponds to a specific WLAN. The SSID acts as a simple password that clients must present to access the AP. APs can also be programmed with a list of MAC addresses of clients who are authorized to access the AP. If a client's MAC address is not included in this list,

the client is not allowed to associate with the AP. The WEP security protocol provides encrypted communication between the client and an AP by using the RC4 algorithm. It also provides a shared key authentication mechanism, where a static, manually preset WEP key on both the AP and the clients is used for authentication. The WEP protocol also insures message content integrity through Cyclic Redundancy Code (CRC) checksums[3].

### B. 802.11 SECURITY WEAKNESSES:

A crucial flaw in WEP is that the encryption/authentication keys remain static. Moreover, 802.11 standard does not provide key management. To update the keys, each machine needs to be manually configured - something that is not feasible in large WLAN settings, and simply impossible in public hot spots. The poor alternative is to leave the keys unchanged, which of course exposes the system to hacker. Another flaw in

WEP is that the size of the initialization vector (IV) used by the RC4 algorithm is only 24-bits, which forces the same IV to be repeated frequently. An attacker can gather transmitted packets to capture the duplicate IVs from which key streams can be inferred to decipher encrypted packets. If the first two bytes of enough key streams can be observed, then the RC4 encryption key can be recovered. This exploit is called an FMS attack. Tools like WEP Crack and Aircrack, freely downloadable from the Internet, make this task effortless.

The WEP shared key authentication is poorly designed and WEP offers no protection against replays. An attacker can sniff the information of someone else's valid authentication with which to authenticate himself later. WEP does not provide any protection against forgery. The WEP CRC-32 checksum function is linear, which allows an attacker to modify the message yet leave the checksum unchanged making man-in-the-middle and session hijacking attacks successful. While the 802.11 standard's WEP-based encryption is weak, its authentication is virtually worthless. An attacker can easily circumvent MAC address lists by spoofing his MAC address. Using SSID as a secret password is of little use because the SSID is transmitted in clear text and can be sniffed for subsequent use by attackers. Moreover, unless explicitly turned off, APs broadcast their SSID, which can be received by anyone within range (including war drivers) to access the AP.

### C. SECURITY UPGRADE FOR 802.11 STANDARD :

To overcome the weaknesses of the 802.11 standard, the IEEE 802.11 Working Group instituted Task Group i (TGi) in 2000

to develop a security upgrade for the 802.11 standard. The security upgrade will be released as a new standard IEEE 802.11i by the end of 2003. The 802.11i includes two main developments: Wi-Fi Protected Access (WPA) and Robust Security Network (RSN)[3].

**Wi-Fi Protected Access:** The WPA was developed by the Wi-Fi Alliance in collaboration with the TGI, as an interim software-based security upgrade for 802.11 before 802.11i became available. The WPA is a subset of draft 802.11i. It overcomes all known weaknesses in WEP by using the 802.11i draft's Temporal Key Integrity Protocol (TKIP) for encryption, 802.1X for authentication, and key hierarchy and management. The WPA replaced WEP as the standard 802.11 WLAN security in March 2003. WPA compliant products started shipping in May 2003. The TKIP is designed as a wrapper around WEP. It uses the RC4 encryption algorithm, but adds dynamic per-session and per-packet keys, which greatly increases the difficulty of decoding the keys. In TKIP, intruders are not allowed enough time to collect sufficient data to decipher the key thus overcoming a major weakness of WEP. TKIP also adds a message-integrity-check function (called Michael) to prevent packet forgeries, and increases the initialization vector size to 48-bits with sequencing to prevent replay attacks. To overcome the weak WEP authentication mechanism, WPA uses the IEEE 802.1X port-based authentication standard along with a RADIUS authentication server to provide centralized access control and encryption key distribution. Where the authentication server is unavailable, WPA uses a pre-shared key resident in the client to be matched with the access point to permit access.

#### D. ROBUST SECURITY NETWORK:

While WPA improves WEP security to an acceptable level, RSN takes WLAN security to a higher level. RSN is the future of over-the-air security for 802.11. RSN is the full implementation of 802.11i (also called WPA2). RSN defines the TKIP encryption for maintaining compatibility with legacy hardware. For future equipment, it defines two new encryption protocols based on the Advanced Encryption Standard (AES) the 'Counter Mode with Cipher Block Chaining Message Authentication Code Protocol' (CCMP), and the 'Wireless Robust Authenticated protocol' (WRAP). WRAP was the original encryption protocol for 802.11i based on the Offset Codebook (OCB) mode of AES, but had to be replaced by CCMP when IPR issues cropped up (three different parties have filed for patents on WRAP). WRAP is optional in RSN. In CCMP, the Counter Mode is the algorithm providing data privacy, while Cipher Block Chaining Message Authentication Code provides data integrity and authentication. CCMP is mandatory for anyone implementing RSN. RSN uses the IEEE 802.1x port-authentication standard to authenticate wireless devices to the network and to provide the dynamic keys it requires. RSN introduces pre-authentication and roaming, secure pre-shared

key mode for ad hoc and home networks, and key hierarchy and key management [3].

## II. DENIAL OF SERVICE ATTACK

Based on the principle that the only way to defend yourself is to understand your attacker in-depth Denial-of-Service[2] (DoS).[5] This attacks set out to remove a service from functional use by its clients. Web servers will stop serving web pages, email servers will stop accepting or delivering email, and routers will go dark, taking you off the Internet all together. Denial of a particular service will come in one of two forms:

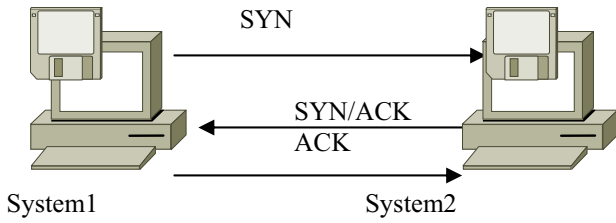
- (1) Complete consumption of a resource such as bandwidth, memory, CPU, file handles, or any other finite asset.
- (2) Exploiting a weakness in the service to stop it functioning causing the service to crash.

## III. MAJOR ISSUES OF DISTRIBUTED DENIAL OF SERVICE ATTACK

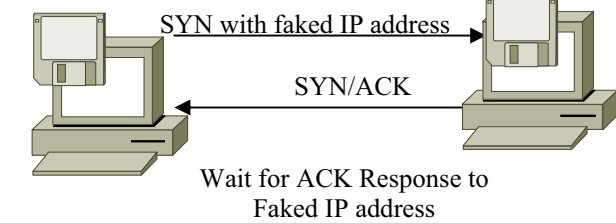
Denial-of-Service attack following on the heels of Y2K Issues and a rash of breaches affecting some of the Internet host well-known web sites like eBay.com, E\*Trade.com, Amazon.com, Yahoo.com, information security has emerged as a point of critical attention for both government and private sectors[4].

## IV. TYPE OF DENIAL OF SERVICE ATTACK

*A. SYN Flooding attack*-This attack may be used to temporarily prevent service to a system in order to take advantage of a trusted relationship that exists between that system and another. SYN Flooding is an example of a DoS attack that takes advantage of the way TCP/IP networks were designed to function, and it can be used to illustrate the basic principles of any DoS attack SYN Flooding utilizes the TCP three-way handshake that is used to establish a connection between two systems. Under normal circumstances, the first system sends a SYN packet to the system it wishes to communicate with. The second system will respond with a SYN/ACK if it is able to accept the request. When the initial system receives the SYN/ACK from the second system, it responds with an ACK packet and communication can then proceed. In a SYN Flooding attack, the attacker sends fake communication requests to the targeted system Figure 1. Each of these requests will be answered by the target system, which then waits for the third part of the handshake. Since the requests are fake (a non-existent IP address is used in the requests, so the target will wait for responses that will never come), as shown in Figure 2. The target system will wait for responses that will never come. The target system will drop these connections after a specific time-out period, but if the attacker sends requests faster than the time-out period eliminates them. The system will



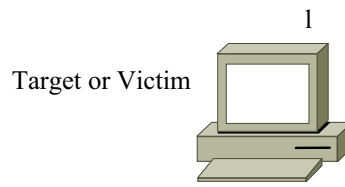
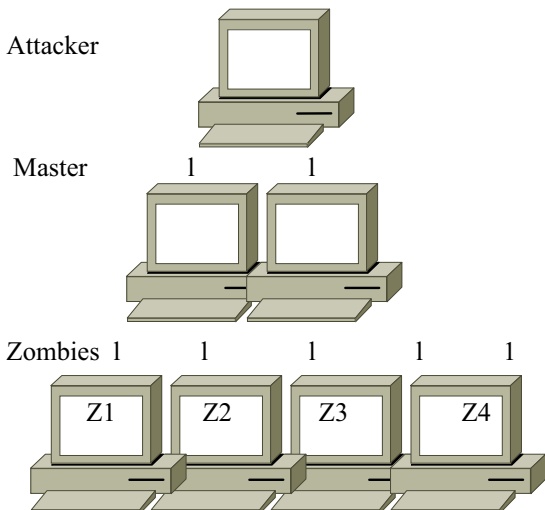
System1 System2  
 Figure1-The TCP three-way handshake



Attacker Target  
 Figure2-A SYN Flooding Denial-of-Service attack

quickly be filled with requests. The number of connections a system can support is finite, so when more requests come in than can be proceed, the system will soon be reserving all its connections for fake requests are simply dropped[1].  
 Prevention and Protection- Changing the timeout option for TCP connections so that attacks such as the SYN Flooding attack, described previously, are harder to perform because unused connections are dropped more quickly.

**B. Ping of Death-** Simple DoS attack is the famous Ping of Death(PoD).this targeted at a specific application or operating system.In the PoD attack, the attacker sends an Internet Control Message Protocol(ICMP).”Ping” packet equal to, or exceeding 64KB.This type of packet should not occur naturally.Certain systems were not able to handle this size of packet, and the system would having crash.  
 Prevention and Protection-This is a traffic pattern for a network Intrusion Detection Systems to identify,as it simply has to look for ICMP packets over a certain size.



Target or Victim  
 Where I=Network messages

Figure3- Distributed Denial-of-Service Attack Architecture

**V. DISTRIBUTED DENIAL OF SERVICE ATTACK**

In DDoS attack, much has been written about distributing own workload across several systems, so that any attack against system would have to target several hosts in order to be completely successful. While this true, if large enough DDoS networks are created tens of thousand of zombies ( A network of attack agents).  
 For any network, no matter how the load is distributed ,can be successfully attacked. Where Z1,Z2,Z3,Z4 are Zombies[1],Figure3.

**VI. FLOODING PATTERNS OF DDOS ATTACKS**

A DDoS attack deploys multiple attacking entities to deny legitimate application from obtaining a service.  
 The DDoS attacks overwhelm the target host and associated network links with extraordinary huge amount of packets that the victims are incapable to handle. Legitimate traffic is simply blocked. Such brute force attacks do not rely on particular network protocols or system weakness.  
 As shown in Fig. 3, the attacker simply exploits the huge resource asymmetry between the Internet and the victim. The magnitude of the increased traffic is large enough to crash the victim machine by resource exhaustion, or jam its Internet connection by bandwidth exhaustion, or both Therefore, DDoS attacks can effectively take the victim off the Internet. To avoid being caught by trace back techniques, attackers launch attacks using spoofed IP addresses form innocent victims.

To overwhelm the victim, DDoS flows converge toward the victim host. Therefore, we can observe abnormal traffic volume changes on routers along the paths of aggregation. The spatio-temporal traffic pattern tends to form a tree rooted the last- hop router to the edge network where the victim resides. By recognizing such tree-like attack patterns at each end router, we can detect the DDoS attacks.

At the early stage of DDoS attack, the abnormal changes are not obvious at each router due to the huge data rate in the core network. Meanwhile, routers cannot afford to monitor traffic on flow or packet level. We define a traffic flow by a set of packets satisfying a 5-tuple qualifier: {source IP address,

*destination IP address, source port, destination port, protocol applied*} during a given observation window. Thus, such a flow is observable by the router.

We monitor the traffic at a level above the flow level. We define a term *super flow* to cover all packets sharing the same  $n$  bit prefix in their destination IP address. In addition, the detection result does not need to specify any threshold in advance. The duty of individual router is to monitor the short-term deviation from long term average behavior. Once certain abnormal change in propagation and aggregation pattern is recognized, the local pattern is sent to a server where the statistic fusion is performed.

## VII. PRINCIPLES OF CHANGE DETECTION

Routers monitor all flows at each interface and count the incoming and outgoing packet number per time slot. If there is abnormal increase of incoming rate on a flow, the router will check the pattern of change propagation. We define the abnormality of a traffic increase using a *deviation from the average* (DFA) to differentiate abnormal short-term behavior from normal long-term behavior. We adopt weighted running average to describe the long-term behavior.

For a given super flow, let  $x(t, i)$  be the number of packets during time slot  $t$  coming in by port  $i$  and  $X(t, i)$  be the average number of packets, then the DFA and the historical average is computed by:

$$DFA_{in}(t, i) = x(t, i) X(t, i) \quad (1)$$

$$X(t, i) = (1-\alpha) \cdot X(t-1, i) + \alpha \cdot x(t, i) \quad (2)$$

Where  $0 < \alpha < 1$ . This shows how sensitive is the long-term average to current variations.  $DFA_{in}$  is defined as abnormality in incoming packet number. While a DDoS flooding attacks start, the current deviation should be noticeably larger than normal random fluctuations. If the abnormality level exceeds a threshold (e.g. 2.0), it is considered suspicious. Similarly, the DFA of outgoing traffic is calculated by:

$$DFA_{out} = y(t, i) Y(t, i) \quad (3)$$

$$Y(t, i) = (1-\alpha) \cdot Y(t-1, i) + \alpha \cdot y(t, i) \quad (4)$$

Where,  $y(t, i)$  be the number of packets in time slot  $t$  leaving by interface  $i$  and  $Y(t, i)$  be the long-term average number of packets.  $DFA_{out}$  is defined as abnormality level of outgoing packet number. With routing table, routers know which port the super flow goes. Therefore, once a  $DFA_{in}$  at port  $i_{in}$  is considered

suspicious, the outgoing port  $i_{out}$  is easily identified. Attack pattern is characterized by the *Deviation Ratio* (DR) and *Offset Ratio* (OR) between the DFAs at the input and output ports of each router. DR specifies the deviation from the average of a super flow at input

port  $i_{in}$  and output port  $i_{out}$ . OR describes the ratio of absolute volume of abnormal changes passed through the router from  $i_{in}$  to  $i_{out}$ .

$$DR(i_{in}, i_{out}) = DFA_{out}(i_{out}) DFA_{in}(i_{in}) \quad (5)$$

$$OR(i_{in}, i_{out}) = \frac{y(t, i_{out}) - Y(t, i_{out})}{x(t, i_{in}) - X(t, i_{in})} \quad (6)$$

Different combinations of DR and OR indicate different patterns of anomaly propagation and aggregations.

The scenarios illustrates how abrupt changes propagate through a router and the aggregation patterns may be looks like. Three of them characterize suspicious traffic flow patterns resulted from DDoS flooding attacks.

Scenarios of changes in traffic aggregation at attack-transit routers:

- (a) Scenario #1:  
 $DR \approx 1$  and  $OR \approx 1$
- (b) Scenario #2:  
 $DR < 1$  and  $OR \approx 1$
- (c) Scenario #3:  
 $DR \approx 1$  and  $OR > 1$
- (d) Scenario #4:  
 $DR < 1$  and  $OR < 1$

A.  $DR \approx 1$  and  $OR \approx 1$ : The flow cuts through the router. The router essentially forwards all increased traffic shown by (a) *Flow through*;

B.  $DR < 1$  and  $OR \approx 1$ : The outgoing flow merges multiple incoming flows, but not all incoming flows contain abnormally increased packets. As all of them are forwarded out through port  $i_{out}$ , this is a partial aggregation pattern 2(b) *Partial Aggregation*;

C.  $DR \approx 1$  and  $OR > 1$ : The outgoing flow merges multiple incoming flows, each incoming flow contains abnormal increases with same deviation rate and they aim at the same destination. The router is a merge point on the attacking path and it is a full aggregation pattern 2(c) *Full Aggregation* ;

D.  $DR < 1$  and  $OR < 1$ : The changes are scattered, so it is not part of a DDoS attack 2(d) *Scattered Pattern*. Scenarios (a), (b), or (c) indicate possible starting of a DDoS flooding attack. Similar works are carried out in parallel for other flows. The pseudo code of the local attack pattern detection is given in Algorithm 1 below. However, the detection cannot be decided with a few incidences. We need aggregate all related traffic information from all nearby routers to raise accurate alerts timely. All incoming and outgoing packets are identified by the time instants and port numbers. The output of this algorithm is the alert packets to be sent to the central server.

*Algorithm 1: Attack Pattern Recognition*

*Input:*  $x(t,i)$ : Incoming packet in time slot  $t$  at port  $i$   
 $y(t,i)$ : Outgoing packet in time slot  $t$  at port  $i$   
 $X(t-1,i)$ : Average of packet arrivals up to time  $t-1$  at port  $i$   
 $Y(t-1,i)$ : Average of outgoing packets up to time  $t-1$  at port  $i$   
*Output:* Alert packets sent to central server.

*Procedure:*

01: Update historical average of I/O packets in a flow  
02: Calculate  $DFA_{in}$  and  $DFA_{out}$  using Eqs. (1) and (3)  
03: **If**  $DFA_{in} > \text{threshold}$  **Then**  
04: Calculate DR and OR using Eqs. (5) and (6)  
05: **If**  $DR \approx 1$  **Then**  
06: **If**  $OR \approx 1$  **Then**  
07: Suspicious pattern detected, alert packet sent;  
08: **Else if**  $OR > 1$  **Then**  
09: Suspicious pattern detected, alert packet sent;  
10: **End If**  
11: **Else if**  $DR < 1$  AND  $OR \approx 1$  **Then**  
12: Suspicious pattern detected, alert packet sent;  
13: **End If**  
14: **End If**

#### CONCLUSIONS

The complexity of DDoS attack patterns grows fast, as new network vulnerability is identified and more sophisticated attack tools are available. There is no magic that can handle all types of DDoS attacks. The shared sources in collaboration Grids and community networks are especially prone to such attacks. One solution works well in a given network environment but may fail in other networks. In this section, we summarize our contributions and then discuss security assurance, system scalability, and limitations of our DDoS detection system.

#### CONCLUDING REMARKS

This paper reports our work in detection of DDoS flooding attacks against Grid resource sites or hotspot servers in community networks. It is essential to detect DDoS attacks sufficiently early before harms are done to legitimate applications.

#### ACKNOWLEDGMENT

I am grateful to Amritanjali and V.V.S.Sriram Lecturer, Department of Computer Science and Engineering for supervising and providing a Opportunity to work in this emerging field of research.

#### REFERENCES

- [1] Wm. Arthur Conklin, Gregory B. White, Chunk Cothren, Dwayne Williams, Roger L. Davis, "Principle of computer security".
- [2] Anton Chuvakin and Cyrus Peikari, "Protect yourself Against Denial-of-Service Attacks", O'REILLY Windows devcenter .com.
- [3] Flexi Mohan, CEO- SecureSynergy posted on 31 october 2003 "Future of Wireless LAN Security" [www.securesynergy.com](http://www.securesynergy.com).
- [4] Mark Grimes, Distributed Denial of Service Attacks (DDoS): Threats and Safeguards.
- [5] Avleen Viq, "Preventing Denial of Service Attacks", 24<sup>th</sup> June 2004 O'REILLY ONLamp.com
- [6] Anderson, T., R. Mahajan, N. Spring, and D. Wetherall, "Rocketfuel: An ISP Topology Mapping Engine," <http://www.cs.washington.edu/research/networking/rocketfuel/>, Feb. 2006
- [7] Monk, T. and K. Claffy, "Cooperation in Internet Data Acquisition and Analysis," Coordination and Administration of the Internet Workshop, Cambridge, MA., Sept. 8-10, 1996. (CAIDA Project, <http://www.caida.org> )
- [8] M. Basseville and I.V. Nikiforov, Detection of Abrupt Changes: Theory and Applications. Prentice Hall, Englewood Cliffs, 1993. Brooks • Clemson University, Suresh Rai • Louisiana State University. [9] R. Oliver. Countering SYN\_flood denial-of-service attacks. In *Tech Mavens, Inc*, August 2001. [http://www.tech-mavens.com/syn\\_flood.htm](http://www.tech-mavens.com/syn_flood.htm).
- [10] Application of Anomaly Detection Algorithms for Detecting SYN Flooding Attacks, Vasilios A. Siris and Fotini Papagalou
- [11] Denial-of-Service Attack-Detection Techniques Glenn Carl and George Kesidis • Pennsylvania State University, Richard R.
- [12] An Active Detecting Method Against SYN Flooding Attack, Bin Xiao, Wei Chen, Yanxiang He, Edwin H.-M. Sha.