Secured Packet Hiding Technique for Packet Jamming Attacks

Varagani Paparao
Mtect Student, CSE
Gudlavalleru Engineering College,
Gudlavalleru

M.N.Satish Kumar
Asst.Prof, CSE dept
Gudlavalleru Engineering College,
Gudlavalleru

Abstract – Wireless networks are built upon a shared medium that makes it easy for adversaries to launch jamming-style attacks. Jamming attacks can severely interfere with the normal operation of Networks and, consequently, mechanisms are needed that can cope with jamming attacks. The Denial of Service attacks (DoS), the most widespread attack to the Network requires great concern and resilient mechanisms. Typically, jamming has been addressed under an external threat model. However, adversaries with internal understanding of protocol specifications and network secrets can launch low-effort jamming attacks which get problematic to detect and counter. Existing work proposed selective jamming attacks in wireless networks has some limitations. First limitation is Performance delay in a selective attack on TCP and maybe on routing. During these attacks, the adversary is active just for a brief period of valuable time, selectively targeting messages of high importance. Second limitation includes problem in real time packet classification. Proposed model evaluates robust selective jamming attacks detection mechanism while performing real-time packet classification at the physical layer. To mitigate these attacks, we develop three schemes that prevent real-time packet classification by combining cryptographic primitives with physical-layer attributes. We analyze the security of our methods and evaluate their computational and communication overhead.

Keywords – JAMMING, Message, PACKET.

I. INTRODUCTION

A flooding-based Distributed Denial of Service (DDoS) attack is a very common way to attack a victim machine by sending a large amount of unwanted traffic. Network level congestion control can throttle peak traffic to protect the network. However, it cannot stop the quality of service (QoS) for legitimate traffic from going down because of attacks. Two features of DDoS attacks hinder the advancement of defense techniques. First, it is hard to distinguish between DDoS attack traffic and normal traffic. There is a lack of an effective differentiation mechanism that results in minimal collateral damage for legitimate traffic. Second, the sources of DDoS attacks are also difficult to find in a distributed environment. Therefore, it is difficult to stop a DDoS attack effectively. The internet rapidly develops on recent times and significantly influences increasingly more industry and business services. When popularity of the broadband, more houses are linked to the web. Therefore, the difficulties of network security are actually. Currently, the primary threats of network security are coming from hacker intrusion, deny of service (DoS), malicious program, spam, malicious code and sniffer since there quite a few weaknesses within the original design of IPv4. The most common weakness is the idea that attackers could send IP spoofing packets and that is he likes to attack. Quite simply, the attackers modify the IP beginning with the true individual to another IP field. If these IPs are randomly generated then it is most more difficult to trace the fundamental cause of attacks from victims. Besides, the cunning attackers won't directly attack the targets. They could construct the botnet first then order them to attack the targets. However, it raises the damage grade of attack and tracing the attacks will be more difficult. The fact is, we are able to morally persuade the attackers or punish them by law after we obtain the way to obtain attacks. The process of searching source is called IP traceback. There are several practices trace attack source with the help of routers.

A Denial-of-Service (DoS) attack is characterized by an explicit attempt by an attacker to avoid legitimate users of a service through the use of the intended resources [1]. While launching their attacks, the attackers usually generate a huge volume of packets introduced to the target systems named victims, causing a network internet traffic congestion problem. Thus the legitimate users will be prevented from getting access to the systems actually being attacked. This paper specializes using an ground breaking marking scheme to defend against DoS attacks. Our company propose a methodology, dependent on a packet discrepancy technique, to trace DoS attacks, especially glow attacks. Reflector attacks be owned by the category of the extremely serious DoS attacks. Unlike other DoS attacks, the number of attack packets served by the reflector attacker would be amplified persistently, flooding the victim's network. The attack packets

reaching the victim are not direct from the attacker; they will be actually generated by some hosts regarded as reflectors. When such reflectors obtain the envelopes typically reflector attack, they might create persistently more packets with the use of a destination address of the victim.

A distance-based rate limit mechanism is used by the traffic control component for dropping attack traffic at the source end. Instead of penalizing each router at the source end equally, the mechanism sets up different rate limits for routers based on how aggressively they

are forwarding attack traffic to the victim. Therefore, a history of the drop rate in each router will affect the calculation of rate limit values in this mechanism. The focus of this paper is to present the distributed distance-based DDoS defense framework and the distance-based attack traffic control mechanism to detect and drop the attack traffic effectively.

II. LITERATURE SURVEY

In [2-3], Y. Kim et al. propose a path signature (PS)-based victim-end defense system. The internal system requires all routers to flip selected bits among the IP identification field for all those incoming packets. Based upon these marking bits, a special PS can be generated for all those packets seen from the same location. At the victim end, the defense system separates traffic based upon PS for every packet and detects DDoS attacks by monitoring anomalous changes of traffic amount given by a PS. Then, a rate limit value will surely be set up with this traffic. However, it is relatively difficult to detect DDoS attacks if PS diversity is quite greater than real router diversity of incoming traffic. Moreover, it is quite likely than a PS is changed after an attack is detected. For that situation, collateral damage for your legitimate traffic cannot be avoided.

S.Saurabh and SaiRam[1] proposed packet marking and IP traceback mechanism called Linear Packet Marking which needs wide range of packets almost total range of hops traversed from the packet. Other IP traceback algorithm requires much high large number of packets in comparison with this algorithm. A lot of them requires packets according to the scale regarding a the largest number packets. Yet as this scheme are able to do IP traceback using a lot of packets, it can also be highly scalable i.e. it might get a job at highly DDoS attack involving a really good deal of attackers distributed across network. Secondly it will be utilized to low rate DoS attacks that could perform attack with very less number packets. This framework are able to be incorporated by other traceback algorithms to scale back the amount of packets important for path reconstruction that may improve their performance too.

ADVANTAGES:
In the recent increase e-crime using DoS/DDoS attacks, victims and security authorities need IP traceback mechanism that could trace back the attack to its source.
This scheme wishes small number of packets hence it is capable of doing very effectively in situations of huge scale DDoS attacks and then in low rate DoS attacks.

DISADVANTAGES:
This method requires the attack to remain alive while performing traceback.Secondly IP traceback itself causes DoS attack while performing traceback.The epilfree solution won't handle packets headers of IPV6 but generated extra traffic for traceback. It entails large variety of hard disk drive storage and hardware changes for packet logging resulting from which it is not just really practically deployable.Unfortunately current proposals for IP traceback mechanism has problems with various drawbacks like require for a very large number packets for performing traceback and to discover the in-ability to handle highly distributed and scaled DDoS attacks.

The overlay-based distributed defense framework [4] detects attacks at victim end. During source finding, the traceback technique SPIE (Source Path Isolation Engine) is made. To handle attack traffic along at the source end, it combines the ancient times of a flow into rate limit calculation by defining a reputation argument. A spoofing DDoS attack tend to make the flow-based rate limit algorithm ineffective.

Ninglu and Yulongwang[2] proposed as Tracing the paths of IP packets returning to their origins, often known as IP traceback is a crucial increase defending against Denial of Service (DoS) attacks employing IP spoofing.In log-based single-packet IP traceback, the path details are logged at routers. Packets are recorded through routers toward the path toward the destination.
DDoS attack occurs by the large amount of zombie PCs. Zombie PCs
are distributed around the globe. Therefore, when an attack occurs, then the attack traffic is transmitted via backbone network of the target system's country. So, if backbone network is monitored and analyzed, DDoS attack could well be detected prior current DDoS prevention systems. It can make damages be minimized plus effective to prevent IP spoofed attack packets. Involving this, attack detection and prevention system offers more than tens of Gbps performance.

Probabilistic Packet Marking:[3] It can be defined to be the most famous packet identification techniques. Within this particular methods, the packets are marked in the router's Internet protocol address which actually they traversed as well as trail edges from which the packet is being transmitted. Marking the packets using router's address happens to be the best approach when compared onto the two alternatives provided here, where in case a packet dissipates of affected with any attack, the

fundamental cause router address can be fetched and send to the entire router. Today the router checks the packets and retransmits the packet in the direction of actual destination. Utilizing this implementation, an accuracy of 95% is possible to in fact notice the actual attack path. Second approach considered in probabilistic bundle marking is edge marking and here the IP address of two nodes would be called for to basically record the packets. This procedure definitely is much complicated in comparison with marking the IP address associated with a given router, where much state information regarding a given packet is essential contained in the former case. There are few techniques to shorten the state detail required in this case they even may also be discussed here. A fundamental XOR operation can possibly be executed between them nodes which generally make up the advantage.
As a way to react effectively against DDoS attack, all the processes for any information gathering, analysis and defense rule generation have to be automated. Furthermore, based on these analysis results attack detection and prevention processes also have to be automated. The IDDI is found in the mid of whole network. With this position, lots of information could possibly be gathered, so when using the information zombie PCs, C&C servers and agent distribution systems also have to be detected. Beyond current visualization tools, it must be be able to show the network traffic and security status in real-time. IDDI also can give direct information about security environment to administrator.

ADVANTAGES:
A single-packet traceback approach according to routing path. The primary design goal will be to conserve the single-packet traceability and, simultaneously, reduces the storage overhead and minimizes the complete number of routers that needs to be queried while in the traceback process.
DISADVANTAGES:
Bandwidth overhead is amazingly high while tracing the attack origin.It might not trace the attack while it is over i.e attack should remain active until such time as the trace is fullfiled.

Vijayalakshmi M and Mercyshaline[3] proposed as DDoS attacks could have been completed along at the network layer, for one example ICMP flooding, SYN flooding and UDP flooding that occur to be called Network Layer DDoS attacks. The proposed Filtering technique performs filtering close to the processes by which to obtain the attack driven by information filed by the injured individual. This can be complemented through proactive traffic shaping mechanism to halt network overload before detection happens in the victim. This procedure detects flooding network attacks, flooding and non flooding application layer attacks.

ADVANTAGES:
The epilfree solution greatly reduces the magnitude of the attack traffic and improves the probability of survival regarding a legitimate flow.Quite simple to trace ip source addresss.So simple to trace router's path.Simple checksum fabricated from utility of alternatively to hash function calculations which decrease the time as well as byte intake IP header fields.

DISADVANTAGES:
Doesn't detect other type of attacks except dos. Overhead while recording packets in network and create use of layers. Found medium range of false positive outcomes.

Okada M,Katsuno[4] Y Proposed as , the large collection of packets that considers the autonomous system (AS) measure of our world wide web topology distribution is calculated. The attack path tracing time is assumed to keep an index based on the expected large variety of collection packets, and to discover the best marking probability is presumed. For estimating best marking probability, PPM (Probabilistic Packet marking)method uses only Identification field of IP header It is constructed as stated by the following considerations.
a. The tactic fails to influence other communications.
b. The strategy is as efficient as they possibly can.

ADVANTAGES:
Suitable for existing protocols Support for incremental implementation Allows post packet analysis Insignificant network traffic overhead Compatible with existing routers and network infrastructure.

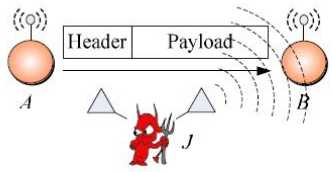
DISADVANTAGES:
Resource incentive with regard to processing and storage requirements. Sharing of logging information among several ISPs gets to logistic and legal challenges.Less Suited to distributed denial of Service strikes

Khan z and Akram[5] N proposed being the new IP traceback technique. This amazing IP traceback technique might work on single packet IP traceback. Single packet IP traceback means it involves just one packet to begin the traceback procedure. Secondly it eliminates needing of basically any marking technique. Proposed work formed a marking technique wherein a 16 bit ID is allocated to each and every ISP. The present ISP gets packet from any attached end user it adds its 16 bit ID straight into the identification field of IP header. Ever since the dimensions of the ISP ID and IP identification field is same so we do not particularly need some other efficient packet marking technique. 16 bits are embedded into 16 bit field.

ADVANTAGES:
It is uncomplicated to implementIt has low processing and no bandwidth overheadIt is acceptable during numerous attacks [not just (D) DoSIt does not have inherent security flaws.

DISADVANTAGES:
Since every router marks packets probabilistically , some packets will walk away from the router without being

markedIt is too expensive to feature this scheme concerning memory overheadOne important assumption for PPM to operate may be that DOS attack traffic will have larger volume than normal traffic.



(a)

Realization of a selective jamming attack.

Existing findings indicate that selective jamming attacks lead to a DoS with very low effort on behalf of the jammer. To mitigate such attacks, we develop three schemes that prevent classification of transmitted packets in real time. Our schemes rely on the joint consideration of cryptographic mechanisms with PHY-layer attributes. We analyze the security of our schemes and show that they achieve strong security properties, with minimal impact on the network performance.

In the first scenario, the attacker targeted a TCP connection established over a multihop wireless route. In the second scenario, the jammer targeted network-layer control messages transmitted during the route establishment process. Selective Jamming at the Transport Layer In the first set of experiments, we set up a file transfer of a 3 MB file between two users A and B connected via a multihop route. The TCP protocol was used to reliably transport the requested file.

III. PROPOSED SYSTEM

REALTIME NETWORK SETUP FOR PACKET CLASSIFICATION.

Nodes SETUP: Wireless lan Network systems setup
System Add: MAC address

```
devices = LivePcapDeviceList.Instance;
```

1) LivePcapDevice device =null; Ibid, you may firstly declare one object.

2) device = devices[select];

Then, the adapter is one of items shown in the list. Select one and it will be passed to the object.

3) device. Open(DeviceMode mode);

device.Open(DeviceMode mode, int read_timeout);

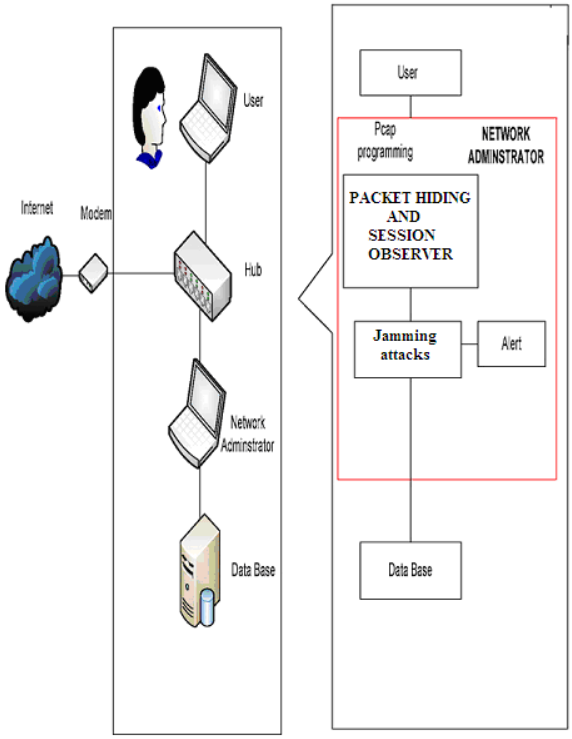
You can choose following code instead.

device.DumpOpen(string filename);

No matter which one you will choose, once you are ready to open one adapter, it will execute following code.

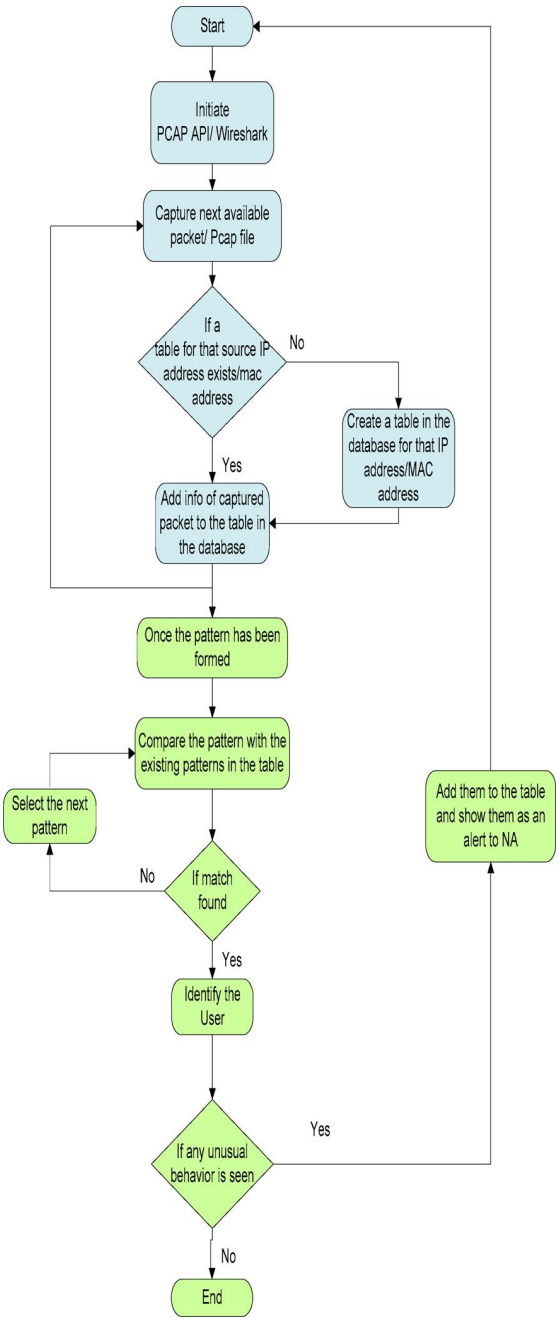
public virtual void Open(DeviceMode mode, int read_timeout)

```
{
if ( !Opened )
{
StringBuilder errbuf = new StringBuilder(
Pcap.PCAP_ERRBUF_SIZE );
PcapHandle = SafeNativeMethods.pcap_open_live
( Name,
Pcap.MAX_PACKET_SIZE,
(short)mode, (short)read_timeout,
errbuf );
if ( PcapHandle == IntPtr.Zero)
{
string err = "Unable to open the adapter ("+Name+").
"+errbuf.ToString();
throw new PcapException( err );
}
}
}
```



General jamming approach

In this approach user program gets the wireless network connection setup and captures services. After getting wireless service packets are masked for jamming detection. If the wireless network is jammed then alert is displayed or else it is stored in the database.



Attack pattern observer

For each packets in the wireless service in the network, store the mac address of the wireless devices. If the new wireless device is found then it will be stored in the table. If the device is already exist then it is passed for pattern detection of jamming attacks. Patterns of jamming may be either number of packets energy per sec or maximum number of packets received within the specified interval. If the patterns are matched with the current network pattern then it will be identified as jam and the device details are saved.

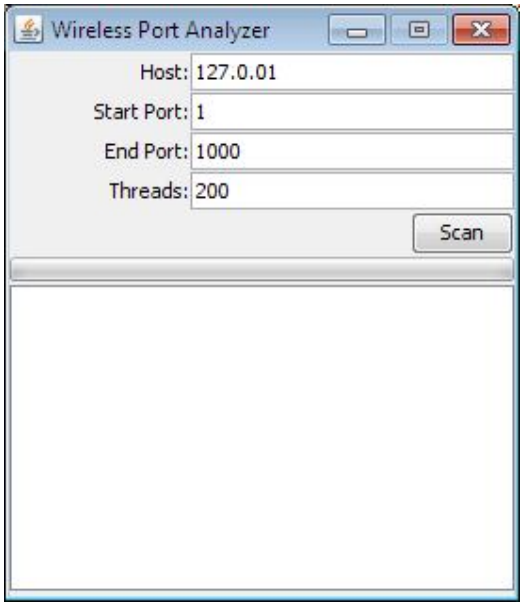
HTTP FLOODS

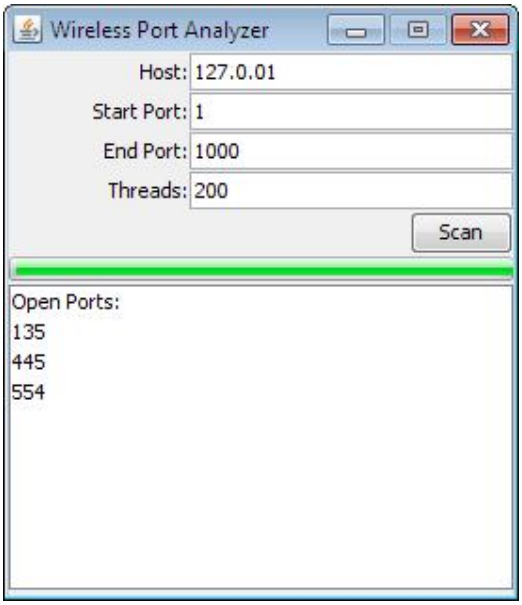
For All Nodes Ni Find SYNin
For All SYNin
If (Ti-Ti-1 = = Γ)
Then valid node
Allow traffic
If (P (SYN/ACKout) = =1)
Normal traffic
Allow SYNin and SYN/ACKout to be in the queue until ACK is arrived
Else
Abnormal traffic
Block traffic
Else
Invalid node
Block traffic

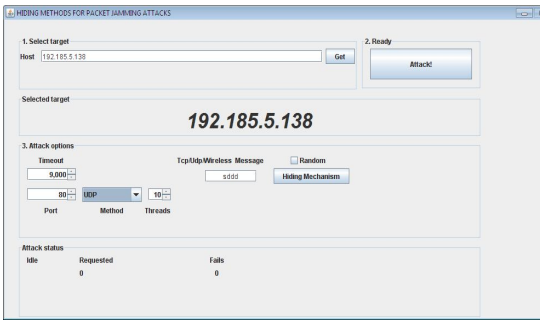
UDP FLOODS

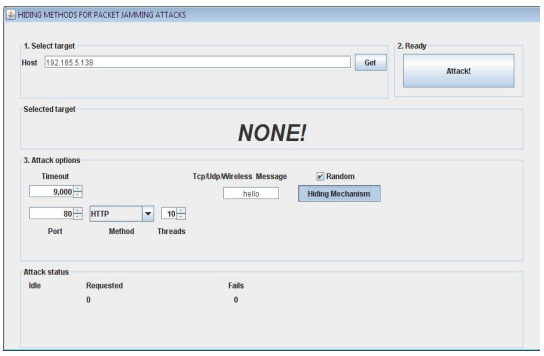
For All Nodes Ni Find REQin
For All REQin
If (Ti-Ti-1 = = Γ)
Then valid node
Allow traffic
If (P (RESPout) = =1)
Then Normal traffic
Allow the traffic
Else
Abnormal traffic
Block traffic
Else
Invalid node
Block traffic

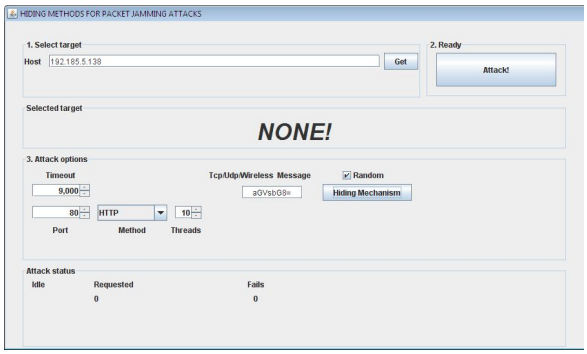
IV RESULTS:











V. CONCLUSION AND FUTURE SCOPE

The major challenge in network forensics is handling the massive size of network packet capture. It is difficult to store, manage and analyze. We address this problem by reducing the packet capture file size by marking the attack packets using the packet header information only. For marking the attack packets, we correlated various attacks and its corresponding identified significant features.This system captures network packets, analyze the application layer packets information and then identifies the attacks in the layer. This system successfully identifies jamming attacks.In future this work can be extended to identify the web application jamming to detect flaw points in the applications.

REFERENCES

[1] Saurabh S,SaiRam,A.S Linear and Remainder Packet Marking for fast IP Traceback COSMNET, fourth international journal 2012.

[2] NingLu;Yulong wang a novel approach for single packet ip traceback based on routing path parallel and distributed systems 20 international conference 2012.

[3] Mercy Shaline and Vijayalakshmi M IP traceback system for network and application layer attacks Recent trends in Information Technology,2012.

[4] Okada M, Katsuno Y 32-BIT as number based ip traceback (IMIS)2011 fifth International conference.

[5] Khan ,Z.S;Akram N; secure single packet ip traceback mechanism to identify the source (ICITST)2010

[6] Integrated DDoS Attack Defense Infrastructure for Effective Attack Prevention, Yang-Seo Choi, Jin-Tae Oh, Jong-Soo Jang.