Network Packet Jamming Detection And Prevention Using Hiding Method

M.VamsiKrishna
Mtech(CSE) VVIT college

R.Sudhakishore
Assistant professor of IT, VVIT college

Abstract –

Jamming attacks are one of the very most urgent threats harming the dependability of wireless communication. Jamming attacks may be viewed as a certain case of Denial of service (DoS) attacks. Typically, jamming has actually been addressed under an external threat model. However, adversaries with internal understanding of protocol specifications and network secrets can launch low-effort jamming attacks that might be hard to detect and counter. In situations of internal threats, the attacker launches selective jamming attacks by which it targets packets of high importance. Wireless networks provide wide variety of services which is certainly never so effortless by any other medium, its means of working tends it to have several security breaches. In modern era of communication trillions of profitable vital information is found at internet but they are accessible through this open medium. Such vital information may be achieved through intentional interference or jamming. With the internal knowledge of protocol specifications and network secrets can launch low-effort jamming attacks that are difficult to detect and counter.In this proposed work wireless packets are observed and analyzed using hidden approaches. Attacks are observed either system services or web service attacks are identified and then we provide a solution to stop these jamming type of attacks. 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.

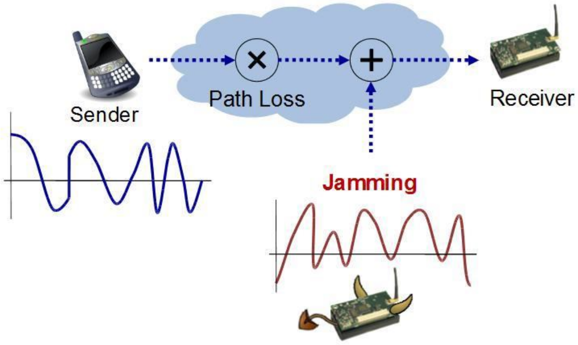
***Keywords* – Selective Jamming, Denial-of-Service, Wireless Networks, Packet Classification..**

I. INTRODUCTION

Wireless networks now enjoy widespread commercial Implementation due to economically priced, ease in use and setup. However, since accessing wireless media is much more easy than tapping a wired network, security becomes a serious concern when implementing any wireless network. We perceive an exact importance of Denial of Service (DoS) attacks called jamming. Among simplest kind of jamming, the adversary interferes in the reception of messages by transmitting never-ending jamming signal, or several short jamming pulses. Jamming results in a loss of link reliability, increased energy consumption, extended packet delays and disruption of end-to-end routes. The utilization of distinct, dedicated communication channels to transmit data and control traffic introduces one point of failure for getting a denial of service attack, in that an adversary probably can jam control channel traffic and stop relevant data traffic[2-3].

We perceive a complicated adversary who might be tuned in to network secrets and to discover the implementation details on network protocols for any layer within the network stack. The adversary exploits his internal knowledge for launching selective jamming attacks in which specific messages of “high importance” are targeted. For instance, a jammer can target route-request/route-reply messages along at the routing layer to prevent route discovery, or target TCP acknowledgments inside a TCP session to severely degrade the throughput associated with an end-to-end flow. To launch selective jamming attacks, the adversary must be good at implementing a “classify-then-jam” strategy before the finishing of a wireless transmission. Such strategy can possibly be actualized either by classifying transmitted packets using protocol semantics or by decoding packets upon the fly. Among the latter method, the jammer may decode the initial few items of a packet for recovering useful packet identifiers such as packet type, source and destination address. After classification, the adversary must induce a sufficient range of bit errors so that the packet can't be recovered at the receiver . Selective jamming requires an intimate familiarity with the physical (PHY) layer, as well as of a given specifics of upper layers[2-3].

In present system Rate adaptation scheme is used to save messages and supports end to end delivery of message. Rate adaptation scheme is implemented by achieving high link utilization by adjusting mode of transmission according to expected maximum throughput. I have given detailed description of this scheme in my last paper. But I can say this scheme is not efficient to secure messages of high importance and also doesn’t assures the uninterrupted service. So we have demonstrated few other schemes. Such as Dissembling commitment scheme and Puzzle dissembling scheme along with All Or Nothing Transformations[4].



Jamming in wireless network

II. LITERATURE SURVEY

The prevailing system address the of problem jamming under an internal adversary model a situation where the jammer is aware of this very implementation details of the network protocols. By optimizing this info, the adversary launches selective jamming attacks by which it targets specific packets of "high" importance. Selective jamming in regards to network performance degradation and adversary effort by presenting two case studies;

The selective jamming attacks can be launched by performing real-time packet classification at the physical layer. To play selective jamming, the adversary will have to be good at classifying transmitted packets in real time, and corrupting them before the top of their transmission.Packet classification can possibly be made by receiving a few bytes of a packet. To launch selective jamming attacks, the jammer needs to be good at implementing a "classifythen- jam" policy just before the completion of a wireless transmission. Jamming attacks are harder to counter and have now more security problems. Woodworking jigs have been proven to cause severe Denial-of-Service (DoS)[7] attacks against wireless networks. Within the simplest method of jamming, the jammer interferes when using the reception of messages by transmitting an eternal jamming signal.Under this model, jamming methods add the continuous or random transmission of high power interference signals.

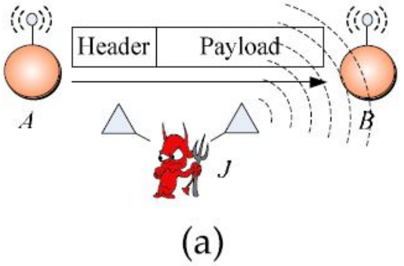
J. E. James and A. Sethi in their paper proposed the encryption technique taken place in the wireless networks [1].

O.Goldreich [2] in his proposed paper discusses about the basic applications of the cryptography and their encryption decryption formulas.

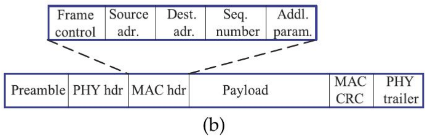
G.Lin and G.Noubir in their paper proposed discusses about the denial of service attacks [3]. Brown illustrated the feasibility of selective jamming based on protocol semantics [1]. They considered several packet identifiers for encrypted packets such as packet size, precise timing information of different protocols.

Lazos [4] proposed an algorithm to protect the control channel from inside jammers In the short paper work proposed by M.Wilhelm and I.Martinovic, J.Schmitt and V.Lenders the "Reactive jamming in the wireless networks:

How realistic is the threat?" the jamming attacks, principles and the selective packet hiding techniques are referred [5].



Realization of a selective jamming attack.



A generic frame format for a wireless network.

Our 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

1. Monitoring: monitoring attack alerts and identifying potential attacks

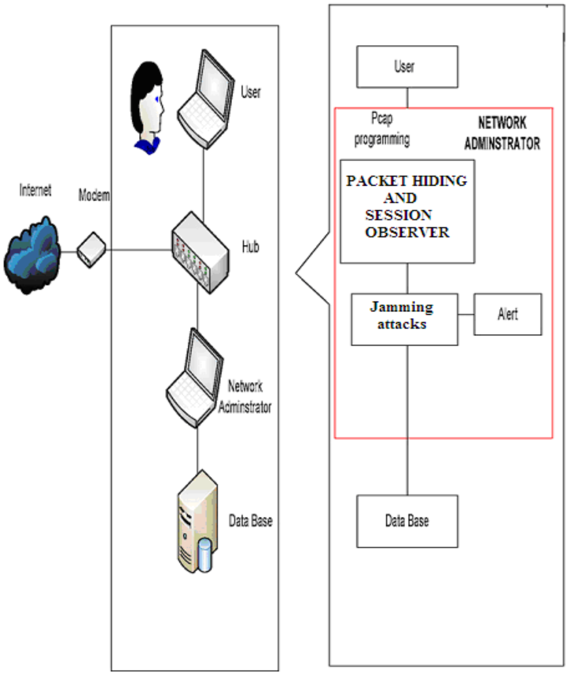
2. Analysis: analyzing alerts and other data to diagnose an at tack

Algorithm to capture n/w packets

REALTIME NETWORK SETUP FOR PACKET CLASSIFICATION.

Nodes: Wireless lan Network systems
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 );
}
}
}
```



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

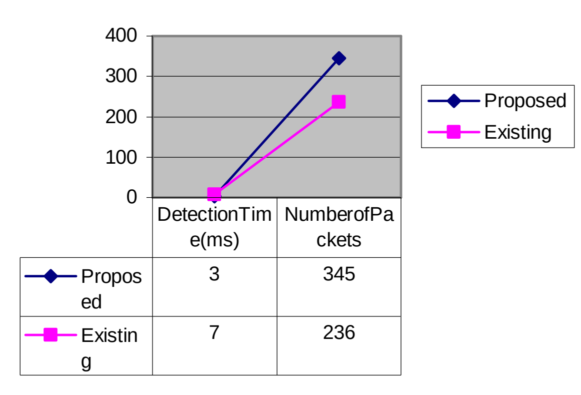
```
For All Nodes Ni Find REQin
For All REQin
If ( Ti-Ti-1 = = Γ )
Then valid node
Allow traffic
If ( P ( RESPout ) = =1 )
Then Normal traffic
Allow the traffic
Else
Abnormal traffic
Block traffic
Else
Invalid node
    Block traffic
```

Selective Jamming Module We illustrate the impact of selective jamming attacks on the network performance. implement selective jamming attacks in two multi-hop wireless network scenarios. In the first scenario, the attacker targeted a TCP connection established over a multi-hop wireless route. In the second scenario, the jammer targeted network-layer control messages transmitted during the route establishment process selective jamming would be the encryption of transmitted packets (including headers) with a static key. However, for broadcast communications, this static decryption key must be known to all intended receivers and hence, is susceptible to compromise. An adversary in possession of the decryption key can start decrypting as early as the reception of the first ciphertext block.

IV. EXPERIMENTAL RESULTS

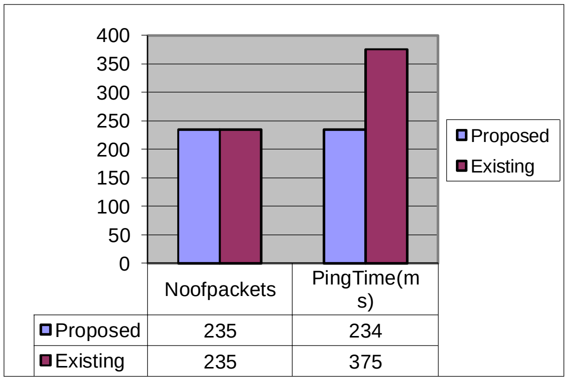
Performance Analysis:

Proposed Approach takes less time to detect the packets information between arriving and displaying each packet on the screen. Proposed approach uses robust normal distribution in order to get the statistical feature of the users behavior.



	DetectionTime(ms)	NumberofPackets
Proposed	3	345
Existing	7	236

Comparison between attack detection time and number of packets size.



	Noofpackets	PingTime(ms)
Proposed	235	234
Existing	235	375

Comparison between pinging time and number of packets

V. CONCLUSION AND FUTURE SCOPE

Information Jamming is one way of effectively communicating information. Deception is one way to negatively affect this capability. Today's systems are being used in critical applications to glean insights that are difficult to see using traditional non-jamming techniques. Even carefully user-customized applications are vulnerable due to incorrect defaults, limitations in the visualizations themselves and weaknesses in the overall system. To help counter these attacks this system will gives better accuracy compare to existing approaches in terms of attack stopping and packets hiding are consider.

REFERENCES

[1].Packet-Hiding Methods for Preventing Selective Jamming Attacks Alejandro Proa˜no

[2].SHCS Technique Defined for Packet Hiding Methods in Wireless Networks Bharath J1, International Journal of Advanced Research in Computer Science and Software Engineering

[3] Providing Network Security by Preventing Selective Jamming Attack G. Sathish Kumar. Journal of Advanced Technology in Engineering, Vol. 1, No. 1, December 2012

[4] Enhanced Packet Dissembling Schemes for Selective Jamming Attacks Prevention in Wireless Networks Pushphas Chaturvedi, International Journal of Scientific and Research Publications, Volume 3, Issue 6.

[5] M.Wilhelm, I.Martinovic , J.Schmitt, and V.Lenders. Reactive Jamming in Wireless Networks: How realistic is the threat? In proceddings of Wisec, 2011.