Thwarting Selective Insider Jamming Attacks in Wireless Network by Delaying Real Time Packet Classification

LEKSHMI.M.R
Department of Computer Science and Engineering, KCG College of Technology
Chennai, TamilNadu-600097, India
itslekshmihere@gmail.com

Prof. N. NITYANANDAM
Department of Computer Science and Engineering, KCG College of Technology
Chennai, TamilNadu-600097, India
nityanandam.cse@kcgcollege.com

Abstract

The major threat to wireless network is Denial of Service attack. An adversary can target on the communication of the nodes and can attempt to create an attack to prevent the efficient communication. Here, we address the problem of jamming under an internal threat model by considering a sophisticated adversary who is aware of the network secrets and the implementation details of network protocols at any layer in the network stack. The jammer can classify the transmitted packets in real time by decoding the first few symbols of an ongoing transmission. With this internal knowledge, the adversary targets specific message of high importance. Our aim is to delay the jamming node from classifying a packet in real time, thus mitigating the jamming node's ability to perform selective jamming by preventing real time packet classification.

Keywords: adversary; selective jamming; packet classification; protocol semantics.

1. Introduction

Wireless networks are computer networks that do not involve any kind of cables for connection and is vulnerable to both internal and external attacks. Internal attacks, which are launched from compromised nodes, are more sophisticated in nature [3]. These attacks exploit knowledge of network secrets and protocol semantics to selectively and adaptively target critical network functions. An investigation is done focusing on the impact of selective jamming on critical network functions and it is shown that these attacks can be launched by performing real-time packet classification at the physical layer. Attack selectivity can be achieved, for example, by overhearing the first few bits of a packet, or classification of transmissions based on protocol semantics. Internal attacks, henceforth referred to as insider attacks, cannot be mitigated using only proactive methods which rely on network secrets, because the attacker already has access to such secrets. They additionally require mechanisms with built-in security measures, through which the selective nature of the attacker can be neutralized.

2. System Model

2.1. Problem definition

Consider two nodes A and B communicating via a wireless link, with a jamming node J within their communication range [1]. When a packet M is transmitted by A to B, node J classifies M on the fly before its reception at B as shown in Fig 1. Our aim is to delay the jamming node from classifying M in real time, thus mitigating J's ability to perform selective jamming.

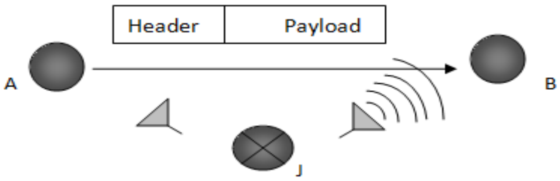


Fig. 1 Inside Jammer Attack

2.2. Network model

The network consists of a collection of nodes connected via wireless links. Nodes can communicate in two ways: they communicate directly if they are within the communication range or they communicate indirectly via multiple hops. Communication can be either encrypted or unencrypted.

2.3. Adversary model

The adversary model considered in this paper is an inside jammer. The adversary can easily launch internal attacks with data alteration, message negligence, selective forwarding, jamming, etc. The insider attackers are severely destructive to the functioning of a network. As the jammer is from within the network, jammer has access to shared cryptographic keys, aware of protocol semantics and the network topologies and may be equipped with advanced hardware like multiple radios, multiple directional antennas and high computational power. The adversary can launch a denial of service attack from within the network.

More precisely, the adversary is not only insider but also selective. It targets messages of high importance like control packets. It follows the strategy of smart jamming i.e. "classify-then-jam" as shown in Fig 2. The jammer classifies the packet into 2 groups, important packets and unimportant packets, from which important packets are selectively jammed [1]. The adversary also has directional antennas which allow reception of signals in one node and jamming the same signal at another node. Furthermore, the adversary can physically compromise network devices and can recover stored information including cryptographic keys [4], PN codes, etc.

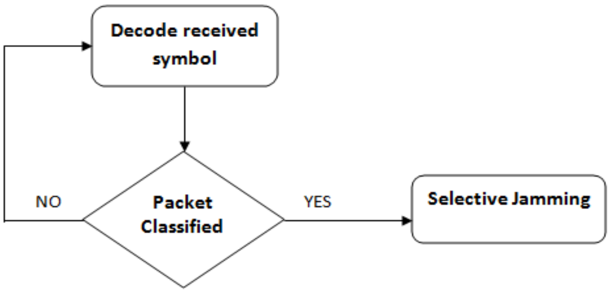


Fig. 2 Classification of Packet leading to Selective Jamming

3. System Design

Design involves two scenarios, one in which the real time packet classification takes place and the other which includes the schemes to mitigate the selective jamming attacks, which results due to classification.

3.1. Real time packet classification

Real time packet classification describes how the adversary can classify the packets in real time, before the packet transmission is completed. When the classification takes place, it is easy to jam the packet based on the strategy of the jammer node. A packet includes the MAC layer header, IP layer header and TCP layer header as shown in Fig 3.

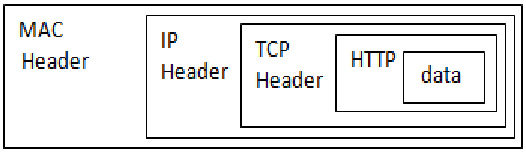


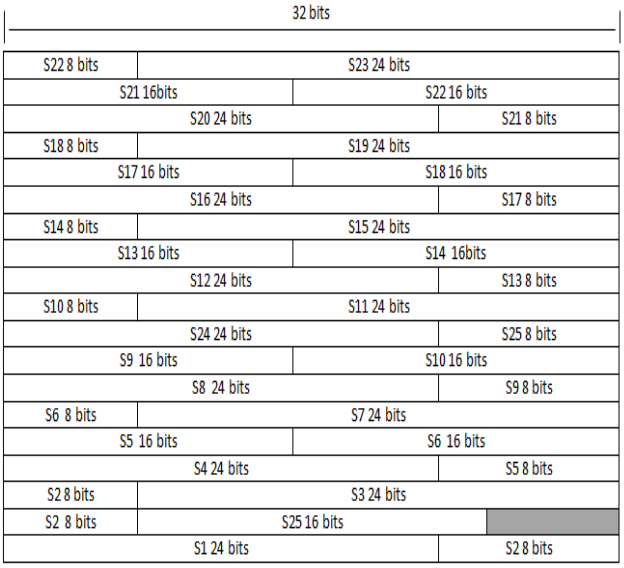
Fig. 3 Headers for each layers appended to data

At the modulator, the output of the interleaver is modulated as 25 OFDM symbols as shown in Fig 4.

Here,

$$1 \text{ symbol} = 24 \text{ bits}$$

$$25 \text{ symbols} = 600 \text{ bits}$$



32 bits

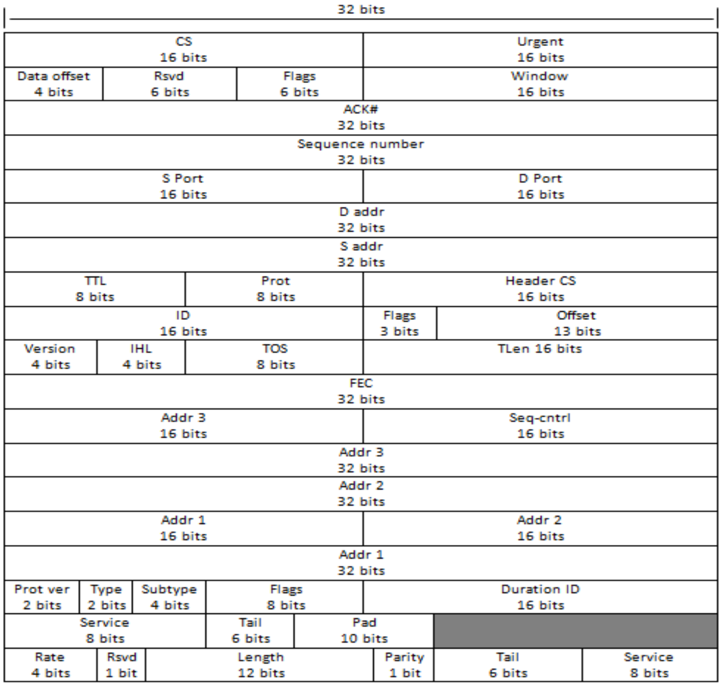
S22 8 bits	S23 24 bits	
S21 16bits	S22 16 bits	
S20 24 bits	S21 8 bits	
S18 8 bits	S19 24 bits	
S17 16 bits	S18 16 bits	
S16 24 bits	S17 8 bits	
S14 8 bits	S15 24 bits	
S13 16 bits	S14 16bits	
S12 24 bits	S13 8 bits	
S10 8 bits	S11 24 bits	
S24 24 bits	S25 8 bits	
S9 16 bits	S10 16 bits	
S8 24 bits	S9 8 bits	
S6 8 bits	S7 24 bits	
S5 16 bits	S6 16 bits	
S4 24 bits	S5 8 bits	
S2 8 bits	S3 24 bits	
S2 8 bits	S25 16 bits	
S1 24 bits	S2 8 bits	

Fig. 4 Header Fields grouped as 25 OFDM symbols

The 600 bits constitutes the header fields of a packet in the following format,

- Physical layer header includes 56 bits. Symbol 1, Symbol 25 and part of Symbol 24 and 2 constitute the physical layer header.
- MAC layer header includes 224 bits. Symbol 3, Symbol 4, Symbol 5, Symbol 6, Symbol 7, Symbol 8, Symbol 9 and part of Symbol 2, 10 and 24 constitutes the MAC layer header.
- IP layer header includes 160 bits. Symbol 11, Symbol 12, Symbol 13, Symbol 14, Symbol 15, Symbol 16 and part of Symbol 10 and 17 constitutes the IP layer header.
- TCP layer header includes 160 bits. Symbol 18, Symbol 19, Symbol 20, Symbol 21, Symbol 22, Symbol 23 and part of Symbol 17 constitutes the TCP layer header.

The details are shown in Fig 5.



32 bits

CS 16 bits	Urgent 16 bits				
Data offset 4 bits	Rsvd 6 bits	Flags 6 bits	Window 16 bits		
ACK# 32 bits					
Sequence number 32 bits					
S Port 16 bits	D Port 16 bits				
D addr 32 bits					
S addr 32 bits					
TTL 8 bits	Prot 8 bits	Header CS 16 bits			
ID 16 bits	Flags 3 bits	Offset 13 bits			
Version 4 bits	IHL 4 bits	TOS 8 bits	TLen 16 bits		
FEC 32 bits					
Addr 3 16 bits	Seq-cntrl 16 bits				
Addr 3 32 bits					
Addr 2 32 bits					
Addr 1 16 bits	Addr 2 16 bits				
Addr 1 32 bits					
Prot ver 2 bits	Type 2 bits	Subtype 4 bits	Flags 8 bits	Duration ID 16 bits	
Service 8 bits	Tail 6 bits	Pad 10 bits			
Rate 4 bits	Rsvd 1 bit	Length 12 bits	Parity 1 bit	Tail 6 bits	Service 8 bits

Fig. 5 Header fields for each layer

3.2. Fields in the headers that leads to packet classification

A packet can be classified based on the headers of various layers. More precisely, if the length of the header increases above a threshold value (includes options in IP header), then the message is treated as an important message and is classified for selective jamming.

For example, the MAC header typically contains information about the next hop and the packet type. The TCP header reveals the end-to-end source and destination nodes, the transport-layer packet type (SYN, ACK, DATA, etc.), and other TCP parameters. Not all the header field can cause classification of a packet. Only certain header fields can reveal whether a packet is having important data or not. Fig.6 shows the header fields that lead to packet classification.

Classification in datalink layer mainly occurs in the symbols, frame type and WEP. Frame type reveals the control information which leads to classification. When the WEP field in Flags is set to 1, it indicates that encryption schemes have been used, leading to classification. Classification in network layer mainly occurs in the symbols, Type of Service, Source Routing and Option. TOS reveals about the type of service provided. Source routing reveals the secure routing paths. Option reveals about the source routing information. Classification in transport layer mainly occurs in the symbols, destination port and URG. Destination port reveals about the destination of the respective packet. When the URG is set to 1, it indicates that the packet is important, leading to classification. One of the important fields that lead to classification is header length (IHL). If header length of the entire packet exceeds 600 bits, then it indicates that encryption schemes have been used. This leads to classification.

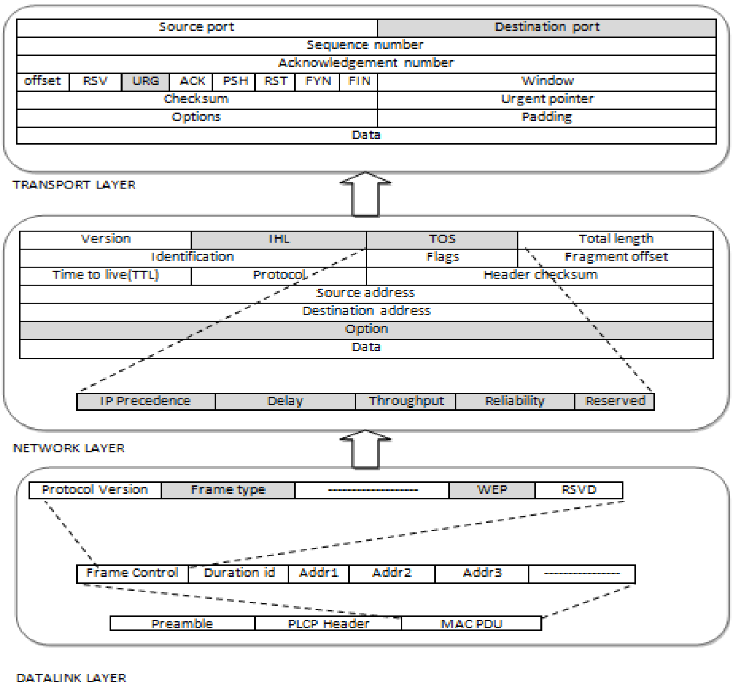


Fig. 6 Architecture for real time packet classification

3.3. Mitigation of real time packet classification

An intuitive solution for preventing packet classification is to encrypt transmitted packets with a secret key. In this case, the entire packet, including its headers, has to be encrypted. But the particular key should be known to all receivers. Thus, this key is also known to an inside jammer which is a compromised node. In symmetric encryption schemes based on block encryption, reception of one cipher text block is sufficient to obtain the corresponding plaintext block, if the decryption key is known. Hence, encryption alone does not prevent insiders from classifying broadcasted packets [6]. To prevent classification, a jammer must be delayed in classifying until the packet is transmitted in its entirety. This can be done using a cryptographic puzzle. The key used to encrypt the message is embedded in a cryptographic puzzle, which has to be solved within a timeslot by the receiver to get the key and decrypt the message. This scheme delays the packet classification as the jammer will take considerable time to solve the puzzle, get the key, decrypt the message and then read the header information to classify the packet.

Another possible technique is Digital enveloping. In Digital enveloping, a message, on entering network should obtain both private and public key through registering authority. Participating node in the network will have the public key of all other nodes. Then using a symmetric key, the packet with the header is encrypted and the symmetric key itself is encrypted by the public key of receiver. Fig 7 show the scheme used to prevent real time packet classification.

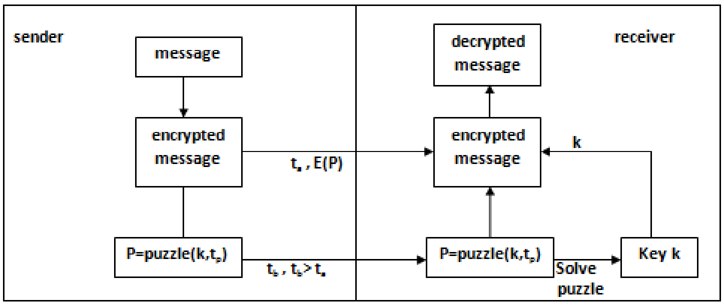


Fig. 7 Mitigation of real time packet classification

4. Simulation Analysis

Network Simulator is an object oriented discrete event simulator which maintains list of events and executes one event after another. Simulation results enable the evaluation of the network performance with respect to the network density/ number of nodes. It explains the network performance with respect to the attacks caused by the selective jammer as a result of packet classification.

4.1. Node vs average throughput

Average throughput can be defined as the average number of packets transmitted per unit time. It is the average rate of successful message delivery over a communication channel. The average throughput is maximum at node 11 with a value of 83% and minimum at node 4 with a value of 72.75%.

Throughput = (total number of packets transmitted / time of simulation) * Packet Size (1)

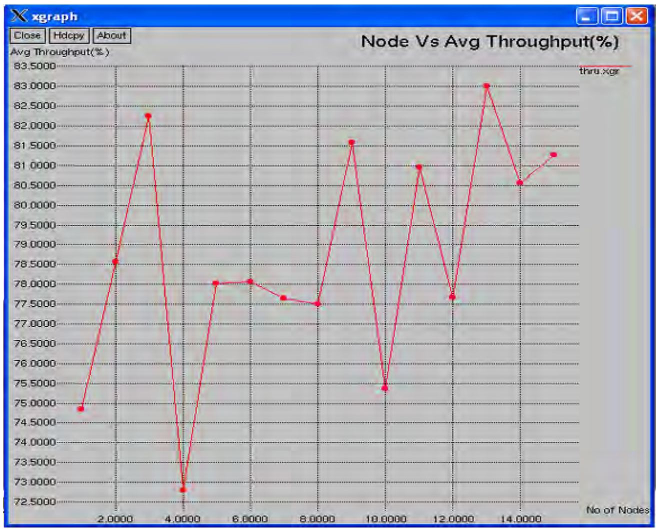


Fig. 8 Node vs Average Throughput

The Fig.8 shows the variation in throughput with respect to the real time packet classification by the jammer node. Due to the variation in the throughput, the performance of the protocol will also be varied. The performance degradation is the overall effect in the presence of a selective inside jammer when a packet of high importance is transmitted within the network.

4.2. Node vs loss rate

Loss rate indicates how many packets are dropped during transit. More precisely, it is the difference between the total number of packets transmitted and the number of packets received .Jamming can lead to an increase in packet loss rate. The packet loss rate is maximum at node 11 with a value of 19.36% and minimum at node 2 with a value of 15.90%.

Packet loss = number of packets send by the sender – number of packets received by the receiver (2)

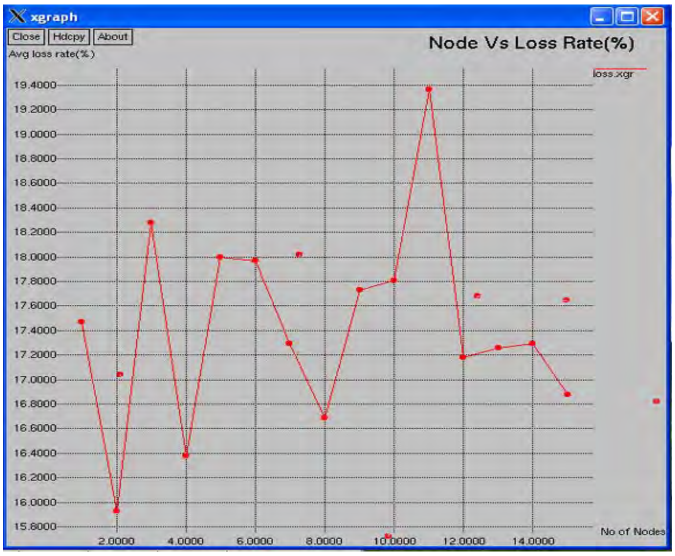


Fig. 9 Node vs Loss Rate

The Fig.9 shows the variation in packet loss rate with respect to the real time packet classification by the jammer node. Due to the variation in the throughput, the performance of the protocol will also be varied. The increase in packet loss rate and thus the performance degradation is the overall effect in the presence of a selective inside jammer when a packet of high importance is transmitted within the network. Unimportant packets are not targeted due to the selective nature of the jammer node.

5. Conclusion

Wireless networks are prone to various internal security threats. While most internal attacks can be mitigated easily, selective internal attacks are much harder to counter. Clear evaluations have been done to understand how real time packet classification is done by a compromised node to identify the packet as a highly important one. In this paper, various header information that reveal the importance of the message have been studied and a scheme has been proposed to prevent the real time packet classification of the packet during transit. Simulation results are based on the network performance with respect to the network density. The conclusions made include how the adversary classified packets in real time, how packet classification can be mitigated through delaying schemes and evaluation of the delaying of packet classification.

References

[1] A. Proa˜no and L. Lazos, “Selective Jamming Attacks in Wireless Networks,” IEEE International Conference on Communications (ICC), pp. 1 – 6, 2010.

[2] Fang Liu, Xiuzhen Cheng, “Insider Attacker Detection in Wireless Sensor Networks”, 26th IEEE International Conference on Computer Communications, IEEE INFOCOM 2007.

[3] Kemal Bicakci, Bulent Tavli, “Denial-of-Service attacks and counter measures in IEEE 802.11 wireless networks”, Elsevier Journal on Computer Standards and Interfaces.

[4] L. Lazos and M. Krunz, “Selective Jamming/Dropping Insider Attacks in Wireless Mesh Networks,” IEEE Network, Vol. 25, No. 1, pp. 30 – 34, 2011.

[5] L. Lazos, S. Liu, and M. Krunz, “Mitigating Control Channel Attacks in Multi-channel Ad-Hoc Networks,” 2nd ACM Conference on Wireless Network Security (WiSec), pp. 169 – 180, 2009.

[6] L. Lazos, S. Liu, and M. Krunz, “Thwarting Inside Jamming Attacks on Wireless Broadcast Communications,” 4th ACM Conference on Wireless Network Security (WiSec), pp. 29 – 40, 2011.

[7] S. Liu, L. Lazos, and Marwan Krunz, “Jamming-resistant Broadcast Communications under Internal Threats,” IEEE Transactions on Mobile Computing (TMC), 14 pages, Feb 2012.

[8] Payal Jain and Sameer Verma, “Study and Analysis of security Issues in Wireless Sensor Networks”, September 2011. Global Journal of Computer Science and Technology, vol 11, issue 16.

[9] S. Liu, L. Lazos, and M. Krunz, “Thwarting Control-Channel Jamming Attacks from Inside Jammers,” IEEE Transactions on Mobile Computing (TMC), 14 pages (plus 2 appendix pages), DOI: 10.1109/TMC.2011.165.

[10] Stallings, W., Wireless Communications and Networks, 2nd Edition, Prentice Hall, 2005.

[11] Timothy X Brown, Jesse E James, Amita Sethi, “Jamming and Sensing of Encrypted Wireless Ad Hoc Networks”, MobiHoc’06 Conference.