International Journal of Engineering Research and Development
e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 8, Issue 4 (August 2013), PP. 26-32

Intrusion Detection and Hindrance for Spot Jamming Attacks in Wireless Network for Packet Concealing Ways

N.Kavitha[1], R.UmaSaraswathi[2], A.K.SathiyaBama[3]
[1,2]*Research Scholars, Department of Computer science, Vivekanandha College, Elayampalayam, Tiruchengode-637205, India*
[3]*Assistant Professor, Department of Computer Application, Vivekanandha College, Elayampalayam, Tiruchengode-637205, India*

Abstract:- Wireless networks are built upon a shared medium that makes it easy for adversaries to launch jamming-style attacks. In wireless networks, the problem of selective jamming attacks is identified. In these attacks, the adversary is active only for a short period of time, selectively targeting messages of high importance. We illustrate the advantages of selective jamming in terms of network performance degradation and adversary effort by presenting two case studies: a selective attack on TCP and routing. We show that selective jamming attacks can be launched by 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 analyse the security of our methods and evaluate their computational and communication overhead.

Keywords:- Denial of Service, Jammer detection, Packet Hiding, Selective Jamming Attacks, Security, TCP, Wireless Network

I. INTRODUTION

Ad hoc networks are envisioned as playing a significant role in mission critical communication for the military utilities, and industry. An adversary may attempt to attack a victim ad hoc network to prevent some or all victim communication. Such denial-of-service (DoS) attacks have been considered in ad hoc wireless networks at several levels. A number of researchers have considered DoS where the attackers are internal participants in the victim ad hoc network. Ad hoc networks require the cooperation of peer nodes for their operation and are especially susceptible to such peer-based attacks. In this paper we consider encrypted victim networks in which the entire packet including headers and payload are encrypted and thus the attacker cannot directly manipulate any of the victim communication. In this case, the attacker must resort to external physical-layer-based DoS, also known as jamming.

Since RF (radio frequency) is essentially an open medium, jamming can be a huge problem for wireless networks. Jamming is one of many exploits used to compromise the wireless environment. It worksby denying service to authorized users as legitimatetraffic is jammed by the overwhelming frequencies of illegitimate traffic. A knowledgeable attacker with the right tools can easily jam the 2.4 GHz frequency in a way that drops the signal to a level where the wireless networks can no longer function.The complexity of jamming is the fact that it may not be caused intentionally, as other forms of wireless technology are relying on the 2.4 GHz frequency as well. Some widely used consumer products includecordless phones, Bluetooth-enabled devices and baby monitors, all capable of disrupting the signal of a wireless network and faltering traffic. The issue of jamming mostly relates to older wireless local area networks as they are not fully equipped to make the adaptation to numerous types of interference. These networks typically call for an administrator to manually adjusteach access point through trial and error. To avoid this daunting task, the best practice is to invest into a newer WLAN.

Wireless networks are susceptible to threats that are not able to be adequately addressed via cryptographic methods. One serious class of such threats are attacks of radio interference. The shared nature of the wireless medium combined with the commodity nature of wireless technologies and an increasingly, sophisticated user-base, allows wireless networks to be easily monitored and broadcast on. Adversaries may easily observe communications between wireless devices and just as easily launch simple denial of service attacks against wireless network by injecting false messages.

A. Jamming Solution

If an attacker truly wanted to compromise your LAN and wireless security, the most effective approach would be to send random unauthenticated packets to every wireless station in the network[3]. This exploit can be easily achieved by purchasing hardware off the shelf from an electronics retailer and downloading free

software from the internet. In some cases, it is simply impossible to defend against jamming as an experienced attacker may have the ability to flood all available network frequencies.

If the major concern relates to malicious jamming, an intrusion prevention and detection system may be your best option. At the bare minimum, this type of system should be able to detect the presence of an RPA (Rogue Access Point) or any authorized client device in your wireless network [4]. More advanced systems can prevent unauthorized clients from accessing the system, alter configurations to maintain network performance in the presence of an attack, blacklist certain threats and pinpoint the physical location of a rogue device to enable faster containment.

II. RELATED WORK

In modern era the accommodations provided by the 802.11 based wireless access network led to its deployment in various sectors such as defence, consumer and industrial sector. Openness of wireless network makes it vulnerable to various types of attacks. Out of various types of attacks, Denial-of-service (DoS) attack is one of the most troublesome threat which prevent legitimate users from accessing the network[2]. It is executed in many ways such as intentional interference or jamming. Jamming is one of many exploits used to compromise the wireless environment. It works by denying service to authorized users as legitimate traffic is jammed by the overwhelming frequencies of illegitimate traffic.

If an attacker truly wanted to compromise your LAN and wireless security, the most effective approach would be to send random unauthenticated packets to every wireless station in the network. To minimize the impact of an unintentional disruption, it is important to identify its presence. Jamming makes itself known at the physical layer of the network, more commonly known as the MAC (Media Access Control) layer[2].

The increased noise floor results in a faltered noisetosignal ratio, which will be indicated at the client. It may also be measurable from the access point where network management features should able to effectively report noise floor levels that exceed a predetermined threshold. From there the access points must be dynamically reconfigured to transmit channel in reaction to the disruption as identified by changes at the physical layer.

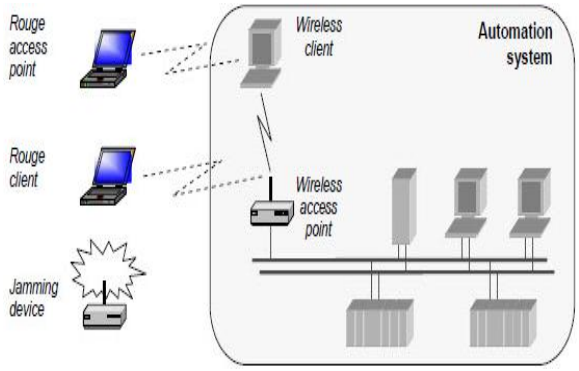

Fig.1: Selective Jamming and Random access point

A.DETECTION OF JAMMING

The network employs a monitoring mechanism for detecting potential malicious activity by a jammer. The monitoring mechanism consists of the following:

(i) determination of a subset of nodes *M* that will act as network monitors

(ii) employment of a detection algorithm at each monitor node.

The assignment of the role of monitor to a node can be affected by energy limitations and detection performance specifications. In this work, we fix *M* and formulate optimization problems for one or more monitor nodes. We now fix attention to detection at one monitor node. First, we define the quantity to be observed at each monitor node. In our case, the readily available metric is probability of collision that a monitor node experiences, namely the percentage of packets that are erroneously received.

During normal network operation, and in the absence of a jammer, we consider a large enough training period in which the monitor node "learns" the percentage of collisions it experiences as the long-term average of the ratio of number of slots in which there was a collision over total number of slots of the training period. Assume now the network operates in the open after the training period and fix attention to a time window much smaller than the training period. An increased percentage of collisions over this time window compared to the learned long-term average may be an indication of an ongoing jamming attack or only a temporary increase of percentage of collisions compared to the average during normal network operation[10][11]. A detection algorithm takes observation samples obtained at the monitor node (i. e, collision or not collision) and decides

whether there exists an attack. On one hand, the observation window should be small enough, such that the attack is detected on time and appropriate countermeasures are initiated. On the other hand, this window should be sufficiently large, such that the chance of a false alarm notification is minimized.

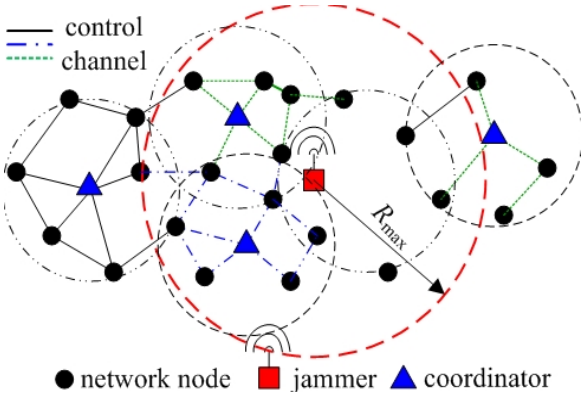

Fig.2: Detection of the Collision and control channel

B.JAMMING TYPE

Jammer is an entity who is purposefully trying to interfere with transmission and reception of message across the wireless channel. Recently, several jamming strategies have been introduced. Later, jammers were categorized into four models. They are

❖ *Constant jammer*

In this model, jammer continuously emits RF signals and it transmits random bits of data to channel. It does not follow any MAC layer etiquette. Being constant to the transfer it does not wait for channel to become an idle.

❖ *Reactive jammer*

In this model, jammer will stay quite when the channel is idle. As soon as it senses activity on channel, it starts transmitting signal. In order to sense the channel jammer is ON and should not consume energy.
To mitigate jamming attacks many hiding schemes were used. These are

- Strong hiding commitment scheme
- Cryptographic puzzle base scheme
- All-or-nothing transmission

❖ *Deceptive jammer*

In this model, jammer constantly injects series packets to the channels without any gap between subsequent transmissions. It also broadcasts fabricated messages and reply old ones. Jammer will pass rambles out to the network and just check the preamble and remain silent.

❖ *Random jammer*

In this model, jammer alternates between period of continuous jamming and inactivity. After jamming for t1 units of time, it stops emitting radio signals and enter into sleep mode. The jammer after sleeping for t2 units of time wakes up and resumes jamming. Both time t1 and t2 is either random or fixed.

III. BASIC STATISTICS FOR DETECTING JAMMING ATTACKS

In this section, the evaluation of the proposed scheme in terms of end-to-end delay and throughput is described. Simulations have been conducted using OPNET Modeler16.0 [9]. We compare the proposed scheme with jammed area mapping scheme [4]. In order to implement proposed robust rate adaptation scheme, we modify IEEE 802.11 DCF (Distributed Coordination Function) scheme in OPNET Modeller. The simulation parameters are summarized in Table 1.

A. REAL-TIME PACKETCLASSIFICATION

In this section, we explain how the opponent can classify packets in real time, previous to the packet broadcast is accomplished. Once a packet is classified, the adversary may choose to jam it depending on his strategy. Consider the generic communication system depicted. At the Physical layer, a packet m is encoded, interleaved, and modulated before it is transmitted over the wireless channel. At the receiver, the signal is demodulated, deinterleaved, and decoded to recover the original packet m.[12].

Table 1: Simulation Parameters

PARAMETER	VALUE
Simulation area	10 Km × 10 Km
Transmission range	5 Km
Traffic model	CBR
Transmission data rate	2 Mbps
Simulation time	10000 second
Signal strength threshold	-75 dBm
PDR threshold	75 %

The adversary's aptitude in classifying a packet m depends on the accomplishment of the blocks in Fig. 2. The channel indoctrination block expands the innovative bit sequence m, adding essential redundancy for defensive m against channel errors. For example, an α/β-block code may protect m from up to e errors per block ([6],[7]-[9]) Alternatively, an α/β-rate convolutional encoder with a constraint length of Lmax, and a free distance of e bits provides similar protection. For our purposes, we assume that the rate of the encoder is α/β. At the next block, interleaving is applied to protect m from burst errors. For simplicity, we consider a block interleaver that is defined by a matrix Ad×_1 [1]. The de-inter-leaver is simply the transpose of A. Finally, the digital modulator maps the received bit stream to symbols of length q, and modulates them into suitable waveforms for transmission over the wireless channel. Typical modulation techniques include OFDM, BPSK,-QAM, and CCK.

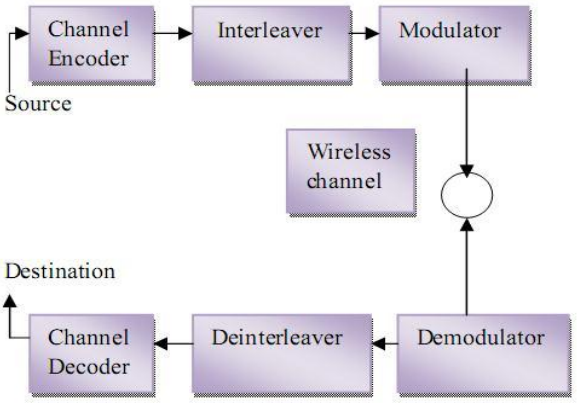

Fig.3: A general communication system diagram.

B. Proposed Detection Algorithm

Step 1

The sender and receiver change channels in order to stay away from the jammer, in channel hoping technique.

Step 2

The pair-wise shared key KS is used for creating a channel key KCh = EKS(1) , which generates a pseudorandom channel sequence

Chs = {EKS(i)mod Ch}, i ≥ 0,

where, Ch is the number of channels available in the band,cmessage mi is transmitted on channel Chi , (unknown to anycbut the two parties involved.)

Step 3

Using packet fragmentation technique, the packets are break into fragments to be transmitted separately on different channels and with different SFD (start of frame delimeter). The last fragment contains a frame check sequence FCS for the entire payload.

Step 4
The above figure shows the way in which fragments are transmitted. To transmit fragment Fri, the sender hops to Chi, fills the transmit FIFO with Fri, sets SFD to Si and issues the transmit command.
Step 5
The time to transmit the fragment is
Tfrag = Th + T ini + Td + Tminhdr + Tfr
Step 6
If the fragments are short, the attacker's jamming message does not start till the sender has finished transmitting and hopped to another channel.
Step 7
In the Pulse Jamming attack, the jammer remains on a single channel, hoping to disrupt any fragment that may be transmitted. As packets cannot be detected quickly enough for selective jamming, the attacker transmits blindly in short pulses. The jamming pulses must occur no less frequently than Tminhdr + Tfr to prevent any fragments from slipping through.
Step 8
The forward ants (FA) explore the network to collect the jammer's information on each channel. It keeps collecting the attackers' data if any and moves forward though channels. When the FA reaches the end of the channel, it is de-allocated and the backward ant (BA) inherits the stack contained in the FA.
Step 9
The BA is sent out on high priority queue. The backward ants retrace the path of the FA and utilize this information to update the data structures periodically.
Step 10
As it reaches the source, the data collected is verifiedwhich channel there is prevalence of attacker long time, and those are omitted. Simultaneously the forward ants are sent through other channels which are not detected before for attacks.
Step 11
The FAs either unicast or broadcast at each node depending on the availability of the channel information for end of the channel.
Step 12
If the channel information is available, the ants randomly choose the next hop. This scheme helps limit the channel maintenance overhead. If the pheromone information is available at the channel i , then the channel probability P (Chi, j,d) of choosing neighbour channel j as the next hop for last.

$$P(Ch_{i,j,d}) = \frac{[\sigma_{i,j,d}]^{\alpha}[\lambda_{i,j}]^{\beta}}{\sum_{l \in N_i}[\sigma_{i,l,d}]^{\alpha}[\lambda_{i,l}]^{\beta}}$$

C. Performance Metrics

The proposed detection algorithm Defence Technique (SBDT) is compared with the DEEJAM detection technique [8]. The performance is evaluated mainly, according to the following metrics.

- Aggregated Throughput
- Packet Delivery Ratio
- Packet Drop

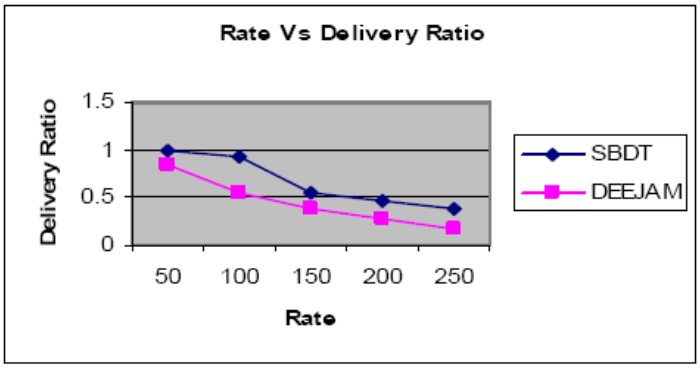

Fig. 2. Rate Vs packet delivery ratio

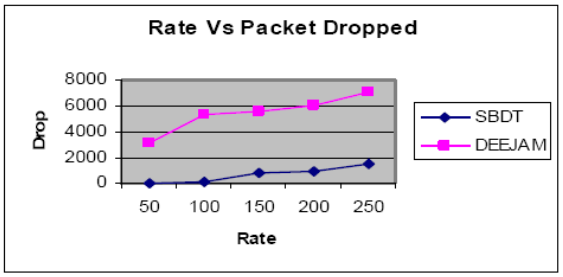

Fig. 3. Rate Vs packet dropped

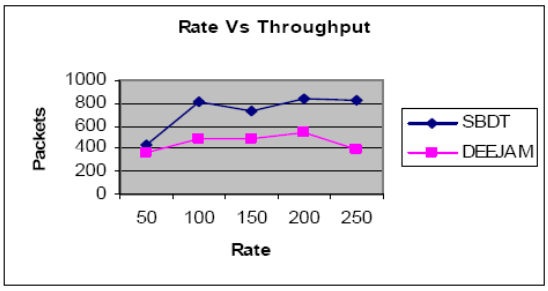

Fig. 4. Rate Vs throughput

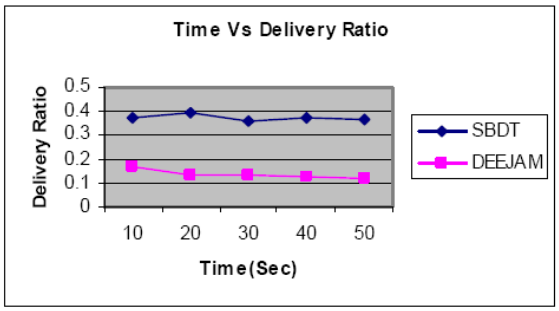

Fig. 5. Time Vs packet delivery ratio

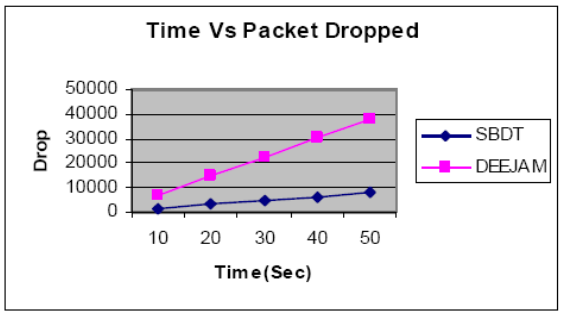

Fig. 6. Time Vs packet dropped

IV. CONCLUSION

An exploit can be either an information-gathering probe or an attack to compromise, disable, or harm a network or network resource. In some cases, the distinction between the two objectives of an exploit can be unclear. Furthermore, because an attacker usually precedes an attack by performing reconnaissance on the target, we can consider information-gathering efforts as a precursor to an impending attack that is, they constitute the first stage of an attack.

Thus, the term exploit encompasses both reconnaissance and attack activities, and the distinction between the two is not always clear. We evaluated the impact of selective jamming attacks on network protocols such as TCP and routing. Our findings show that a selective jammer can significantly impact performance with very low effort. We developed three schemes that transform a selective jammer to a random one by preventing real-time packet classification.

REFERENCES

[1] Timothy X Brown Jesse E. James.*Jamming and Sensing of Encrypted Wireless Ad Hoc Networks.* Amita Sethi University.

[2] Mr. Pushphas Chaturvedi Mr. Kunal Gupta.*Detection and Prevention of various types of Jamming Attacks in Wireless Networks.* Dept. Of Computer Science, Amity University.

[3] Neha Thakur.*Introduction to Jamming Attacks and Prevention Techniques using Honeypots in Wireless Networks.* Dept. of Software Engineering ,SRM University,Chennai, India.

[4] Kwangsung Ju and Kwangsue Chung .*Jamming Attack Detection and Rate Adaptation Scheme for IEEE 802.11 Multi-hop Tactical Networks.* Department of Communications Engineering Kwangwoon University, Seoul, Korea.

[5] S. Periyanayagi and V. Sumathy.*A Swarm Based Defense Technique for Jamming Attacks in Wireless Sensor Networks.*

[6] Alejandro Proa˜no and Loukas Lazos . *Packet-Hiding Methods for Preventing Selective Jamming Attacks.* Dept. of Electrical and Computer Engineering, University of Arizona, Tucson, AZ, USA.

[7] T. X. Brown, J. E. James, and A.Sethi. *Jamming and sensing of encrypted wireless ad hoc networks.* In Proceedings of MobiHoc, pages 120–130, 2006.

[8] M. Cagalj, S. Capkun, and J.-P. Hubaux.*Wormhole-based antijamming techniques in sensor networks.* IEEE Transactions on Mobile Computing, 6(1):100–114, 2007.

[9] A. Chan, X. Liu, G. Noubir, and B. Thapa. *Control channel jamming: Resilience and identification of raitors.* In Proceedings of ISIT, 2007.

[10] T. Dempsey, G. Sahin, Y. Morton, and C. Hopper.*Intelligent sensing and classification in ad hoc networks: a case study.* Aerospace and Electronic Systems Magazine, IEEE, 24(8):23–30, August 2009.

[11] Y.Desmedt.*Broadcast anti-jamming systems. Computer Networks.* 35(2-3):223–236, February 2001.

[12] K. Gaj and P. Chodowiec.*FPGA and ASIC implementations of AES.* Cryptographic Engineering, pages 235–294, 2009.