Introduction to Jamming Attacks and Prevention Techniques using Honeypots in Wireless Networks

Neha Thakur
Dept. of Software Engineering
SRM University

Aruna Sankaralingam
Dept. of Software Engineering
SRM University
Chennai, India

***Abstract*— Built upon a shared wireless medium, wireless networks are susceptible to jamming attacks. These types of attacks can easily be accomplished by an adversary by either bypassing MAC layer protocol or by emitting RF signals. Typically, jamming can be referred as intentional interference attacks on wireless networks. It is an attempt of making the users not possible to use network resources. Jamming attacks are severe Denial-of-service attacks against wireless medium. In this work, considering the role of wireless adversary, which targets the packets of high importance by emitting radio frequency signals and do not follow underlying network architecture. Typically, jamming attacks have been considered under external threat model, in which jammer is not part of network. However, adversaries with internal knowledge of protocol and network specification can introduce jamming attacks that are difficult to detect and prevent. First, emphasizing the four jamming models that an attacker can use to disable the operation of wireless networks. And then we will discuss about different measurements that can serve as the purpose for detecting jamming attacks. Further, it is shown that such attacks can be introduced by performing real-time packet classification at physical layer. To prevent these attacks, some schemes such as Triple DES, multilevel steganography. This paper also investigates the solutions to reduce the effectiveness of jammer as well as to decrease the jamming rate.**

Keywords-Selective Jamming, Denial of service, Packet classification, All-or-nothing Transmission.

I. INTRODUCTION

Wireless networks are meant for transferring information of any kind between two or more points that are not physically connected. Wireless networks are vulnerable to various kinds of attacks because of its shared medium. There is need to deal with numerous security issues. Attackers with a transceiver can be able to hinder wireless transmission, insert unwanted messages, or jam messages of high importance. Jamming can be considered as one of fundamental way of degrading network performance. In the simplest form of jamming, the adversary corrupts the content of original message by transmitting radio frequency signals in the network or by blocking the message so that it cannot be able to reach to the intended receiver. Radio interference attacks cannot be easily addressed by conventional security methods. An adversary can simply disregard the medium access protocol and continually transmitting on a Wireless networks. Typically, jamming can be done in two forms. One is external threat model in which jammer will not be the part of network. Other one is internal threat model in which jammer will be the part of network. In this paper, we will focus on external threat model where jammer with some secrets about internal network can be able to introduce jamming attacks.

In this paper, network model is considered where nodes are communicating with each other and there adversary node also exist, which will jam messages going through network. As we are considering that jammer is following external threat model and jammer will not be the part of network but jammer is aware of all the implementation details of network protocols. By using this knowledge, jammer targets the packets of high importance or high priority. For example, jamming of TCP acknowledgement can degrade the throughput of TCP connection. To perform selective jamming, adversary must be capable of real time packet classification and corrupting packets before the end of their transmission.

II. RELATED WORK

Although several studies have targeted jamming attacks but definition of jamming was unclear. An assumption is made that jammer transmits RF signal in wireless channel, so that channel is completely blocked and intended receiver may not be able to receive message. Therefore, 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
- Reactive jammer
- Deceptive jammer
- Random jammer

A. 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.

B. Deceptive Jammer

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

C. 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.

D. 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

III. EXISTING SYSTEM

Considering scenario where jammer jams the channel by blocking one or more nodes and block or corrupts the packets. This continuous jamming can be used as denial-of-service attacks. The jammer controls the probability of jamming and transmission range to cause maximal damage to the network in terms of corrupted transmission links. The jammer action ceases when it is monitored detecting node and notification message is passed out of jamming region. To detect jamming attacks some statistics are used such as signal strength, carrier sensing time, packet delivery ratio. In the existing system, objective of jammer is to interfere with legitimate wireless networks and assumptions is made such as A and B are participating nodes and X is jamming node, now A is unable to send the packets for many reasons. For example, X can continuously transmits the signal so that a can never sense channel idle or, A can send packets to A and force A to receive the junk packets all the time. So, it is necessary to measure the effectiveness of jammer and for this two matrices has been defined which are packet send ratio and packet delivery ratio.

IV. PROPOSED SYSTEM

Jamming attacks are usually introduced by emitting radio frequency signal,such attacks cannot be preventable by conventional security measures. The objective of a jammer is to interfere with legitimate wireless traffic. Jammer can achieve this goal by either blocking real traffic or, by preventing reception of messages. There are different jamming models which can be used by jammer to address jamming attacks. This is the main reason why detecting jamming is very difficult as well as important as it is the first step towards building secure and dependable wireless channel. In existing systems, jammer jams an area in single wireless channel. Jammer controls the probability of jamming and transmission range in order to cause maximal damage. In this paper multiple wireless channels are used, where jammer is trying to jam multichannel wireless network. To addressing jamming attacks jammer must be capable of classifying packets in real time. In order to launch jamming attacks, feasibility of real time packet classification is also introduced. To mitigate jamming attacks different techniques have been introduced such as steganography, multilevel steganography, triple DES, Hidden communication system.

This paper is introducing, honeypots technique to reduce the effectiveness of jammer as well as to decrease the jamming rate.

V. SYSTEM ARCHITECTURE AND MODELS

A. Network model

This paper models multi-hop wireless network as directed graph G= (V,E,C). This wireless network consists of collection of nodes. Nodes may communicate directly if they are within communication range or, indirectly via multi hops. Nodes can communicate in both unicast and broadcast mode. Communication can be either unencrypted or encrypted. For encrypted communication, symmetric key is shared among intended receivers. For encryption asymmetric key encryption is used.

B. Communication model

All packets are transmitted at some predefined rate. Spread spectrum technique such as frequency hopping spread spectrum or, direct hopping spread spectrum may be used at physical layer. As shown in figure. 1(b), each transmitted packet have generic frame format. The preamble is used for synchronizing sampling process at receiver. The PHY layer header includes information regarding length of frame, and transmission rate. The MAC header determines the MAC protocol version, source and destination addresses, sequence number plus additional fields. The MAC header is followed by frame body that typically contains an ARP packets or IP datagram. Finally, MAC frame is protected by cyclic redundancy check (CRC) code. At the PHY layer, trailer may be appended to synchronizing sender and receiver.

C. Jamming model

Consider multi-hop wireless network under jamming model. It has constant traffic generating rate and jamming range. Assume that they are smart jammers and can occupy channels when sending jamming traffic. Jamming node can operate in full-duplex mode, thus being able to transmit and receive simultaneously. To achieve this, each network node is equipped with multiple radios and jammer node is equipped with one radio, which can transmit jamming data to any of the network node. Jammer can also use its sensing capability to sense on going activity.

The adversary is assumed to be computationally and storage bounded, it can be far superior to network nodes. In particular, jammer is equipped with special purpose hardware in order to perform cryptanalysis or any other computation required. The implementation details of every layer of network stack known to be public. So, jammer is capable of compromising network devices and recovering stored information including cryptographic keys and PN codes.

D. Real-Time Packet Classification

In order to address jamming attacks, jammer will use classify then jam strategy. For this jammer has to classify packet in the real time, before the packet transmission completed. After classifying packet, jammer may choose to jam it depending on his strategy.

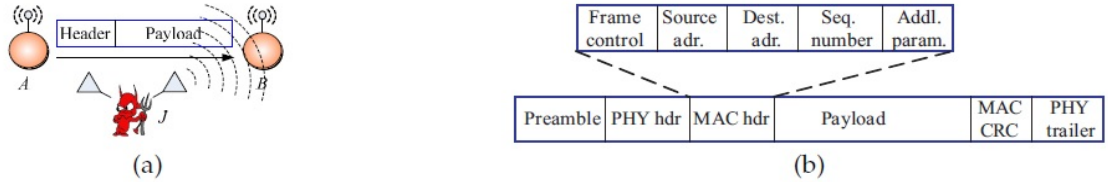

Fig. 1. (a) Realization of a selective jamming attack, (b) a generic frame format for a wireless network.

Consider the generic communication system as given in fig. 3. At PHY layer, a packet m is encoded, interleaved, modulated before it is transmitted over wireless channel. At receiver side, signal is demodulated, de-interleaved, decoded, to recover original packet m.

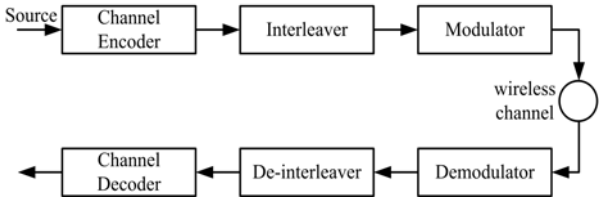

Figure 3.Real Time Packet Classification

The jammer's ability of classifying packet m depends on the implementation of blocks. In fig. 2 encoder is used to convert the original message into the bits. In this paper, 64-bit encoder is used for encoding. Channel encoder adds some redundant bits to protect packet m against channel errors. At next block, interleaving is performed to classify bits into the packets. Finally, the digital modulator maps received bit stream to length of symbol q, and modulates them into suitable waveforms for transmission over wireless channel. Typical modulation techniques include OFDM, 16(64)-QAM, BPSK, CCK.

E. Jamming Detection model

The network employs a mechanism for monitoring network status and detecting potential malicious activity. The monitoring mechanism consists of: 1) determination of subsets of nodes that acts as monitors and, 2) employment of detection algorithm at each node. The assignment of the role of monitor to node is affected by potential existing energy consumption and node computational complexity limitations, and by detecting performance specification. This paper fixes attention to a specific monitor node and the detection scheme that it employs. First, it needs to define the quantity to be observed at each monitor. In this case, the readily available metric is the 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, it consider a large enough training period in which the monitor node learns the percentage of collisions it experiences as the long-term limit of the ratio of number of slots where there was collision over total number of slots of the training period. Now let the network operate in the open after the training period has elapsed and fix attention to a time window much smaller than the training period. An increased percentage of collisions in the time window compared to the learned long-term ratio may be an indication of an ongoing jamming attack that causes additional collisions. However, it may happen as well that the network operates normally and there is just a temporary irregular increase in the percentage of collisions compared to the learned ratio for that specific interval. A detection algorithm is part of the detection module at a monitor node; it takes as input observation samples obtained by the monitor node (i.e., collision/not collision) and decides whether there is an attack or not. On one hand, the observation window should be small enough, such that the attack is detected in a timely manner 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 reduced.

The sequential nature of observations at consecutive time slots motivates the use of sequential detection techniques. A sequential decision rule consists of: 1) a stopping time, indicating when to stop taking observations, and 2) a final decision rule that decides between the two hypotheses (i.e., occurrence or not of jamming). A sequential decision rule is efficient if it can provide reliable decision as fast as possible.

The probability of false alarm PFA and probability of missed detection PM constitute inherent trade-offs in a detection scheme in the sense that a faster decision unavoidably leads to higher values of these probabilities while lower values are attained at the expense of detection delay. For given values of PFA and PM, the detection test that minimizes the average number of required observations (and thus average delay) to reach a decision among all sequential and non- sequential tests for which PFA and PM do not exceed the predefined values above is Wald's Sequential Probability Ratio Test (SPRT) . When SPRT is used for sequential testing between two hypotheses concerning two probability distributions, SPRT is optimal in that sense as well.

SPRT collects observations until significant evidence in favour of one of the two hypotheses is accumulated. After each observation at the kth stage, choose between the following options: accept one or the other hypothesis and stop observing, or defer decision for the moment and obtain another observation k + 1. In SPRT, there exist two thresholds a and b that aid the decision. The computed figure of merit at each step is the logarithm of the likelihood ratio of the accumulated sample vector until that step. In this case, the test is between hypotheses H0 and H1 that involve Bernoulli with probability mass functions (p.m.fs.) f0 and f1 defined by Pr(c=1) = .i=1 - Pr(C=0) where c = 1 denotes the event of collision in a slot. That is, H0 concerns the hypothesis about absence of jamming

with Bernoulli p.m.f. f0 with parameter .0, while H1 corresponds to the hypothesis of jamming with a Bernoulli p.m.f. f1 with parameter .1. Thus, the logarithm of likelihood ratio at stage k with accumulated samples x1,…..,xk is: where f1(x1,….xk) is the joint probability mass function of sequence (x1,….xk) based on hypothesis Hi, for I = 0,1. The decision is taken based on the following criteria:

Sk>a : accept H1,

Sk<b : accept H0,

b = Sk<a : take another observation.

The objective of the detection rule is to minimize the number of required observation samples to derive a decision about existence or not of jamming. The detection performance is quantified by the average sample number (ASN), needed until a decision is reached, where the expectation is with respect to the distribution of the observations.

VI. TECHNIQUES FOR PREVENTING JAMMING ATTACKS

For mitigating jamming attacks, many prevention techniques have been proposed. Typically, jammer introduces jamming by entering jamming messages in the wireless network. Transmission of jamming messages can be prevented by cryptanalysis and steganography techniques.

A. Steganography

InCryptography protects messages from being captured by unauthorized party, steganography techniques enable concealment of the fact that a message is being sent, and, if not detected make the sender and receiver invisible. Thus, steganography provides not only security, but also anonymity and security. All the information hiding methods that may be used to exchange steganogram in telecommunication network is described by term network steganography. Steganography can be seen as rising threat to network security. Network steganography utilizes communication protocol to control elements and their intrinsic functionality. Typical network steganography method uses modification of a single network protocol. The protocol modification may be applied to the PDU (Protocol Data Unit), time relations between exchanged PDUs, or both (hybrid methods). Moreover, usage of relation between two or more different network protocols to enable secret communication is possible. It is so called inter-protocol steganography.

Typically, steganography techniques make the use of digital data (audio, video, images) to hide secret message. But, this paper will implement algorithms to hide secret message (SM) in cover file (CF) which will be text file or doc file. This paper, introduced new data hiding method that hides bit patterns of SM in random locations of CF.

Algorithm for hiding SM in CF:

1. Start
2. Read host file name
3. Read secret message file name
4. Calculate NHOST= no. of blank spaces in host file
5. Calculate NSTAG= size of secret message file
6. Calculate n1= integer(NSTAG/32)
7. Calculate r1= NSTAG-n1*32
8. i) Set n= 2560 for .doc file ii) set n=0 for.txt file
9. Calculate size1=(n1+1)*256+32
10. If size1>NHOST then exit otherwise continue from step 11
11. Read 256 blank space positions from nth position of host file.
12. Update ‘n’ with the location right after last read blank space.
13. Read 32 bytes from secret messages.
14. Take 1 byte from 32 byte block and divide it into 8 bit pattern.
15. For each bit select a random blank space location
16. If SM bit is 1, then replace this randomly selected blank space with ASCII 32.
17. Repeat steps 14 to 16 for all 32 bytes of secret message block.
18. Repeat steps 11 to 17 for n1 times.
19. Repeat same process for remaining r1 bytes of secret message.
20. End.

B. Multi-Level Sreganography

MLS is based on combining two or more steganography methods in such a way that one method (upper-level) is a carrier for other method (lower-level). This form of information hiding gives some benefits

- Increased capability for hiding upper level.
- Increased steganographic bandwidth.
- Ability to verify integrity of steganogram after its reception.
- Limiting chance of extracting and reading steganogram.

C. Triple DES

Triple DES uses a key bundle which comprises 3 DES keys K1, K2, K3, each of which 56 bits excluding parity bits. Encryption algorithm is:

Cipher text = $E_{K3}(D_{K2}(E_{K1}(\text{plaintext})))$

In encryption process, plaintext is encrypted with K1, decrypted with K2 and again encrypted with K3. Decryption algorithm is:

Plain text = $D_{K1}(E_{K2}(D_{K3}(\text{cipher text})))$.

In decryption process, cipher text is decrypted with K3, encrypted with K2, and again decrypted with K1. Each triple DES encryption encrypts one block of 64 bits of data. In each case middle operation is reverse of first and last. There are 3 keying option which can improve strength of algorithm.

Keying option 1: All three keys are independent.

Keying option 2: keys K1 and K2 are independent and K3=K1

Keying option 3:All three keys are identical, i.e. K1=K2=K3.

Keying option 1 is strongest with 3*56=168 bits independent key bits. Keying option 2 provides less security, with $2 \times 56 = 112$ key bits. This option is stronger than simply DES encrypting twice, e.g. with K_1 and K_2,

because it protects against meet-in-the-middle attacks. Whereas, Keying option 3 is equivalent to DES, with only 56 key bits. This option provides backward compatibility with DES, because the first and second DES operations cancel out.

VII. HONEYPOTS FOR REDUCING EFFECTS OF JAMMING

Honeypots are basically a great security measure which is used to fool attacker present in network. While deploying in a network, honeypot acts as a most important part of the network and trying to gain attention of attackers. Honeypots trap the attackers in a way that attacker attacks on honeypot by thinking that it is the important part of network and at the same time honeypot collects all the information about attacker such as attacking strategy, purpose and techniques.In this section, an approach is provided which will use honeypots to provide an efficientsolution to jamming attacks which can be easily integrated into the existing network architecture while providing a mechanism for attack prevention. In the following sections, we explain in detail the proposed mechanism for handling jamming type Denial-of-service attacks in wireless infrastructure network.

A. Architecture for Implementing HONEYPOTS

Fig. 4 describes the architecture for implementing honeypots. The various network components are:

1. Base-station
2. Mobile nodes
3. Honeynodes (nodes where honeypots are deployed).

Honeynodes as secondary interfaces present on base-stations (primary being used for communication with mobile nodes) which guard the frequency of operation of the actual communicating nodes by sending out a fake signal on a nearby frequency to prevent the attack by deceiving the attacking entity to attack the honeynode. This gives enough time for the normal nodes to switch to a new frequency of operation.

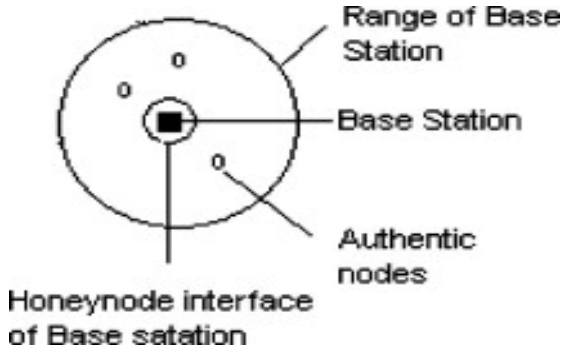

Figure 4 Network Architecture

B. Implementation Algorithms

This algorithm is expected to run all the nodes. When any of the nodes detects an attack, Itchanges its frequency of operation. However, if the honeynode detects an attack, it continues to send signals on that channel and at the same time informs the base-station of the impending attack (there are two interfaces of the same node, which facilitates communication between them). The base-station, in turn, issues a frequency change command to all its associated nodes, telling them to switch to a frequency decided as per the dynamic channel selection algorithm. Later on, the honeynode switches its frequency.

Algorithm:

1 If (Attack detected= true) then
2 If (Node is a honeynode) then
3 Inform base station of attack
4 Continue communications to deceive jammer
5 End.
6 Change frequency of operation
7 else
8 If (node is a base station) then
9 If (honeynode has informed of attack) then
10 select frequency to jump using dynamic selection
11 Inform associated node to switch to this frequency
12 Change frequency of operation
13 Else
14 Find the node that did not respond
15 If (any node did not respond) then
16 Broadcast frequency change command
17 Change frequency of operation
18 End

VIII. CONCLUSION

In this paper, we studied the jamming attacks in wireless networks. We also studied system models to introduce jamming attacks. And attack detection model is also presented. Then we discussed real-time packet classification to classify the packet before reaching at destination. After that, prevention techniques for mitigating jamming attacks by using cryptanalysis and steganography have been discussed. To reduce the effect of jamming honeypot techniques has been used and algorithm is used to fool jammer and decrease jamming rate.

REFERENCES

[1] B. Awerbuch, A. Richa and C. Sheideler, " A Jamming Resistance MAC Protocol for Single-Hop Wireless Networks," In proceedings of Principles of Distributed Computing, 2008.

[2] 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.

[3] W. Xu, W. Trappe, Y. Zhang. The Feasibility of Launching and Detecting jamming attacks in Wireless Networks. In proceedings of MobiHoc, 2005.

[4] Y. Desmedt. Broadcast anti-jamming systems. Computer Networks, Feb. 2001.

[5] G. Thamilarasu, S. Mishra and R. Sridhar. " Improving reliability of Jamming Attack Detection in Ad-hoc Networks," In proceedings of IJCNIS, April 2011.

[6] G. Noubir and G. Lin. " Low-Power Dos attacks in data wireless LANs and Countermeasures. SIGMOBILE mobile computing and communications, 2003.

[7] R. Ibrahim and Teoh Suk Kuan. "Steganography Algorithm to hide secret message inside an Image". Computer application and technology, February 2011.

[8] Dr. AtefJawad AL-Najjar." The decoy: Multi-level Digital multimedia steganography model." 12th WEASE international conference on communications, July 2008.

[9] M. Strasser, C. Popper, S. Capkun. "Efficient uncoordinated fhss anti-jamming communication." In Proceedingd of Mobihoc, 2009.

[10] E. Bayraktaroglu, C. King, X. Liu, G. Noubir, R. Rajaraman and B. Thapa. "On the performance of IEEE 802.11 under jamming". In proceedings of IEEE INFOCOM, pages ,april 2008.