ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

Jamming Attacks Prevention in Wireless Sensor Networks Using Secure Packet Hiding Method

G. Jayanthi Lakshmi [1], S. Babu [2], B Lakshmana Rao[3], P Mohan[4], B Sunil Kumar[5]

M.Tech Student, Dept. of CSE, AVS CET, Nellore, India [1]

Assoc prof, Dept. of CSE, AVSCET,Nellore, India[2]

Asst.Professor, Dept. of CSE, NBKRIST, Nellore, India[3]

Asst.Professor, Dept. of CSE, NEC, Gudur, India[4]

Asst.Professor, Dept. of CSE, NEC, Gudur, India[5]

Abstract: The Wireless Networks are exposed to serious security threat called jamming. This intentional interference with wireless transmissions can be used as a launch pad for mounting Denial-of-Service attacks on wireless networks This paper considers the problem of jamming under an internal threat model, where the attacker who is aware of all the network secrets and the details of implementation which results in the difficulty of detection. Jamming is broken down in to layers and this paper focuses on jamming at the Transport/Network layer. To overcome these attacks, we develop three schemes that prevent the attacker from attacking the packets. Then we analyse the security of our schemes.

Keywords: Selective Jamming, Denial-of-Service, Wireless Sensor Network's, Packet Classification.

I. INTRODUCTION

Wireless technologies have become increasingly popular in our everyday business and personal lives. It enables one or more devices to communicate without physical connections-without requiring network or peripheral cabling. As we know that wireless networks serve as the transport mechanism between devices and among devices. However, because of this wireless nature these are prone to multiple security threats in which one of the major serious security threat is jamming. Jamming can disrupt wireless transmission and can occur either unintentionally in the form of noise or interference at the receiver side. Jamming attacks may be viewed as a special case of Denial of service (DOS) attacks [1]. In simplest form of jamming, the attacker interferes with the set of frequency bands used for communication by transmitting a continuous jamming signal [2] or several short jamming pulses [3].

Normally Jamming attacks have been considered under an external threat model, but here we are considering jamming attacks under an internal threat model. Under an external threat model, jamming strategies transmits high power interference signals continuously or randomly [2] [4]. This type of strategies has several disadvantages. First, the attacker has to spend huge amount of energy in order to jam certain frequency bands. Second, these types of attacks are easy to detect because of continuous presence of unusually high interference levels. [3], [4], [6].

A well-known countermeasure against this type of jamming attacks are spread spectrum techniques such jamming is referred as jamming gain. In targeted jamming, it may jam particular nodes, flows or links. As frequency hopping, direct sequence spread spectrum and chirp spread spectrum [5]. With respect to these entire techniques one thing that is common is that they rely on secret codes that are user between the communicating parties.

In this paper, we deal with the problem of jamming under an internal threat model. Here the attacker who is aware of network secrets and the implementation details of all the layers of network protocols in the network stack. The attacker uses his internal knowledge for launching selective jamming attacks in which high importance messages are targeted. For example, a jammer can target TCP acknowledgments in a TCP session or target route request/reply messages at the routing layer.

II. TYPES OF JAMMER

Continuous blocking has been used as a denial-of-service (DoS) attack against voice communication since the 1940s.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

Recently, several alternative jamming strategies have been Categorized jammers into four models, (a) a constant jammer that continuously emits noise, (b) a deceptive jammer that continuously broadcasts fabricated messages or replays old ones, (c) a random jammer that alternates between periods of continuous jamming and inactivity, and (d) a reactive jammer who jams only when transmission activity is detected.

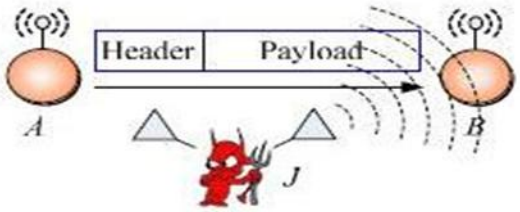

Fig1:Realization of a selective jamming attack

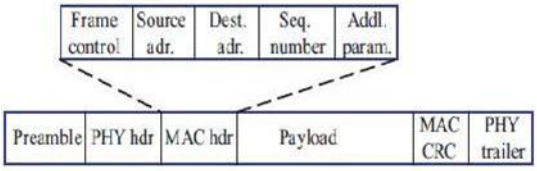

Fig 2: A generic frame format for a wireless network

A. Constant jammer

The constant jammer continually emits a radio signal. It has implemented a constant jammer using two types of devices. The first type of device to use is a waveform generator which continuously sends a radio signal. The second type of device it used is a normal wireless device. In this author, it will focus on the second type, which it built on the MICA2 Mote platform. This constant jammer continuously sends out random bits to the channel without following any MAC-layer etiquette. Specifically, the constant jammer does not wait for the channel to become idle before transmitting. If the underlying MAC protocol determines whether a channel is idle or not by comparing the signal strength measurement with a fixed threshold, which is usually lower than the signal strength generated by the constant jammer, a constant jammer can effectively prevent legitimate sources from getting hold of channel and sending packets

B. Deceptive jammer

Instead of sending out random bits, the deceptive jammer constantly injects regular packets to the channel without any gap between subsequent packet transmissions. As a result, a normal communicator will be received into believing there is a legitimate packet and will be duped to remain in the receive state. For example, in Tiny OS, if a preamble is detected, a node remains in the receive mode, regardless of whether that node has a packet to send or not. Hence, even if a node has packets to send, it cannot switch to the send state because a constant stream of incoming packets will be detected. Further, it also observe that it is adequate for the jammer to only send a continuous stream of preamble bits (0xAA in Tiny OS) rather than entire packets.

C. Random jammer

Instead of sending out a radio signal continuously, a random jammer alternates between sleeping and jamming. Specifically, after jamming for tj units of time, it turns on its radio, and enters a sleeping mode. It will resume jamming after sleeping for ts time. tj and ts can be either random or fixed values. During its jamming phase, it can either behave like a constant jammer or a deceptive jammer. Throughout this art hour, this random jammer will operate as a constant jammer during jamming. The distinction between this model and the previous two models lies in the fact that this model tries to take energy conservation into consideration, which is especially important for those jammers that do not have unlimited power supply. By adjusting the distribution governing the values of tj and ts, it can achieve various levels of tradeoff between energy efficiency and jamming effectiveness.

D. Reactive jammer

The three models discussed above are active jammers in the sense that they try to block the channel irrespective of the traffic pattern on the channel. Active jammers are usually effective because they keep the channel busy all the time. These methods are relatively easy to detect. An alternative approach to jamming wireless communication is to employ a reactive strategy. For the reactive jammer, it takes the view point that it is not necessary to jam the channel when nobody is communicating. Instead, the jammer stays quiet when the channel is idle, but starts transmitting a radio signal as soon as it senses activity on the channel. As a result, a reactive jammer targets the reception of a message. It would like to point out that a reactive jammer does not necessarily conserve energy because the jammer's radio must continuously be on in order to sense the channel. The primary advantage for a reactive jammer, however, is that it may be harder to detect.

III PROBLEM STATEMENT AND ASSUMPTIONS

A. *Problem Statement*

Consider the scenario depicted in Nodes A and B communicate via a wireless link. Within the communication range of both A and B, there is a jamming node J. When A transmits a packet m to B, node J classifies m by receiving only the first few bytes of m. J then corrupts m beyond recovery by interfering with its reception at B. We address the problem of preventing the jamming node from

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

classifying m in real time, thus mitigating J's ability to perform selective jamming. Our goal is to transform a selective jammer to a random one. Note that in the present work, we do not address packet classification methods based on protocol semantics, as describe.

B. System and Adversary Model

Network model- The network consists of a collection of nodes connected via wireless links. Nodes may communicate directly if they are within communication range, or indirectly via multiple hops. Nodes communicate both in unicast mode and broadcast mode. Communications can be either unencrypted or encrypted. For encrypted broadcast communications, symmetric keys are shared among all intended receivers. These keys are established using pre-shared pairwise keys or asymmetric cryptography.

Communication Model– Packets are transmitted at a rate of **R** bauds. Each PHY-layer symbol corresponds to q bits, where the value of q is defined by the underlying digital modulation scheme. Every symbol carries $^{\alpha}_{\beta}$ q data bits, where α/β is the rate of the PHY-layer encoder. Here, the transmission bit rate is equal to q**R** bps and the information bit rate is $^{\alpha}_{\beta}$ q**R** bps. Spread spectrum techniques such as frequency hopping spread spectrum (FHSS), or direct sequence spread spectrum (DSSS) may be used at the PHY layer to protect wireless transmissions from jamming. SS provides immunity to interference to some extent (typically 20 to 30 dB gain), but a powerful jammer is still capable of jamming data packets of his choosing.

Transmitted packets have the generic format depicted in Fig. 2. The preamble is used for synchronizing the sampling process at the receiver. The PHY layer header contains information regarding the length of the frame, and the transmission rate. The MAC header determines the MAC protocol version, the source and destination ad-dresses, sequence numbers plus some additional fields. The MAC header is followed by the frame body that typically contains an ARP packet or an IP datagram. Finally, the MAC frame is protected by a cyclic redundancy check (CRC) code. At the PHY layer, a trailer may be appended for synchronizing the sender and receiver.

Adversary Model– We assumes the adversary is in control of the communication medium and can jam messages at any part of the network of his choosing (similar to the Dolev-Yao model). The adversary can operate in full-duplex mode, thus being able to receive and transmit simultaneously. This can be achieved, for example, with the use of multi-radio transceivers. In addition, the adversary is equipped with directional antennas that enable the reception of a signal from one node and jamming of the same signal at another. For analysis purposes, we assume that the adversary can pro-actively jam a number of bits just below the ECC capability early in the transmission. He can then decide to irrecoverably corrupt a transmitted packet by jamming the *last symbol*. In reality, it has been demonstrated that selective jamming can be achieved with far less resources [8]. A jammer equipped with a single half-duplex transceiver is sufficient to classify and jam transmitted packets. However, our model captures a more potent adversary that can be effective even at high transmission speeds.

The adversary is assumed to be computationally and storage bounded, although he can be far superior to normal nodes. In particular, he can be equipped with special purpose hardware for performing cryptanalysis or any other required computation. Solving well-known hard crypto-graphic problems is assumed to be time-consuming. For the purposes of analysis, given a cipher text, the most efficient method for deriving the corresponding plaintext is assumed to be an exhaustive search on the key space.

The implementation details of every layer of the network stack are assumed to be public. Furthermore, the adversary is capable of physically compromising network devices and recovering stored information including cryptographic keys, PN codes, etc. This internal adversary model is realistic for network architectures such as mobile ad-hoc, mesh, cognitive radio, and wireless sensor networks, where network devices may operate unattended, thus being susceptible to physical compromise

IV RELATED WORK

Here the contribution towards jamming attacks is reduced by using the two algorithms 1) Symmetric encryption algorithm 2) Brute force attacks against block encryption algorithms the proposed algorithm keeps these two in mind as they are essential in reducing the jamming attacks by using the packet hiding mechanism. In this paper, we address the problem of jamming under an internal threat model. We consider a sophisticated adversary who is aware of network secrets and the implementation details of network protocols at any layer in the network stack. The adversary exploits his internal knowledge for launching selective jamming attacks in which specific messages of "high importance" are targeted. For example, a jammer can target route-request/route-reply messages at the routing layer to prevent route discovery, or target TCP acknowledgments in a TCP session to severely degrade the throughput of an end-to-end flow to launch selective jamming attacks, the adversary must be capable of implementing a classify-then-jam strategy before the completion of a wireless transmission. Such strategy can be actualized either by classifying transmitted

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

packets using protocol semantics, or by decoding Packets on the fly. In the latter method, the jammer may decode the first few bits of a packet for recovering useful packet identifiers such as packet type, source and destination address. After classification, the adversary must induce a sufficient number of bit errors so that the packet cannot be recovered at the receiver. Selective jamming requires an intimate knowledge of the physical layer, as well as of the specifics of upper layers

A. Network model

The network consists of a collection of nodes connected via wireless links. Nodes may communicate directly if they are within communication range, or indirectly via multiple hops. Nodes communicate both in unicast mode and broadcast mode. Communications can be either unencrypted or encrypted. For encrypted broadcast communications, symmetric keys are shared among all intended receivers. These keys are established using presaged pair wise keys or asymmetric cryptography.

B. Real Time Packet Classification

Consider the generic communication system depicted in Fig. At the PHY layer, a packet m is encoded, interleaved, and modulated before it is transmitted over the wireless channel. At the receiver, the signal is demodulated, DE interleaved, and decoded, to recover the original packet m. Moreover, even if the encryption key of a hiding scheme were to remain secret, the static portions of a transmitted packet could potentially lead to packet classification. This is because for computationally-efficient encryption methods such as block encryption, the encryption of a prefix plaintext with the same key yields a static cipher text prefix. Hence, an adversary who is aware of the underlying protocol specifics (structure of the frame) can use the static cipher text portions of a transmitted packet to classify it.

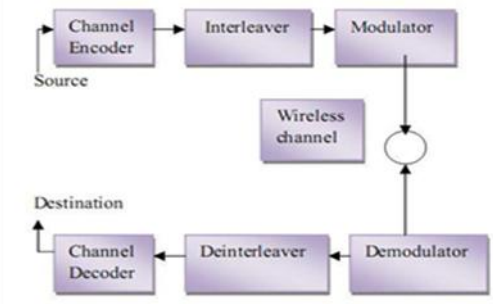

Figure 3: System architecture for packet hiding methods

We propose a strong hiding commitment scheme (SHCS), which is based on symmetric cryptography. Our main motivation is to satisfy the strong hiding property while keeping the computation and communication overhead to a minimum

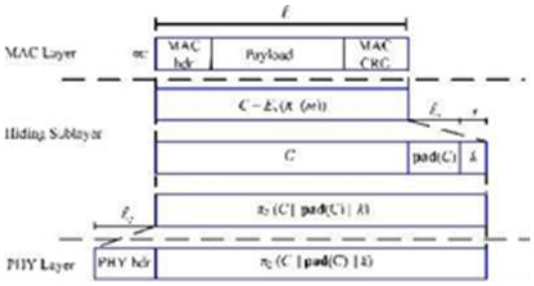

Fig4: processing at hiding sub layer

The computation overhead of SHCS is one symmetric encryption at the sender and one symmetric decryption at the receiver. Because the header information is permuted as a trailer and encrypted, all receivers in the vicinity of a sender must receive the entire packet and decrypt it, before the packet type and destination can be determined. However, in wireless protocols such as 802.11, the complete packet is received at the MAC layer
before it is decided if the packet must be discarded or be further processed. If some parts of the MAC header are deemed not to be useful information to the jammer, they can remain unencrypted in the header of the packet, thus avoiding the decryption operation at the receiver

Cryptographic Puzzle Hiding Scheme

We present a packet hiding scheme based on cryptographic puzzles. The main idea behind such puzzles is to force the recipient of a puzzle execute a pre-defined set of computations before he is able to extract a secret of interest. The time required for obtaining the solution of a puzzle depends on its hardness and the computational ability of the solver. The advantage of the puzzle based scheme is that its security does not rely on the PHY layer parameters. However, it has higher computation and communication overhead we consider several puzzle schemes as the basis for CPHS.

Hiding based on All-Or-Nothing Transformation

The packets are pre-processed by an AONT before transmission but remain unencrypted. The jammer cannot perform packet classification until all pseudo-messages corresponding to the original packet have been received and the inverse transformation has been applied. Packet m is partitioned to a set of x input blocks m = {m1, m2, m3….}, which serve as an input to an The set of pseudo-messages m

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 9, September 2013

= {m1, m2, m3,…..} is transmitted over the wireless medium Recently Rivets motivated by different security concerns arising in the context of block ciphers, introduced an intriguing primitive called the *All-Or-Nothing Transform (***AONT***)*. An AONT is an efficiently computable transformation Ton strings such that For any string x, given *all* of T(x), one can efficiently recover x There exists some threshold such that any polynomial time adversely that learns all but bits of T(x) obtains no information about X.

The AONT solves the problem of partial key exposure: Rather than storing a secret key directly, we store the AONT applied to the secret key. If we can build an AONT where the threshold value `is very small compared to the size of the output of the AONT, we obtain security against almost total exposure. Notice that this methodology applies to secret keys with arbitrary structure, and thus protects all kinds of cryptographic systems. One can also consider AONT's that have a two-part output: a public output that doesn't need to be protected, and a secret output that has the exposure-resilience property stated above. Such a notion would also provide the kind of protection we seek to achieve. The AONT has many other applications, as well, such as enhancing the security of block- ciphers and making fixed-block size encryption schemes more efficient [6] For an excellent exposition on these and other applications of the AONT

V. CONCLUSION

In this paper we addressed the problem of selective jamming attacks under an internal threat model, where the attacker is a part of the network, who is aware of network secrets and also the implementation details. In order to overcome these kinds of attacks we develop three schemes that combine cryptographic primitives such as strong hiding commitment scheme, cryptographic puzzle hiding scheme and all or nothing transformations. We analyze the security of above mentioned schemes and through simulation we can achieve the higher throughput by analyzing the comparative study of these schemes.

1

REFERENCES

[1] A.D. Wood and J.A.Stankovic, "Denial of Service in Sensor networks",computer, vol.35, no.10, pp. 54-62,2002
[2] M.K.Simon, J.K.Omura, R.A.Scholtz, and B.K.Levitt, "Spread Spectrum Communications Handbook," McGraw-Hill, 2001
[3] G.Noubir, and G.Lin,"Low Power DOS Attacks in Data Wireless LANs and Countermeasures," in proc.ACM MobiHoc, 2003
[4] W.Xu, W.Trappe,Y.zhang and T.wood. The feasibility of launching and detecting jamming attacks in wireless networks. In proceedings of MobiHoc,pages 46-57, 2005
[5] R.A.Poisel.Modern Communications Jamming principles and techniques. Artech House Publishers,2006
[6] R.C Merkle, secure communications over insecure channels. Communications of the ACM,21(4):2994-299,1978.
[7] M.Wilhelm, I.Martinovic, J.Schmitt and V.Lenders. Reactive jamming in wireless networks: How realistic is the threat? In proceedings of WiSec,2011.
[8] D.Stinson. Cryptography:theory and practice.CRC press,2006
[9] Ravneet Kaur and Amandeep Kaur. Digital Signature, in International Conference on Computing Sciences, 2011