Countermeasures Against Internal Jammer in Wireless Broadcast Networks

P.VENKATESWARAN
Department of Computer Science &Engineering
Pavendar Bharathidasan College of Enginnering & Tech.
Tiruchirappalli, India.
Email: venki2015@gmail.com

D.SARAVANAN, Associate Professor
Department of Computer Science &Engineering
Pavendar Bharathidasan College of Enginnering & Tech.
Tiruchirappalli, India.
Email: dsarav23@gmail.com

***Abstract*:**

A wireless network is highly sensitive to Denial of Service (DoS) attacks. The wireless network is affected by the numerous security threats such as jamming. Jamming attacks interrupts the normal operations in the wireless networks. Due to the open nature of the wireless medium the jamming leads to the Denial of Service attacks. Jamming is an external threat model and it can be done by transmitting the continuous interference signal to interrupt the packet transmission. The anti-jamming techniques such as spread-spectrum communications and the other jamming evasion techniques provide the bit level protection and it can be known only to the communicating nodes. But, it only protects wireless under an external threat model. An adversary with internal knowledge of network topology and the protocol specification can make the selective jamming attacks with low effort. The inside adversary targets the highly important message by using its internal knowledge of the network secrets and it degrades the network performance. The adversary uses the packet classification method and targets the first few bits of packet so that it can not be easily recovered by the receiver. To mitigate these selective jamming three methods has been proposed to reduce the impact of the inside adversaries. The cryptographic primitives can be combined with the physical layer attributes to prevent the packet classification.

Keywords— Selective jamming, denial-of-service, real time packet classification, data selective jamming, channel selective jamming.

1. INTRODUCTION

The wireless networks are susceptible to numerous security threats due to the open nature of the wireless medium. Any node with a transceiver can block the ongoing transmission. One of the easiest ways for degrading the perfomance of the network is by jamming wireless transmissions. Jamming can be considered as an external threat model in which jammer is a not a part of the network. Jamming strategies are either in continuous transmission or in a random transmission.

In the simplest form of jamming,[5] the adversary corrupts transmitted packets by causing electromagnetic interference in the network's operational frequencies and in proxmity to the targeted receivers. Due to the open nature of the wireless medium jamming leads to the Denial-of-Service attacks. The jamming attack degrades the performance of the network.

These attacks can be reduced by the spectrum spectrum communications, spatial retreats [6] or localization and removal of the jamming nodes. A spread specturm techniques provide bit level protection by spreading the bits according to the secret pseudo noise code, which is known only to the communicating parties. These methods can only protect wireless transmissions under an external threat model.

Broadcast communications are particularly vulnerable under an internal threat model because all intended receivers must be aware of the secrets used to protect transmissions. The compromise of a single receiver is sufficient to know the relevant information about the cryptographic secrets.

An adversary with internal knowledge of network topology and the protocol specification can make the selective jamming attacks [1] with low effort. The selective jamming can be categorized into two types. The first type is channel selective jamming and another type is data selective jamming. In this model jamming can be considered as an internal threat model. The inside adversary targets the highly important message by using its internal knowledge of the network secrets and it degrades the network performance. Compare to continuous jamming, the adversary is active for a short period of time and jam the packet with less energy.

To implement the selective jamming [8] the adversary must be capable of implementing a "classify-then-jam" strategy before the completion of the packet transmission. The jammer may decode the first few bits of a packet for recovering the useful packet identifier such as packet type, source and destination address. After classification has been occurred the adversary may induce a sufficient number of bit errors so that the packet can not be recovered at the receiver and it reduces the performance of the network. The selective jamming requires a detailed knowledge of the physical layer and some of the information in the upper layers.

In the channel selective jamming, some channels are reserved for broadcasting control information. These channels are referred to as control channels, and it facilitate the operations such as networks discovery, time synchronization, coordination of shared medium access, routing path discovery.

An adversary who selectively targets the control channels can efficiently launch a DoS attack with a limited amount of resources. To launch a channel selective jamming, the adversary must be aware of the location of the targeted channel, whether defined by a separate frequency band, time slot, or PN code. An adversary [10] who exploits the knowledge of protocol mechanics along with cryptographic quantities extracted from compromised nodes to maximize the impact of the attack on the higher layer functions.

The rest of the paper is organized as follows. A related work are included in Section 2. The various types of selective jamming attacks and counter measures against such attacks are given under Section 3. The conclusion of the paper is illustrated in Section 4.

2. RELATED WORK

Continous jamming has been used as a denial-of-service attack against voice communication. Several alternative jamming strategies have been demonstrated. Xu et. al. 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 interactivity, and (d) a reactive jammer who jams only when transmission activity is targeted.

Intelligent attacks which target the transmission of specific packetes. Thuente considered an attacker who infers eminent packet transmission based on timing information at the MAC layer. Law et. al. considered selective jamming attacks in muti-hop wireless networks, where future transmission at one hop were inferred from prior transmission in other hops. However, the real time packet classification was considered beyond the capabilities of the adversary. Selectivity was achieved via interference from the control messages already transmitted.

Channel-selective jamming attacks were also considered in intelligent jamming. It was shown that targeting the control channel reduces the required power for performing a DOS attack by several orders of magnitude. To protect control channel traffic, control information was replicated in multiple channels. The "locations" of the channels where control traffic was broadcasted at any given time, was cryptographically protected.

The compromise of any node reveals the control-channel hopping sequence to the adversary. The problem of control channel jamming in the presence of the node compromise was previously addressed in the context of GSM networks. In such networks , multiple control channels are implemented over specified frquency bands and time slots. The randomized frequency hopping approach is presented to protect the control channel inside jammers.

3. PROPOSED SYSTEM

The open nature of the wireless medium leaves it vulnerable to jamming attacks [9]. Jamming in wireless networks has been primarily analyzed under an external adversarial model, as a severe form of denial of service (DoS) against the PHY layer. In the selective jamming, once the node is compromised the inside jammer launches internal attacks. The adversary can operate in full duplex mode, thus being able to receive and transmit concurrently. The selective jamming has been categorized as data selective jamming and channel selective jamming.

3.1 Data Selective Jamming

In the data selective jamming, an inside adversary can exercise a greater degree of selectivity by targeting specific packets of high importance. One way of launching a data-selective jamming attack, is by classifying packets before the transmission is completed. The data-selective jamming uses real time packet classification method in order to jam the packet.

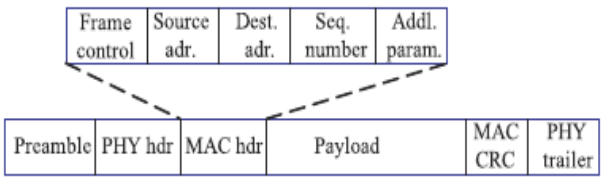

Fig. 1. A generic format for a wireless networks.

Transmitted packets [3] have the generic frame format depicted in Fig. 1. The preamble is used for synchronizing the sampling process at the receiver. The PHY header contains information regarding the length of the frame and the transmission rate. The MAC header contains information relevant to the MAC layer. The MAC header determines the MAC protocol version, the type of packet (managment, control, or data) and its subtype, the source and destination addresses plus some additional fields regarding power management, security parameters, and information for future transmissions. The MAC header is followed by the frame body that contains higher layer functions. Finally, the MAC frame is protected by a CRC code attached in the CRC field.

3.1.1 Problem Statement

Consider the scenario depicted in Fig. 2. 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. The problem of preventing the jamming node from classifying m in real time, thus mitigating J's ability to perform selective jamming is addressed. Our goal is to transform a selective jammer to a random one.

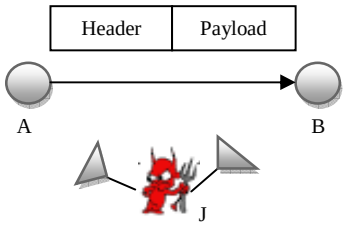

Fig. 2. Realization of a selective jamming attack

3.1.2 Real Time Packet Classification

The inside jammer [3] can classify the packet in real time, before the packet tranmission is completed. Once the packet is classified, the adversary may choose to jam it depends on the strategy. The generic communication system is depicted in Fig. 3. 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, deinterleaved, and decoded to recover the original packet *m*.

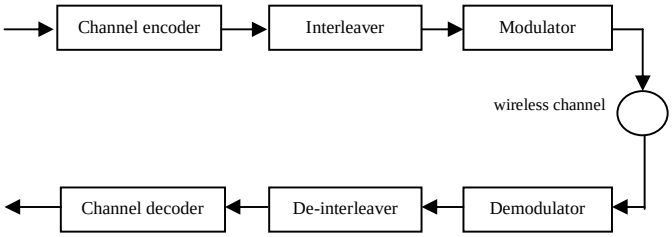

Fig. 3. A generic communication system diagram

As an example, the 802.11 standard uses a convolutional encoder of various rates to achieve different transmission speeds, with interleaving occurring per OFDM symbol. At the lowest rate of 6 Mbps, data is passed by a ½ rate encoder before it is mapped to OFDM symbol of 48 bits. In this case, decoding of one OFDM symbol provides 24 bits of data.At the highest data rate of 54 Mbps, 216 bits of data are recovered per OFDM symbol.

Using the first few symbols, the adversary can obtain the header information for the transmitted packet and classify it accordingly. As an example, a MAC layer packet in the 802.11 standard can have a size up to l = 2344 bytes with a header of 30 bytes. At a rate of 6 Mbps, 98 OFDM symbols are needed to complete the transmission of the entire packet (24bits per symbol), while the header is contained in only 10 symbols. The adversary has the opportunity to corrupt the remaining symbols to successfully jam a transmitted packet.

3.1.3 Countering Data-Selective Jamming Attacks

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. While a shared key suffices to protect point-point communications, for broadcast packets, this key must be shared by all intended receivers. Thus, this key is also known to an inside jammer. In symmetric encryption schemes based on block encryption, reception of one ciphertext 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.

To prevent classification, a packet must remain hidden until it is transmitted in its entirety. There are three techniques proposed for countering data-selective jamming. The goal is to transform a selective jammer to a random one. This can be achieved by overwhelming the adversary's computational ability to perform real time packet classification. The three techniques are.

A. Strong Hiding Commitment Scheme

A strong hiding commitment scheme [3] is based on the symmetric cryptography. The goal of this method is to satisfy the strong hiding property and keeping the computation and communication overhead to minimum. This scheme is used to transform the selective jammer into the random one by preventing the real time packet classification and improve the performance of the network. Commitment schemes are cryptographic primitives that allow an entity A, to commit to a value m, to an entity V while keeping m hidden.

A commitment scheme is a two-phase interactive protocol can be defined as a triple. Set X= {A, V} denotes two probabilistic polynomial-time interactive parties, here A is known as the committer and V as the verifier; set M denotes the message space.

During commitment stage t1, A uses a commitment function f1 = commit ( ) to generate a pair (C, d) = commit (m) where (C, d) is called the commitment/decommitment pair. At the end of stage t1, A releases the commitment C to V. In the stage t2, A releases the opening value d. The committer is assumed by the transmitting node S. The role of the verifier is assumed by any receiver R, including the jammer J. After the reception of d value, V opens the commitment C, by applying the function f2 = open (), thus obtaining a value of m1 = open (C, d). This stage culminates in either acceptance (m1= m) or rejection (m1 ≠ m). The commitment schemes have to satisfy the following two constraints.

Hiding: For every polynomial-time party V interacting with A, there is no polinomially efficient algorithm that would allow V to associate C with m and C1 with m1, without access to the de-commitment values d or d1, respectively and with non-negligible probability.

Binding: For every polynomial-time party A interacting with A, there is no polynomially efficient algorithm that would allow A to generate a triple (C, d, d1), such that V accepts the commitments (C, d) and (C, d1), with non negligible property.

B. Cryptographic Puzzle Hiding Commitment Scheme

Cryptographic puzzles [2] involve the creation of problems that are solvable within a finite time interval tp which depends on the hardness of the puzzle and the computatioanl ability of the solver. The real time packet classification is controlled by cryptographic puzzle hiding scheme. The idea behind such puzzles is to force the recipient of a puzzle execute a predefined set of computations before the adversary is able to extract the 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. The cryptographic puzzles have been used to hide the transmitted packets temporally. A packet m is encrypted with randomly selected symmetric key k of a desirable length s. The key k is blinded using a cryptographic puzzle and sent to the receiver. It can be described in the following way.

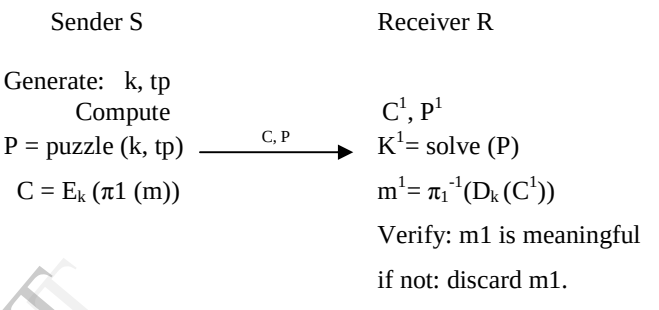

Fig. 4. Cryptographic puzzle hiding commitment scheme

In the cryptographic puzzle based hiding scheme the key k is blinded and sent to the receiver. The computationally bounded adversary can not solve the puzzle carrying k before the transmission of the encrypted version of m is completed and the puzzle is received. The adversary can not classify m for the purpose of selective jamming.

C. All-Or-Nothing Transformation

The All-or-Nothing Transformation introduces a modest communication and computation overhead. An AONT serves as a publicly known and completely invertible preprocessing step to a plaintext before it is passed to an ordinary block encryption algorithm. In this the packets are preprocessed by an AONT [7] before transmission but it remains unencrypted.

The jammer cannot perform packet classification until all psedudomessages corresponding to the original packet have been received and the inverse transformations have been applied. The All-or-Nothing transformation is described as follows.

Transform:

$m^1 = f(m \| pad(m))$ —m1→ Receive m1

Compute

$m \| pad(m) = f^{-1}(m^1)$

recover m

Fig. 5. All-Or-Nothing transformations

A transformation f, mapping message m = {m1,…,mx}, to a sequence of pseudomessages m1 = {m1,...,m1x1} is an AONT if f is a bijection, it is computationally infeasible to obtain any part of the original plaintext, if one of the pseudomessgaes is unknown. At the receiver, the inverse transformation f-1 is applied after all x1 pseudomessages are received, in order to recover m.

When a plaintext is preprocessed by an AONT before encryption, all ciphertext blocks must be received to obtain any part of the plaintext. So the brute force attacks are slowed down by a factor equal to the number of ciphertext blocks, without any change on the size of the secret key.

3.2 Channel Selective Jamming

The increased capacity of multi-channel networks can be translated into actual throughput only if critical network functions such as channel allocation and routing are efficiently coordinated. These functions are collaboratively coordinated by exchanging messages on a broadcast channel known as control channel.In a wireless network, one or more channels are reserved for broadcasting control information. These channels, referred to as control channels, facilitate operations such as network discovery, time synchronization, coordination of shared medium access, routing path discovery and others, without interfering with the communications.

An adversary who selectively targets the control channels can efficiently launch a DoS[8] attack with a fairly limited amount of resources (control traffic is low-rate compared to data traffic) due to the availability of multiple data channels. Tradionally, jamming attacks have been analyzed and addressed as a degradation in performance at the physical layer. To launch a channelselective jamming attack [4], the adversary must be aware of the location of the targeted channel, whether defined by a separate frequency band, time slot, or PN code. The control channels are inherently broadcast and hence, every intended receiver must be aware of the secrets used to protect the transmission of control packets. The compromise of a single receiver, reveals those secrets to the adversary.

Example: The impact of channel selective jamming on CSMA/CA-based medium access control (MAC) protocols for multi-channel WMNs [3]. A multi-channel MAC (MMAC) protocol is employed to coordinate access of multiple nodes residing in the same collision domain to the common set of channels. A class of MMAC protocols proposed for ad hoc networks such as WMNs follows a split-phase design. In this design, time is split into alternating control and data transmission phases. During the control phase, every node converges to a default channel to negotiate the channel assignment. In the data transmission phase, devices switch to the agreed on channels to perform data transmissions. The alternating phases of a split-phase MMAC are shown in Fig. 6.

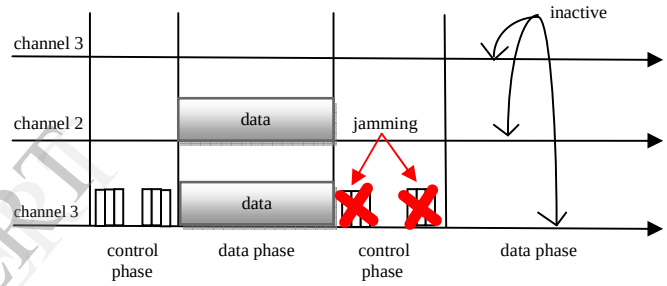

Fig. 6. Channel-selective jamming of the default channel during the control phase prevents the use of all channels during the data transmission phase.

By employing a channel-selective strategy, an inside adversary can jam only the default channel and only during the control phase. Any node that is unable to access the default channel during the control phase must defer the channel negotiation process to the next control phase, thus remaining inactive during the following data transmission phase. This attack is illustrated in Fig. 6. However, a sophisticated adversary can intelligently utilize jamming to attack higher layer functionalities and deny network availability at a very small energy. The control channel is used as a frequency band used to broadcast messages for coordinating network functions. The impact of this channel-selective jamming attack propagates to all frequency bands at a low energy overhead, since only a single channel is targeted and only for a fraction of time.

3.2.1 Countering Channel-Selective Jamming Attacks

Several anti-jamming methods have been proposed to address channel-selective attacks from insider nodes. To mitigate the impact of the channel selective jamming attacks, a randomized distributed channel establishment scheme is introduced. This scheme allows nodes to establish a new control channel using frequency hopping. Under this scheme, network nodes are able to temporaily construct a control channel until the jammer is from the network.

A. Randomized Distributed Scheme

A method for neutralizing channel-selective attacks is to dynamically vary the location of the broadcast channel, based on the physical location of the communicating nodes.The main motivation for this architecture [4] is that any broadcast is inherently confined to the communication range of the broadcaster. Hence, for broadcasts intended for receivers in different collision domains, there is no particular advantage in using the same broadcast channel, other than the design simplicity. The assignment of different broadcast channels to different network regions leads to an inherent partitioning of the network into clusters. Information regarding the location of the control channel in one cluster cannot be exploited at another. Moreover, broadcast communication can be repaired locally should a jammer appear, without the need for re-establishing a global broadcast channel.

To protect the control channel within each cluster, following cluster formation, one mesh node is elected as the clusterhead (CH). The CH assigns its cluster members unique PN hopping sequences, that have significant overlap. The common locations among these PN sequences implement a broadcast channel. If an insider uses the PN sequence to jam this broadcast channel, it becomes uniquely identifiable by the CH. Once identified, the CH updates all nodes of the cluster with new PN sequences, except for the identified attacker.

The idea of assigning unique PN codes to various nodes in the network was also exploited. In this work nodes of a cluster are represented by the leaves of a binary tree. Each node of the tree is assigned a unique key, corresponding to a seed for the generation of a unique PN [3] code. Every node knows all the keys along the path from the corresponding leaf to the root. In the absence of jamming, the PN code known to all receivers (generated by the root key) is used. If jamming is detected, transmitting nodes switch to a PN code known only to a subset of nodes. The compromised node is uniquely identified in a number of steps that is logarithmic to the number of nodes within the cluster.

4. CONCLUSION

The proposed system addressed the problem of selective jamming such as Data Selective Jamming and Channel Selective Jamming. The effectiveness of the selective jamming attacks can be implemented against TCP protocol. The adversary had been considered as an internal jammer and aware of the protocol specification and shared network secrets. It is showed that an adversary can exploit its knowledge of the protocol implementation to increase the impact of the attack at a significantly lower energy cost. To mitigate the Data Selective jamming, several methods combined with cryptographic primitives such as commitment schemes, cryptographic puzzles, and all-or-nothing transformations with physical layer attributes. To reduce the impact of the Channel Selective Jamming Randomized Distributed scheme are utilized.

REFERENCES

[1] Brown .T.X, James J.E, and Sethi .A, (2006), Jamming and Sensing of Encrypted Wireless Ad Hoc Networks, Proc, ACM. Int'l Symp. Mobile and Ad Hoc Networking and Computing, pp. 120-130.

[2] Juels .A and Brainard .J , (1999), Client Puzzles: A Cryptographic Countermeasure against Connection Depletion Attacks , Proc. Network and Distributed system Security Symp. (NDSS), pp. 151-165.

[3] Lazos .L and Krunz .M, (2011) , Selective Jamming / Dropping Insider Attack in wireless Mess Networks. Networking, pp. 30-35.

[4] Lazos .L, Liu .S, & Krunz .M,(2009) , Mitigating Control Channel Jamming Attacks in Multi-Channel Ad Hoc Networks , Proc. Second ACM conf. Wireless Network Security, pp.169-180.

[5] Pelechrinis .K, Iliofotou .M, (2011), Denial of Service Attacks in Wireless Networks: The Case of Jammers , Univ. of California, pp. 245-257.

[6] Popper .C ,Strasser .M & Capkun .S, (2009), Jamming - Resistant Broadcast Communication without Shared Keys, Security.

[7] Rivest .R, (1997) , All-or-Nothing Encryption and the Package Transform , Proc. Int'l Workshop Fast Software Encryption, pp. 210-218.

[8] Strasser .M, Popper .C and Capkun .S, (2009) , Efficient Uncoordinated FHSS Anti - Jamming Communication , Proc. ACM Int'l Symp. Mobile Ad- Hoc Networking and Computing, pp. 207-218.

[9] Thuente .D and Acharya .M, (2006), Intelligent Jamming in Wireless Networks with Applications to

802.11b and Other Networks , Proc. IEEE Military Comm, Conf.

[10] Xu .W, Wood .T, Trappe .W and Zhang .Y, (2005) , The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks , Proc. ACM Int'l Symp. Mobile Ad Hoc Networking and Computing, pp. 46-57.

P.Venkateswaran was born in Trichy, Tamilnadu, India. He received the B.Sc degree in computer science from Bharathidasan University in 2006 and M.C.A degree from Bharathidasan University in 2009. From 2009 to 2011 he was a Lecturer in the Department of Computer Science at Bharathidasan University. He is currently doing Master of Engineering degree in computer science and engineering at Anna University. His main interest includes Network Security and Wireless Networks.

D. Saravanan received the Bachelor of Engineering degree in electrical and electronics engineering from Bharathiyar University in 2000 and Master of Engineering in computer science and engineering from Annamalai University in 2005. He is working toward the PhD degree in MANET at Anna University. He is currently an associate professor in the Department of Computer Science and Engineering. He published 4 International Journals and Participated 7 International Conferences. His research interest includes mobile computing and ad-hoc networks.