NOVATEUR PUBLICATIONS
INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING RESEARCH AND TECHNOLOGY [IJIERT]
ISSN: 2394-3696
VOLUME 2, ISSUE 7, JULY-2015

ADVANCED TECHNIQUES FOR PREVENTING SELECTIVE JAMMING ATTACKS USING PACKET-HIDING METHODS

Divyashree G
Student
Vidya Vikas Institute of Technology
Mysuru, India

Shruthi H O
Student
Vidya Vikas Institute of Technology
Mysuru, India

Dr. Bindu A. Thomas
Professor & H O D
Vidya Vikas Institute of Technology
Mysuru, India

ABSTRACT

The wireless networks are more vulnerable to jamming. This jamming can be used as a launch pad for mounting Denial-Of-Service attack on wireless networks. Typically, jamming has been address under an external threat model. However, adversaries with internal knowledge of protocol specification and network secrets can launch low-effort jamming attacks that are difficult to detect and counter. In this work we address the problem of jamming attacks as internal threat model, where the attacker is aware of all network secrets and details of implementation. These types of attackers are difficult to identify. In this work we address the problem of selective jamming attacks. In these attacks the attacker is active for only short period of time, selectively targeting the messages. The selective jamming attacks can be launched by performing real-time packet classification at the physical layer. To mitigate these attacks, we illustrate different schemes that prevent real-time packet classification by combining cryptographic primitives with physical-layer attributes.

KEYWORDS— selective-jamming, denial-of-service, wireless networks, packet classification.

INTRODUCTION

Wireless technologies have become increasingly popular everyday business and personal lives. It enables one or more devices to communicate with each other without any physical connections. As we know that this wireless networks serve as transport mechanism between devices and among devices. However because of this wireless nature these are more prone to multiple security threats, in which jamming is one of the serious security threat. Jamming can disrupt wireless transmission and this can occur either unintentionally or unintentionally.

Typically jamming attacks have been considered under an external threat model, in which the jammer is not part of the network. Under this model, jamming strategies include the continuous or random transmission of high-power interference signals. However, adopting an "al- ways-on" strategy has several disadvantages. First, the adversary has to expend a significant amount of energy to jam frequency bands of interest. Second, the continuous presence of unusually high interference levels makes this type of attacks easy to detect.

Conventional anti-jamming techniques extensively on spread-spectrum communications, or some form of jamming evasion (e.g., slow frequency hopping or spatial retreats). SS techniques provide bit-level protection by spreading bits according to a secret pseudo noise (PN) code, Known only to the communicating parties. These methods can only protect wireless transmissions under the external threat model. Potential disclosure of secrets due to node compromise neutralizes the gains of SS. Broadcast communications are particularly vulnerable under an internal threat model because all intended receivers must be aware of the secrets used to protect transmissions. Hence, the compromise of a single receiver is sufficient to reveal relevant cryptographic information.

In this paper the problem of jamming is addressed under an internal threat model. A sophisticated adversary who is aware of network secrets and the implementation details of network protocols at any layer in the network stack is addressed. 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 jam attack, 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 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 (PHY) layer, as well as of the specifics of upper layers.

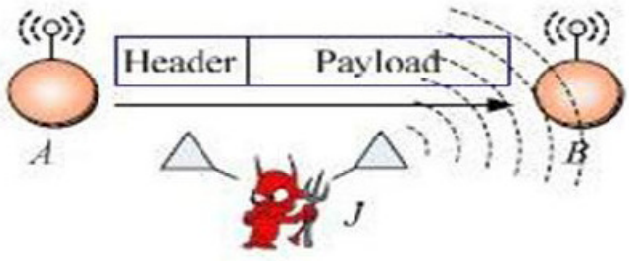

Fig. 1. Realization of a selective jamming attack

TYPES OF JAMMING

Although several strategies 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 [1]. Recently, several jamming strategies have been introduced. Later, jammers were categorized into four models. They area

- Constant jammer
- Deceptive jammer
- Random jammer
- Reactive jammer

A. Constant Jammer

The constant jammer continuously emits radio signal and sends out random bits to the channel without following any MAC layer etiquette.

B. Deceptive Jammer

In this model jammer constantly injects regular packets to the channel without any gap between subsequent packet 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

The constant jammer continuously emits a radio signal. After jamming for t1 units of time, it stops emitting radio signals and enter into sleeping 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 is quite when 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

PROBLEM STATEMENT AND ASSUMPTIONS

A. Problem Statement

Consider the scenario that 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 o f m. J then corrupts m beyond recovery by interfering with its reception at B. We address the problem of preventing the jamming node from classifying m in real time, thus mitigating J's ability to perform selective jamming.

B. System Adversary model

Network Model- The network consists of 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 uncast mode and broadcast mode. Communications can be either unencrypted or encrypted. Symmetric keys are shared among all intended receivers in broadcast communication. These keys are established using pre shared pair wise keys or asymmetric cryptography.

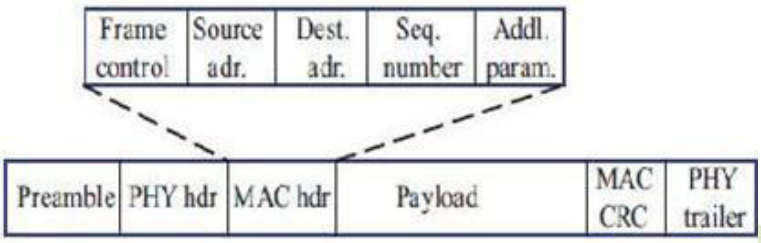

Fig. 2. A generic frame format for a wireless network

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 q data bits, where the rate of the PHY-layer encoder. Here, the transmission bit rate is equal to qR bps and the information bit rate is qR 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 addresses, 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.

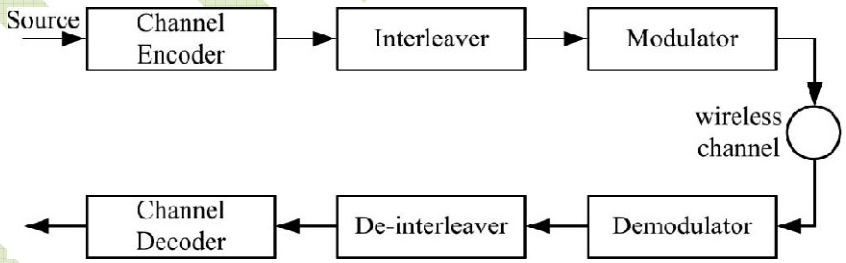

Fig. 3. A generic communication system diagram

C. Real Time Packet Classification

In this section we describe how the adversary can classify the packets in real time, before the packet transmission is completed. Once a packet is classified, the adversary may choose to jam it depending on his strategy.

Consider the generic communication system depicted in Fig. 4. 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.

The adversary's ability in classifying a packet m depends on the implementation of the blocks in Fig. 3. The channel encoding block expands the original bit sequence m, adding necessary redundancy for protecting m against channel errors. For example, an α/β-block code may protect m from up to e errors per block. Alternatively, an α/β-rate convolution encoder with a constraint length of L max, 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.

TECHNIQUESN TO PREVENT JAMMING ATTACKS

A. Strong Hiding Commitment Scheme

Strong hiding commitment scheme is based on asymmetric cryptography. Here the main motivation is to satisfy the strong hiding property while keeping the computation and communication overhead to a minimum. Commitment scheme must satisfy the two properties:

- Binding: Deliver the committed value to the receiver, here the sender cannot alter the value once it is committed

- The receiver cannot see the message until he gets the key, after receiving the key receiver verifies that it is indeed the message to which the sender is committed.

Assume that the S has a packet m for R. First S constructs (C, d) = commit (m), where

$$C = E_k(\pi_1(m)), \qquad d = k$$

Here the commitment function Ek() is an off-the-shelf symmetric encryption algorithm, π1 is a publicly known permutation and k is a randomly selected key of some desired key length s. The sender broadcasts (C//d), where "//" denotes the concatenation operation. Upon reception of d, any receiver R computes

$$m = {\pi_1}^{-1}(D_k(C))$$

Where ${\pi_1}^{-1}$ is the inverse permutation of π_1.

To satisfy the strong hiding property, the packet carrying d is formatted so that all bits of d are modulated in the last few PHY-layer symbols of the packet. To recover d, any receiver must receive and decode the last symbols of the transmitted packet, thus preventing early disclosure of d.

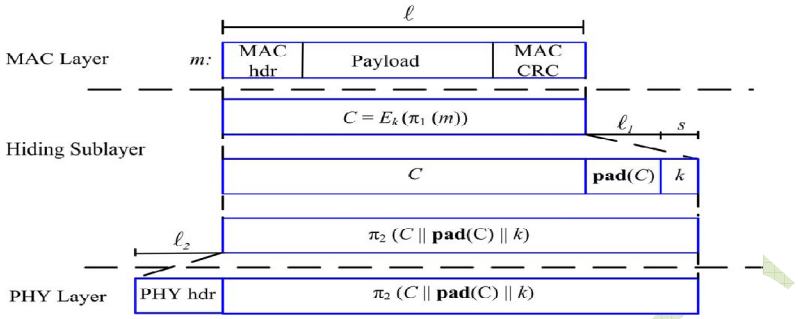

Fig. 4. Processing at hiding sub-layer

B. An AONT-Based Hiding Scheme (AONT-HS)

A solution based on All-or-Nothing Transformations is proposed, that introduces a modest communication and computation overhead. Such transformations were originally proposed by Rivets to slow down brute force attacks against block encryption algorithms. 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.

A transformation f, mapping message $m=(m_1.....m_x)$ to a sequence of pseudo messages $m^1=(m_1{}^1.....m_x{}^1)$, is an AONT if 1) f is a bijection, 2) it is computationally infeasible to obtain any part of the original plaintext, if one of the pseudo messages is unknown, and 3) f-1 and its inverse are efficiently computable. Packets are preprocessed 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. Fig. 5. Shows the details of AONTHS.

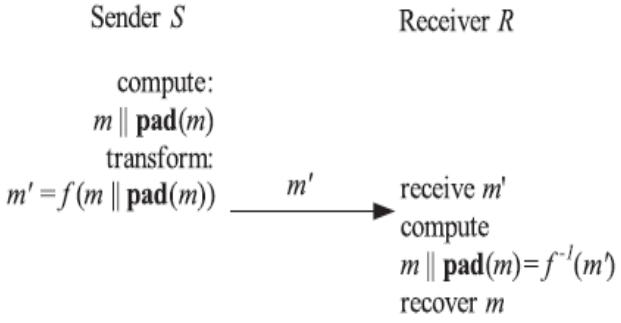

Fig. 5. An AONT based hiding scheme

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.

C. Cryptographic Puzzle Hiding Scheme

Here a packet hiding scheme based on cryptographic puzzles is presented. The main idea behind such puzzles is to force the recipient of a puzzle execute a predefined 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 overheads. There are several ways of classifying cryptographic algorithms. They will be categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use. The three types of algorithms that will be discussed

- Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption.
- Public key Cryptography (PKC): Uses one key for encryption and another for decryption.
- Hash functions: Uses a mathematical transformation to irreversibly encrypt information.

Let a sender S have a packet m for transformation. The sender S selects a random key k of desired length. S generates a puzzle P=puzzle (k, t_p), where puzzle () denotes the puzzle generator function, and t_p denotes the time required for the solution of the puzzle. Parameter t_p is measured in units of time, and it is directly dependent on the assumed computational capability of the adversary, denoted by N and measured in computational operations per second. After generating the puzzle P, the sender broadcasts (C, P), where $C = E_k(\pi_1(m))$.

At the receiver side, any receiver R solves the received puzzle P^1 to recover key k^1 and then computes $m^1 = \pi_1^{-1}(D_k(C))$. If the decrypted packet m^1 is meaningful (i.e., is in the proper format, has a valid CRC code, and is within the context of the receiver's communication), the receiver accepts that m^1 =m. Else, the receiver discards m^1. Fig. 6. shows the details of CPHS.

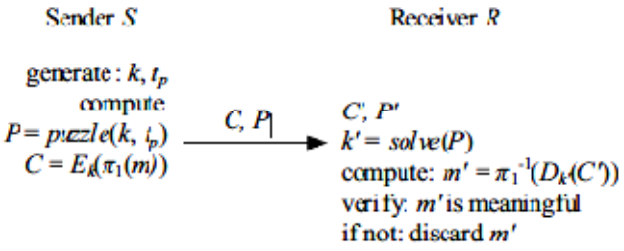

Fig. 6. A Cryptographic puzzle based hiding scheme

D. Random Key Distribution

Random key distribution is proposed to hide the location of control channels in time and/or frequency [7]. The performance metrics of resilience to control channel jamming

identification of compromised users, and delay due to jamming as a function of the number of compromised users are evaluated.

There are some other techniques to reduce the effects of jamming such as using Honeypots and Wormholes.

E. Honeypots for reducing effects of jamming

Honey pots are basically a great security measure which is used to fool attacker present in network [1]. While deploying in a network, honey pot acts as a most important part of the network and trying to gain attention of attackers. Honey pots trap the attackers in a way that attacker attacks on honey pot by thinking that it is the important part of network and at the same time honey pot collects all the information about attacker such as attacking strategy, purpose and techniques. In this section, an approach is provided which will use honey pots to provide an efficient solution 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.

F. Wormholes

A Wormhole is used to generate an alarm to indicate the presence of jammer to all access point in the network. The presence of jammer can be identified if repeated acknowledgements are received or channel is held by a node for longer duration [5]. If presence of any jammer is detected a method called packet hiding is used to transmit message through the network. Wormholes can be used as a reactive defense mechanism. After receiving repeated acknowledgements, the source becomes the wormhole and sends the information regarding the jammer to all other nodes. This wormhole, then prevent the jamming activity of particular jammer. By this method, all other nodes within that network can understand the information about the jammer.

G. Swarm Intelligence

Swarm intelligence is an artificial intelligence technique. It is the collective behavior of decentralized, self-organized systems, natural or artificial. Generally it is the discipline that deals with natural and artificial systems composed of many individuals in that co-ordinate using de-centralized control and self-organization.

Two common SI algorithms are

- Ant Colony Optimization(ACO)
- Particle Swarm Optimization

AOC algorithm techniques can be used in number of applications like controlling unmanned vehicles, control nanobots within the body for the purpose of killing cancer tumors [6]. Swarm intelligence has also been applied for data mining. Meta-Heuristic algorithms have been applied to three areas of software engineering: test data generation, module construction and cost/effort prediction. But these algorithms can be applied to many other operations in software engineering and much research should be done in this field.

CONCLUSION

In this paper the problem of selective jamming attacks in wireless networks has been addressed and considered an internal adversary model in which the jammer is part of the network which is under attack, thus being aware of the protocol specifications and shared network secrets. Here it is showed that the jammer can classify transmitted packets in real time by decoding the first few symbols of an ongoing transmission. Evaluated the impact of selective jamming attacks on network protocols such as TCP and routing and show that a selective jammer can significantly impact performance with very low effort and developed three schemes that transform a selective jammer to a random one by preventing real-time packet classification. Schemes combine cryptographic primitives such as commitment schemes, cryptographic puzzles, and all-or-nothing transformations with physical layer characteristics and analyzed the security of our schemes and quantified their computational and communication overhead. With these schemes a random key distribution has been implemented to more secure the packet transmission in the wireless networks.

REFERENCES

[1] Neha Thakur, Aruna Sankaralingam, on *"Introduction to jamming attacks and prevention techniques using honeypots in wireless networks", IRACST vol 3, April 2013.*

[2] G Jayanthi Lakshmi, S Babu, B Lakshmana Rao, P Mohan, B Sunil Kumar, on *"Jamming attacks prevention in wireless sensor networks using secure packet hiding method", Vol 2, Issue 9, September 2013.*

[3] O S C Kesavulu, B B V Satya varaprasad, on "*Enhanced packet delivery techniques using crypto-logic riddle on jamming attacks for wireless communication medium ", IJLTET, Vol.2, Issue 4, July 2013.*

[4] Divya Ann Luke, Dr. Jayasudha J S, on *"Selective jamming attack prevention based on packet hiding methods and wormholes", IJNSA, vol.6, May 2014.*

[5] M Ramesh kumar, Dr. S Sakthival, on *"Packet hiding methods for preventing selective jamming attacks using Swarm intelligence techniques", IJETAE, Vol.3, Issue 10, October 2013.*

[6] Mr. Pushphas Chaturvedi, Mr. kunal Gupta, on *"Detection and Prevention of various types of jamming attacks in wireless networks", IRACST vol 3, April 2013.*

[7] Ngangbam herjit Singh, A. kayalvizi, on "*Combining cryptographic primitives to prevent jamming attacks in wireless networks".*