www.ioirp.com
International Journal of Innovative Research in Computer Science and Engineering (IJIRCSE)
ISSN: 2394-6364, Volume – 2, Issue – 3. March 2016

PREVENTING SELECTIVE JAMMING BY ALL OR NOTHING TRANSFORMATION

Siva Prakash S, Rajesh C, Kathiravan P
Department of Information Technology,
Dr.Mahalingam College of Engineering and Technology
Email: sivapr00@gmail.com

Ram Prasath J,
Assistant Professor,
Department of Information Technology,
Dr.Mahalingam College of Engineering and Technology
Email: jrprasath@gmail.com

ABSTRACT

The open nature of the wireless medium leaves it susceptible to intentional interference attacks, naturally referred to as jamming. This jamming with wireless transmissions can be used as a launch pad for mounting Denial-of-Service attacks on wireless networks. Typically, jamming has been addressed under an external threat model. However, adversaries with internal knowledge of protocol specifications and network secrets can launch low-effort jamming attacks that are problematic to detect and counter. In this work, we address the problem of selective jamming attacks in wireless networks. In these attacks, the adversary is active only for a short period of time, selectively targeting messages of high importance. We illustrate the advantages of selective jamming in terms of network performance degradation and adversary effort by presenting two case studies; a selective attack on TCP and one on routing. We show that selective jamming attacks can be launched by performing real-time packet classification at the physical layer. To alleviate these attacks, we develop three schemes that prevent real-time packet classification by combining cryptographic primitives with physical-layer attributes. We analyze the security of our methods and evaluate their computational and communication overhead.

Keywords— Selective jamming, denial-of-service, wireless networks, packet classification.)

I. INTRODUCTION

Wireless networks rely on the uninterrupted availability of the wireless medium to interconnect participating nodes. However, the open nature of this medium leaves it vulnerable to multiple security threats. Anyone with a transceiver can eavesdrop on wireless transmissions, inject spurious messages, or jam legitimate ones. While eavesdropping and message injection can be prevented using cryptographic methods, jamming attacks are much harder to counter. They have been shown to actualize severe Denial-of-Service (DoS) attacks against wireless networks. In the simplest form of jamming, the adversary interferes with the reception of messages by transmitting a continuous jamming signal, or several short jamming pulses. 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. 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 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.

II. EXISTING SYSTEM

` Wireless networks rely on the sustained availability of the wireless medium to interconnect participating nodes. However, the open nature of this medium leaves it susceptible to numerous security threats. Someone with a transceiver can eavesdrop on current transmissions, infuse spurious messages, or jam legitimate ones. While snooping and message addition can be debarred using cryptographic methods, blocking attacks are much harder to counter. They are actually attacked in Dos (denial

of service) Attack compared with wireless Attack. It is very easy technique of jamming; this signal is interrupted by receiving of messages by transmitting an uninterrupted jamming signal. The existing system mainly focuses on an external threat model. That is why the attacker within the wireless network can easily establish the selective jamming attack. There are two reasons for this problem, first one is the broadcast communication between nodes within the wireless network and second one is that the existing system uses the Spread Spectrum concept. Conventional anti jamming technique use Spread Spectrum (SS) communication. The Spread Spectrum system take a user bit stream and perform an XOR with a pseudo noise sequence. Figure III(a) is the spreading of the user data with the pseudo noise .The spread signal is then modulated with a radio carrier.

Suppose for an example a user signal with a bandwidth of 1 MHz spreading with the PN code (10110111000 - known as 11-chip Barker code) would result in a signal with 11 MHz bandwidth. The radio carrier then shifts this signal to the carrier frequency (2.4 GHz in the ISM band). This signal is then transmitted. Figure III(b) shows the simplified block diagrams of SS receiver .The SS receiver is more 12 complicated than transmitter. The first step in the receiver involves demodulating the received signal. The receiver has to know the original PN code. This is the one main drawbacks of the existing system. In Existing System Wireless networks rely on the uninterrupted availability of the wireless medium to interconnect participating nodes. However, the open nature of this medium leaves it vulnerable to multiple security threats. Anyone with a transceiver can eavesdrop on wireless transmissions, inject spurious messages, or jam legitimate ones. While eavesdropping and message injection can be prevented using cryptographic methods, jamming attacks are much harder to counter. Monitors located in inner zones experience a more aggressive attack and can detect it faster, but they delay in passing the message out of the jammed area. They have been shown to actualize severe Denial-of-Service (DoS) attacks against wireless networks.

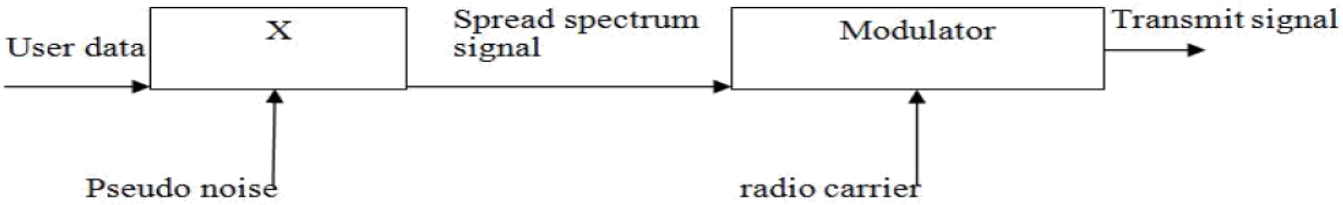

Figure III(a) Spread spectrum transmitter

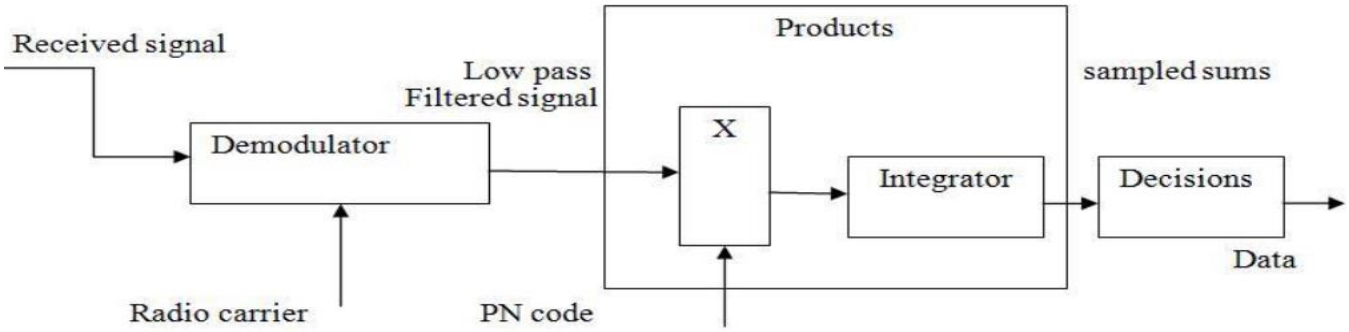

Figure III(b) Spread Spectrum receiver

Spread Spectrum technique provides bit-level protection by spreading bits according to a secret pseudo noise (PN) code. That is known only to the communicating parties. This method can only protect the wireless networks under an external threat model. The communication within the wireless network is done through the broadcast communication. So, this is vulnerable under an internal threat model. All intended receivers must know about the secrets used to protect transmissions. Another one drawback is compromise of a single receiver. So, the sender needs to reveal relevant cryptographic information to its receiver. A packet hiding technique is introduced for sending messages among nodes within the wireless network.

III. PROPOSED SYSTEM

The proposed system gives a solution based on All-or-Nothing Transformations that introduces a modest communication and computation overhead. Such transformations were originally proposed by Rivest to slow down brute force attacks against block encryption algorithms. An AONT serves as a publicly known and completely invertible pre-processing step to a plaintext before it is passed to an ordinary block encryption algorithm. The study of controllable jamming attacks in wireless sensor networks, which is easy to launch and difficult to detect and confront. The derived solutions to the optimization problems dictate optimal attack and network defence strategies. Of particular interest is the comparison between the case of perfect knowledge and that of lack of knowledge of the attacker and the network about the strategy of each other. In the latter, the attacker and the network respond optimally to the worst-case strategy of the other. 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. A transformation f, mapping message m = 14 {m1; . . .; mx} to a sequence of pseudo messages ml = {ml1; . . .; mlxl}, is an AONT if [9]: 1) f is a bijection, 2) it is computationally infeasible to obtain any part of the original plaintext.

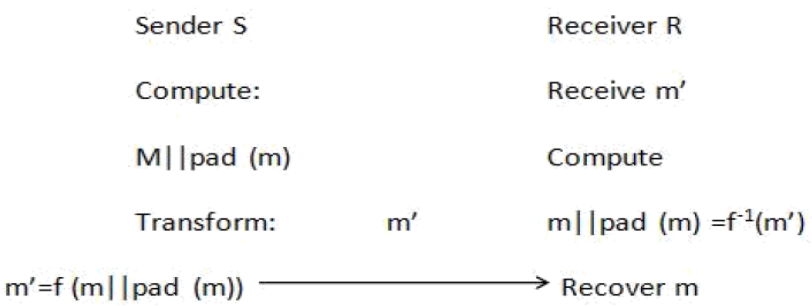

Figure IV(a) AONT based hiding scheme

Packets are pre-processed by an AONT before transmission as shown in Figure IV(a) 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; . . .; mx}, which serve as an input to an AONT f: {IFu}x _ {IFu}x. Here, IFu denotes the alphabet of blocks mi and x0 denotes the number of output pseudo messages with xl => x. The set of pseudo messages ml = {ml1; . . .; mlxl} is transmitted over the wireless medium. At the receiver, the inverse transformation f-l is applied after all xl pseudo messages are received, in order to recover m.

IV. SYSTEM IMPLEMENTATION

A.Network Module
B.Real Time Packet Classification
C.All Or Nothing Transformation
a)Linear AONT
b)Package Transform
D.Test Cases

A.Network Module

Client-server computing or networking is a distributed application architecture that partitions tasks or workloads between service providers (servers) and service requesters, called clients. Often clients and servers operate over a computer network on separate hardware. A server machine is a high-performance host that is running one or more server programs which share its resources with clients. A client also shares any of its resources; Clients therefore initiate communication sessions with servers which await (listen to) incoming requests.

B.Real Time Packet Classification

At the Physical layer, a packet m is encoded, interleaved, and modulated before it is transmitted over the wireless channel. At the receiver, the signal is demodulated, de-interleaved and decoded to recover the original packet m. 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.

C.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 20 pseudo-messages m = {m1, m2, m3,…..} is transmitted over the wireless medium.

- Linear AONT
- Package Transform

D.Test Cases

Test cases involve a set of steps, conditions, and inputs that can be used while performing testing tasks. The main intent of this activity is to ensure whether software passes or fails in terms of its functionality and other aspects.There are many types of test cases such as functional, negative, error, logical test cases, physical test cases, UI test cases, etc. Generally, there are no formal templates that can be used during test case writing. However, the following components are always available and included in every test case:

- Test case ID
- Scenario
- Description
- Status

Test ID	Scenario	Description	Status
1	Network module	Client-Server communication and Attacker Initialisation.	
2	Real Time Packet Classification	Based on priority of messages Jamming is performed.	
3	Linear AONT	Pre-processing of original plain text message using invertible matrix.	
4	Package Transform AONT	Pre-processing of original plain text message using xor and hash function.	

Table V(a) Test Case

V. CONCLUSION

The problem of selective jamming attacks in wireless networks is addressed. Consider an internal adversary model in which the jammer is part of the network under attack, thus being aware of the protocol specifications and shared network secrets. All Or Nothing Transform is merely a pre-processing step, and so it can be used with already existing encryption devices and software, without changing encryption algorithm.It improves the performance and reliability of wireless networks. This technique is very effective in emergency response operations, military, police networks etc.

VII. REFERENCES

[1] Alejandro Proano and Loukas Lazos,"Packet-Hiding methods for preventing Selective Jamming attack", IEEE Transactions on dependable and secure computing, vol. 9, no. 1,Feb-2012.
[2] Brown T.X., James J.E., and Sethi A., "Jamming and Sensing of Encrypted Wireless Ad Hoc Networks," Proc. ACM Int'l Symp. Mobile Ad Hoc Networking and Computing (MobiHoc), pp. 120-130, 2006.
[3] Cagalj M., Capkun S., and Hubaux J.P., "Wormhole-Based Anti- Jamming Techniques in Sensor Networks," IEEE Trans. Mobile Computing, vol. 6, no. 1, pp. 100-114, Jan. 2007.
[4] Chan A., Liu X., Noubir G., and Thapa B., "Control Channel Jamming: Resilience and Identification of Traitors," Proc. IEEE Int'l Symp. Information Theory (ISIT), 2007.
[5] Dempsey T., Sahin G., Morton Y., and Hopper C., "Intelligent Sensing and Classification in Ad Hoc Networks: A Case Study," IEEE Aerospace and Electronic Systems Magazine, vol. 24, no. 8, pp. 23-30, Aug. 2009.
[6] Desmedt Y., "Broadcast Anti-Jamming Systems," Computer Networks, vol. 35, nos. 2/3, pp. 223-236, Feb. 2001.
[7] Gaj K. and Chodowiec P., "FPGA and ASIC Implementations of AES," Cryptographic Engineering, pp. 235-294, Springer, 2009. [7] O. Goldreich, **61** Foundations of Cryptography: Basic Applications. Cambridge Univ. Press, 2004.
[8] Greenstein B., Mccoy G., Pang J., Kohno T., Seshan S., and Wetherall D., "Improving Wireless Privacy with an Identifier-Free Link Layer Protocol," Proc. Int'l Conf. Mobile Systems, Applications, and Services (MobiSys), 2008.
[9] Rivest R., "All-or-Nothing Encryption and the Package Transform," Proc. Int'l Workshop Fast Software Encryption, pp. 210 218, 1997.
[10] Stinson D., "Something about All or Nothing (Transforms)," Designs,
Codes and Cryptography, vol. 22, no. 2, pp. 133-138, 2001.