A NOVEL CRYPTOGRAPHY BASED METHOD FOR PREVENTING SELECTIVE JAMMING ATTACKS IN WIRELESS NETWORK

Rajesh Kumar Chakravarti[1], Sonam Choubey[2]

[1,2]*Computer Science S.V.I.T.S Indore, (India)*

ABSTRACT

An absolute solution to selective jamming would be the encryption of transmitted packets with a static key. This is the encryption of packet with the packet header. For broadcast communications the static decryption key must be known to all intended receivers. So it is more secure. The open nature of the wireless network makes it vulnerable to intentional interference attacks, commonly 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. The jamming has been addressed under an external threat model. The adversaries with internal knowledge of protocol specifications and network secrets can launch low-effort jamming attacks that are difficult to detect and counter.

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 Jamming or dropping attacks have been considered under an external threat model[9][11], in which the attacker is not a part of the network. In this model, the jamming methods include the continuous or random transmission of high-power interference signals and attackers can launch low-effort jamming attacks that are difficult to detect and counter. In these attacks, the jammer is active only for a short period of time, selectively aiming messages of high importance. Selective jamming attacks [7][8][10] can be launched by performing real-time packet classification at the physical layer. There For executing selective jamming the adversary must be capable of classifying transmitted packets and corrupting them before the end of their transmission. Packet classification is done by receiving just a few bytes of a packet. To launch selective jamming attacks, the jammer must be capable of implementing a classify-then-jam [12] policy before the completion of a wireless transmission. Such method can be actualized by classifying transmitted packets using protocol semantics. Jamming attacks are much harder to counter and face more security problems. In the simplest form of jamming, the jammer interferes with the reception of messages by transmitting a continuous jamming signal.

1.1 Related Work

Authors in [1] considers the problem of an attacker disrupting an encrypted victim wireless ad hoc network through jamming. The authors in [2] address the problem of control-channel jamming attacks in multi-channel ad hoc networks. They deviated from the traditional view that sees jamming attacks as physical-layer vulnerability. In paper [3], authors examine radio interference attacks from both sides of the issue. Firstly, they study the problem of conducting radio interference attacks on wireless networks, secondly they examine the critical issue of diagnosing the presence of jamming attacks. There are many different scenarios where a jamming style DoS may take place, but the authors in [4] focused on three basic classes of wireless networks. First is Two-Party Radio Communication. The second is The two-party scenario is the baseline case in which A and B communicate with each other on a specific channel. In this work[5], authors focus on a related but different problem for broadcast communication. They examined the thing that How to enable robust anti-jamming broadcast without shared secret keys.

II. OBJECTIVES

The first objective is to elaborate that selective jamming attacks can be launched by performing real time packet classification at the physical layer. To overcome these attacks develop a schemes that prevent real-time packet classification by combining cryptographic primitives with physical layer attributes.

III. PROPOSED SYSTEM

An absolute solution to selective jamming would be the encryption of transmitted packets with a static key. This is the encryption of packet with the packet header. For broadcast communications the static decryption key must be known to all intended receivers. So it is more secure.

IV. MODULES

- Real Time Packet Classification
- A Strong Hiding Commitment Scheme
- Cryptographic Puzzle Hiding Scheme
- Packet Hiding based on All-Or-None Transformations

V. MODULES DESCRIPTION

5.1 Real Time Packet Classification

At the Physical layer, first a packet m is encoded, second interleaved, and then modulated before it is transmitted over the wireless channel. At the receiver end, it is demodulated, de-interleaved and decoded to recover the original packet m. Two nodes A and B communicate via a wireless link. In the communication range of both A and B there is a jamming node J. When Node A transmits a packet m to Node B, then node J classifies m by receiving only the first few bytes of m. Node J then corrupts m beyond recovery by interfering with its reception at B.

5.2 Strong Hiding Commitment Scheme

A strong hiding commitment scheme, it is based on the concept of symmetric cryptography. Let us assume that the sender has a packet for Receiver. First S constructs commit(message) the commitment function is an off-the-shelf symmetric encryption algorithm is a publicly known permutation and k is a randomly selected key of some desired key length s , where the length of k is a security parameter. To recover d any receiver must receive and decode the last symbols of the transmitted packet thus preventing early disclosure of d.

5.3 Cryptographic Puzzle Hiding Scheme

A sender S has a packet m for transmission. The sender selects a key k randomly of a desired length. Then S generates a puzzle (key, time), where function puzzle() denotes the puzzle generator function, and function tp denotes the time required for the solution of the puzzle. After generating the puzzle P, the sender broadcasts (C, P). Where C is encrypted message. At the receiver side any receiver R solves the received puzzle to recover key and then computes the decryption to get the m..

VI. EXPECTED OUTCOMES

- A new preventing selective jamming attack method. It will include the encryption of transmitted packets with a static key
- It will be more secure

VII. CONCLUSION

In this paper, we have proposed a novel cryptography based technique to prevent the selective jamming attack. It will be more secure & it is based on the concept of static key, which will be used to encrypt the transmitted packets. We have also presented the introduction to jamming attacks. Also the related work is described in brief.

REFERENCES

[1] Alejandro Proano And Loukas Lazos January/February 2012Packet Hiding Methods for Preventing Selective JammingAttacksIEEE TRANSACTIONS ON DEPENDABLE ANDSECURE COMPUTING (vol. 9 no. 1)

[2] Lookas Lazos and Marwan Krunz February 2012 SelectiveJamming/Dropping Insider Attacks in Wireless Mesh NetworksIEEE NETWORK Volume:25 Issue:4

[3] Wenyuan Xu, Timothy Wood, Wade Trappe, Yanyong Zhang2004Channel Surfing and Spatial Retreats: Defenses againstWireless Denial of Service WiSe ’04 Proceedings of the 3rd ACM workshoponWirelesssecurityPages 80-89ACM New York, NY, USA

[4] SudipMisra,Sanjay.K.Dhurander,AvanishRayankulaand DeepanshAgarwal 26-31 Oct. 2008 Using Honeynodes along with ChannelSurfing for Defense against Jamming Attacks in Wireless Networks3rd International Conference on System and Network Communications Page-197-201

[5] Shio Kumar Singh , M P Singh , and D K Singh May to June Issue 2011 A Survey on Network Security and Attack Defense Mechanism For Wireless Sensor Networks International Journal of Computer Trends and TechnologyVolume 1

[6]. Alnifie G., Simon R., "A Multi-channel Defense Against Jamming Attacks in Wireless Sensor Networks" In Proc. of the third ACM International Workshop on QoS and Security for Wireless and Mobile Networks (Q2SWinet 2007). Chania, Crete Island, Greece, October 22, 2007. pp: 95–104.

[7]. Acharya M., Thuente D., "Intelligent JammingAttacks, Counterattacks and (Counter)2Attacks in 802.11b Wireless Networks", inProceedings of the OPNETWORK Conference,Washington DC, USA, August 2005.

[8]. Wood A. D., Stankovic J. A., Son S. H.,"JAM: A Jammed-Area Mapping Service forSensor Networks," in Proceedings of 24thIEEE Real-Time Systems Symposium (RTSS),3-5 December, 2003. pp: 286 - 297

[9]. Ma K., Zhang Y., Trappe W., "Mobile Network Management and Robust Spatial Retreats via Network Dynamics," in Proceedings of the 1st International Workshop on Resource Provisioning and Management in Sensor Networks (RPMSN05), Ohio, USA, November 7th, 2005.

[10]. Xu W., Trappe W., Zhang Y., "DefendingWireless Sensor Networks from RadioInterference through Channel Adaptation,"ACM Transactions on Sensor Networks(TOSN), Volume 4, Issue 4, August 2008.

[11]. Mahadevan K., Hong S., Dullum J."Anti-Jamming: A Study". 2005

[12]. Li M., Koutsopoulos I., Poovendran R., "Optimal Jamming Attacks and Network Defense" In IEEE International Conference on Computer Communications (INFOCOM), Anchorage, Alaska, USA, 6-12 May, 2007.