Volume : 2 | Issue : 5 | May 2013 • ISSN No 2277 - 8179

Research Paper

# A Novel Method for Preventing Selective Jamming Attacks

Engineering

**KEYWORDS :** wireless, attacks, transmissions, jamming, degradation, cryptographic

**K. Mohan** — Department of Information Technology, Padaleswarar Polytechnic College, Cuddalore

**P. Kumaran** — PG Scholar, Dept. of Electronics & Telecommunication Engg., Sathyabama University, Chennai

## ABSTRACT

*The wireless medium leaves it vulnerable to intentional interference attacks, typically referred to as jamming. This intentional interference with wireless transmissions can be used as a launch pad for mounting DoS attacks on wireless networks. Typically, jamming bas been addressed under an external threat model. The internal knowledge of protocol specifications and network secrets can launch low-effort jamming attacks that are difficult to detect and counter. Here we find the problem of selective jamming attacks in wireless networks. 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. An intuitive solution to selective jamming would be the encryption of transmitted packets (including headers) with a static key. However, for broadcast communications, this static decryption key must be known to all intended receivers and hence, is susceptible to compromise. 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. We analyse the security of our methods and evaluate their computational and communication overhead.*

## 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 [12]. 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.

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 "always- 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.

## 3. PROBLEM STATEMENT

Consider the scenario depicted in Fig. 1a. 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 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.

## 3. IMPACT OF SELECTIVE JAMMING

In this section, we illustrate the impact of selective jamming attacks on the network performance.

### 3.1. Selective Jamming at the Transport Layer

In the first set of experiments, we set up a file transfer of a 3 MB file between two users A and B connected via a multihop route. The TCP protocol was used to reliably transport the requested file. At the MAC layer, the RTS/ CTS mechanism was enabled. The transmission rate was set to 11 Mbps at each link. The jammer was placed within the proximity of one of the intermediate hops of the TCP connection. Four jamming strategies were considered:

1. Selective jamming of cumulative TCP-ACKs.
2. Selective jamming of RTS/CTS messages.
3. Selective jamming of data packets.
4. Random jamming of any packet.

### 3.2. Selective Jamming at the Network Layer

In this scenario, we simulated a multihop wireless network of 35 nodes, randomly placed within a square area. The AODV routing protocol was used to discover and establish routing paths [19]. Connection requests were initiated between random source/destination pairs. Three jammers were strategically placed to selectively jam nonoverlapping areas of the network. Three types of jamming strategies were considered: 1) a continuous jammer, 2) a random jammer blocking only a fraction p of the transmitted packets, and 3) a selective jammer targeting route-request (RREQ) packets.

## 4. IMPLEMENTATION OF PROPOSED SYSTEM

An intuitive solution to selective jamming would be the encryption of transmitted packets (including headers) with a static key. However, for broadcast communications, this static decryption key must be known to all intended receivers and hence, is susceptible to compromise. 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.

### ADVANTAGES OF PROPOSED SYSTEM:

- Relatively easy to actualize by exploiting knowledge of network protocols and cryptographic primitives extracted from compromised nodes
- Our findings indicate that selective jamming attacks lead to DoS with very low effort on behalf of the jammer.
- Achieve strong security properties

### IMPLEMENTATION

- Real Time Packet Classification
- A Strong Hiding Commitment Scheme
- Cryptographic Puzzle Hiding Scheme
- Hiding based on All-Or-Nothing Transformations

### 4.1. 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, deinterleaved 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.

Volume : 2 | Issue : 5 | May 2013 • ISSN No 2277 - 8179

### 4.2. A STRONG HIDING COMMITMENT SCHEME

A strong hiding commitment scheme (SHCS), which is based on symmetric cryptography. 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 (the length of k is a security parameter). Upon reception of d, any receiver R computes.

### 4.3. CRYPTOGRAPHIC PUZZLE HIDING SCHEME

A sender S have a packet m for transmission. The sender selects a random key k, of a desired length. S generates a puzzle (key, time), where puzzle () denotes the puzzle generator function, and tp denotes the time required for the solution of the puzzle. Parameter 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). At the receiver side, any receiver R solves the received puzzle to recover key and then computes.

### 4.4. HIDING BASED ON ALL-OR-NOTHING TRANSFORMATIONS

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 = {m1, m2, m3…} is transmitted over the wireless medium.

### 5. ARCHITECTURE

### 6. CONCLUSION

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. We showed that the jammer can classify transmitted packets in real time by decoding the first few symbols of an ongoing transmission. We evaluated the impact of selective jamming attacks on network protocols such as TCP and routing. Our findings show that a selective jammer can significantly impact performance with very low effort. We developed three schemes that transform a selective jammer to a random one by preventing real-time packet classification.

## REFERENCE

[1] T.X. Brown, J.E. James, and A. Sethi, "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. | | [2] M. Cagalj, S. Capkun, and J.-P. Hubaux, "Wormhole-Based Anti-Jamming Techniques in Sensor Networks," IEEE Trans. Mobile Computing, vol. 6, no. 1, pp. 100-114, Jan. 2007. | | [3] A. Chan, X. Liu, G. Noubir, and B. Thapa, "Control Channel Jamming: Resilience and Identification of Traitors," Proc. IEEE Int'l Symp. Information Theory (ISIT), 2007. PROA~NO AND LAZOS: PACKET-HIDING METHODS FOR PREVENTING SELECTIVE JAMMING ATTACKS 113 | | [4] T. Dempsey, G. Sahin, Y. Morton, and C. Hopper, "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. | | [5] Y. Desmedt, "Broadcast Anti-Jamming Systems," Computer Networks,vol. 35, nos. 2/3, pp. 223-236, Feb. 2001. | | [6] K. Gaj and P. Chodowiec, "FPGA and ASIC Implementations of AES," Cryptographic Engineering, pp. 235-294, Springer, 2009. | | [7] O. Goldreich, Foundations of Cryptography: Basic Applications. Cambridge Univ. Press, 2004. | | [8] B. Greenstein, D. Mccoy, J. Pang, T. Kohno, S. Seshan, and D.Wetherall, "Improving Wireless Privacy with an Identifier-Free Link Layer Protocol," Proc. Int'l Conf. Mobile Systems, Applications, and Services (MobiSys), 2008. | | [9] IEEE, IEEE 802.11 Standard, http://standards.ieee.org/getieee802/download/802.11-2007.pdf, 2007. | | [10] A. Juels and J. Brainard, "Client Puzzles: A Cryptographic Countermeasure against Connection Depletion Attacks," Proc. Network and Distributed System Security Symp. (NDSS), pp. 151-165, 1999. |