Combining Cryptographic Primitives to Prevent Jamming Attacks in Wireless Networks

Ngangbam Herojit Singh [1], A.Kayalvizhi, M.Tech.[2],
[1]*M.Tech (IT) Student-VelTech Multitech Dr.Rangarajan Dr.Sakunthala Engg College*
[2]*Assistant Professor- VelTech Multitech Dr.Rangarajan Dr.Sakunthala Engg College*
E-mail: herojitng@gmail.com, 7200141176

Abstract: The Open Nature of wireless medium leaves an intentional interference attack, typically referred to as jamming. This intentional interference with wireless transmission launch pad for mounting Denial-Of-Service attack on wireless networks. Typically, jamming has been addresses 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 and adversary is active for short period of time, selectively targeting the messages of high importance. We show that the selective jamming attacks can be launched by performing real-time packet classification at the physical layer. To mitigate these attacks, we develop three schemes that prevent real-time packet classification by combining cryptographic primitives with physical-layer attributes. They are Strong Hiding Commitment Schemes (SHCS), Cryptographic Puzzles Hiding Schemes (CPHS), All-Or-Nothing Transformation Hiding Schemes (AONTS-HS). Random key distribution methods are done along with three schemes to give more secured packet transmission in wireless networks.

Index Terms—Selective jamming, denial-of-service, wireless networks, packet classification.

1. 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 eaves- dropping 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.

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 ant-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, 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. 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 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.

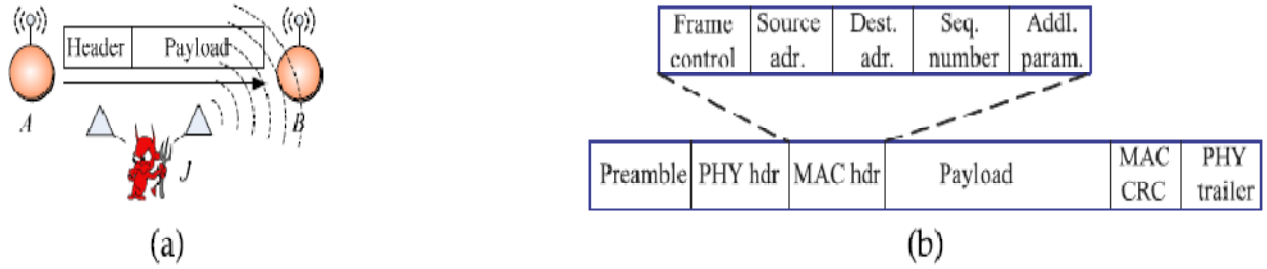

Fig. 1. (a) Realization of a selective jamming attack. (b) A generic frame format for a wireless network.

2.PROBLEM STATEMENTS AND ASSUMPTION:

2.1 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.

2.2 System and Adversary Model:

2.2.1 Network Model:

The network consists of a 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 unicast 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 preshared pair wise keys or asymmetric cryptography.

2.2.2 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. 1b. the preamble is used for synchronizing the sampling process at te 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.

2.2.3 Adversary Model:

We assume the adversary is in control of the communication medium and can jam messages at any part of the network of his choosing (similar to the Dolev-Yao model). The adversary can operate in full-duplex mode, thus being able to receive and transmit simultaneously. This can be achieved, for example, with the use of multi-radio transceivers. In addition, the adversary is equipped with directional antennas that enable the reception of a signal from one node and jamming of the same signal at another. For analysis purposes, we assume that the adversary can proactively jam a number of bits just below the ECC capability early in the transmission. He can then decide to irrecoverably corrupt a transmitted packet by jamming the last symbol. In reality, it has been demonstrated that selective jamming can be achieved with far less resources. A jammer equipped with a single half-duplex transceiver is sufficient to classify and jam transmitted packets. However, our model captures a more potent adversary that can be effective even at high transmission speeds.

The adversary is assumed to be computationally and storage bounded, although he can be far superior to normal nodes. In particular, he can be equipped with special purpose hardware for performing cryptanalysis or any other required computation. Solving well-known hard cryptographic problems is assumed to be time consuming. For the purposes of analysis, given a cipher text, the most efficient method for deriving the corresponding plaintext is assumed to be an exhaustive search on the key space.

The implementation details of every layer of the network stack are assumed to be public. Furthermore, the adversary is capable of physically compromising network devices and recovering stored information including cryptographic keys, PN codes, etc. This internal adversary model is realistic for network architectures such as mobile ad hoc, mesh, cognitive radio, and wireless sensor networks (WSNs), where network devices may operate unattended, thus being susceptible to physical compromise

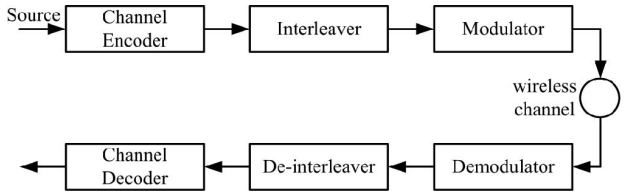

Fig. 2. A generic communication system diagram.

3. REAL-TIME PACKET CLASSIFICATIONS:

In this section, we describe how the adversary can classify 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. 2. 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. 2. The channel encoding block expands the original bit sequence m, adding necessary redundancy for protecting m against channel errors. For example, a 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.

4.A Strong Hiding Commitment Scheme (SHCS):

We propose a strong hiding commitment scheme, which is based on symmetric cryptography. Our main motivation is to satisfy the strong hiding property while keeping the computation and communication overhead to a minimum.
Assume that the sender S has a packet m for R. First S construct (C,d)=commit(m),where

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

Here the commitment function $E_k()$ is an off-the-shelf symmetric encryption algorithm,π_1 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 π_1^{-1} denotes 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.

5. Cryptographic Puzzle Hiding Scheme (CPHS):

We present a packet-hiding scheme based on cryptographic puzzles. 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.

Let a sender S have a packet m for transmission. The senders select 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 tp 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. 4 show the details of CPHS.

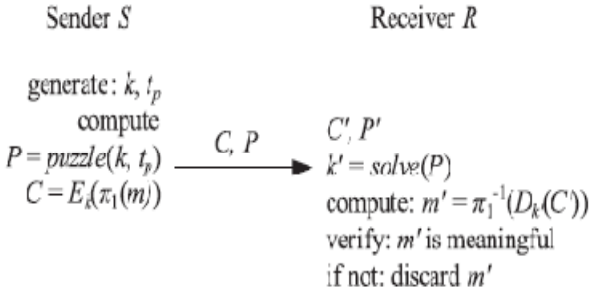

Fig 4: The cryptographic puzzles-based hiding scheme

5 An AONT-Based Hiding Scheme (AONT-HS):

We propose a solution based on All-or-Nothing Transformations 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 $m^1=(m^1.....m_x)$, 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 show the details of AONT-HS.

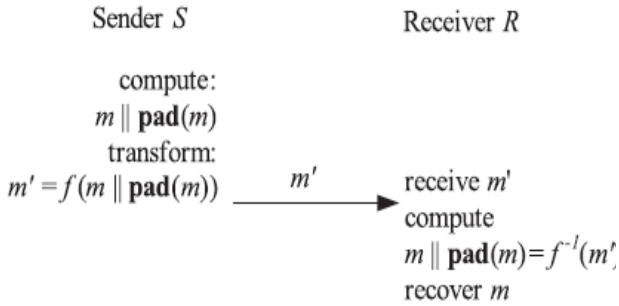

Fig. 5. The AONT-based hiding scheme.

6. Random Key Distribution:

We propose the use of random key distribution to hide the location of control channels in time and/or frequency. We evaluate 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.

7. 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 under attack, thus being aware of the protocol specifications and shared network secrets. 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.

8. References:

[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.

[4] W. Xu, W. Trappe and Y. Zhang, "Anti-Jamming Timing Channels for Wireless Networks," Proc. ACM Conf. Wireless Network Security (WiSec), pp. 203-213, 2008.

[5] R. Rivest, "All-or-Nothing Encryption and the Package Trans- form," Proc. Int'l Workshop Fast Software Encryption, pp. 210-218,1997.

[6] R. Rivest, A. Shamir, and D. Wagner, "Time Lock Puzzles and Timed-Release Crypto," technical report, Massachusetts Inst. of Technology, 1996.

[7] P. Tague, M. Li, and R. Poovendran, "Mitigation of Control Channel Jamming under Node Capture Attacks," IEEE Trans. Mobile Computing, vol. 8, no. 9, pp. 1221-1234, Sept. 2009

[8] 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.