Internally Selective Jamming Attacks Prevention in Wireless Networks using Packet Hiding Techniques

N. Vijaya Gopal[#1], Dr.V.Srikanth[*2], M. Anil Kumar[#3]

[#] Department of cse, Kluniversity,Vaddeswaram.India

nvgopal63@hotmail.com, modhugula.anilkumar@hotmail.com,vsrikanth@kluniversity.in

[*]second author Dr.V.Srikanth, Head of the department of cse, Kluniversity, India.

Abstract:

Network security consists of provision policies adopted by network administrators to prevent illegal access of network available resources. The open nature of the wireless medium leaves it vulnerable to intentional attacks, typically referred to as jamming. Jamming can be view as a form of Denial-of-Service attacks, whose goal is to prevent users from receiving timely and sufficient information. If an attacker actually wanted to compromise your LAN and wireless security, the most successful approach would be to send random unauthenticated packets to every wireless station in the network. In the previous technique selective jamming in TCP transmission can be performed by classifying transmitted packets in real time and corrupting them before the end of their communication. In the proposed system, the selective jamming attack encountered by wireless networks using UDP protocol for transmission can be prevented internal attacks by using both the cryptographic and steganography techniques**.**

Keywords:

Selective jamming, denial-of-service, wireless networks, packet classification, Steganography.

Introduction:

The Wireless networks depend up on the continuous availability of the wireless medium to interconnect participating nodes. On the other hand the open nature of this middle leaves it susceptible to several security threats. Any person with a transceiver can eavesdrop on wireless transmissions, inject spurious messages, or jam legal one. While eavesdropping and message injection can be prevented using cryptographic method, jamming attacks are much harder to counter. They have been exposed to actualize severe Denial-of-Service (DoS) attacks against wireless networks. In the simplest type of jamming, the opponents interfere with the response of messages by transmit a ceaseless jamming signal, or few short jamming pulses.

Jamming attacks may be viewed as a special case of Denial of Service (DoS) attacks. DoS attack are any event that diminishes or eliminates a network's capacity to perform its expected function. Typically, DoS prevents or inhibits the normal use or management of communications through flooding a network with ineffective information. In a jamming attack the Radio Frequency (RF) signal emitted by the jammer corresponds to the ineffective information received by all

sensor nodes. This signal can be sallow noise or any signal that resembles network traffic. Typically, jamming attacks have been cautious under an external hazard model, wherein the jammer is not branch of the network. Under this model, jamming strategy includes the incessant or random broadcast of high-power interfering signals. However, adopting an "always-on" approach has several disadvantages. First, the adversary has to expend an important amount of energy to jam frequency bands of awareness. Second, the permanent presence of unusually high interference levels makes this type of attacks simple to detect. Conventional anti-jamming techniques rely widely on spread-spectrum (SS) communications, or some form of jamming evasion (e.g., slow frequency hopping, or spatial retreats). SS techniques present bit-level protection by spreading bits according to a secret pseudo-noise (PN) code, known only to the communicate parties. These methods can only defend wireless transmissions under the outside threat model. Potential discovery of secrets due to node cooperation neutralizes the gains of SS. Broadcast communications are mostly weak under an internal threat model because all proposed receivers must be aware of the secrets used to protect transmissions. Consequently, the concession of a solo recipient is enough to reveal relevant cryptographic information. Within this paper, we tackle to the problem of jamming under an inside threat model. We consider a complicated adversary who is aware of network secrets and the implementation detail of network protocols at any layer in the network stack. The adversary exploits his inside knowledge for initiation selective jamming attacks in which particular messages of "high importance" are targeted. For example, a jammer can target route-request/route-reply messages at the routing layer to stop route discovery, or aim TCP acknowledgments in a TCP session to cruelly degrade the throughput of an end-to-end flow. To launch selective jamming attacks, the adversary must be skilled of implementing a "classify-then-jam" strategy before the conclusion of a wireless transmission. Such approach can be actualized either by classifying transmitted packets using protocol semantics, or by decoding packets on the fly. In the final method, the jammer may decode the first few bits of a packet for improving useful packet identifiers such as packet type, source and destination address. After organization, 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.

Steganography is the art and science of writing secreted messages in the approach that no one, apart from the sender and intended receiver, suspects the extension of the message, an arrangement of security through obscurity. Steganography includes the suppression of information within computer records. In digital Steganography, electronic communications may take in Steganographic coding within of a transport layer, such as a manuscript file, image file, program or protocol. Media files are perfect for Steganographic transmission because of their large size.

Problem Statement and Assumptions

Problem Statement

Consider the picture depict in Fig. 1. Nodes A and B communicate by a wireless connection. Surrounded by the contact assortment of both A and B there is a congestion node J. When A transmits a carton m to B, lump J classifies m by receiving only the first few bytes of m. J then corrupts m beyond recovery by

interfere 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.

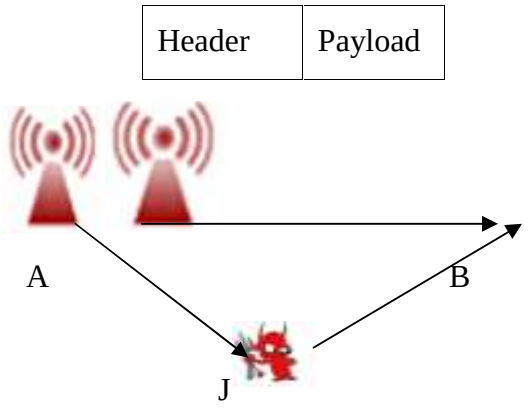

Fig: 1 Realization of a selective jamming attack.

System and Adversary Model

Network model

The network consists of a group of nodes connected via wireless links. Nodes may communicate straight if they are within communication range, or indirectly via many hops. Nodes communicate mutually in unicast mode and broadcast mode. Communications can be both unencrypted and encrypted. For encrypted broadcast communications, symmetric keys are shared among all future receivers. These keys are reputable using presaged pair wise keys or asymmetric cryptography.

Communication Model

Packets are transmitting at a rate of R bauds. Each PHY-layer symbol corresponds to q bits. Where the value of q is define by the original digital modulation scheme. Every symbol carries q data bits, where α/β is the speed of the PHY-layer encoder. Here, the broadcast bit rate is equal to qR bps and the in sequence 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 defend wireless transmissions from jamming. SS provides protection to interfering 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 variety process at the receiver. The PHY layer header contains information about 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.

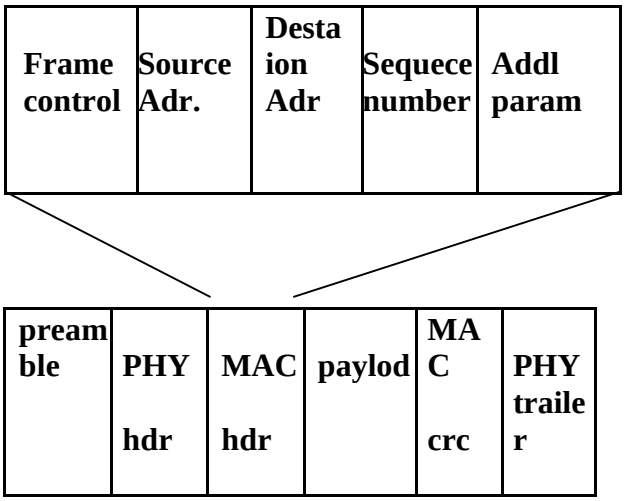

Fig 2.A generic frame format for a wireless network

Real-Time Packet Classification

In this section, we describe how the adversary can classify packets in genuine time, prior to the packet communication 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. 3. At the PHY layer, a packet m is programmed, interleaved, and adapted prior to it is transmitted over the wireless feed. At the recipient, the signal is demodulated, de intersperse, and deciphered, to improve the original packet m.

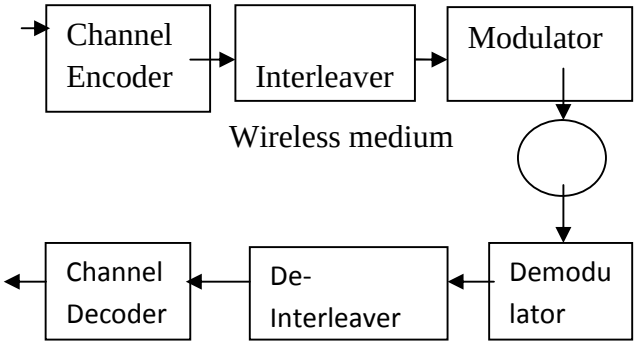

Fig 3 A generic communication system diagram.

Impact Selective Jamming

We show the impact of selective jamming attacks on the network performance, realize selective jamming attacks in two multi-hop wireless network scenarios. In the first scenario, the attacker targeted a TCP connection establishes over a multi-hop wireless route. In the second scenario, the jammer targeted network-layer control messages transmitted during the route enterprise procedure selective jamming would be the encryption of transmitted packets (including headers) with a static key. However, for broadcast transportation, this static decryption key must be known to all proposed receivers and hence, is vulnerable to compromise. An adversary in control of the decryption key can create decrypting as early on as the reception of the first cipher text block.

Strong Hiding Commitment Scheme (SHCS)

We suggest a strong hiding commitment scheme (SHCS), which is based on symmetric cryptography. Our main incentive is to satisfy the strong hiding property while keeping the calculation and statement overhead to a minimum.

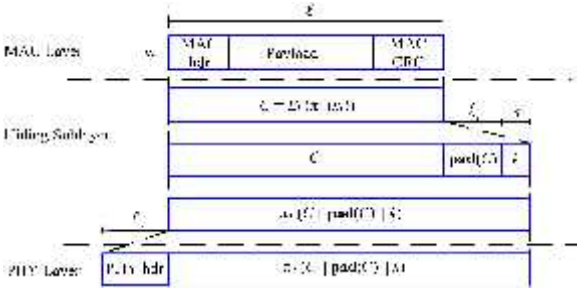

Fig 4: Strong Hiding Commitment Scheme (SHCS)

The calculation overhead of SHCS is one symmetric encryption at the sender and one symmetric decryption at the receiver. Because the heading information is permuted as a trailer and encrypted, all receivers in the vicinity of a sender must receive the entire packet and decrypt it, previous to the packet type and destination can be dogged. Though, in wireless protocols such as 802.11, the whole packet is acknowledged at the MAC stratum in front of it is determined if the packet have to be unnecessary or be additional processed. If some parts of the MAC description are deemed not to be handy in order to the jammer, they can linger unencrypted in the description of the packet, thus keep away from the decryption procedure at the recipient.

The AONT-based Hiding Scheme (AONT-HS)

We propose a solution based on All-Or-Nothing Transformations (AONT) that introduces a modest communication and calculation slide. Such transformations were initially anticipated by Rivest to slow down brute force attacks against block encryption algorithms. An AONT serves as a visibly recognized and wholly invertible pre-processing step to a plaintext before it is passed to an ordinary block encryption algorithm.

1. Symmetric encryption algorithm

2. Brute force attacks against block encryption algorithms

Algorithm Description

Sender S Receiver R

Compute:

m||pad (m)

Transform:

m`= f(m||pad(m))----------receive m`

Compute

m||pad (m) = f-1(m`)

Recover m

CONCLUSION

The problem of selective jamming attacks in wireless networks considered under an internal adversary model in which the jammer is part of the network under an attack, thus being aware of the protocol specifications and shared network secrets. The Steganography has its arrangement in security. It is not intended to replace cryptography but complement it. Hiding a message with steganography methods reduces the chance of a message creature detected. However, if that message is also encrypted, if exposed, it must also be cracked. The selective jammer can extensively impact performance with very low effort and identify jammer positions with attacks on network protocol such as UDP/TCP and Routing.

REFERENCES

1. Alejandro Proa˜no and Loukas Lazos Dept. of Electrical and Computer Engineering,
University of Arizona, Tucson, AZ, USA ” Packet-Hiding Methods for Preventing SelectiveJamming Attacks”, 2012.
2. T. X. Brown, J. E. James, and A. Sethi. Jamming and sensing of encrypted wireless ad hoc networks. In Proceedings of MobiHoc, pages 120–130, 2006.
3. M. Cagalj, S. Capkun, and J.-P. Hubaux. Wormhole-based antijamming techniques in sensor networks. IEEE Transactions on Mobile Computing, 6(1):100–114, 2007.
4. A. Chan, X. Liu, G. Noubir, and B. Thapa. Control channel jamming: Resilience and identification of traitors. In Proceedings of ISIT, 2007.
5. T. Dempsey, G. Sahin, Y. Morton, and C. Hopper. Intelligent sensing and classification in ad hoc networks: a case study. Aerospace and Electronic Systems Magazine, IEEE, 24(8):23–30, August 2009.
6. Y. Desmedt. Broadcast anti-jamming systems. Computer Networks, 35(2-3):223–236, February 2001.
7. K. Gaj and P. Chodowiec. FPGA and ASIC implementations of AES. Cryptographic Engineering, pages 235–294, 2009.
8. O. Goldreich. Foundations of cryptography: Basic applications. Cambridge University Press, 2004.
9. B. Greenstein, D. Mccoy, J. Pang, T. Kohno, S. Seshan, and D. Wetherall.

Improving wireless privacy with an identifier-free link layer protocol. In Proceedings of MobiSys, 2008.