Volume 3, Issue 5, May 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Framework for Identifying Packet Loss and Jamming Attacks in Wireless Network

S.Joe Prabhu Deep*
M.Tech 2nd year, Dept of CSE,
ASCET, GUDUR, India
prabhudeep2008@gmail.com

S.Surekha
Assistant Professor, Dept of CSE,
ASCET, GUDUR, India
sure.surekha5@gmail.com

Abstract— ***The open nature of 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 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 difficult 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 those selective jamming attacks can be launched by performing real-time packet classification at the physical layer. We analyze the security of our methods and evaluate their computational and communication overhead. Multiple-path source routing protocols allow a data source node to distribute the total traffic among available paths. In this paper, we consider the problem of jamming-aware source routing in which the source node performs traffic allocation based on empirical jamming statistics at individual network nodes. We formulate this traffic allocation as a lossy network flow optimization problem using portfolio selection theory from financial statistics. We show that in multi source networks, this centralized optimization problem can be solved using a distributed algorithm based on decomposition in network utility maximization (NUM). We demonstrate the network's ability to estimate the impact of jamming and incorporate these estimates into the traffic allocation problem. Finally, we simulate the achievable throughput using our proposed traffic allocation method in several scenarios. In Future we can gather the Jamming node information on the server where as, Here we have done on the client side. On gathering this jamming node information from the client to server side we can produce an effective path table to the client node to transfer the data..***

Keywords: Network Security, Wireless Communications, piggybacking, Encryption.

I. INTRODUCTION

This 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. 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 . Conventional anti-jamming techniques rely extensively on spread-spectrum (SS) 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.

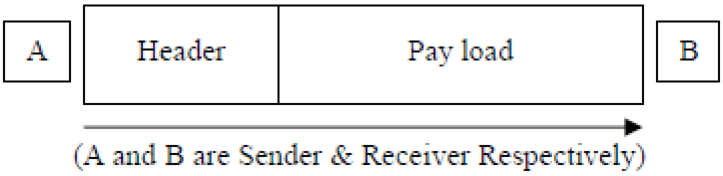

Fig. 1

II. PROBLEM STATEMENT AND ASSUMPTIONS

2.1 Problem Statement

Consider the scenario depicted in Fig. 1(a). 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.

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. For encrypted broadcast communications, symmetric keys are shared among all intended receivers. These keys are established using pre shared pair wise keys or asymmetric cryptography.

2.2.2 Communication Model

Packets are transmitted at a rate of R bauds. Each PHYlayer 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 α/β is the rate of the PHY-layer encoder. Here, the transmission bit rate is equal to qR bps and the information bit rate is R 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.The preamble is used for synchronizing the sampling process at the 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 multiradio 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 pro-actively 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 halfduplex 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 ciphertext, 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, where network devices may operate unattended, thus being susceptible to physical compromise.

III. REAL-TIME PACKET CLASSIFICATION

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. 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 . The channel encoding block expands the original bit sequence m, adding necessary redundancy for protecting m against channel errors. For example, an α/β- block code may protect m from up to e errors per block. Alternatively, an α/β-rate convolutional encoder with a constraint length of Lmax, 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. For simplicity, we consider a block interleaver that is defined by a matrix Ad×_ 1. The de-interleaver is simply the transpose of A. Finally, the digital modulator maps the received bit stream to symbols of length q, and modulates them into suitable waveforms for transmission over the wireless channel. Typical modulation techniques include OFDM, BPSK, 16(64)-QAM, and CCK. In order to recover any bit of m, the receiver must collect d・β bits for de-interleaving. The d・β de-interleaved bits are then passed through the decoder. Ignoring any propagation and decoding delays, the delay until decoding the first block of data is ⌈ d_ q ⌉ symbol durations. As an example, in the 802.11a standard, operating at the lowest rate of 6 Mbps, data is passed via a 1/2-rate encoder before it is mapped to an OFDM symbol of q = 48 bits. In this case, decoding of one symbol provides 24 bits of data. At the highest data rate of 54 Mbps, 216 bits of data are recovered per symbol. From our analysis, it is evident that intercepting the first few symbols of a packet is sufficient for obtaining relevant header information. For example, consider the transmission of a TCP-SYN packet used for establishing a TCP connection at the transport layer.

Assume an 802.11a PHY layer with a transmission rate of 6 Mbps. At the PHY layer, a 40- bit header and a 6-bit ta il are appended to the MAC packet carrying the TCP-SYN packet. At the next stage, the 1/2- rate convolutional encoder maps the packet to a sequence of 1,180 bits. In turn, the output of the encoder is split into 25 blocks of 48 bits each and interleaved on a per-symbol basis. Finally, each of the blocks is modulated as an OFDM symbol for transmission. 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. An adversary in possession of the decryption key can start decrypting as early as the reception of the first ciphertext block.

For example,consider the cipher-block chaining (CBC) mode of encryption [27]. To encrypt a message m with a key k and an initialization vector IV, message m is split into x blocks m1,m2, . . .mx. One solution to the key compromise problem wouldbe to update the static key whenever it is compromised. However, such a solution is not useful if the compromised node obtains the new key. This can only be avoided if there is a mechanism by which the set of compromised nodes can be identified. Such a task is non-trivial when the leaked key is shared by multiple nodes. Any node that possesses the shared key is a candidate malicious node. 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. This is because for computationally-efficient encryption methods such as block encryption, the encryption of a prefix plaintext with the same key yields a static ciphertext prefix. Hence, an adversary who is aware of the underlying protocol specifics (structure of the frame) can use the static ciphertext portions of a transmitted packet to classify it.

IV. IMPACT OF SELECTIVE JAMMING

In this section, we illustrate the impact of selective jamming attacks on the network performance. We used OPNETTM Modeler 14.5 to implement selective jamming attacks in two multi-hop wireless network scenarios. In the first scenario, the attacker targeted a TCP connection established over a multi hop wireless route. In the second scenario, the jammer targeted network-layer control messages transmitted during the route establishment process.

V. SECURITY ANALYSIS

In this section, we analyze the security of SHCS by evaluating the ability of J in classifying a transmitted packet at different stages of the packet transmission. Release of C–We first examine if J can classify m by observing the commitment value C. Though C and k are part of the same packet, symbols corresponding to C are received first. The jammer can attempt to classify m by launching a ciphertext-only attack on C as early as the reception of the first ciphertext block. Because the encryption key is refreshed at every transmission, a very small number of ciphertext blocks are available for cryptanalysis. Appropriate selection of the key length s can prevent this type of attack. Note that s can be well below the cryptographic standards, due to the limited time available to the adversary (until the transmission is completed). For instance, a 56-bit long DES key is more than adequate for our purposes, since the fastest known brute force attack on DES takes almost a day. Other types of known attacks such as differential and linear cryptanalysis are not applicable, because they require the collection of a large number of chosen or known plaintext/ciphertext pairs . Even if the key for a particular packet is revealed to the adversary, packet classification is delayed until the end of C's transmission.

The application of the permutation function π1 distributes frame fields to ciphertext blocks in the reverse order of transmission, with the MSBs from each field appearing on the last ciphertext block. Hence, reception of all blocks of C is required for the complete recovery of headers. To minimize the communication overhead, k must be selected to be of the smallest length adequate for the protection of C, for the time required to transmit one packet. However, special care must be taken to withstand codebooks attacks on k. In such attacks, the adversary can encrypt a particular message of interest with all possible keys and construct a look-up table (codebook) of all possible ciphertexts. If the encryption of all possible messages with all possible keys results in unique ciphertexts, there is a 1-1correspondence between a ciphertext and the generating plaintext/key pair. This property is guaranteed with high probability when the plaintext space M and the key space K are much smaller than the ciphertext space C. Assuming the encryption of a plaintext block mi with a key ki randomly maps to a ciphertext ci = Eki (mi), every ciphertext ci ∈ C occurs with probability pc = 1 |C|. As an example, consider the encryption of a message m = {m1,m2, . . .mx} with a key k of length 56 bits, using blocks of 128 bits. For a fairly small plaintext space (e.g., |M| = 16), the probability of ciphertext uniqueness is equal to 99.8%.Thus, the adversary can recover k, by launching a codebook attack on m1. The remaining ci's are decrypted in real-time, using the known value of k. Here, the plaintext space for m1 is considered to be small because of the structure imposed by the static header of a packet (all fields of the header are known to the adversary). Randomization of the plaintext, ensures that all plaintexts are possible, thus equating the plaintext space with the ciphertext space.

VI. EVALUATION OF PACKET-HIDING TECHNIQUES

In this section, we evaluate the impact of our packet hiding techniques on the network performance via extensive simulations. We used the OPNETTM Modeler 14.5 to implement the hiding sublayer and measure its impact on the effective throughput of end-to-end connections and on the route discovery process in wireless ad-hoc networks. We chose a set of nodes running 802.11b at the PHY and MAC layers, AODV for route discovery, and TCP at the transport layer. Aside from our methods, we also implemented a simple MAC layer encryption with a static key.

6.1 Impact on Real-Time Systems

Our packet-hiding methods require the processing of each individual packet by the hiding sublayer. We emphasize that the incurred processing delay is acceptable, even for real-time applications. The SCHS requires the application of two permutations and one symmetric encryption at the sender, while the inverse operations have to be performed at the receiver. Such operations can be implemented in hardware very efficiently. Symmetric encryption such as AES can be implemented at speeds of tens of Gbps/s when realized with Application Specific Integrated Circuits (ASICs) or Field Programmable Gate Arrays (FPGAs) . These processing speeds are orders of magnitude higher than the transmission speeds of most current wireless technologies, and hence, do not impose a significant delay. Similarly, the AONT-HS performs linear operations on the packet that can be efficiently implemented in hardware. We note that a non-negligible processing delay is incurred by the CPHS. This is due to the cryptographic puzzle that must be solved at the receiver. As suggested in Section 6, CPHS should only be employed when the symbol size at the PHY layer is too small to support the SHCS and AONTHS solutions. The processing delays of the various schemes are taken into account in our experimental evaluations.

6.2 Experimental Evaluation

In the first set of experiments, we setup a single file transfer between a client and server, connected via a multi-hop route. The client requested a 1 MB file from the server.

VII. RELATED WORK

Jamming attacks on voice communications have been launched since the 1940s. In the context of digital communications, the jamming problem has been addressed under various threat models. We present a classification based on the selective nature of the adversary.

7.1 Prior Work on Selective Jamming

In, Thuente studied the impact of an external selective jammer who targets various control packets at the MAC layer. To perform packet classification, the adversary exploits inter-packet timing information to infer eminent packet transmissions. In, Law et al. proposed the estimation of the probability distribution of inter-packet transmission times for different packet types based on network traffic analysis. Future transmissions at various layers were predicted using estimated timing information. Using their model, the authors proposed selective jamming strategies for well known sensor network MAC protocols. Several researchers have suggested channel selective jamming attacks, in which the jammer targets the broadcast control channel. It was shown that such attacks reduce the required power for performing a DoS attack by several orders of magnitude . To protect control channel traffic, the replication of control transmission in multiple channels. The "locations" of the control channels where cryptographically protected. In, Lazos et al. proposed a randomized frequency hopping algorithm to protect the control channel from inside jammers. Strasser et al. proposed a frequency hopping anti-jamming technique that does not require the existence of a secret hopping sequence, shared between the communicating parties.

VIII. CONCLUSION

We addressed the problem of selective jamming attacks in wireless networks. We 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. 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. Our schemes combine cryptographic primitives such as commitment schemes, cryptographic puzzles, and all or nothing transformations (AONTs) with physical layer characteristics. We analyzed the security of our schemes and quantified their computational and communication overhead. Future we can gather the Jamming node information on the server where as, Here we have done on the client side. On gathering this jamming node information from the client to server side we can produce an effective path table to the client node to transfer the data.

REFERENCES

[1] 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.

[2] M. Cagalj, S. Capkun, and J.-P. Hubaux. Wormholebased antijamming techniques in sensor networks. IEEE Transactions on Mobile Computing, 6(1):100–114, 2007.

[3] A. Chan, X. Liu, G. Noubir, and B. Thapa. Control channel jamming: Resilience and identification of traitors. In Proceedings of ISIT, 2007.

[4] 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.

[5] Y. Desmedt. Broadcast anti-jamming systems. Computer Networks, 35(2-3):223–236, February 2001.

[6] K. Gaj and P. Chodowiec. FPGA and ASIC implementations of AES. Cryptographic Engineering, pages 235–294, 2009.

[7] O. Goldreich. Foundations of cryptography: Basic applications. Cambridge University Press, 2004.

[8] B. Greenstein, D. Mccoy, J. Pang, T. Kohno, S. Seshan, and D. Wether all. Improving wireless privacy with an identifier-free link layer protocol. In Proceedings of 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. In Proceedings of NDSS, pages 151–165, 1999.