ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Cryptographic Techniques to Prevent Jamming Attacks in Wireless Networks

G.Kiran Kumar
Associate Professor & HOD,
MLR Institute of Technology, Hyd.

T.Sreenidhi
B.Tech (CSE),
MLR Institute of Technology, Hyd.

M.Udayasree
B.Tech (CSE),
MLR Institute of Technology, Hyd.

B.Swapna
B.Tech (CSE),
MLR Institute of Technology, Hyd.

A.Prasad
B.Tech (CSE),
MLR Institute of Technology, Hyd.

G.Saketh
B.Tech (CSE),
MLR Institute of Technology, Hyd.

N.Sirisha
Associate Professor, Dept of CSE, MLR Institute of Technology, Hyd.

Abstract:
In this paper the problem of selective jamming attacks in wireless networks. In these attacks, the adversary selectively targets specific packets of "high" importance by exploiting his knowledge on the implementation details of network protocols at various layers of the protocol stack. We illustrate the impact of selective jamming on the network performance by illustrating various selective attacks against the TCP protocol. We show that such attacks can be launched by performing real-time packet classification at the physical layer. We examine the combination of cryptographic primitives with physical layer attributes for preventing real-time packet classification and neutralizing the inside knowledge of the attacker.

I. INTRODUCTION:

Wireless networks are susceptible to numerous security threats due to the open nature of the wireless medium. Anyone with a transceiver can eavesdrop on ongoing transmissions, inject spurious messages, or block the transmission of legitimate ones. One of the fundamental ways for degrading the network performance is by jamming wireless transmissions in the simplest form of jamming; the adversary corrupts transmitted messages by causing electromagnetic interference in the network's operational frequencies, and in proximity to the targeted receivers. For an adversary agnostic to the implementation details of the network, a typical jamming strategy is the continuous emission of high-power interference signals such as continuous wave tones, or FM modulated noise. However, adopting an "always-on" jamming 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 high interference levels makes this type of jamming easy to detect. Third, these attacks are easy to mitigate either by spread spectrum communications, spatial eats, or localization and removal of the jamming nodes. In this paper, we consider a sophisticated adversary model in which the adversary is aware of the implementation details of the network protocols. By exploiting this knowledge, the adversary launches selective jamming attacks in which it targets specific packets of "high" importance.

For example, jamming of TCP acknowledgments (ACKs) can severely degrade the throughput of a TCP connection due to the congestion control mechanism of the TCP protocol. Compared to continuous jamming, the adversary is active for a short period of time, thus expending orders of magnitude less energy. To perform selective jamming, the adversary must be capable of classifying transmitted packets in real time, and corrupting them before the end of their transmission. Packet classification can be performed by receiving just a few bytes of a packet, for example, by decoding the frame control field of a MAC-layer frame.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

We are interested in developing resource-efficient methods for preventing real-time packet classification and hence, mitigating selective jamming. Our contributions are summarized below.

A. Our Contributions

We investigate the feasibility of real-time packet classification for launching selective jamming attacks. We consider a sophisticated adversary who exploits his knowledge on net-work protocols along with secrets extracted from compromised nodes to maximize the impact of his attack. To mitigate selective jamming, we combine cryptographic mechanisms such as commitment schemes, cryptographic puzzles, and all-in-one transformations, with physical-layer parameters. We further study the impact of various selective jamming strategies on the performance of the TCP protocol.

The remainder of the paper is organized as follows. Section II, presents related work, In Section III, we describe the problem addressed, and state the system and adversarial model assumptions. In Section IV, we illustrate the feasibility of selective jamming attacks. In Section V, we develop methods for preventing selective jamming. Section VI, illustrates the impact of selective jamming on the performance of TCP. In Section VII, we conclude.

II. RELATED WORK

Continuous jamming has been used as a denial-of-service (DoS) attack against voice communication since the 1940s. Recently, several alternative jamming strategies have been demonstrated. Xu et. al. categorized jammers into four models, (a) a constant jammer that continuously emits noise, (b) a deceptive jammer that continuously broadcasts fabricated messages or replays old ones, (c) a random jammer that alternates between periods of continuous jamming and inactivity, and (d) a reactive jammer who jams only when transmission activity is detected. Intelligent attacks which target the transmission of specific packets were presented. Considered an attacker who infers eminent packet transmissions based on timing information at the MAC layer.

Law et. al. considered selective jamming attacks in multi-hop wireless networks, where future transmissions at one hop were inferred from prior transmissions in other hops. However, in both real-time packet classification was considered beyond the capabilities of the adversary. Selectivity was achieved via inference from the control messages already transmitted. Channel-selective jamming attacks were considered. It was shown that targeting the control channel reduces the required power for performing a DoS attack by several orders of magnitude. To protect control channel traffic, control information wasreplicated in multiple channels. The “locations” of the channels where control traffic was broadcasted at any given time, was cryptographically protected. We proposed a randomized frequency hopping algorithm, to protect the control channel inside jammers.

III.PROBLEM STATEMENT AND MODEL ASSUMPTIONS

A. Problem Statement

Consider the scenario depicted in Figure 1(a). Nodes A and B communicate over the wireless medium and a jamming node J is within communication range of both A and B. Node A transmits a packet m to B which is eavesdropped by node J. Node J is able to classify m by receiving only its first few bytes. J then corrupts m by interfering with its reception at B. We address the problems of (a) evaluating the ability of the adversary in classifying transmitted messages in real-time, and
(b) Developing resource-efficient mechanisms for preventing real-time packet classification.

B. System and Attacker Model

Network model–Our network consists of a collection of nodes connected via wireless links. Nodes may communicate directly, or over multiple hops. The nodes of the network can establish globally shared keys, either by manual preload, or via an online key distribution center.

Communication Model–Communication can be either broad-cast or uncast. Packets are transmitted at a rate of R bauds. Each symbol corresponds to q bits according to the underlying digital modulation scheme.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Here the transmission bit rate is equal to qRbps. To generalize our analysis, we do not consider any spreading of the data. However, our results hold even if data is spread to a wider spectrum according to any technique such as DSSS or FHSS. The preamble is used for synchronizing the sampling process at the receiver. The PHY header contains information regarding the length of the frame and the trans-mission rate. The MAC header contains information relevant to the MAC layer. In particular, the MAC header determines the MAC protocol version, the type of packet (management, con-trol, or data) and its subtype (e.g. association request/response, RTS, CTS, ACK, etc.), the source and destination addresses plus some additional fields regarding power management, security parameters, and information for future transmissions. The MAC header is followed by the frame body that contains higher layer information. Finally, the MAC frame is protected by a CRC code attached in the CRC field.

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. The adversary can operate in full-duplex mode, thus being able to receive and transmit concurrently. This can be achieved, for example, with the use of multiple radios. 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. The adversary is assumed to be computationally bounded, although he can be significantly more powerful than the network devices. Solving well-known hard cryptographic problems is assumed to be time-consuming. The implementation details of the network functions at every layer of the protocol stack are assumed to be public. For example, the adversary is aware of the digital modulation scheme, the error correction and detection schemes, the MAC, and routing protocol specifications, etc. Furthermore, the adversary is capable of physically compromising network devices and recovering stored information including crypto-graphic keys, pseudo-random (PRN) sequences, certificates, etc.

Hence, the adversary can decrypt any information encrypted with globally known keys, or jam communications protected by globally known PRN sequences.

IV. REAL-TIME PACKET CLASSIFICATION

In this section, we describe methods for real-time packet classification. Once a packet is classified, the adversary may choose to jam it depending on his strategy. Consider the communication system depicted in Figure 2. At the transmitter, a message m of length _ passes through a channel encoder and an interleaver before it is digitally modulated for transmission in the wireless channel. At the receiver, the received signal is demodulated, de-interleaved, and decoded before the original message m is recovered.

Several methods may be used for channel encoding. For example, a (n, k) block code can protect m from up to e errors per block. Alternatively, a/b convolutional encoder can be considered with a constraint length of Lmax, and a free distance of e bits. Interleaving is used to protect m from burst errors. For simplicity, consider a block inter-leaver of depth d that processes blocks of length n (in the case of convolution encoding, blocks of n bits do not correspond to code words). Finally, the digital modulator maps the bit stream into symbols to be transmitted over the wireless channel. Assume here that q bits are mapped to a single symbol.

To decode any data, the receiver must first collect $d \cdot n$ bits before it is able to de-interleave them. Once the received data is de-interleaved, it can be decoded using either block or convolution decoding. As an example, the 802.11 standard uses a convolution encoder of various rates to achieve different transmission speeds, with interleaving occurring per OFDM symbol. At the lowest rate of 6 Mbps, data is passed by a 12 -rate encoder before it is mapped to an OFDM symbol of 48 bits. In this case, decoding of one OFDM symbol provides 24 bits of data. At the highest data rate of 54 Mbps, 216 bits of data are recovered per OFDM symbol. Using the first few symbols, the adversary can obtain the header information for the transmitted packet and classify it accordingly.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

As an example, a MAC layer packet in the 802.11 standard can have a size up to = 2344 bytes with a header of 30 bytes. At a rate of 6 Mbps, 98 OFDM symbols are needed to complete the transmission of the entire packet (24 bits per symbol), while the header is contained in only 10 symbols. Note that the frame type and sub-type are contained in the first two bytes of the MAC frame. Hence, a MAC frame can be classified after the reception of the first OFDM symbol, following the physical layer preamble and header. The adversary has the opportunity to corrupt the remaining symbols to successfully jam a transmitted packet.

A typical method of combating jamming is by using spread spectrum (SS) communications. However, not all wire-less system are allocated sufficient bandwidth for spreading. Moreover, SS can prevent jamming only if the PRN sequence used to spread the signal is kept secret. For broadcast communications such as the transmission of control information, any PRN sequence must be known to all intended receivers. Our adversary model assumes that nodes can be physically compromised and secrets such as global PRN sequences are revealed to the adversary. In this case, SS alone cannot prevent the real-time packet classification and jamming.

An obvious solution to packet classification is the encryption of transmitted packets with a resource-efficient crypto-graphic mechanism such as symmetric key encryption. In this case, the entire packet has to be encrypted including headers (it is a standard practice to leave headers unencrypted, so that receivers can abort early the reception of packets not destined to them).

V. MITIGATION OF SELECTIVE JAMMING

In this section, we propose three schemes for countering selective jamming. Our goal is to transform a selective jammer to a random one. This can be achieved by overwhelming the adversary's computational ability to perform real-time packet classification. We first show that our problem can be mapped to the hiding property of commitment schemes.

A. Mapping to Commitment Schemes

Commitment schemes are fundamental cryptographic prim-itives that allow a committer P, commit to a value m to a verifier V while keeping mhidden. Initially, P provides V with a commitment C = commit (m, r), where commit is some commitment operation, and r is a random number. At a later stage, P can release additional information that reveals m. A scheme that does not allow the computation of m from C without additional information from P is called perfect or hiding, while a scheme that does not allow P to change m to a value m_ once C is released, is called binding.

In our context, the role of the committee is assumed by the transmitting node S. The role of the verifier V is assumed by any receiver R within the communication range of S, including the jammer J. Note that S has no particular interest in modifying m after he has committed to it, since its primary goal is to communicate m. However, satisfying the binding property ensures that, (a) only S can release information that reveals m, and (b) the only value that R can accept is m. To prevent selective jamming, S first transmits C that hides m from any receiver, including J. Once the transmission of is completed, S reveals additional information that "opens" c. Intended receivers are able to read m. We now provide a scheme that prevents packet classification based on the idea of commitments.

B. A Scheme Based on Commitments

Assume that S wants to communicate a message m ∈ {0, 1}lfor R. First, S selects a random key k ∈ {0, 1}q, where q is the number of bits mapped to a symbol at the physical layer. To utilize off-the-shelf encryption algorithms, k is expanded to k1 = f (k), where f :{0, 1}q → {0, 1}z is a public injective function, and z = |k1| is the length required by a block encryption mechanism such as DES or AES [16]. After the generation of k1, S generates the commitment value C = Ek1 (m), and broadcasts {C, hk1 (m||k)}, where hk1 () is a collision-resistant keyed one-way hash function. and|| denotes the concatenation operation. S chooses a new k for every transmission, ensuring the randomness

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

of C and hk1 (m||k) when the same m has to be transmitted. To "open" C, S releases the random key k. Upon reception of a k_, R computes k1_ = f (k _), and obtains m_ = Dk1 (C_). The integrity of the message (i.e., m_ = m) is verified by checking that hk1 (m_||k_) = hk1 (m||k). Upon verification, R obtains m_ = m. The proposed scheme is shown in Figure 3(a). To classify m, the jammer must be capable of obtaining any part of mbefore the end of the transmission of k. The classification can be initated as early as the reception of the first ciphertext block of C. For a packet of length l and a ciphertext block of size n, the available decryption time is td= sec, where R is the transmission rate in bauds. Assuming a key pool of size |K|, the adversary must be capable of performing on average N = |K| decryptions per second (on average, the decryption key will be found after |K|2 keys have been tried).

As an example, consider the 802.11a standard which achieves a rate of 6 Mbps rate using BPSK modulation, with 24 bits being mapped to a single OFDM symbol (i.eq = 24). There are 224 choices for k, hence |K| = 224. In the worst case scenario, a packetm of length l = 2344 bytes (maximum length at the MAC layer) has to be transmitted, providing the adversary with the longest time for finding k. To send a packet m, S transmits C (2344 bytes), hk(m||r) (20 bytes), and k (3 bytes). In total, the adversary has 0.393 msec to find k and classify m, before k is transmitted. Thus, the adversary must be capable of performing N = 2.13 × 10(10) decryptions per second. This number only increases for higher values of q.

C. A Scheme Based on Cryptographic Puzzles

Cryptographic puzzles involve the creation of problems that are solvable within a finite time interval tpwhich depends on the hardness of the puzzle and the computational ability of the solver. Such puzzles were first suggested by Merkle and have found various applications including the prevention of DoS attacks.
In our context, the idea of cryptographic puzzles is employed to overwhelm the computational ability of the adversary in classifying packets.

In essence, this is an implementation of a commitment scheme where the committer never reveals the information needed to open the commitment, but such information is obtained after solving a puzzle. The time required for solving a puzzle can be controlled by using time-lock puzzles [14]. Assume that S wants to broadcast a message m ∈ {0, 1}l. S generates a composite modulus n = p × q where p and q are two large random prime numbers. Then he computes φ(n) = (p − 1)(q − 1) and t = D ×T , where D is the number of squarings modulo n per second that a device can perform, and T is the time that it takes to solve the puzzle. S encrypts m with a randomly selected key, k ∈ {0, 1}s, using a conventional symmetric algorithm such as AES [16], getting Ek(m).

Then S chooses a random number a modulo n and computes Ck= k + a2t (mod n), that could be done efficiently by defining e = 2t (mod φ(n)) and computing Ck= k + ae (mod n). Finally, S transmits {n, a, t, Ek(m), Ck}. Receiver R has to compute b = a2t (mod n) to get k, and then m. Note that, without knowing p and q there is no efficient alternative to get b, but to perform the necessary squaring operations. A value of T equal to the transmission delay of Ckis sufficient to prevent the disclosure of any part of mbefore of the end of the transmission of CkIn this scheme, the transmission of {n, a, t, Ck}introduces a communication overhead of 40 bytes per packet (n, a, t are double numbers of 8 bytes, and Ckis a key of size 128 bits). As in the case of commitment schemes, to improve the efficiency of this scheme, we can use the same key to encrypt n consecutive data messages. In this case, the receiver only solves the puzzle once for every n data packets transmitted, and the delay is reduced by (n − 1) × T amount of time.

D. A Scheme Based on All-or-nothing Transformations

We now examine a solution based on All-Or-Nothing Trans-formations (AONT). Such transformations were originally proposed by Rivest to slow down brute force search attacks. An AONT serves as a publicly known and completely invertible pre-processing step to a plaintext, before it is passed to an ordinary block

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

encryption algorithm. The defining property of an AONT is that the entire output of the transformation must be known before the input can be computed. When combined with block encryption, all blocks of the cipher text must be decrypted to obtain any part of the plaintext, thus slowing down a brute force attack by a factor equal to the number of cipher text blocks.

VI. IMPACT OF SELECTIVE JAMMING ON TCP

In this section, we illustrate the impact of selective jamming attacks on the network performance. In particular, we implemented a selective jamming attack against a TCP connection established over a multi-hop wireless route. In our experiments, we used the OPNETTM Modeler 14.5 [1]. In the simulated scenario, a user requested a 106bytes file from a server node several hops away, and the TCP protocol was used to transport the requested file. At the MAC layer, the RTS/CTS mechanism for implementing virtual carrier sensing was enabled. The transmission rate was set to 11 Mbps. The jammer was placed within the proximity of one of the inter-mediate hops of the TCP connection. Four jamming strategies were considered: (a) selective jamming of data packets, (b) selective jamming of RTS messages, (c) selective jamming of CTS messages, and (d) selective jamming of cumulative TCP-ACKs. In all four strategies only a fraction p of the selected messages was jammed.

A. Performance Evaluation

In order to quantify the impact of selective jamming, we measured the application delay until the file transfer was completed. We also measured the average effective throughput of the TCP connection as the fraction of the file size over the time until the file transfer was completed. Finally, we measured the number of packets that the adversary blocked in each of the four jamming strategies. In Figure 4(a), we show the application delay as a function of the jamming probability p. In Figure 4(b), we show the average effective throughput of the TCP connection as a function of p. Finally, Figure 4(c) depicts the number of packets that were jammed by the adversary for each value of p.

We observe that for a TCP connection, a selective jamming attack against TCP ACKs is significantly more harmful and efficient than all other jamming strategies. By jamming 40% of TCP ACKs, the application delay is one order of magnitude larger compared to jamming just data, and two orders of magnitude larger than jamming RTS or CTS messages at the MAC layer. Moreover, for values of p larger than 0.4, the TCP connection was aborded due to the repeated timeout of the sender.

VII. CONCLUSION

We addressed the problem of selective jamming in wireless networks. We illustrated the effectiveness of selective jamming attacks by implementing such attacks against the TCP proto-col. We showed that an adversary can exploit its knowledge of the protocol implementation to increase the impact of his attack at a significantly lower energy cost. We illustrated the feasibility of selective jamming attacks by performing real-time packet classification. To mitigate selective jamming, we proposed several methods that combine cryptographic primitives such as commitment schemes, cryptographic puzzles, and all-or-nothing transformations with physical layer attributes.

REFERENCES

[1]OPNET tmmodeler 14.5. http://www.opnet.com/solutions/networkrd/modeler.html.

[2]IEEE 802.11 standard. http://standards.ieee.org/getieee802/download/ 802.11-2007.pdf, 2007.

[3] A. Al Hanbali, E. Altman, and P. Nain. A survey of tcp over ad hoc networks. IEEE Communications Surveys & Tutorials, 7(3):22–36, 2005.

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

[5]D. Comer. Internetworking with TCP/IP: principles, protocols, and architecture. Prentice Hall, 2006.

[6]I.Damgard. Commitment schemes and zero-knowledge protocols. Lecture notes in computer science, 1561:63–86, 1999.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[7] A. Juels and J. Brainard. Client puzzles: A cryptographic countermea-sure against connection depletion attacks. In Proceedings of the Network and Distributed System Security Symposium, pages 151–165, 1999.

[8] Y. W. Law, M. Palaniswami, L. V. Hoesel, J. Doumen, P. Hartel, and P. Havinga. Energy-efficient link-layer jamming attacks against WSN MAC protocols. ACM Transactions on Sensor Networks, 5(1):1–38, 2009.

[9] L. Lazos, S. Liu, and M. Krunz.Mitigating control-channel jamming attacks in multi-channel ad hoc networks. In Proceedings of the second ACM conference on wireless network security, pages 169–180, 2009.

[10] R. C. Merkle. Secure communications over insecure channels. Com-munincations of the ACM, 21(4):294–299, 1978.