Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 4, April 2013, pg.238 – 241

RESEARCH ARTICLE

Encryption of Data to Prevent Jamming Attacks

N. Abirami[1], R. Jeeva[2], L. Revathi[3], U. Safiya[4], Mrs. E. Baby Anitha[5]
[1,2,3,4]Department of Computer Science and Engineering, Anna University Chennai, India
[5]Assistant Professor, Department Of Computer Science and Engineering,
K.S.R. College Of Engineering, Tiruchengode, India

[1] abiksrce@gmail.com; [2] k.keeva57@gmail.com; [3] revathi11.ksrce@gmail.com; [4] safiyausman@gmail.com

Abstract— ***In this paper, 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 that 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. We analyze the security of our methods and evaluate their computational and communication overhead.***

Key Terms: - Selective Jamming; Denial-of-Service; Wireless Networks; Packet Classification

I. INTRODUCTION

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. We investigate the feasibility of realtime packet classification for launching selective jamming attacks, under an internal threat model. We show that such attacks are relatively easy to actualize by exploiting knowledge of network protocols and cryptographic primitives extracted from compromised node.

II. BACKGROUND

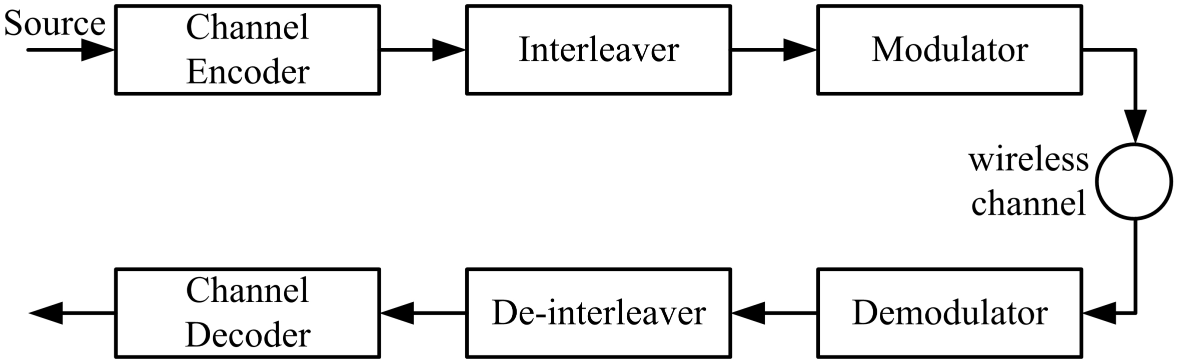
Jamming attacks are much harder to counter and more security problems. They have been shown to actualize severe Denial-of-Service (DoS) attacks against wireless networks. In the simplest form of jamming, the adversary interferes with the reception of messages by transmitting a continuous jamming signal, or several short jamming pulses 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. The nodes to be operate in the conventional relay mode and a number of intermediate nodes to be transmitted the signal.

III. LITERATURE REVIEW

Thuente and Acharya studied the impact of an external selective jammer who targets various control packets at the MAC layer. To perform packet classification, the adversary exploits interpacket timing information to infer eminent packet transmissions. In [11], Law et al. proposed the estimation of the probability distribution of interpacket 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.

IV. REAL TIME PACKET CLASSIFICATION

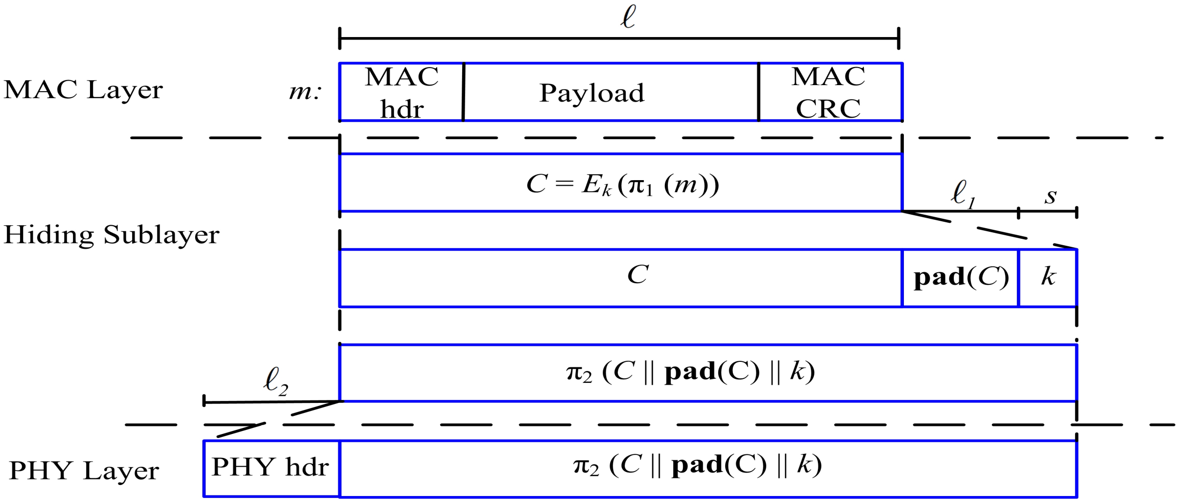
At the Physical layer, a packet m is encoded, interleaved, and modulated before it is transmitted over the wireless channel. At the receiver, the signal is demodulated, deinterleaved and decoded to recover the original packet m. Nodes A and B communicate via a wireless link. Within the communication 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. Consider the generic communication system depicted in Fig. 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, deinterleaved, and decoded, to recover the original packet m.



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.

V. STRONG HIDING COMMITMENT SCHEME (SHCS)

We propose a strong hiding commitment scheme (SHCS), 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.



The computation overhead of SHCS is one symmetric encryption at the sender and one symmetric decryption at the receiver. Because the header information is permuted as a trailer and encrypted, all receivers in the vicinity of a sender must receive the entire packet and decrypt it, before the packet type and destination can be determined. However, in wireless protocols such as 802.11, the complete packet is received at the MAC layer before it is decided if the packet must be discarded or be further processed. If some parts of the MAC header are deemed not to be useful information to the jammer, they can remain unencrypted in the header of the packet, thus\ avoiding the decryption operation at the receiver. 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.

VI. Cryptographic Puzzle Hiding Scheme

A sender S has 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. Cryptographic Puzzle includes two types of scheme.

1. Time-lock Puzzles
2. Puzzles based on hashing

Time-lock Puzzles proposed a construction called *time-lock puzzles,* which is based on the iterative application of a precisely controlled number of modulo operations. Time-lock puzzles have several attractive features such as the fine granularity in controlling tp and the sequential nature of the computation. Moreover, the

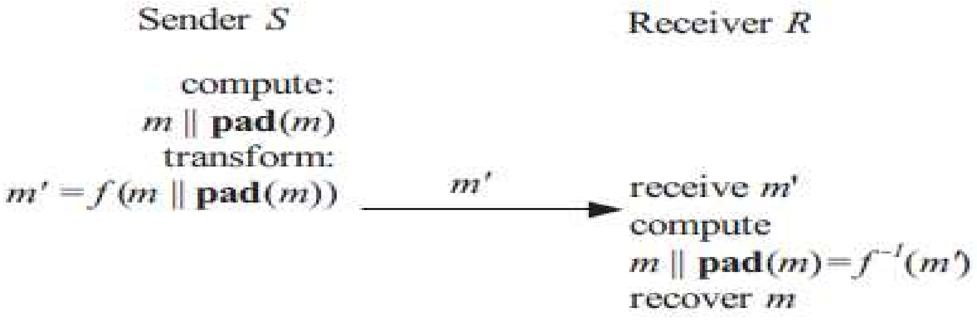
Puzzle generation requires significantly less computation compared to puzzle solving. Computationally limited receivers can incur significant delay and energy consumption when dealing with modulo arithmetic. In this case, CPHS can be implemented from cryptographic puzzles which employ computationally efficient cryptographic primitives. Client puzzles proposed in, use one-way hash functions with partially disclosed inputs to force puzzle solvers search through a space of a precisely controlled size. In our context, the sender picks a random key k with k = k1||k2. The lengths of k1 and k2 are s1, and s2, respectively.

He then computes C = Ek(π1(m)) and transmits (C, k1, h(k)) in this particular order. To obtain k, any receiver has to perform

On average 2s2−1 hash operations (assuming perfect hash functions). Because the puzzle cannot be solved before h (k) has been received, the adversary cannot classify m before the completion of m’s transmission.

VII. All-or-Nothing Scheme

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. The 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. We propose a solution based on All-Or- Nothing Transformations (AONT) that introduces a modest communication and computation overhead. Such transformations were originally proposed by Rivest to slow down brute force attacks against block encryption algorithms. An AONT serves as a publicly known and completely invertible pre-processing step to a plaintext before it is passed to an ordinary block encryption algorithm.


Sender S
Receiver R
compute:
$m \,||\, \mathbf{pad}(m)$
transform:
$m' = f(m \,||\, \mathbf{pad}(m))$
m'
receive m'
compute
$m \,||\, \mathbf{pad}(m) = f^{-1}(m')$
recover m

The AONT-based Hiding Scheme (AONT-HS).

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.

References

[1] Alejandro Proano and Loukas Lazos. Packet-Hiding Methods for Preventing Selective Jamming Attacks. IEEE Transactions on Dependable and Secure Computing, VOL.9, NO.1,JAN-FEB 2012.

[2] B.Thapa,G.Noubir,R.Rajaramanand, and B.Sheng. On the robustness of IEEE802.11 rate adaptation algorithms against smart jamming.In Proceedings of WiSec,2011.

[3] Y.Liu,P.Ning,H.Dai,and A.Liu.Randomized differential DSSS: jamming-Resistant wireless broadcast communication. In Proceedings of INFOCOM,San Diego, 2010.

[4] M. Wilhelm, I. Martinovic, J. Schmitt, and V. Lenders. Reactive jamming in wireless networks: How realistic is the threat? In Proceedings of WiSec, 2011

[5] P. Tague, M. Li, and R. Poovendran. Mitigation of control channel jamming under node capture attacks. IEEE Transactions on Mobile Computing, 8(9):1221–1234, 2009.

[6] M. Wilhelm, I. Martinovic, J. Schmitt, and V. Lenders. Reactive jamming in wireless networks: How ealistic is the threat? In Proceedings of WiSec, 2011.