# Packet-Hiding Methods for Preventing Selective Jamming Attacks

Pratik Kharwadkar, Vaishnav Dhore , Piyush Tagade, Abhijeet Dalvi

*Department of Computer Engineering,SIT Lonavala*

pra.kharwadkar@gmail.com
vaishnavdhore@yahoo.com
piyush.tagade1@gmail.com
meetabhidalvi@gmail.com

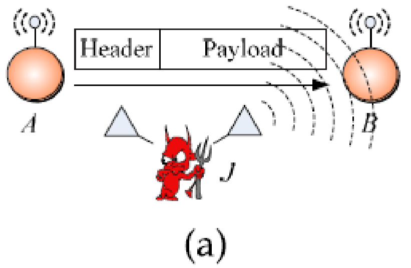
***Abstract***- The Wireless medium due to its open nature is vulnerable to intentional interference attacks, typically referred to as jamming. Jamming is one of many exploits used compromise the wireless environment. It works by denying service to authorized users as legitimate traffic is jammed by the overwhelming frequencies of illegitimate traffic. If an attacker truly wanted to compromise your LAN and wireless security, the most effective approach would be to send random unauthenticated packets to every wireless station in the network. To minimize the impact of an unintentional disruption, it is important the identify its presence. Jamming makes itself known at the physical layer of the network, more commonly known as the MAC (Media Access Control) layer. The increased noise floor results in a faltered noise-to-signal ratio, which will be indicated at the client. It may also be measurable from the access point where network management features should able to effectively report noise floor levels that exceed a predetermined threshold. From there the access points must be dynamically reconfigured to transmit channel in reaction to the disruption as identified by changes at the physical layer.

## 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 make this type of jamming easy to detect . Third, these attacks are easy to mitigate either by spread spectrum communications , spatial retreats 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 [3]. 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. We are interested in developing *resource efficient* methods for preventing real-time packet classification and hence, mitigating selective jamming. Our contributions are summarized below.

## II. PROBLEM STATEMENT

Previous research had found that jammers influence the performance of WLAN networks. However, most research could not demonstrate how different jammers and changed characteristics vary the result of jamming attacks. Jammers disturb networks in different situations in order to achieve various jamming effects. Also, because of the mobility of the WLAN, users cannot be simulated by only using a fixed node or a specific trajectory. Random trajectories in both nodes and jammers have to be considered a real world simulation Scenario. Finally, most esearch used single ad-hoc routing protocols in the network. A comparison of multiple routing protocols needs to be simulated.



. (a) Realization of a selective jamming attack.

## III. EXISTING SYSTEM

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 highpower interference signals.

## IV. IMPLEMENTATION

Continuous jamming has been used as a denial-of-service (DoS) attack against voice communication since the 1940s . Re cently, several alternative jamming strategies have been demonstrated . 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 in Thuente considered an attacker who infers eminent packet transmissions based on timing information at the MAC layer.

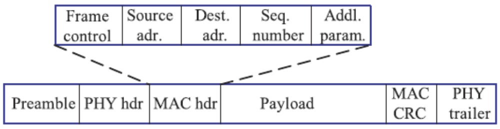
## V. MODULE DESCRIPTIONS

### *A. Network Model*

We address the problem of preventing the jamming node from classifying m in real time, thus mitigating J's ability to perform selective jamming. 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 preshared pairwise keys or asymmetric cryptography.

### *B. 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 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 _ _ 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. 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.



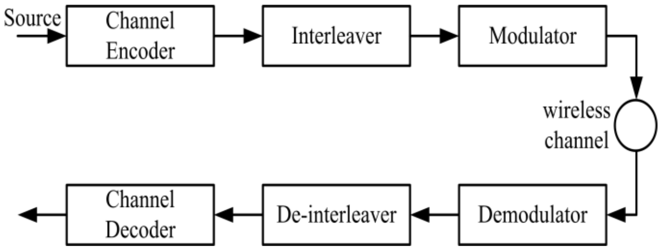
A generic frame format for a wireless network.

### *C. 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 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 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, where network devices may operate unattended, thus being susceptible to physical compromise.

## VI. ARCHITECTURE

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.



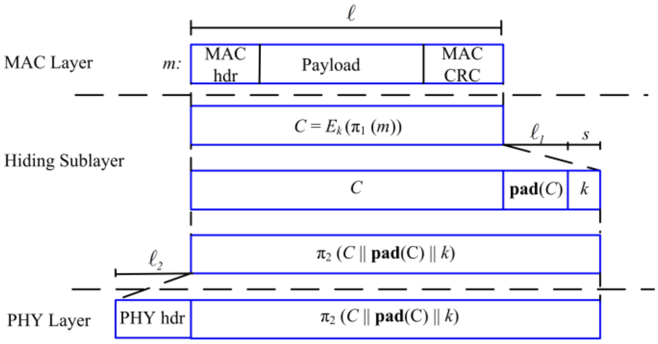
Moreover, even if the encryption key of a hiding scheme were to remain secret, the static portions of a transmitted packet could potentially lead to packet classification. This is because for computationally-efficient encryption methods such as block encryption, the encryption of a prefix plaintext with 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.

## VII. SELECTIVE JAMMING MODULE

We illustrate the impact of selective jamming attacks on the network performance. 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.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.

## VIII. STRONG HIDING COMMITMENT SCHEME (SHCS)

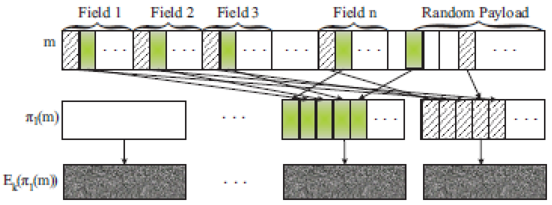
We propose a strong hiding commitment scheme (SHCS), which is based on symmetric cryptography. Our main motivation is to satisfy the strong hiding property while keeping the computation and communication overhead to a minimum.



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.

## IX. CRYPTOGRAPHIC PUZZLE HIDING SCHEME (CPHS)

Here 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 pre-defined 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 puzzlebased scheme is that its security does not rely on the PHY layer parameters. However, it has higher computation and communication overhead. We consider several puzzle schemes as the basis for CPHS. For each scheme, we analyze the implementation details which impact security and performance. Cryptographic puzzles are primitives originally suggested by Merkle as a method for establishing a secret over an insecure channel. They find a wide range of applications from preventing DoS attacks to providing broadcast authentication and key escrow schemes.



Application of permutation $\pi_1$ on packet $m$.

## X. PROPOSED SYSTEM

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

## XI. CONCLUSION

In this approach we have addressed and implemented the problem of selective jamming attacks in wireless networks. We have used 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 have implemented that the first few bytes can be decoded by jammer during ongoing transmission.We have judeded the TCP and routing protocol impacted by selective jamming attacks .Our findings show that a selective jammer can significantly impact performance with very low effort. We developed the schemes that transform a selective jammer by preventing real-time packet classification. Our schemes combine cryptographic primitives such as commitment schemes, cryptographic puzzles,all-or-nothing transformations (AONTs) and Diffie Hellman algorithm with physical layer characteristics. We analyzed the security of our schemes and quantified their computational and communication overhead.

## ACKNOWLEDGEMENT

We express our hearty gratitude towards our guide Prof. A.M.Kanthe, Head of Computer Department Prof. T.J.Parvat and Principal Dr.M.S.Gaikwad of S.I.T. Lonavala for guiding us to understand the work conceptually and also for their constant encouragement.

## 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. Wormhole-based 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. Wetherall. Improving wireless privacy with an identifier-free link layer protocol. In Proceedings of MobiSys, 2008.
[9]IEEE.IEEE802.11standard.
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.