Packet-Hiding Methods for Preventing Selective Jamming Attacks

[1,]Ashish Kumar, [2,]Sachin Kumar Gupta, [4,]Shubham Singh

[1,2,3,4,]Department of Information Technology , Institute Of Technology And Management , AL-1 Sector-7 Gida , Gorakhpur

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 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.

Keywords – Selective Jamming, Denial of Service, Wireless Network , Packet Classification .

I. INTRODUCTION

Wireless Local Area Networks (WLANs) are becoming an increasingly important technology that is bringing the world closer together. WLANs are used in every area, such as education, agriculture, pharmaceuticals, manufacturing, transportation, military, and research. Therefore, the importance of WLAN security is significant. There are two popular styles of WLANs: client-server networks and ad-hoc networks. The difference between these two networks is that client-server networks use access points or routers to transmit data, but ad-hoc networks do not rely on any pre-existing transmitters. Instead, all the nodes in an ad-hoc network participate in the routing process by forwarding messages to each other. According to The Institute of Electrical and Electronics Engineers (IEEE) 802.11g standards (IEEE Org., 2012), all wireless network nodes transmit data packets in different channels. Since channels in WLANs are defined by frequencies, they are susceptible to malicious jamming attacks. It is easy for attackers to accomplish sending multitudes of useless packets in a specific frequency. Jamming attacks attempt to make the system crash by flooding it with useless traffic, and use all the resources in the network so users in the network cannot connect to the system. It is consistently used by hackers to break network systems, because of ease and security issues. In this thesis, client-server networks and ad-hoc networks were simulated by using the simulation tool OPNET Modeler (OPNET Technologies, Inc., 2012). During the simulation, factors that may influence the result of the simulation were taken into consideration such as the distance, power level, and protocols used in ad-hoc networks.

1.1 Statement Of The Problem

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.

1.2 Significance of the Study

It is worth mentioning that the work presented here contributes several issues relevant in the field of jamming attacks in WLAN. First this thesis had provided a better understanding of jamming behavior in WLANs. Multiple experiments had shown a comparison of different jammer performances. Second, this thesis demonstrated the use of different jammers in various environments, including the feasibility of switching channels to avoid jamming attacks. Third, it also provided a way to simulate random trajectory jamming attacks, and used it to simulate and compare the performance of multiple ad-hoc routing protocols.

2. LITERATURE SURVEY

In this Chapter, references of previous research that utilized the concepts in Introduction are introduced. For each of the concepts, an overview of related literature is provided. In section 2.1, WLAN is introduced. Specifically, client-server and ad-hoc networks are explained. In section 2.2, DoS attacks, especially jamming attacks are presented. In Section 2.3, detection methods of jamming attacks are analyzed. Section 2.4 examines the simulation tools that can be used to simulate networks. In section 2.5, the simulation tool OPNET Modeler which is used in this thesis is introduced. Finally, in section 2.6, ad-hoc routing protocols are presented.

WLAN – Client-Server & Ad-Hoc Network.

2.1 WLAN – Client-Server & Ad-Hoc Network

Because WLAN provides users the mobility to move around within a local area without a wire and still connect to the network, it is widely used in many important areas. Banks, governments, corporations, and institutions transmit highly important data through WLANs. The security problems of WLANs become important for the users.Most WLANs are based on the IEEE 802.11 standard, which transmits data in different channels based on frequencies. Due to the ease of installation and convenience, WLAN is regularly used in daily life. An introduction of WLANs was done by Gast (2005) and Mark (2005). They presented basic wireless LAN technology, why the technology had emerged, how it works, the architecture of WLANs, and the types of WLANs.Because of the popularity of WLANs, security research must be done in various types of WLANs. Experiments were done by Varadarajan , Kumar, and Reddy (2011) about improving WLAN performance under DoS attacks. DoS attacks on the physical layer were analyzed and expanded to the security of the physical layer of the sensor network model. This research was done by using the ant system. By using Receiver Operating Characteristics (ROC) on nodes, DoS 8 attacks can be predicted by formulating the classification of jammers under various attack scenarios. This approach can help improving detecting DoS attacks in WLANs.Research in this thesis was focuses on two types of WLANs: client-server and ad-hoc networks.

2.2 Jamming Attacks

The DNS is a hierarchical tree structure whose root node is known as the root domain. A label in a DNS name directly corresponds with a node in the DNS tree structure. A label is an alphanumeric string that uniquely identifies that node from its brothers. Labels are connected together with a dot notation, ".", and a DNS name containing multiple labels represents its path along the tree to the root. Labels are written from left to right. Only one zero length label is allowed and is reserved for the root of the tree. This is commonly referred to as the root zone. Due to the root label being zero length, all FQDNs end in a dot [RFC 1034].A study into DoS attacks and defense was done by Raymond and Midkiff (2008). Since WSNs are used in monitoring medical uses, homeland security, industrial automation, and military applications, security of WSNs must be guaranteed. Defeating many threats of DoS attacks on WSNs can be done by encryption and authentication, but some other techniques still need to be found to prevent from special DoS attacks, especially Denial of Sleep attacks, which are still critical threats in WSNs.

2.3 Detection of Jamming

WLANs are built upon a shared medium that makes it easy to launch jamming attacks. These attacks can be easily accomplished by sending radio frequency signals that do not follow any MAC protocols. Detection of jamming attacks can be done in multiple ways. One of the most efficient ways is to jump channels. Because communication between two legitimate nodes is done through a specific frequency, the frequency can be changed if necessary. While a jammer is attacking the wireless network, there are other effective ways to continue legitimate communication in the network. Engaging the jammer on the jammed channel and continuing communication in another channel was introduced by Beg, Ahsan, and Mohsin (2010). When the nodes detected the jamming in the wireless network, they jumped to another channel to continue legitimate communication. In the experiments, both 10 and 20 nodes experiments were done, and in both scenarios, after channels were jumped, the network resumes communications as normal. In both scenarios, the amount of packets dropped reduced immediately. The research concluded that channel jumping will decrease the throughput of the network. Also, it was easier to detect jamming through intermitted channel jumping. Concluded, channel jumping was a superior method of combating network interference, rather than changing network protocols (Jeung, Jeong, and Lim, 2011).The research concluded that channel jumping will decrease the throughput of the network. Also, it was easier to detect jamming through intermitted channel jumping. Concluded, channel jumping was a superior method of combating network interference, rather than changing network protocols (Jeung, Jeong, and Lim, 2011).In order to prevent from multi-channel jamming attacks, a cross-layer jamming detection method was developed (Chiang and Hu, 2011). Cross-layer jamming detection is a tree-based approach. A jamming detection algorithm was utilized in all legitimate nodes; when the communication process began, all the nodes had the ability to report jamming attacks in different layers, and only the reports which were generated by nodes with jamming detection algorithm were accepted by the system in order to avoid error. Research was also done about multi-channel jamming attacks by Jiang and Xue (2010). The difference from the jamming detection algorithm was that it focused on network restoration and design of traffic rerouting.

2.5 Algorithm

1. Symmetric encryption algorithm
2. Brute force attacks against block encryption algorithms.

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

Algorithm Description

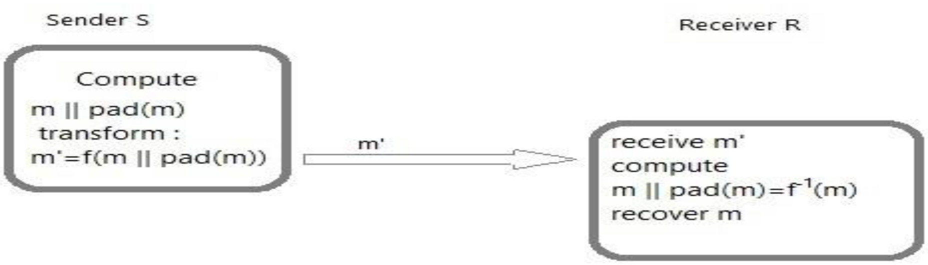


fig-2.5 :The AONT-based Hiding Scheme (AONT-HS)

The Package Transform- In the package transform ,given a message m, and a random key k′, the output pseudo-messages are computed as follows:–

$$m'_i = m_i \oplus E_{k'} (i) \text{ , for } i=1,2,3……..,x$$

$$m'_{x+1} = k' \oplus e_1 \oplus e_2 \oplus e_3 \oplus ………… \oplus e_x \text{ ,}$$

Where $e_i = E_{k0} (m'_i \oplus i)$, for i = 1, 2, . . . , x, and k0 is a fixed publicly-known encryption key. With the reception of all pseudo-messages message m is recovered as follows:

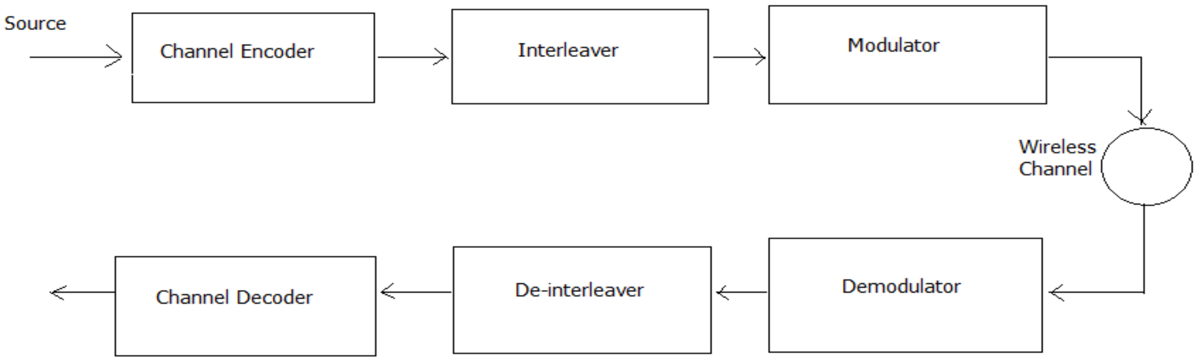
$$k' = m'_{x+1} \oplus e_1 \oplus e_2 \oplus e_3 \oplus ………… \oplus e_x \text{ ,}$$

$$m_i = m'_i \oplus E_{k'} (i) \text{ , for } i=1,2,3……..,x,$$

Note that if any m'_i is unknown, any value of k′ is possible, because the corresponding e_i is not known. Hence, $E_{k'}$ (i) cannot be recovered for any i, making it infeasible to obtain any of the m_i .

Hiding Sublayer Details- AONT-HS is implemented at the hiding sublayer residing between the MAC and the PHY layers. In the first step, m is padded by applying function pad() to adjust the frame length so that no padding is needed at the PHY layer, and the length of m becomes a multiple of the length of the pseudo-messages m′ i. This will ensure that all bits of the transmitted packet are part of the AONT. In the next step, m||pad(m) is partitioned to x blocks, and the AONT f is applied. Message m′ is delivered to the PHY layer. At the receiver, the inverse transformation f−1 is applied to obtain m||pad(m). The padded bits are removed and the original message m is recovered. The steps of AONT-HS are shown in Fig. 2.5.

3. ARCHITECTURE



4. PROBLEM FORMULATION

4.1 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.

4.2 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.

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.

5. MODULES

1. Network module
2. Real Time Packet Classification
3. Selective Jamming Module
4. Strong Hiding Commitment Scheme (SHCS)
5. Cryptographic Puzzle Hiding Scheme (CPHS)

Module Descriptions

6. Network module

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 pre shared pair wise keys or asymmetric cryptography.

7. Real Time Packet Classification

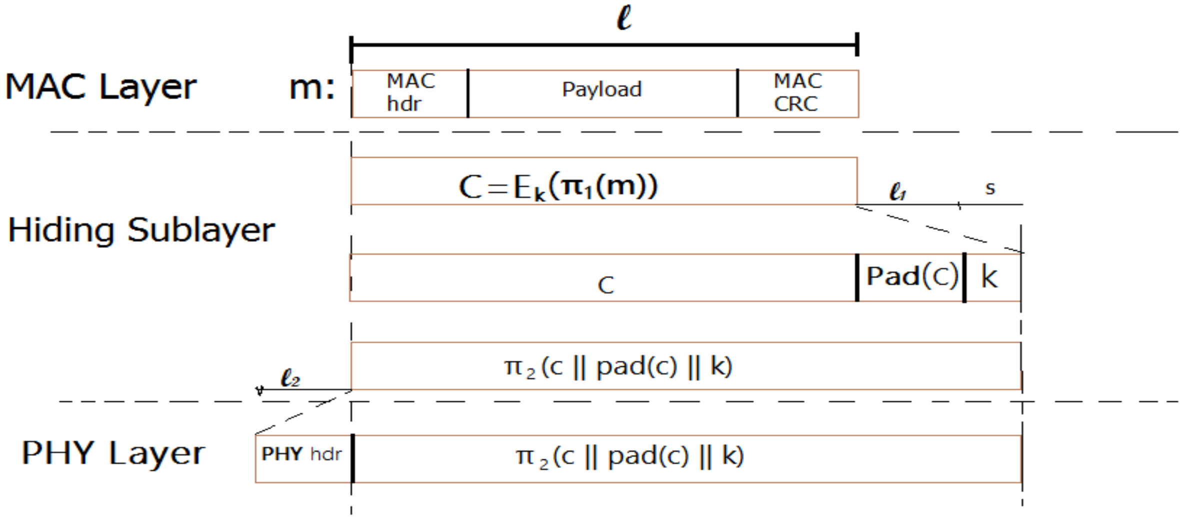
Consider the generic communication system depicted in Fig. At the PHY layer, a packet m is encoded, interleaved, and modulated before it is transmitted over the wireless channel. At the receiver, the signal is demodulated, deinterleaved, and decoded, to recover the original packet. Moreover, even if 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 cipher text prefix. Hence, an adversary who is aware of the underlying protocol specifics (structure of the frame) can use the static cipher text portions of a transmitted packet to classify it.

8. 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 cipher text block.

9. 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.

10. Cryptographic Puzzle Hiding Scheme (Cphs)

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 puzzle based 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.

11. 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.

12. Acknowledgements

This work is supported by BBN Technologies and the Air Force. The authors thank Dan Coffin and Jeff Ward for the many conversations in developing this paper and the helpful comments of the anonymous reviewers. Jesse James is currently with the Air Force.

REFERENCES

Journal Papers:

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

[3] W. Xu, W. Trappe, Y. Zhang, and T.Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In Proceedings of MobiHoc, pages 46–57, 2005.

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

[5] Akyildiz, I. F., Wang, W., & Wang, W. (2005, January). Wireless mesh networks: a survey. Computer Networks Journal, 47(4), 445-487.

[6] D. Stinson. Cryptography: theory and practice. CRC press, 2006.

[7] Eriksson, J. and Koivunen, V.: Identi¯ability, separability, and uniqueness of linear ica models. IEEE Signal Processing Letters, 11(7), July 2004.

[8] 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.