Packet-Hiding Methods for Preventing Selective Jamming Attacks

Guttula Pavani

Abstract— The open nature of the wireless medium leaves it weak to intentional interference attacks, typically referred to jamming. The intentional interference with wireless transmission can be worn as a launch pad for increasing Denial-of-Service attack on wireless networks. In general, jamming has been addressed under an external threat model. However, adversary with internal knowledge of protocol condition and network secrets can start low-effort jamming attacks that are hard to detect and counter. In this work, we deal with the problem of selective jamming attacks in wireless networks. In these attacks, the adversary is vigorous only for a short period of time, selectively targeting messages of high importance. We demonstrate the advantages of selective jamming within network performance deprivation and adversary effort by presents two case studies; a selective attack on TCP and one on routing. We show that selective jamming attacks can be launch by performing real-time packet classification at the physical layer. To diminish these attacks, we develop 3 schemes that avoid real-time packet classification by combining cryptographic primitives with physical-layer attributes. We examine the security of our methods and evaluate their computational and communication overhead.

Index Terms— cryptographic, Denial-of-Service attacks, physical layer, selective jamming attacks

1. INTRODUCTION

Wireless networks be dependent on the unobstructed availability of the wireless medium to interconnect participating nodes. However, the open nature of this medium leaves it vulnerable to multiple security threats. Any of one with a transceiver can monitor on wireless transmissions, inject illegitimate messages, or jam legitimate ones. While monitoring and message injection can be stop using cryptographic methods, jamming attacks are much difficult to counter. They have been shown what is actually attacks (Denial of Service attacks) against wireless networks. In the easiest form of jamming, the conflict interferes with the process of receiving of messages by transferring a continuous jamming signal, or several short jamming pulses. Typically, jamming attacks have been analyzed under an external bug model, in which the jammer is not part of the system network. In this model, jamming scheme include the constant or random transmission of huge power interference signals. However, method of "always-on" strategy has several disadvantages. First, the adversary has to expend a considerable amount of energy to struck frequency bands of interest. Second, the frequent presence of unusually high interference stages makes this type of attacks easy to detect. Conventional anti-jamming techniques dependent on extensively on spread spectrum communications, or some form of jamming avoidance (e.g., slow frequency hopping). Spread Spectrum techniques gives bit-level protection by expanding bits as stated to a secret pseudo noise code, known only to the communicating (each other) parties. These scheme can only protect wireless transmissions under the external bug model. Potential disclosure of secrets due to hub compromise neutralizes the gains of Spread Spectrum. Broadcast communications are particularly open to attack under an internal bug model because all intentional receivers must be knowing of the secrets used to protect transmissions. Hence, the compromise of a one receiver is sufficient to reveal relevant cryptographic data. In this
Analyzes, we are address the issue of jamming under an internal threat model. We consider an elegant adversary who is knowing of network secrets and the enhancement details of network protocols at any of the layer in the network bucket. The adversary exploits his internal skill for launching selective jamming attacks in which particular messages of "great importance" are targeted. For example, a jammer can target route request or route reply messages at the layer of routing to stop route discovery, or target Transmission Control Protocol acceptance in a Transmission Control Protocol session to severely reduce 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 method can be actualized either by classifying transmitted packets using protocol semantics, or by decoding packets on the fly. In the after method, the jammer may decode the first few bits of a packet for recovering needful packet identifiers like packet type, source and destination address. After division, the conflict must induce a required number of bit errors so that the packet cannot be recovered at the receiver. The Selective jamming wants an intimate skill of the physical layer, as well as particulars of the upper layers.

2. ANALYSIS

Jamming attack is much harder to counter and more security problems. They have been shown to actualize

- *Guttula Pavani is currently pursuing master's degree program in computer science engineering in Grandhi Vara Lakshmi Venkata Rao Institute of Technology,JNTU Kakinada University, India, PH-9493039220. E-mail: pavani0518@gmail.com*

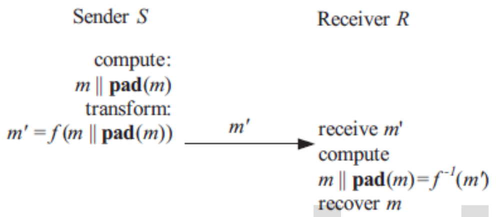
severe Denial-of-Service (DoS) attack against wireless networks. In simplest form of jamming, the adversary interferes with the reception of messages by transmit a continuous jamming signal, or several short jamming pulses jamming attacks have been measured under an exterior threat model, in which jammer is not part of network. Under this model, jamming strategy include the continuous or random transmission of high power interfering signals.

3. RELATED WORK

Algorithm

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

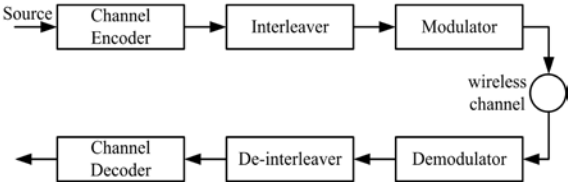
Algorithm Description

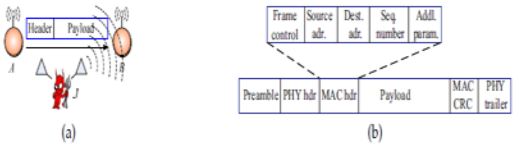

Sender S
Receiver R
compute:
$m \,||\, \mathbf{pad}(m)$
transform:
$m' = f(m \,||\, \mathbf{pad}(m))$
m'
receive m'
compute
$m \,||\, \mathbf{pad}(m) = f^{-1}(m')$
recover m

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

We suggest a solution depends on All -Or- zero Transformations (AONT) that introduces a modest communication and computation overhead. Such transformations were initially proposed by Rivest to slow down brute force attack against block encryption algorithms. An AONT serves as publicly known and completely invertible pre-processing step to plaintext before it is accepted to an ordinary block encryption algorithm.

Architecture





(a) Realization of a selective jamming attack, (b) a generic frame format for a wireless network.

4. PROPOSED METHODOLOGY

In this paper, we handle the problem of jamming beneath an internal threat model. We consider a sophisticated adversary who is conscious of network secrets and the execution details of network protocols at any layer in the network stack. The adversary exploits his internal knowledge for beginning selective jamming attacks in which specific messages of "high importance" are targeted. for instance, a jammer can target route-request/route-reply messages at the routing layer to avoid route discovery, or target TCP acknowledgments in a TCP session to severely degrade the throughput of an end-to-end flow.

To initiate selective jamming attacks, the adversary must be capable of implementing a "classify-then-jam" strategy before the finishing point of wireless transmission. Such strategy can be actualized either by classifying transmitted packets by means of protocol semantics, or by decoding packets on the fly. In latter method, the jammer might decode the first few bits of a packet for improving helpful packet identifiers such as packet type, source and destination address. After taxonomy, 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 layer, as well as of the specifics of upper layers.

5. EXPERIMENTAL RESULTS

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

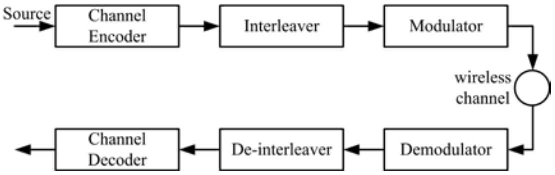
5.1 Network module

We deal with the problem of preventing the jamming node from classifying m in real time, thus justifying J's ability to achieve selective jamming.

The network consists of a collection of nodes connected via wireless links. Nodes can communicate directly if they are within communication range, or indirectly via multiple hops. Both nodes communicate in unicast mode and broadcast mode. Interactions can be either unencrypted or encrypted. For encrypted broadcast communications, symmetric keys are shared among all intentional receivers. These keys are established using preshared pairwise keys or asymmetric cryptography.

5.2 Real Time Packet Classification

Consider the general communication system depicted in Fig. At the PHY layer, a packet m is encoded, interleaved, and modulate before it is transmitted over wireless channel. At the receiver, the signal is de-modulated, de-interleaved, and decoded, to recover the original packet m.



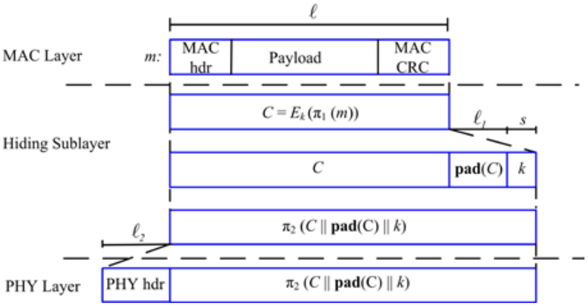
Moreover, still if the encryption key of a hiding scheme were to remain secret, the static portions of a transmitted packet can potentially lead to packet classification. This is because for computationally-efficient encryption methods for example block encryption, the encryption of a prefix plaintext with the same key yields a static cipher text prefix. Hence, an adversary who is conscious of the underlying protocol specifics structure of the frame can use the static cipher-text portions of a transferred packet to classify it.

5.3 Selective Jamming Module

We demonstrate the impact of selective jamming attacks on the network performance. Implement selective jamming attacks in two multi-hop wireless network scenario. In the first scenario, the attacker targeted a TCP connection established over a multi-hop wireless route. In 2 scenario, the jammer targeted network-layer control messages transmitted during the route establishment process selective jamming will be the encryption of transmitted packets (including headers) with a static key. Yet, for broadcast communications, this static decryption key must be known to all intended receivers and hence, is vulnerable to compromise. An adversary in possession of the decryption key can start decrypting as early as the reception of the first cipher text block.

5.4 Strong Hiding Commitment Scheme (SHCS)

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



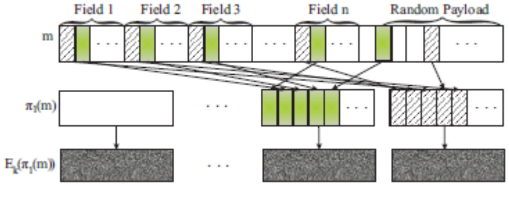
The computation slide of SHCS is one symmetric encryption at the sender and one symmetric decryption at the receiver. Due to the header

information is permuted as a trailer and encrypted, all receivers in the locality of a sender must receive the whole 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 reached at the MAC layer before it is decided if the packet must be discarded or be additionally processed. If some parts of the MAC header are deemed not to be useful information to the jammer, they can stay unencrypted in the header of the packet, thus\ avoiding the decryption operation at the receiver.

5.5 Cryptographic Puzzle Hiding Scheme (CPHS)

We present a packet hiding scheme depends on cryptographic puzzles. The main idea behind such puzzles is to compel the recipient of a puzzle execute a pre-defined set of computation before he is able to extract a secret of interest. The time required for obtaining the solution of a puzzle based on its hardness and the computational ability of the solver. The advantage of the puzzle depends on scheme is that its security does not rely on the PHY layer parameters. However, it has higher computation & communication overhead.

We consider several puzzle schemes as the basis for CPHS. For each scheme, we evaluate the implementation details which impact security and performance. Cryptographic puzzles are primitives originally recommended 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 provided that broadcast authentication and key escrow schemes providing broadcast authentication and key escrow schemes



Application of permutation π_1 on packet m.

6. CONCLUSION AND FUTURE WORK

We addressed the Issue of selective jamming attacks in wireless networks. We examine an internal adversary structure in which the jammer is part of the network under an attack, thus being known of the protocol specifications and shared network secrets. We displayed that the jammer can classify transmitted packets in real time by decoding the first of some symbols of an ongoing transmission. We calculated the impact of selective jamming attacks on network protocols such as Transmission Control Protocol and routing. Our findings will appear that a selective jammer can significantly impact performance with very less effort. We implemented three schemes that transform a selective jammer to a random one by preventing real-time packet classification. Our methods combine cryptographic primitives such as commitment schemes, cryptographic puzzles, & all or nothing transformations with physical layer characteristics. We analyzed the security of our methods and quantified their computational and communication overhead.

7. 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. 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.

[11] 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. ACMTransactions on Sensors Networks, 5(1):1–38, 2009.

[12] L. Lazos, S. Liu, and M. Krunz. Mitigating control-channel jamming attacks in multi-channel ad hoc networks. In Proceedings of the 2nd ACM conference on wireless network security, pages 169–180, 2009.

[13] G. Lin and G. Noubir. On link layer denial of service in data wireless LANs. Wireless Communications and Mobile Computing, 5(3):273–284, May 2004.

[14] X. Liu, G. Noubir, and R. Sundaram. Spread: Foiling smart jammers

using multi-layer agility. In Proceedings of INFOCOM, pages 2536–2540, 2007.

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

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

[17] G. Noubir and G. Lin. Low-power DoS attacks in data wireless lans and countermeasures. Mobile Computing and Communications Review, 7(3):29–30, 2003.

[18] OPNET. OPNETtm modeler 14.5. http://www.opnet.com/.

[19] C. Perkins, E. Belding-Royer, and S. Das. RFC 3561: Ad hoc ondemand distance vector (AODV) routing. Internet RFCs, 2003.

[20] C. P¨opper, M. Strasser, and S. ˇCapkun. Jamming-resistant broadcast communication without shared keys. In Proceedings of the USENIX Security Symposium, 2009.

[21] R. Rivest. All-or-nothing encryption and the package transform. Lecture Notes in Computer Science, pages 210–218, 1997.

[22] R. Rivest, A. Shamir, and D. Wagner. Time-lock puzzles and timedrelease crypto. Massachusetts Institute of Technology, 1996.

[23] B. Schneier. Applied cryptography: protocols, algorithms, and source code in C. John Wiley & Sons, 2007.

[24] SciEngines. Break DES in less than a single day. http://www.sciengines.com, 2010.

[25] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt. Spread Spectrum Communications Handbook. McGraw-Hill, 2001.

[26] D. Stinson. Something about all or nothing (transforms). Designs, Codes and Cryptography, 22(2):133–138, 2001.

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

[28] M. Strasser, C. P¨opper, and S. ˇCapkun. Efficient uncoordinated fhss anti-jamming communication. In Proceedings of MobiHoc, pages 207–218, 2009.

[29] M. Strasser, C. P¨opper, S. ˇCapkun, and M. Cagalj. Jamming-resistant key establishment using uncoordinated frequency hopping. In Proceedings of IEEE Symposium on Security and Privacy, 2008.

[30] P. Tague, M. Li, and R. Poovendran. Probabilistic mitigation of control channel jamming via random key distribution. In Proceedings of PIMRC, 2007.

[31] 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.

[32] 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.

[33] D. Thuente and M. Acharya. Intelligent jamming in wireless networks with applications to 802.11 b and other networks. In Proceedings of the IEEE Military Communications Conference MILCOM, 2006.

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

[35] W. Xu, W. Trappe, and Y. Zhang. Anti-jamming timing channels for wireless networks. In Proceedings of WiSec, pages 203–213, 2008.

[36] 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.

[37] W. Xu, T. Wood, W. Trappe, and Y. Zhang. Channel surfing and spatial retreats: defenses against wireless denial of service. In Proceedings of the 3rd ACM workshop on Wireless security, pages 80–89, 2004.