www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2 Issue 6 June, 2013 Page No. 1806-1811

COUNTERMEASURE AGAINST SELECTIVE JAMMING ATTACKS BY USING PACKET-HIDING METHODS

***Sathishkumar.S*[1], *Mr. Vnslssr.Murthy M.E*[2]**

[1]Computer Science and Engineering, Sri Krishna Engineering College, Panapakkam, (Near) Padappai, Chennai – 601 301.
E-mail: skumarscse@gmail.com

[2]Assistant Professor, Computer Science and Engineering, Sri Krishna Engineering College,
Panapakkam, (Near) Padappai, Chennai – 601 301

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 launchpad 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 networks, packet classification.

1 INTRODUCTION

Wireless networks rely on the uninterrupted availability of the wireless medium to interconnect participating nodes. However, the open nature of this medium leaves it vulnerable to multiple security threats. Anyone with a transceiver can eavesdrop on wireless transmissions, inject spurious messages, or jam legitimate ones. While eavesdropping and message injection can be prevented using cryptographic methods, jamming attacks are much harder to counter. 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.

Typically, 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. However, adopting an “always-on” 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 unusually high interference levels makes this type of attacks easy to detect. Conventional anti-jamming techniques rely extensively on spread-spectrum (SS) communications, or some form of jamming evasion (e.g., slow frequency hopping, or spatial retreats). SS techniques provide bit-level protection by spreading bits according to a secret pseudonoise (PN) code, known only to the communicating parties.

These methods can only protect wireless transmissions under the external threat model. Potential disclosure of secrets due to node compromise neutralizes the gains of SS. Broadcast communications are particularly vulnerable under an internal threat model because all intended receivers must be aware of the secrets used to protect transmissions. Hence, the compromise of a single receiver is sufficient to reveal relevant cryptographic information. 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.

2 RELATED WORK

T.X. Brown, J.F. James and A. Sethi, discussed the problem of an attacker disrupting an encrypted victim wireless ad hoc network through jamming. Jamming is broken down into layers and this paper focuses on jamming at the Transport/Network layer. Jamming at this layer exploits AODV and TCP protocols and is shown to be very effective in simulated and real networks when it can sense victim packet types, but the encryption is assumed to mask the entire header and contents of the packet so that only packet size, timing, and sequence is available to the attacker for sensing. A sensor is developed and tested on live data. The classification is found to be highly reliable for many packet types.

The relative roles of size, timing, and sequence are discussed along with the implications for making networks more secure.

Y. Liu, P. Ning, H. Dai, and A. Liu, discussed Jamming resistance is crucial for applications where reliable wireless communication is required. Spread spectrum techniques such as Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS) have been used as countermeasures against jamming attacks. Traditional anti-jamming techniques require that senders and receivers share a secret key in order to communicate with each other. However, such a requirement prevents these techniques from being effective for anti-jamming broadcast communication, where a jammer may learn the shared key from a compromised or malicious receiver and disrupt the reception at normal receivers.

A. Chan, X. Liu, G. Noubir, and B. Thapa, addressed the problem of countering the control channel jamming in wireless communication systems. Targeting control traffic on a system like GSM (e.g., BCCH channel) leads to smart attacks that are four orders of magnitude more efficient than blind jamming. We propose several schemes based on coding theory and its applications that can counter both external and internal attackers (traitors). We introduce a T-(traitor) resilient scheme that requires less than control information retransmissions and guarantees delivery of control information against any coalition of traitors.

L. Lazos, S.Liu, and M. Krunz, addressed the problem of control-channel jamming attacks in multi-channel ad hoc networks. Deviating from the traditional view that sees jamming attacks as physical-layer vulnerability, we consider a sophisticated adversary who exploits knowledge of the protocol mechanics along with cryptographic quantities extracted from compromised nodes to maximize the impact of his attack on higher-layer functions. We propose new security metrics that quantify the ability of the adversary to deny access to the control channel, and the overall delay incurred in re-establishing the control channel. We also propose a randomized distributed scheme that allows nodes to establish a new control channel using frequency hopping.

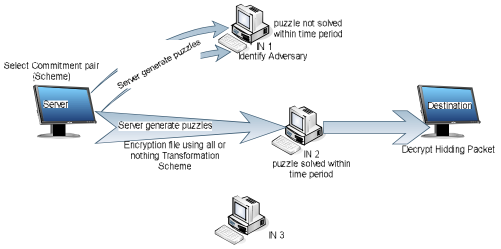
3 PROPOSED WORK

The problem of jamming under an internal threat model. 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 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. Three schemes that transform a selective jammer to a random one by preventing real-time packet classification. This schemes combine cryptographic primitives such as commitment schemes, cryptographic puzzles, and all-or-nothing transformations.

SYSTEM ARCHITECTURE

This architecture description is a formal description of a system, organized in a way that supports reasoning about the structural properties of the system. It defines the system components or building blocks and provides a plan from which products can be procured, and systems developed, that will work together to implement the overall system. This may enable one to manage investment in a way that meets business needs. The fundamental organization of a system, embodied in its components, their relationships to each other and the environment, and the principles governing its design and evolution. The composite of the design architectures for products and their life cycle processes. A Rep of a system in which there is a mapping of functionality onto hardware and software components, a mapping of the software architecture onto the hardware architecture, and human interaction with these components.



An allocated arrangement of physical elements which provides the design solution for a consumer product or life-cycle process intended to satisfy the requirements of the functional architecture and the requirements baseline. Architecture is the most important, pervasive, top-level, strategic inventions, decisions, and their associated rationales about the overall structure (i.e., essential elements and their relationships) and associated characteristics and behavior.

METHODOLOGY

A. COMMITMENT SCHEME

In this context, the role of the committer is assumed by the transmitting node S. The role of the verifier is assumed by any receiver R, including the jammer J. The committed value m is the packet that S wants to communicate to R. To transmit m, the sender computes the corresponding commitment/decommitment pair and broadcasts C. The hiding property ensures that m is not revealed during the transmission of C. To reveal m, the sender releases the decommitment value d, in which case m is obtained by all receivers, including J. Note that the hiding property, as defined in commitment schemes, does not consider the partial release of d and its implications on the partial reveal of m. In fact, a common way of opening commitments is by releasing the committed value itself.

B. CRYPTOGRAPHIC PUZZLE SCHEME

Cryptographic puzzle 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 predefined 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.

C. IDENTIFY ADVERSARY/ LEGITIMATE NODE

Identify the adversary using cryptographic puzzles within the network. When the node can solve the within the time period then the server can be assumed as a legitimate node otherwise adversary node. The cryptographic puzzle is very complicated to solve because it is randomly generated and that solving key known only by the legitimate node. If the server node identify that the node is adversary then it will alter commitment pair and then allocate cryptographic puzzle to commitment intermediate node.

D. ALL OR NOTHING TRANSFORMATIONS SCHEME

An All or Nothing Transformation (AONT) serves as a publicly known and completely invertible preprocessing step to a plaintext before it is passed to an ordinary block encryption algorithm. A transformation f, mapping message m to a sequence of pseudo messages is an AONT. 1) f is a bisection, 2) it is computationally infeasible to obtain any part of the original plaintext, if one of the pseudo messages is unknown, and 3) f and its inverse f_1 are efficiently computable. In our context, packets are preprocessed 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. At the receiver, the inverse transformation f_1 is applied after all x0 pseudo messages are received, in order to recover m.

E. RECEIVE HIDING PACKETS

When the receiver node receives the all or nothing transformations data and gives proper response to server. Then the receiving packets are extracts in the receiver side. In this proposed system more secure in packet transmission within the network. Here, initially the puzzle is sent to all the nodes which are present in the network. Based on the response and puzzle solving time, the legitimate node can be identified. This scheme preventing the real time packets transmission by combining the commitment scheme, cryptographic puzzles, all (or) nothing transformations scheme.

4 CONCLUSION

In this project, 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 with physical-layer characteristics. We analyzed the security of our schemes and quantified their computational and communication overhead.

REFERENCES

1. A.Chan, X. Liu, G. Noubir, and B. Thapa, "Control Channel Jamming: Resilience and Identification of Traitors," Proc. IEEE Int'l Symp. Information Theory (ISIT), 2007. PROA~NO AND LAZOS: PACKET-HIDING METHODS FOR PREVENTING SELECTIVE JAMMING ATTACKS 113

2. B.Greenstein, D. Mccoy, J. Pang, T. Kohno, S. Seshan, and D. Wetherall, “Improving Wireless Privacy with an Identifier-Free Link Layer Protocol,” Proc. Int’l Conf. Mobile Systems, Applications, and Services (MobiSys), 2008.
3. IEEE, IEEE 802.11 Standard, http://standards.ieee.org/getieee802/download/802.11-2007.pdf, 2007.
4. K. Gaj and P. Chodowiec, “FPGA and ASIC Implementations of AES,” Cryptographic Engineering, pp. 235-294, Springer, 2009.
5. L. Lazos, S. Liu, and M. Krunz, “Mitigating Control-Channel Jamming Attacks in Multi Channel Ad Hoc Networks,” Proc. Second ACM Conf. Wireless Network Security, pp. 169-180, 2009.
6. M. Cagalj, S. Capkun, and J.-P. Hubaux, “Wormhole-Based Anti-Jamming Techniques in Sensor Networks,” IEEE Trans. Mobile Computing, vol. 6, no. 1, pp. 100-114, Jan. 2007.
7. O. Goldreich, Foundations of Cryptography: Basic Applications. Cambridge Univ. Press, 2004.
8. T. Dempsey, G. Sahin, Y. Morton, and C. Hopper, “Intelligent Sensing and Classification in Ad Hoc Networks: A Case Study,” IEEE Aerospace and Electronic Systems Magazine, vol. 24, no. 8, pp. 23-30, Aug. 2009.
9. T.X. Brown, J.E. James, and A. Sethi, “Jamming and Sensing of Encrypted Wireless Ad Hoc Networks,” Proc. ACM Int’l Symp. Mobile Ad Hoc Networking and Computing (MobiHoc), pp. 120-130, 2006.
10. Y. Desmedt, “Broadcast Anti-Jamming Systems,” Computer Networks, vol. 35, nos. 2/3, pp. 223-236, Feb. 2001.