Volume 4, Issue 5, May 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Cryptography Based Method for Preventing Selective Jamming Attack in Wireless Network

Ms. Sonam Choubey
Computer Science Department
RGPV University, India

Abstract- The open nature of the wireless network makes it vulnerable to intentional interference attacks, commonly referred to as jamming. This jamming with wireless transmissions can be used as a launch pad for mounting Denial-of-Service attacks on wireless networks. Typically, the jamming has been addressed under an external threat model. The 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 synopsis, we have addressed the problem of selective jamming attacks in wireless networks. In these attacks, adversary is active only for a short period of time, generally it target messages of high importance. We elaborate the advantages of selective jamming in terms of network performance degradation and adversary effort. In this paper, a survey on some modern methods to encounter selective jamming attacks, is proposed.

Keyword-

I. INTRODUCTION

Jamming or dropping attacks have been considered under an external threat model[9][11], in which the attacker is not a part of the network. In this model, the jamming methods include the continuous or random transmission of high-power interference signals and attackers can launch low-effort jamming attacks that are difficult to detect and counter. In these attacks, the jammer is active only for a short period of time, selectivel y aiming messages of high importance. Selective jamming attacks [7][8][10] can be launched by performing real-time packet classification at the physical layer. For executing selective jamming the adversary must be capable of classifying transmitted packets and corrupting them before the end of their transmission. Packet classification is done by receiving just a few bytes of a packet. To launch selective jamming attacks, the jammer must be capable of implementing a classify-then-jam [12] policy before the completion of a wireless transmission. Such method can be actualized by classifying transmitted packets using protocol semantics. Jamming attacks are much harder to counter and face more security problems. In the simplest form of jamming, the jammer interferes with the reception of messages by transmitting a continuous jamming signal.

II. LITERATURE SURVEY

Authors in [1] considers the problem of an attacker disrupting an encrypted victim wireless ad hoc network through jamming. The jamming is broken down into layers and this paper focuses on jamming at the transport or network layer. At these layers, jamming 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, and sequence is available to the attacker for sensing.

Within a framework defined so far this paper provides seven contributions. First it demonstrates the potential Transport/Network layer jamming gains within a simulated environment. Second a simulated jamming protocol is developed that allows testing on an ad hoc network of lap top computers. Third the potential jamming gains are demonstrated on a live network using the simulated jamming protocol. Fourth a sensor is developed that uses packet size, timing, and sequence. It uses off-line sensing to adapt an online sensor to the current network conditions and a probabilistic model of the sizes and inter-packet timing of different packet types. A historical method for detecting known protocol sequences is used to develop the probabilistic models. The fifth is an active jamming mechanism to force the victim network to produce known sequences for the historical analyzer. The sixth is the online classifier that makes packet type classification decisions. The method is tested on live data and found that for many packet types the classification is highly reliable. Finally the relative roles of size, timing, and sequence are discussed along with the implications for making networks more secure.

The simulation and experimental results show that jamming has the potential for large gains, if the packet types are identified. This section describes the approach to sensing packet types. There are two approaches to classifying packets into types. The first classifies packets as they arrive (so-called online classification). The second is allowed to collect more observations before making the decision on packet type (socalled offline classification). Online

classification is the preferred approach, but as will be shown in the following subsections, both online and offline classification have a role.

This paper presented initial results in designing such a layered attacker for the Transport/Network layer. Jamming can get significant jamming gains, well over 100, when it knows the packet type and timing. Interestingly most of these gains were produced by attacking packets above the ad hoc network layer. Protocols introduce highly predictable timing that can be exploited. The limited information of packet size, timing, and sequence is enough to accurately predict packet types. Future work will fully connect and test the jamming and sensing which were treated separately. The statistical sensing tools continue to be refined. A few representative attacks were presented and the test bed tools described here are being used to methodically evaluate other attacks. Scaling to larger ad hoc networks and networked attackers is the long term goal.

The authors in [2] address the problem of control-channel jamming attacks in multi-channel ad hoc networks. They deviated from the traditional view that sees jamming attacks as physical-layer vulnerability. They 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

New security metrics are defined that quantify the adversary's ability to localize and deny legitimate nodes access to the control channel. We develop a randomized distributed channel establishment scheme that allows nodes to establish a new control channel using frequency hopping. In this scheme network nodes are able to temporarily construct a control channel until the jammer is removed from the network. Our scheme differs from classical frequency hopping in that the communicating nodes are not synchronized on the same hopping sequence, but each node follows a unique hopping sequence. This leads to unique identification of the set of compromised nodes by nearby nodes. Assuming perfect random sequence generators, we analytically evaluate the expected delay until a control channel is re-established and the expected fraction of time that the control channel is available. We verify our analytic results via extensive simulations.

Consider a single cluster with each node being within one hop from the CH. Let us assume that the current control channel is jammed by an adversary. The main idea behind our scheme is to have each node of the cluster hop between channels in a pseudo-random fashion, following a unique hopping sequence not known to other nodes. In this way if the jammer captures the hopping sequence of a compromised node, then in that case this node can be uniquely identified. After identification of the compromised node, this method CH updates the hopping sequences of all nodes in the cluster except the compromised one. In this way the effectiveness of a jammer that exploits knowledge from compromised nodes becomes equivalent to the effectiveness of a jammer that randomly hops between channels. Note that our method is not a permanent solution for the control channel allocation, nor can it permanently be used for data communications due to its high communication overhead and delay. Rather, our scheme temporarily restores a control channel until the jammer and any com-promised nodes are removed from the network.

From we conclude that, a randomized distributed channel establishment scheme that allows nodes to select a new control channel using frequency hopping. Our method differs from classical frequency hopping in that the communicating nodes are not synchronized to the same hopping sequence. Each node follows a unique hopping sequence. We showed that our scheme can uniquely identify compromised nodes through their unique sequence and exclude them from the network. We evaluated the performance of our scheme based on the newly proposed metrics of evasion entropy, evasion delay, and evasion ratio. Our proposed scheme can by utilized as a temporary solution for the control channel re-establishment until the jammer and the compromised nodes are removed from the network.

In paper [3], authors examine radio interference attacks from both sides of the issue. Firstly, they study the problem of conducting radio interference attacks on wireless networks, secondly they examine the critical issue of diagnosing the presence of jamming attacks. They proposed four different amming attack models that can be used by an adversary to disable the operation of a wireless network. They also evaluated their effectiveness in terms of how each method affects the ability of a wireless node to send and receive packets. Then they discussed different measurements that serve as the basis for detecting a jamming attack.

They proposed two enhanced detection protocols that employ consistency checking. First scheme employs signal strength measurements as a reactive consistency check for poor packet delivery ratios. Second scheme employs location information to serve as the consistency check. They examined the feasibility and effectiveness of jamming attacks and detection schemes using the MICA2 Mote platform.

In order to understand the effect that a jammer would have on the received signal strength, we performed six experiments. In the first two experiments, we have two Motes, a sender A and a receiver B, which are 30 inches apart from each other. In the ¯ first case, A transmits 20 packets per second, corresponding to a traffic rate of 5.28kbps, which we refer to as a CBR source. In the second case, A transmits at its maximum rate; as soon as the send function returns to the application level asynchronously, either because the packet is successfully sent or because the packet is dropped (the packet pumping rate is larger than the radio throughput), it posts the next send function.

We then studied the issue of detecting the presence of jamming attacks, and examined the ability of different measurement statistics to classify the presence of a jammer.

There are many different scenarios where a jamming style DoS may take place, but the authors in [4] focused on three basic classes of wireless networks. First is Two-Party Radio Communication. The second is The two-party scenario is the baseline case in which A and B communicate with each other on a specific channel. The transmission will interfere with the transmission and reception of packets by A and B as long as interferer X is close enough to either A or B. The third is Infrastructure Wireless Networks. The Infrastructure wireless networks include such as cellular networks or wireless local area networks (WLANs), it consists of two main types of devices: access points and mobile devices. All the access

points are connected to each other via a separate and wired infrastructure. The mobile devices communicate via the access point in order to communicate with each other or the Internet. The presence of an interferer might make it impossible for nodes to communicate with their access point.

In this work[5], authors focus on a related but different problem for broadcast communication. They examined the thing that How to enable robust anti-jamming broadcast without shared secret keys. Generally broadcast applications share the need for authenticity and availability of messages that are transmitted by base stations to a large and unknown number of potentially untrusted receivers. In such case a sender communicates to a dynamic set of trusted receivers or to untrusted

III. CONCLUSION

In this paper, we have presented a basic introduction to the selective jamming attacks in wireless networks. Some modern algorithms are also presented in the literature survey section. There problem definition, proposed solution, findings and drawbacks are analyzed.

REFERENCES

[1] 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.

[2] 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.

[3] 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: PACKETHIDING METHODS FOR PREVENTING SELECTIVE JAMMING ATTACKS 113

[4] 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.

[5] Y. Desmedt, "Broadcast Anti-Jamming Systems,"Computer Net-works,vol. 35, nos. 2/3, pp. 223-236, Feb. 2001.

[6] O. Goldreich,Foundations of Cryptography: Basic Applications. Cambridge Univ. Press, 2004.

[8] Alejandro Proano And Loukas Lazos January/February 2012Packet Hiding Methods for Preventing Selective JammingAttacksIEEE TRANSACTIONS ON DEPENDABLE ANDSECURE COMPUTING (vol. 9 no. 1)

[9] Lookas Lazos and Marwan Krunz February 2012 SelectiveJamming/Dropping Insider Attacks in Wireless Mesh NetworksIEEE NETWORK Volume:25 Issue:4

[10] Wenyuan Xu, Timothy Wood, Wade Trappe, Yanyong Zhang2004Channel Surfing and Spatial Retreats: Defenses againstWireless Denial of Service WiSe '04 Proceedings of the 3rd ACM workshoponWirelesssecurityPages 80-89ACM New York, NY, USA

[11] SudipMisra,Sanjay.K.Dhurander,AvanishRayankulaand DeepanshAgarwal 26-31 Oct. 2008 Using Honeynodes along with ChannelSurfing for Defense against Jamming Attacks in Wireless Networks3rd International Conference on System and Network Communications Page-197-201

[12] Shio Kumar Singh , M P Singh , and D K Singh May to June Issue 2011 A Survey on Network Security and Attack Defense Mechanism For Wireless Sensor Networks International Journal of Computer Trends and TechnologyVolume 1

