International Journal of Technology Research and Management
ISSN (Online): 2348-9006
Vol 1 Issue 4 Aug. 2014

A Cryptography Based Method for Preventing Jamming Attacks In Network

*Sapna Maheshvari, **Teena Patel
** Jhalawar Rajasthan, India
*Maheshvari_sapna@yahoo.co.in, **teena.patel21@outlook.com

ABSTRACT: - *The open nature of the wireless network makes it vulnerable to intentional interference attacks, usually cited as ECM(electronic countermeasure). These ECM with wireless transmissions could also be used as a launch pad for mounting Denial-of-Service attacks on wireless networks. Typically, the ECM has been addressed beneath associate degree external threat model. The adversaries with internal knowledge of protocol specifications and network secrets can launch low-effort ECM attacks that unit of measurement powerful to sight and counter. During this précis, we have got addressed the matter of selective jamming attacks in wireless networks. In these attacks, antagonist is active only for a quick quantity of some time, usually it target messages of high importance. We have a tendency to tend to elaborate the advantages of selective jamming in terms of network performance degradation and antagonist effort. Throughout this paper, a survey on some trendy ways in which to encounter selective jamming attacks is projected.*

1. INTRODUCTION

Jamming or dropping attacks are thought of below an external threat model[9][11], within which the aggressor isn't a section of the network. during this model, the ECM strategies embody the continual or random transmission of dynamic interference signals and attackers will launch low-effort jamming attacks that are troublesome to observe and counter. In these attacks, the sender is active just for a brief amount of your time, selectively y aiming messages of high importance. Electronic jamming attacks [7][8][10] will be launched by playing period packet classification at the physical layer. For corporal punishment electronic jamming the human should be capable of classifying transmitted packets and corrupting them before the end of their transmission. Packet classification is completed by receiving simply some bytes of a packet. To launch electronic jamming attacks, the sender should be capable of implementing a classify-then-jam [12] policy before the completion of a wireless transmission. Such methodology will be actualized by classifying transmitted packets exploitation protocol linguistics. Jamming attacks are a lot of more durable to counter and face a lot of security issues. Within the simplest variety of jamming, the sender interferes with the reception of messages by transmission an eternal jamming signal.

2. Literature Survey

Authors in [1] considers the drawback of an aggressor disrupting an encrypted victim wireless ad hoc network through jamming. The ECM is broken down into layers and this paper focuses on jamming at the transport or network layer. At these layers, jamming exploits AODV and transmission control protocol protocols and is shown to be terribly effective in simulated and real networks once it will sense victim packet varieties. However the secret writing is assumed to mask the entire header and contents of the packet therefore that solely packet size and sequence is out there to the aggressor for sensing.

Within a framework outlined therefore way this paper provides seven contributions. Initial it demonstrates the potential Transport/Network layer jamming gains at intervals simulated surroundings. Second a simulated jamming protocol is developed that permits testing on an ad hoc network of lap high computers. Third the potential ECM gains are incontestable on live network exploitation the simulated jamming protocol. Fourth a detector is developed that uses packet size, timing, and sequence. It uses off-line sensing to adapt an on-line detector to the current network conditions and a probabilistic model of the sizes and inter-packet temporal arrangement of totally different packet varieties. A historical methodology 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 turn out illustrious sequences for the historical analyzer. The sixth is that the on-line classifier that makes

packet kind classification selections. The methodology is tested on live information and found that for several packet varieties the classification is extremely reliable. Finally the relative roles of size, timing, and sequence are mentioned on with the implications for creating networks more secure.

The simulation and experimental results show that jamming has the potential for massive gains, if the packet varieties are known. This section describes the approach to sensing packet varieties. There are 2 approaches to classifying packets into varieties. The primary classifies packets as they arrive (so-called on-line classification). The second is allowed to gather a lot of observations before creating the call on packet kind (so called offline classification). On-line classification is the most well-liked approach, however as can be shown in the following subsections, each on-line and offline classification have a task.

This paper bestowed initial results in coming up with such a bedded aggressor for the Transport/Network layer. ECM will get vital jamming gains, well over a hundred, once it is aware of the packet kind and temporal arrangement. Curiously most of these gains were created by offensive packets on top of the ad hoc network layer. Protocols introduce extremely sure temporal arrangement that will be exploited. The restricted data of packet size, timing, and sequence is enough to accurately predict packet varieties. Future work can absolutely connect and take a look at the jamming and sensing that were treated singly. The applied math sensing tools continue to be refined. A few representative attacks were bestowed and therefore the take a look at bed tools described here are being used to methodically assess alternative attacks. Scaling to larger accidental networks and networked attackers is that the long run goal.

The authors in [2] address the matter of control-channel jamming attacks in multi-channel accidental networks. They deviated from the standard read that sees jamming attacks as physical-layer vulnerability. They contemplate a complicated human who exploits information of the protocol mechanics beside cryptanalytic quantities extracted from compromised nodes to maximize the impact of his attack on higher layer functions

New security metrics are outlined that quantify the adversary's ability to localize and deny legitimate nodes access to the management channel. We tend to develop a randomized distributed channel institution scheme that enables nodes to determine a replacement management channel exploitation frequency hopping. During this scheme network nodes are ready to briefly construct an impact channel till the sender is off from the network. Our scheme differs from classical frequency hopping in this the act nodes aren't synchronic on identical hopping sequence; however every node follows a novel hopping sequence. This ends up in distinctive identification of the set of compromised nodes by near nodes. Assuming good random sequence generators, we tend to analytically assess the expected delay till a sway channel is re-established and therefore the expected fraction of your time that the control channel is offered. We tend to verify our analytic results via intensive simulations.

Consider one cluster with every node being at intervals one hop from the CH. allows us to assume that this management channel is packed by an human. The most plans behind our scheme is to possess every node of the cluster hop between channels in an exceedingly pseudo-random fashion, following a novel hopping sequence not illustrious to alternative nodes. During this manner if the sender captures the hopping sequence of a compromised node, then in this case this node will be unambiguously known. Once identification of the compromised node, this methodology CH updates the hopping sequences of all nodes within the cluster except the compromised one. during this manner the effectiveness of a sender that exploits information from compromised nodes becomes comparable to the effectiveness of a sender that willy-nilly hops between channels. Note that our methodology isn't a permanent answer for the management channel allocation, nor will it for good be used for information communications due to its high communication overhead and delay. Rather, our scheme briefly restores an impact channel till the sender and any com-promised nodes are off from the network.

From we tend to conclude that, a irregular distributed channel institution scheme that enables nodes to pick out a replacement management channel exploitation frequency hopping. Our methodology differs from classical frequency hopping in this the communicating nodes aren't synchronized to identical hopping sequence. Every node follows a novel hopping sequence. We tend to showed that our scheme will uniquely establish compromised nodes through their distinctive sequence and exclude them from the network. We tend to evaluated the performance of our scheme supported the fresh projected metrics of evasion entropy, evasion delay, and evasion quantitative

relation. Our projected theme will by utilized as a brief answer for the management channel restoration till the sender and therefore the compromised nodes are off from the network.

In paper [3], authors examine radio interference attacks from either side of the problem. Firstly, they study the matter of conducting radio interference attacks on wireless networks, second they examine the vital issue of designation the presence of jamming attacks. They projected four totally different amming attack models that may be utilized by a human to disable the operation of a wireless network. They additionally evaluated their effectiveness in terms of however every methodology affects the power of a wireless node to send and receive packets. Then they mentioned totally different measurements that function the idea for sleuthing a jamming attack.

They projected 2 increased detection protocols that use consistency checking. Initial scheme employs signal strength measurements as a reactive consistency check for poor packet delivery ratios. Second scheme employs location data to function the consistency check. They examined the feasibility and effectiveness of jamming attacks and detection schemes exploitation the MICA2 mote platform.

In order to understand the result that a sender would wear the received signal strength, we tend to performed six experiments. Within the initial 2 experiments, we've got 2 Motes, a sender A and a receiver B, that are thirty inches excluding one another. Within the ¯ initial case, A transmits twenty packets per second; appreciate a traffic rate of 5.28kbps that we tend to discuss with as a cbr source. within the second case, A transmits at its most rate; as shortly because the send operate returns to the appliance level asynchronously, either as a result of the packet is with success sent or as a result of the packet is dropped (the packet pumping rate is larger than the radio throughput), it posts the next send function.

We then studied the problem of detecting the presence of jamming attacks, and examined the power of various measuring statistics to classify the presence of a sender.

There are many various scenarios wherever a jamming vogue DoS might occur, however the authors in [4] targeted on 3 basic categories of wireless networks. Initial is Two-Party Radio Communication. The second is that the two-party situation is that the baseline case within which A and B communicate with one another on a particular channel. The transmission can 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 embody like cellular networks or wireless local area networks (WLANs), it consists of 2 main forms of devices: access points and mobile devices. All the access points are connected to every alternative via a separate and wired infrastructure. The mobile devices communicate via the access purpose so as to speak with one another or the web. The presence of an interferer would possibly build it not possible for nodes to speak with their access purpose.

In this work [5], authors specialize in a connected however totally different drawback for broadcast communication. They examined the factor that a way to modify robust anti-jamming broadcast while not shared secret keys. Usually broadcast applications share the necessity for authenticity and availability of messages that are transmitted by base stations to an oversized and unknown variety of probably untrusted receivers. In such case a sender communicates to a dynamic set of trusted receivers or to untrusted

3. Conclusion

In this paper, we've got presented a basic introduction to the electronic jamming attacks in wireless networks. Some modern algorithms also are bestowed within the literature survey section. There drawback definition, projected answer, findings and disadvantages 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.

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

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

[9]. 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

[10]. SudipMisra,Sanjay.K.Dhurander,AvanishRaya nkulaand 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

[11]. 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