Security Methods For Preventing Selective Jamming Attack

[1]Rohit. A. Deshpande, [2]R. S. Kadam

[1,2]M.E.S. College of Engineering, Pune
Email: deshpande.rohit001@gmail.com

Abstract—This paper investigate packet hiding method to avoid attack from jammers. In wireless medium leaves it vulnerable to intentional interference attacks, such type of attack is referred as jamming attack. Launch pad is used for such type of intentional interference with wireless transmissions for mounting[DOS] Denial-of-Service attacks on wireless networks. Typically, under an external threat mode, such types of attacks is addressed. However, system with protocol specifications having internal knowledge it is very difficult to counter such attack. In this work, we study the wireless network and different method to avoid jamming attack . In such type of jamming attack , the system is active for high important massage that is only for a short and specific period of time, it means targeting high valuable massage

Index Terms— Selective Jamming, Denial-of-Service, Wireless Networks, Packet Classification.

I.INTRODUCTION

Wireless Local Area Networks (WLANs) are becoming an most important technology that is bringing the world closer together. WLANs are used in different field, such as pharmaceuticals, transportation, military, manufacturing education, agriculture, as well as 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 use access points or routers to transmit data in client-server network , but in case of ad-hoc networks access point or router is not used . Instead, all the nodes in an ad-hoc network participate in the routing process by forwarding messages to each other. **Packet switching** is a digital networking communications method that groups all transmitted data into suitably sized blocks, called packets, which are transmitted via a medium that may be shared by multiple simultaneous communication sessions. Packet switching increases network efficiency, robustness and enables technological convergence of many applications operating on the same network.

Early commercial networks were composed of dedicated, analog circuits used for voice communications. The concept of packet switching was introduced to create a communications network that would continue to function in spite of equipment failures throughout the network. In this paradigm shift, networks are viewed as collections of systems that transmit data in small packets that work their way from origin to destination by any number of routes. Initial packet processing functions supported the routing of packets through the network, transmission error detection and correction and other network management functions

A network packet is the fundamental building block for packet-switched networks.[14] When an item such as a file, e-mail message, voice or video stream is transmitted through the network, it is broken into chunks called packets that can be more efficiently moved through the network than one large block of data. Numerous standards cover the structure of packets, but typically packets are composed of three elements: Header – contains information about the packet, including origin, destination, length and packet number. Payload (or body) – contains the data that comprises the packet Trailer – indicates the end of the packet and frequently include error detection and correction information In a packet-switched network, the sending host computer packetizes the original item and each packet is routed through the network to its destination. Some networks used fixed length packets, typically 1024 bits, while others use variable length packets and include the packet length in the header. Individual packets may take different routes to the destination and arrive at the destination out of order. The destination computer verifies the correctness of the data in each packet (using information in the trailer), reassembles the original item using the packet number information in the header, and presents the item to the receiving application or user.

II. LITERATURE SURVEY

The shared nature of the medium in wireless networks makes it simple for an adversary to commence a Wireless Denial of Service attack. Jamming in different type of transmission like point-to-point transmissions in a wireless mesh network can have debilitating effects on data transfer through the network. The simplest technique to protect a wireless network against selective jamming attacks encompass physical layer solutions such as beam forming spread-spectrum, forcing the jammers to use a greater resource to achieve the same goal.[1]

Wireless Local Area Networks (WLANs) are becoming an most important method that is bringing the world

closer together. WLANs are used in different field, such as pharmaceuticals, transportation, military, manufacturing education, agriculture, as well as 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 use access points or routers to transmit data in client-server network , but in case of ad-hoc networks access point or router is not used [2]

In paper [3] The problem of countering the control channel jamming in wireless communication systems. Targeting control traffic on a system like GSM (global system for mobile communication) leads to smart attacks that are four orders of magnitude more efficient than blind jamming. In this paper several schemes based on coding theory and its applications that can counter both internal as well as external attack attackers

Due to open in nature the Wireless networks are more vulnerable to interference attacks as they .such type of attack is also called as (DOS) Denial-of-Service attacks that cause some sort of jamming in the network. there are different technique to prevent selective jamming attacks employed external threat model. However, there is possibility of internal as well as external attack attacks. System with good knowledge of network details including protocol specifications and other secret can make jamming attacks that are not easy to handle so such type of attack is introduced in wireless network [4]

The paper [5] reviews the network's ability to estimate the impact of jamming and incorporate these estimates into the traffic allocation problem. the Jamming node information on the server whereas, they have done on the client side. On gathering this jamming node information from the client to server side and also they can produce an effective path table to the client node to transfer the data. So they provide technique to avoid jamming attack

In paper [6], explains the problem of selective jamming attacks in wireless networks. In this work, we study the wireless network and different method to avoid jamming attack . In such type of jamming attack , the system is active for high important massage that is only for a short and specific period of time, it means targeting high valuable massage.

III. PROBLEM STATEMENT AND METHODOLOGY

3.1 Problem Statement

Consider the Fig. 1(a). Nodes A and B communicate via a wireless link. That means data is transmitted from node A to node B by using this wireless link. There is jamming node J within the communication range. When data M is transmitted from node A to node B there is intermediate node that is J node , so this node J classifies M by receiving only the first few bytes of data m. J then corrupts m data beyond recovery and then transmit to node B. Diagram of Realization of selective jamming attack is given bellow where J node is introduced between node A and node B

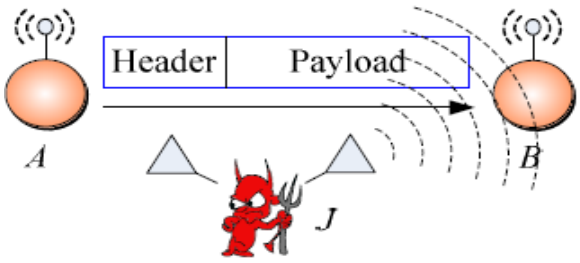
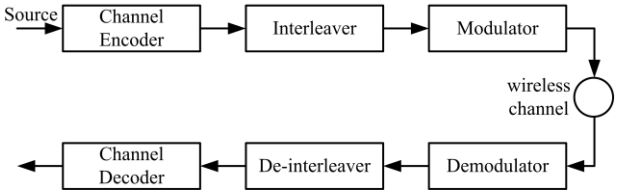


Fig 3.1 Realization of selective jamming attack

3.2 SYSTEM BLOCK DIAGRAM



A generic communication block diagram

According to block diagram Data is transmitted from transmitter to receiver and data M is classify as follows . initally The channel encoding block which expands the original bit sequence m, and to protecting m against channel errors add some necessary redundancy . For example, e is error per block an α/β-block code may protect m from up to e errors per block. Alternatively, convolution encoder an α/β-rate with a constraint length of Lmax, and a free distance of e bits provides same protection. For our purposes, we assume that the encoder rate is α/β. At the next block, interleaving is applied to protect m from burst errors. ,then next block is Interleaver at the transmission side that is defined by a matrix Ad×_ 1. The de-Interleaver at receiver side is simply the transpose of A. Finally, for maps the received bit stream to symbols of length q the digital modulator is used , and modulates them into suitable waveforms for transmission over the wireless link..

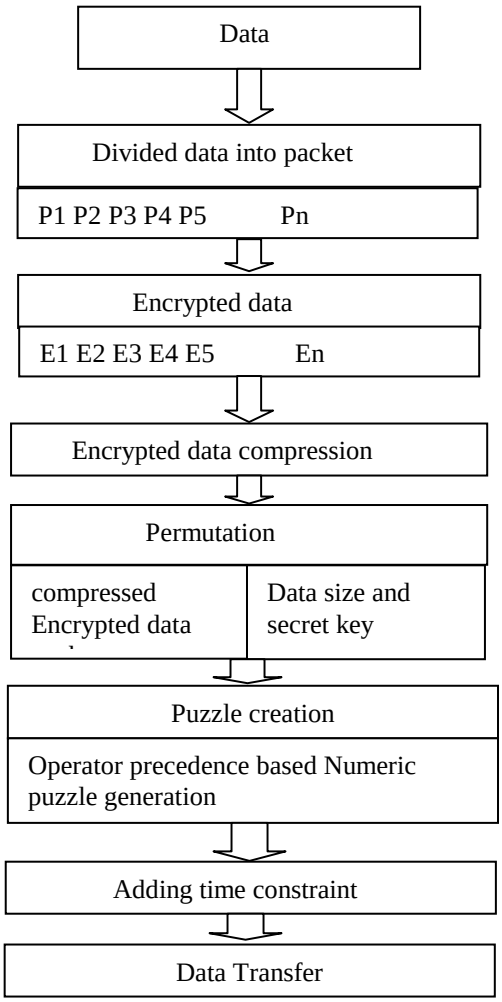
3.3 METHODOLOGY

3.3.1 HIDING BASED ON CRYPTOGRAPHIC PUZZLES

In this section, by using cryptographic puzzle we describe packet hiding method . The main concept

behind such puzzles is that there is numerical puzzle at the receiver and also some time constraint is add in that puzzle so if receiver able to solve this puzzle within set time then only data is transmitted from transmitter to receiver and Sometime depending on hardness of puzzle, time require for obtaining solution is set as well as the computational ability of the solver is depend 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.

Implementation of cryptographic puzzle Method



3.3.2 Implementation Details of CPHS

In this section, consider several puzzle schemes as the

basis for CPHS. For each scheme, we analyze the implementation details which impact security and performance. Initially data is divided into small segment called packet. this packet division leads to better security and lesser need of bandwidth. These packets are further encrypted for security and to avoid noise interference. After encryption the encrypted packet is compressed and its combination with secret key is transmitted further after this the cryptographic puzzle is added which binds decryption of packet into time constraint at receiver side

Time-lock Puzzles–Time-lock puzzles have several attractive features such as the fine granularity in controlling and the sequential nature of the computation. Moreover, the puzzle generation requires significantly less computation compared to puzzle solving.

If the receiver is not able to solve the puzzle in given time lock then the receiver section will not be permitted to decrypt the transmitted packet

IV. CONCLUSION

An internal adversary model in which the jammer is part of the network under attack, the adversary is active for high important massage that is only for a short and specific period of time, it means targeting high valuable massage. We showed that while transmitting data from one node to other node initially divide the data into packet, after that encrypted that packet and compressed this encrypted data and at last create puzzle and adding some time constraint. if receiving node able to solve this numerical puzzle then only data is transmitted successfully and avoiding jamming attack jammer can classify transmitted packets in real time by decoding the first few symbols of an ongoing transmission. We study the impact of selective jamming attacks on wireless network protocols such as routing and TCP . In these paper we list out different method to avoid selective jammer attack .

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 anti-jamming 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.