In Wireless Networks Data Hiding Methods for Preventing Selective Jamming Attackers

Venkatesh.P and Revathi.v

Abstract: The Wireless medium leaves are always subjected to intentional interference attacks referred to as jamming attacks. These jamming attacks can be used as a launch pad for mounting Denial of Service (DoS) attacks on wireless network. Typically jamming is one of many exploits used in compromise the wireless environment. This scheme works by denying service to authorized customers as legitimate traffic is jammed by the over frequencies of illegal traffic. An attacker really wanted to compromise your LAN (Local Area Network) and wireless security is the most effective approach would be to send randomly unauthenticated data to wireless network station. Reduce the impact of an unintentional distribution to identify its presence. It makes hamming itself to know at the physical layer, this commonly known as the MAC (Media Access Control) layer. The noise floor results increased in faltered noise to signal ratio, that noise will be displayed at the client system. In the physical layer can be classified by the performance of selective jamming attacks. We are developing real time packet classification combining cryptographic primitives with attributed of physical layer. And also we analyze computational and communication overhead in the security analysis.

Keywords: Selective Jamming, Denial of Service, Wireless Networks, packet Classification.

1. Introduction

Wireless network rely on the uninterrupted availability of the wireless medium to interconnect participating nodes. Jamming or dropping attacks have been considered under an external threat model, in which the attacker is not a part of the network. Under this model the jamming methods include the continuous random transmission of high power interference signals and attackers cab launch low effort jamming attacks are difficult to detect and counter. These attacks, the jammer is active in a short period of time, selectively the aiming messages of more importance. The selective jamming attacks [1] can be launched by performing real time packet classification at the physical layer. In paper, we consider a sophisticated adversary model to which the adversary is aware of implementation details of the network protocols. To exploiting this knowledge, the adversary launches in selective jamming attacks in which it targets specific packets are high importance. To examine the jamming of TCP acknowledgment can severely degrade throughput of a TCP connection due to the congestion control mechanism to the TCP protocol.

The continuous jamming and adversary is active for short period of time, thus to expending orders of magnitude less energy. The classifying transmitted packets in real time and corrupting them before to end their transmission. The packet classification can be performed and receiving just a few bytes of a packet, for example by decoding the frame control filed of a MAC layer frame. We are interest to developing resource efficient methods to preventing real time packet classification and hence, to mitigating selective jamming.

2. Related Work

The continuous jamming has been used as a Denial of Service (DoS) attack against the voice communication since 1940s. Nowadays several alternative jamming strategies have been demonstrated [2]. Categorized jammers into four models, i) a constant jammer that continuously emits noise, ii) a deceptive jammer that continuously broadcasts fabricated messages or replays old ones, iii) a random jammer that alternates between periods of continuous jamming and inactivity, and iv) a reactive jammer who jams only when transmission activity is detected.

The intelligent attacks which target the transmission of specific packets were presents. An attacker who infers eminent packer transmission based on timing information at the MAC layer.

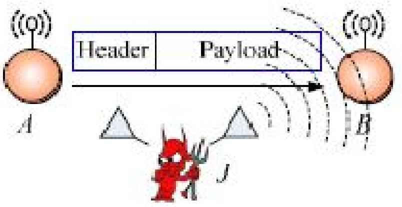

Fig.2.1 Realization of selective jamming attacks

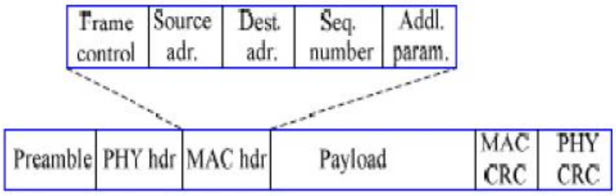

Fig2.2 A generic frame format for a wireless network

The selective jamming attacks in multi-hop wireless networks, where the future transmissions at one hop were inferred from prior transmission in other hops. In both real

Venkatesh.P is a M.tech (CSE) Student Department of CSE, EVMCET, Narasaraopet, Guntur(Dist), Ap, India. and Revathi.v is working as Assistant Professor, Department of CSE, EVMCET, Narasaraopet, Guntur(Dist), Ap, India, Palavarthivenkatesh1@rediffmail.com#1, vrevathi530@gmail.com#2

times packet classification was considered beyond the capabilities of the adversary. The selectivity is achieved via interface from the control of messages already transmitted. Channel selectivity jamming were considered. It was shown that targeting the control channel reduces the required power for performing a DoS attack by several orders of magnitude. To protect the control channel traffic control information was replicated in multiple channels. We are proposed a randomized frequency hopping algorithm to protect the control channels inside jammers.

3. Proposed system

We are proposed a method to investigate the impact of selective jamming on critical network functionalities. Finding and indicate that selective jamming attacks lead to a DoS with very low effort on behalf of the jammer. To resolve such attacks a method that prevent classification of transmitted packets in real time is developed. The problem of real time packet classifications can be mapped to the hiding property of commitment methods in which transmitter and receiver commitment on static key.

Algorithm

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

A solution based on All-Or-Nothing Transformations (AONT) that introduces a modest communication and computation overhead. We are proposed algorithm keeps these two in mind as they are essential to reducing the jamming attacks by using the packet hiding mechanism.

If the fragments are short, the attackers jamming message does not start till the transmitter has finished transmitting and hopped to another channel.

4. Problem statement and assumption

a) Problem Statement

Consider the scenario depicted in Fig.2.1 Nodes A and B communicate via a wireless link. In the communication range of both A and B there is a jamming node J. when A transmits a packet n to B, node J classifies n by receiving only the first few bytes of n, J then corrupts m beyond recovery by interfering with its reception at B. we address the problem of preventing the jamming node from classifying n in real time, thus mitigating J's ability to perform selective jamming. Our goal is to transform a selective jammer to random one. Note that in the present work, we do not address packet classification methods based on protocol semantics.

b) Adversary Model

1. Network model

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

2. Communication Model

Data hiding is based on symmetric cryptography. Our main goal is to satisfy the strong hiding characteristics while keeping the computation and communication overhead to a minimum. The proposed SHCS requires the joint consideration of MAC and PHY layers. To decrease the overheads of SHCS the de commitment value d is carried in the same packet as the committed value. This helps to save the extra packet header needed for transmitting individually. Packets are transmitted at a rate of R bauds. Each PHY-layer symbol corresponds to q bits, where the q is defined by the underlying digital modulation scheme. Every symbol carries q data bits, where α/β is the rate of the PHY-layer encoder. Here the transmission bit rate is equal to qR bps and the information direct sequence spread spectrum (DSSS) may be used at the PHY layer to protect wireless transmission from jamming. SS provides immunity to interface to some extent gain, but a powerful jammer is still capable of jamming data packets of his choosing. Transmitted packets have the generic format layer header contains information regarding the length of the frame, and the transmission rate. The MAC header determines the MAC protocol version, the source and destination addresses, sequence number plus some additional fields. The aim of this communication is strong hiding characteristics, otherwise keeping the computation and communication overhead to a minimum. This help to save another packet header as the recommend value. By using this technique to save extra packet header needed for transmitting individually. We achieve strong hiding characteristics, and a sub layer called the canceling sub layer, it is increased between the MAC and PHY layers. Frame n at the MAC layer delivered to the hiding sub layer. That frame contains a MAC header and a payload, followed by the trailer containing the Cyclic Redundancy Check (CRC) code.

3. Adversary model

The adversary is in the control of the communication technique can manage jam message at any situation of the network of user choosing. It can also operate the full-duplex mode, thus being able to perform transceiver simultaneously. It can be achieved with the use of multi-ratio transceivers. Finally the user can decide to irrecoverably corrupt a transmitted packet by jamming the last symbol. In reality it demonstrated by selective jamming can be achieved with far less resources. Jammer can be equipped with a single half duplex transceiver is sufficient to classify and the jam transmitted packets. The user can be equipped by special purpose hardware for performing cryptanalysis or any other available computation. The well known hard cryptographic problem is assumed be a time consuming. To proposes of these analysis are given a cipher text, the most efficient method for deriving the corresponding plaintext is assumed to be an exhaustive key spaces.

5. Implementation

The jamming attacks in wireless sensor network are proposed. The swarm intelligence algorithm is capable enough to adapt changes in network topology and traffic. In the communication the transceiver change channels in order to connect and away from the jammer channel changing techniques. Based environment the software such as JDK 1.6 running in windows XP operating system. This system takes a support of Java technology such as Remote Method Invocation (RMI). Java's SWING API gives support to build user interfaces. The introduced RMI technology is communicated remotely. It has three type's nodes namely centralized server, server and client. The source person is sent the data to the destination. In wireless sensor communication the server node is ready to send the data to the client nodes based on the port numbers and the communication is routed by one of the centralized services. Then the user is able to select a file by clicking browse button. The information or file selected and is broken into each packet with a length of 48 bytes. The source select required data and sends it to a interested client. The information is sent in the form of packets and the packet length is 48 bytes. The server has to maintain a specific IP address and port number based on centralized server through which to send the message to the client. The error controlling by using channel encoding during the transmission through the communication channel. It transforms the information by a sequence to the encoder sequence. After modulation technique we get the Code Word. After the completion of encoding the message will be displayed. A way to arrange a data in terms of non-contiguous way to increase the performance. The interleaving process is done then the data is converted into packets. After then we use these packets for transmission. In between transmission the destination is identified and data is converted into the packets and send to select destination. After reach the information to the destination we get the acknowledgement.

Jamming Attacker Analysis

Applications are made with two clients, two servers and a packet hiding queue. Initially the communication flow starts when the source person is ready to send data to the client. It randomly selects the packets and centralized the server to send files in terms of packets of size 48 bytes. The server monitors communication and finding any jamming attacks. The attacker can be viewed by Jamming Attack Analysis. In future data is sent from source to destination by using the packets hiding queue. It can analyze the attacks and also find whether the attacker is made or not. Then we consider the packet loss.

6. Conclusion

We find the selective problem of jamming address in wireless network. To illustrate the effectiveness of jamming attacks by implementing such jamming attacks against the TCP protocol. Jamming attacks can be launched by performing real time packet classification. In proposed technique investigates the impact of selective jamming on critical network developed three methods that prevent classification of transmitted packets in real time. We are showed an adversary can exploit knowledge on the protocol implementation and to increase the impact of his attack and significantly the energy cost is very low. Mitigate the selective jamming, and we are proposed several methods that combine cryptographic primitives such as commitment schemes crypto puzzles, and all or nothing transformation with physical layer attributes.

References

[1] OPNETtm modeler 14.5. http://www.opnet.com/ solutions/network rd/ modeler.html.

[2] IEEE 802.11 standard. http://standards.ieee.org/ getieee802/download/ 802.11-2007.pdf, 2007.

[3] Wenyuan Xu, Timothy Wood, Wade Trappe, Yanyong Zhang2004"Channel Surfing and Spatial Retreats: Defenses againstWireless Denial of Service" WiSe '04 Proceedings of the 3^{r} ACM workshoponWirelesssecurityPages 80-89ACM New York, NY, USA.

[4] SudipMisra, Sanjay.K. Dhurander, Avanish Rayankula and Deepansh Agarwal 26-31 Oct. 2008 "Using Honeynodes along with ChannelSurfing for Defense against Jamming Attacks in Wireless Networks"3rd International Conference on System and Network Communications Page-197-201

[5] D. Comer. Internetworking with TCP/IP: principles, protocols, and architecture. Prentice Hall, 2006.

[6] I. Damgard. Commitment schemes and zero-knowledge protocols. Lecture notes in computer science, 1561:63–86, 1999. 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.