ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)
Vol. 3, Issue 1 (Jan. - Mar. 2015)
International Journal of Advanced Research in Computer Science & Technology (IJARCST 2015)

Prevent Selective Jamming Attack Using Packet Hiding Method

[I]Pooja Avasare, [II]Priyanka Nile, [III]Tanvi Pardeshi, [IV]Pooja Sanap
[I,II,III,IV]Computer Science, Savitribai Phule, Pune University, India

Abstract
The open nature of the wireless medium leaves it vulnerable to interference attacks, typically referred to as jamming. This interference attacks can be used for performing Eavesdropping & Denial-of-Service attacks on wireless network while eavesdropping can be prevented using cryptographic methods, in this work, we address the problem of selective jamming attacks in wireless networks. In these attacks, the attacker is active only for a short period of time; attacker is targeting messages of high importance. We describe the advantages of selective jamming in terms of network performance degradation and attacker effort by presenting two cases. a selective attack on TCP and one on routing. To avoid these attacks, we develop three schemes that prevent real-time packet classification by cryptographic primitives with physical-layer attributes [1]. We analyze the security of our methods and evaluate their computational and communication overhead [1].

Keywords
Cryptographic Method, Denial-of-Service, Selective Jamming, Denial-of-Service, Wireless Networks, Packet Classification, TCP

I. Introduction

Wireless networks rely on the uninterrupted convenience of the wireless medium to interconnect participating nodes. However, the open nature of this medium leaves it at risk of multiple security threats [1]. Anyone with a transceiver will eavesdrop on wireless transmissions, inject spurious messages, or jam legitimate ones [1]. Whereas eavesdropping and message injection are often prevented using cryptographic strategies, jamming attacks are a lot of harder to counter. They need been shown to actualize severe Denial-of-Service (DoS) attacks against wireless networks. Within the simplest form of jamming, the adversary interferes with the reception of messages by transmittal a continual jamming signal [1], or many short jamming pulses .Typically, jamming attacks are thought-about under an external threat model, within which the jammer isn't a part of the network. Under this model, jamming methods include the continuous or random transmission of high-power interference signals [1]. However, adopting associate "always-on" strategy has several disadvantages. First, the soul has got to expend a big quantity of energy to jam frequency bands of interest. Second, the continual presence of unusually high interference levels makes this sort of attacks simple to observe. Typical anti-jamming techniques bank extensively on spread-spectrum (SS) communications, or some sort of jamming evasion (e.g., slow frequency hopping, or spatial retreats). SS techniques offer bit-level protection by spreading bits per a secret pseudo-noise (PN) code, known only to the human activity parties. These strategies will only protect wireless transmissions under the external threat model. Potential disclosure of secrets due to node [1] compromise neutralizes the gains of SS. Broadcast communications are notably vulnerable under an indoor threat model as a result of all intended receivers should remember of the secrets used to protect transmissions. Hence, the compromise of one receiver is comfortable to reveal relevant science info. During this paper, we have a tendency to address the matter of jamming under an indoor threat model. We consider a sophisticated adversary who [1] is responsive to network secrets and also the implementation details of network protocols at any layer within the network stack. The attacker exploits his internal data for launching selective jamming attacks within which specific messages of "high importance" are targeted. as an example, a jammer will target route-request/route-reply messages at the routing layer to prevent route discovery, or target TCP acknowledgments TCP session to severely degrade the outturn of an end-to-end flow[1]. To launch selective jamming attacks, the adversary should be capable of implementing a "classify-then-jam" strategy before the completion of a wireless transmission. Such strategies are often actual either by classifying transmitted packets mistreatment protocol linguistics or by decoding packets on the fly. Within the latter technique, the jammer might decode the primary few bits of a packet for recovering helpful packet identifiers like packet type, supply and destination address. When classification, the adversary should induce a comfortable range of bit errors so the packet can not be recovered at the receiver. Selective jamming needs associate intimate data of the physical (PHY) layer.

II. Related Works

A. Need of system

In planned system, "jamming and sensing of encrypted wireless ad-hoc network 2008" has data of current jamming attacks encryption. The SS communications enchiridion 2010 data of technique to defend against attacks however it fails for internal threat jamming attacks. Broadcast anti-jamming system 2010 contains data of code packets and send broadcast them, it also fails for internal threat model as a result of within threat could compromise decoding data. The channel surfing and abstraction retreats defences against wireless denial of service 2011 data of advanced anti-jamming technique move mobile nodes to safe locations however it's not invariably doable to manoeuvre mobile devices. All higher than mentioned researches tend using to implement such project wherever our work is to forestall jam attacks by mistreatment packet activity methodology.

B. Existing Tools

The software demand Specification describes the scope of the project, in operation setting, user characteristics, style and constraints. It conjointly elaborates the system design of the packet hiding technique. Contemplate the state of affairs wherever Nodes X and Y communicate via a wireless link. at intervals the communication ranges of each X and Y there's a electronic jamming node J. once X transmits a packet m to Y, node J classifies packet m by receiving only the primary few bytes of m. J then corrupts m on the far side recovery by officious with its reception at Y. we have a tendency to address the matter of preventing

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

the electronic jamming node from classifying packet m in real time, thus mitigating J's ability to perform jam attack. Our goal is to rework a selective transmitter to a random one. Note that within the gift work, we have a tendency to don\'t address packet classification ways supported protocol linguistics.

III. System And Adversary Model And Network Model

The network consists of a collection of nodes connected via wireless links [2] for communicate and sharing of knowledge. Nodes could communicate directly if they're inside communication vary, or indirectly via multiple hops. Nodes will communicate each in unicast mode and broadcast mode. Communications may be either unencrypted or encrypted type. For encrypted broadcast communications, even keys area unit shared among all supposed receivers. These keys area unit established exploitation pre shared pair wise keys or asymmetric cryptography.

A. Network module

Packets are transmitted at a rate of R bauds [3]. Every PHY layer image corresponds to q bits, wherever the worth of q is outlined by the underlying digital modulation theme [1]. Each image carries q information bits, wherever the speed of the PHY-layer encoder is. The mac header determines the mac protocol version, the source and destination addresses, sequence numbers and some extra fields. The mac header is followed by the frame body that usually contains an arp packet or an information processing datagram. Finally, the mac frame is protected by a cyclic redundancy check (CRC) code. At the PHY layer, a trailer is also appended for synchronizing the sender and receiver [1].

B. Adversary Model

We assume the attacker is up to speed of the communication medium and may jam messages at any a part of the network of his selecting. The adversary can operate in full-duplex mode [1], therefore having the ability to receive and transmit at the same time. This may be achieved, for instance, with the use of multi-radio transceivers. Additionally, the resister is provided with directional antennas that modify the reception of a signal from one node and jam of an equivalent signal at another .For analysis functions, we have a tendency to assume that the resister will pro-actively jam variety of bits just under the ecc capability early within the transmission [3]. For the needs of study, given a cipher text, the foremost economical technique the corresponding plain text is assumed to be associate complete search on the key area. The implementation details of each layer of the network stack square measure assumed to be public. moreover, the adversary is capable of physically compromising network devices and sick hold on data together with cryptanalytic keys, PN codes etc. resister model is realistic for network architectures like mobile ad-hoc, mesh, cognitive radio, and wireless device networks, wherever network devices could operate unattended, therefore being vulnerable to physical compromise.

IV. Requirement and Specification for Implementation

Piggybacking is well known and extensively used for real-world applications. For large packets like I, the supply produces an additional compressed packet by discarding the less- important bits and attaches this tiny and redundant packet to information packet. During this projected work we tend to propose 2 new methodologies to send information between the server and various clients within the secure manner. Initial the information encryption technique is handled by the RSA algorithmic program. Second the encrypted text is transfer over the network .When the decryption is completed on the clients there the piggy backing operation takes place. For packet hiding technique. A robust hiding Commitment Scheme (SHCS) is enforced. Hiding technique. A robust hiding Commitment Scheme (SHCS) is enforced.

A. A Strong Hiding Commitment Scheme (SHCS)

We propose a strong hiding commitment scheme that is based on the symmetric cryptography method. Main impetus is to satisfy the strong hiding property while keeping the computation and the communication overhead to a minimum. The proposed SHCS requires the joint consideration of the MAC and PHY layers [1]. To reduce the overhead the de-commitment value or the decryption key value is done in the same packet in which the encryption is taken place. A new sub layer is found between the existing two layers, which is responsible for the packet formatting and data hiding .It will form as a frame structure. The purpose of this is to randomize the input to the encryption algorithm.

Encryption of Data

The data is encrypted by using the RSA Algorithm. It is the public key algorithm that uses the huge prime numbers in their factoring and their multiples as the code or key to encode the data given. Since the key size is large the intruders cannot be easily able to hack the data. Through this RSA (Rivest, Shamir, and Adleman) algorithm the data will be more secure.

B. Piggybacking Technique

In this technique, we proposed a novel method using piggybacking technique of packet loss during large volume of packets sent to more number of clients. At the decryption end, the data in huge volume will be loss due to congestions. But by piggybacking the packets along ith the header and sequence ID and the host name the data will be send directly to the selected host. Hence, the data will be buffered and after that process the data will be sending to all the clients that are alive on the network. Thus the piggybacking techniques the data will be directly send to the client network, after the acknowledgement is received. The TCP protocol is responsible for the processing.

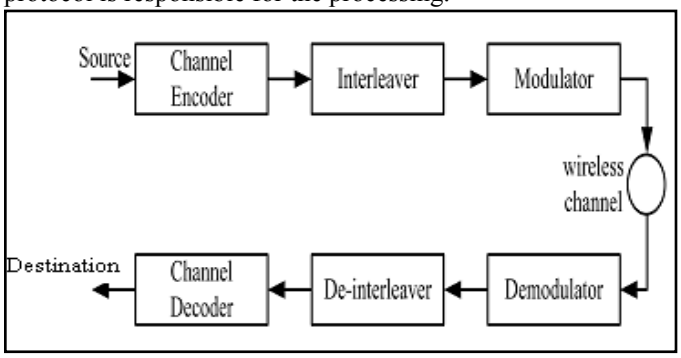

Fig 1: A generic communication system diagram [1]

V. Conclusion

We studied 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

VI. Acknowledgment

We have taken efforts in this paper. However, it would not have been possible without the kind support and help of many individual. Our thanks and appreciation also goes to our beloved parents for their blessings, all the staff members, friends and colleagues for providing help and support in our work.

References

[1] *Alejandro Proan˜o and Loukas Lazos," Packet-Hiding Methods for Preventing Selective Jamming Attacks", IEEE transactions on dependable and secure computing, vol. 9, no. 1, January/February 2012*

[2] *Divya Ann Luke, Dr. Jayasudha. J .S SELECTIVE JAMMING ATTACK PREVENTION BASED ON PACKET HIDING METHODS AND WORMHOLES International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.3, May 2014*

[3] *Divya. S1, Manohar Gosul Jamming Attacks Prevention in Wireless Networks Using Packet Hiding Methods Journal of Computer Engineering (IOSRJCE) ISSN: 2278-0661, ISBN: 2278-8727 Volume 5, Issue 3 (Sep-Oct. 2012), PP 13-20*