IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Countering Selective Jamming Attacks in Wireless Networks

Prathyusha[*1], Y.R.K.Paramahamsa[2]

[*1,2]Sri Sunflower College of Engineering & Technology, Lankapalli, India

alihussain.phd@gmail.com

Abstract

Wireless Networks constituting a large number of nodes are becoming viable solution to many challenging commercial, domestic, and military applications. Wireless Networks collect and disseminate information from the fields where ordinary networks are unreachable for various environmental and strategic reasons. Wireless networking has emerged as one of the most promising concept for auto-configurable and self-organizing wireless networking to provide flexible and adaptive wireless connectivity to mobile users. Wireless networks can be vulnerable to active and also passive attacks. These types of attacks include Denial- of- Service (DoS), Man- in- the-Middle (MITM), spoofing, jamming, war driving, network hijacking, packet sniffing, and many more. This paper presents a way for countering selective jamming attacks in wireless networks.

Keywords: Cryptography, Jammer, Physical layer, TCP.

Introduction

Wireless networks[4][5] succeeded much theoretical impossibility and simplified the architecture of the networks implementation. The networks established using traditional approaches has significant conditions on extension of the nodes or sensors and connecting the nodes through physical cables. The expenditure and constraints were too difficult to be obeyed in the traditional approaches of implementing the network. On the other hand, the wired networks were too vulnerable to the attackers too. The entry procedure of any user is clearly monitored which restricted many imperfect hackers. Speaking of the attackers in the wireless networks in the internet services specifically, there has been no limit to be defined. High accessibility and usability made the wireless networks a bit insecure to that of the wired networks. Limited access with physical links is thus a secure method to protect the resources of a network from outside users. But in a view of a large organization, there is a serious necessity of providing access to multiple users with the easier protocols [1].

Internet has been proven to be a good solution for every doubt of any kind of user. The boundless internet services provide accessibility to every user who possesses the connectivity. Designed for simplicity and accessibility, the immense structure of the internet is far easier to obtain services from. Similar to that a private network can establish its framework for multiple users through the wireless medium. Wireless communication between the nodes and the server needs a transceiver of prescribed frequency [2] and appropriate authentication. This allows the attackers to easily enter and block the services of the original users. The open structure of the wireless networks facilitates the attackers to enter and exit with only less effort. Compromising the nodes and acting as the legal user is also possible with enough details on the authentication codes. Disclosures of the secret codes even in the presence of highly secure algorithms would invite the hackers. Independent nodes in the networks are taken over by the knowledge on the internal activities of the network.

Attacks in the wireless networks may be of any kind to disturb the normal functioning of any network. Attacks may jam or block the communication channel [3], corrupt the packets, inject wrong messages, flood the medium with false messages or simply eavesdrop the activities of the networks. Any of these kind of attacks would greatly influence the control and efficiency of the wireless networks. Measures have to be taken immediately to identify, mitigate and isolate the attacks and attacker. This paper presents a method for countering selective jams in wireless networks.

Existing System

Jamming attacks have been considered as an external threat model, in which the jammer is not part of the network. Under this model, jamming strategies include the continuous or the random transmission of high power interference signals. Anti-jamming techniques rely extensively on spread-spectrum (SS)

communications[6], or some form of jamming evasion [7] (e.g., slow frequency hopping, or spatial retreats). SS techniques provide bit-level protection by spreading the bits according to a secret pseudo-noise (PN) code, known only to the communicating parties. These methods can only protect the wireless transmissions under the external threat model. Always-on strategy has the continuous presence of unusually high interference levels makes this type of attacks very easy to detect.

The disadvantages of the existing system are:

- Jamming attacks under the internal threat model is not considered.
- Always-on strategy has disadvantages such as- first the adversary has to expend a significant amount of energy to jam frequency bands of interest.

Proposed System

In the proposed work, the problem of jamming under an internal threat model has been considered. Adversary who is aware of the network secrets and the implementation details of network protocols at any layer in the network stack has been designed. The adversary exploits the internal knowledge for launching the selective jamming attacks in which specific messages of "high importance" are targeted. A jammer can target the route-request/route-reply messages at the routing layer to prevent route discovery, or target TCP acknowledgments in a TCP session to severely degrade the throughput of an end-to-end flow.

The modules in the proposed system are:

- Adversary Design
- Packet Classification
- A Strong Hiding Commitment Scheme
- Cryptographic Puzzle Hiding Scheme
- Hiding Based On All-Or-Nothing Transformations
- Hiding Based On Md5

A. ***Adversary Design***

Adversary is in control of the communication medium and can jam messages at any part of the network of his/her choosing. The adversary can operate in the full-duplex mode, thus being able to receive and transmit simultaneously. This can be achieved, for example, with the help of multi radio transceivers. Adversary is equipped with the directional antennas that enable the reception of a signal from one node and jamming of the same signal at another. It is assumed that the adversary can pro-actively jam a number of bits below the ECC capability early in the transmission. When the adversary is introduced, the data packets from the node cannot be reached at the receiver.

B. ***Packet Classification***

At the Physical layer, a packet, say m, is encoded, interleaved, and modulated before it is transmitted over the wireless channel. At the receiver side, the signal is demodulated, de- interleaved and decoded to recover the original packet m. Nodes A and B communicate via a wireless channel. Within the communication range of both A and B there is a jamming node, say J. When A transmits a packet m to B, node J classifies m by receiving only the first few bytes of packet m. Node J then corrupts m beyond recovery by interfering with its reception at B.

C. A Strong Hiding Commitment Scheme

A strong hiding commitment scheme (SHCS), which is based on the symmetric cryptography. Assume that the sender has a packet for the Receiver. First, S (Sender) constructs commit(message) the commitment function is an off-the-shelf symmetric encryption algorithm is a publicly known permutation, and k is the randomly selected key of some desired key length s (the length of k is a security parameter). The role of the committer is assumed by the transmitting node "S". The role of the verifier is assumed by any receiver "R", including the jammer J. The committed value m is the packet that S wants to communicate to "R". To transmit packet m, the sender computes the corresponding commitment/decommitment pair (C, d), and broadcasts C. The hiding property ensures that packet m is not revealed during the transmission of C. To reveal m, the sender releases the decommitment value d, in which case packet m is obtained by all receivers, including J.

D. Cryptographic Puzzle Hiding Scheme

A sender S has a packet m for transmission. The sender selects a random key "k" , of a desired length. "S" generates a puzzle (key, time), where puzzle() denotes the puzzle generator function, and tp denotes the time required for the solution of the puzzle. Parameter is measured in units of time, and it is directly dependent on the assumed computational capability of the adversary, denoted by "N" and measured in computational operations per second. After generating the puzzle "P", the sender broadcasts (C, P). At the receiver side, any receiver R solves the received puzzle to recover key and then computes the packet. Server to solve the puzzle in time tp and solved puzzle should be correct get the data packet at server side.

E. Hiding Based On All-Or-Nothing Transformations

The packets are pre-processed by an AONT before transmission but remain un- encrypted. The jammer cannot perform packet classification until all the pseudo-messages corresponding to the original

packet have been received and the inverse transformation has been applied. Packet m is partitioned to a set of x input blocks m = {m1, m2,m3….}, which serve as an input to an The set of pseudo-messages m = {m1, m2,m3,…..} is transmitted over the wireless link.

F. Hiding Based On Md5

A sender S has a packet m for transmission. The sender selects a random key "k" , of a desired length. The message m is split into number blocks {m1,m2,…mn} and the message blocks are encrypted using the algorithm md5. The role of the Receiver "R" is to receive the multiple blocks of data packets and decrypt them. The pre-computed MD5 checksum for the files, so that the user can compare the checksum of the downloaded file to it. The receiver also performs the packet sequence checking while receiving the data packet.

Conclusion

We addressed the problem of selective jamming attacks in wireless networks. We illustrated the effectiveness of the selective jamming attacks by implementing such attacks against the TCP protocol. We showed that an adversary can exploit its knowledge of the protocol implementation to increase the impact of his/her attack at a significantly lower energy cost. We illustrated the feasibility of selective jamming attacks by performing a real time packet classification. To mitigate selective jamming attacks, we proposed several methods that combine cryptographic primitives such as commitment schemes, cryptographic puzzles, and all-or-nothing transformations with physical layer attributes.

The proposed system has the following advantages:

- Internal threat model has been considered
- DoS attacks can be avoided
- Three schemes such as- Hiding Based On Commitments, A Strong Hiding Commitment
- Scheme (Shcs) and Hiding Based On Cryptographic Puzzles has been proposed

References

[1] M. Strasser, C. Po¨pper, S. _Capkun,and M. Cagalj, "Jamming-ResistantKey Establishment UsingUncoordinated Frequency Hopping,"Proc. IEEE Symp. Security andPrivacy, 2008.

[2] B. Greenstein, D. Mccoy, J. Pang, T.Ko-hno, S. Seshan, and D.Wetherall, "Improving Wireless Privacy with an Identiftifier-Free Link Layer Protocol," Proc.Int'l Conf. Mobile Systems,Applications,and Services (MobiSys), 2008.

[3] C. Popper, M. Strasser, and S. _Capkun"Jamming-Resistant BroadcastCommunication without Shared Keys,"Proc. USENIX Security Symp., 2009.

[4] Feng Zhao,Leonidas Guibas,,"Wireless Sensor Networks", Morgan Kaufmann Publications.

[5] M. Tubaishat, S. Madria, (2003) "Sensor Networks : An Overview ", IEEE Potentials, April/May 2003.

[6] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt. Spread Spectrum Communications Handbook. McGraw-Hill, 2001.

[7] W. Xu, W. Trappe, Y. Zhang, and T.Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In Proceedings of MobiHoc, pages 46–57, 2005.