Volume 3, Issue 4, April-2016, pp. 194-196 ISSN (O): 2349-7084

International Journal of Computer Engineering In Research Trends

Available online at: www.ijcert.org

Prevention of Packet Hiding Methods In Selective Jamming Attack

Shital Patil , Vishaka Patil , Rupali Warke , Priyanka Patil

Abstract:- The sharing nature of wireless medium provides various challenging features among various set of users. It is very important in real world and it provides better transfer rate but authentication is ignored. The limitations of existing wired network are overcome by wireless network. These networks act as source for various types of jamming attacks. In analysis and detection of jamming attack various methods are available but sometime they fail. In case of external threat the analysis and reporting of jamming attack is very easy model but it is quite difficult in terms of internal threat model, these internal term uses the knowledge about network secrets and network protocols to launch various attacks with very low effort. Various cryptographic techniques are implemented to prevent these attacks. The main goal of this project is to prevent the information at the wireless physical layer and allowed the safe transmission among communicated nodes although the attacker is present.

Keywords – Commitment scheme, Network Protocols, Packet hiding methods, Real time packet classification and Selective jamming attacks**.**

1. INTRODUCTION

The faster accessibility, compatibility and connectivity between different users is provided by wireless network. Various types of attacks are invited because of the sharing medium of wireless network and it also provides it provide additional features. The adversaries with internal knowledge of network secrets take more effort on jamming the network or decrease the network performance [1], [2]. Anyone which has transceiver can easily inject spurious messages or create noise or interference or produce jamming attack in an ongoing transmission or block the transmission of legitimate users .In the simplest form, the attacker classifies first few bytes of transmitted packet and destroy the message Attacker must have knowledge about each layer of the TCP protocol. The actual format for frame in wireless

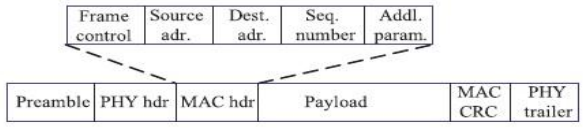

Figure 1: Generic frame format for wireless network.

A.Motivation

The motivation for proposed solution lies in problem with sharing nature of wireless network [1]. Sometimes in the prevention of packet hiding methods in selective jamming attack the how many packet are loss or send to destination. For that purpose the packet hiding methods are detected the packet hiding method are strong packet hiding method ,puzzle hiding ,all-or-nothing transformation, to Overcome the disadvantage of this method we have proposed packet hiding without packet loss method.

B. Problem Definition

Because of sharing nature Of wireless network the various jamming attack are occurred and the wireless medium provides various challenging features. Because of internal knowledge of network and its secrets the jamming attack in which jammer attacks the importance message .We propose the packet hiding scheme without packet loss. In PHSPL, the data is send to the selective host and packets are sending with Header, Sequence ID and host name . Consider in given figure. Node A and B communicates with wireless network. Both A and B there is a jamming Node and communicated with each other. Node j classifies m by receiving only the first few Bytes of m when node A transfer the packet from m to node B, With the reception at B the J corrupts m beyond recovery by interfering in jamming node . We address the problem of preventing the jamming node from classifying m in real time, thus mitigating J's ability to perform selective jamming. Our goal is to transform a selective host note that in the present work, based on protocol semantics we do not address packet classification methods.

Fig 2. Realization of a selective jamming attack

2. RELATED WORK

In related work, we are studying the reasons for jamming, spread spectrum techniques used by the conventional systems and the disadvantages of existing system, prevention mechanism they used and at the last we are studying how the real time packet classification is performed and strong hiding commitment scheme which is used by our proposed system. Because of jamming, the wireless network either stopped or disturbed. Noise, collision, interference these are various forms of jamming. Jamming may be performed intentionally or unintentionally, depending upon either performing attack or due to network load. There is no need of special hardware to execute these attacks only knowledge of preserved information is required.

2.1. STRONG HIDING COMMITMENT SCHEME (SHCS)

In prevention of packet hiding methods in selective jamming attack, A strong hiding commitment scheme (SHCS) is one of technique , and which is based on symmetric cryptography. Assume that the sender has a packet for sending to Receiver. First, the sender S constructs message and the commitment function is an off-the-shelf symmetric encryption algorithm is a publicly known permutation, and k is a randomly selected key of some desired key length s. Both the sender and receiver are randomly selected key and send the packet to destination.

2.2. CRYPTOGRAPHIC PUZZLE HIDING SCHEME

In cryptographic puzzle scheme the sender S has a packet m for transmission. The sender selects a random key k, of a desired length for sending packet to the receiver. Sender S generates a puzzle (key, time), where puzzle () denotes the puzzle generator function, and the time required for the solution of the puzzle. After generating the puzzle P, the sender broadcasts the puzzle. At the receiver side, any receiver R solves the received puzzle to recover key and then computes.

2.3. ALL-OR-NOTHING TRANSFORMATION

The packets are pre-processed by an All-or-nothing transformation (AONT) before transmission of all packet but remain packet are unencrypted. The attacker cannot perform packet classification until all pseudo-messages corresponding to the original packet have been received and then the packet transformation has been applied in inverse way. Packet m is partitioned to a set of x input blocks m = {m1, m2, m3….}, which serve as an input to a set of pseudo-messages m = {m1, m2, m3…} is transmitted over the wireless medium.

3. PROPOSED SYSTEM

In prevention of packet hiding methods in selective jamming attack proposed system gives brief

introduction along with its benifits .The packet hiding without packet loss scheme gives better solution for jamming. for that packets are sending with Header, Sequence ID and host name and the data is send to the destination host. That's why the packet loss is minimum. So the sender and receiver can communicate with each other securely.in packet hiding without packet loss all the information about packet and data is in the header of packet. The PHSPL is more effective over other real time classification methods. There are some advantages of proposed system- Very easy for exploiting knowledge from compromised nodes. The proposed system gives selective jamming attack to DOS with very low effort and this is another advantage of. By using proposed system strong security protocols are achieved.

4. ACTUAL IMPLEMENTATION

In prevention of packet hiding methods in selective jamming attack we uses the Network Simulator 2.34 tool in which front end is tcl and back end is c++. Here are two protocols are used. TCP and AODV protocol and TCP is used for establishing the connection and AODV routing protocol is used for finding routing path for data packets. The transmission rate is 11Mbps for every link. But due to flooding feature of AODV the random attacker fails in disturbing route path. The continuous, random, targeted RREQ the attacker are kept between the communicated pairs.

- Using AODV the Implementation of wireless node in NS-2.
- Implementation of jamming attack with selective transmission.
- In wireless network the Implementation of packet classification is done.
- Implementation of packet hiding for real packet.
- Detection of jamming attack and analysis with throughput.

5. CONCLUSION

In this paper, the prevention of packet hiding methods in selective jamming attacks generated a problem in LAN or wireless networks. Attacker attacks the importance message because of internal knowledge of network and its secrets. We quantified the effectiveness of packet and analysed the security of packet hiding schemes. We propose the packet hiding scheme without packet loss (PHSPL) in which the packet loss is minimum and the sender and receiver can communicate with each other securely. All the information about packet and data is in the header of packet. The PHSPL is more effective over other real time classification methods. So the sender and receiver can communicate securely.

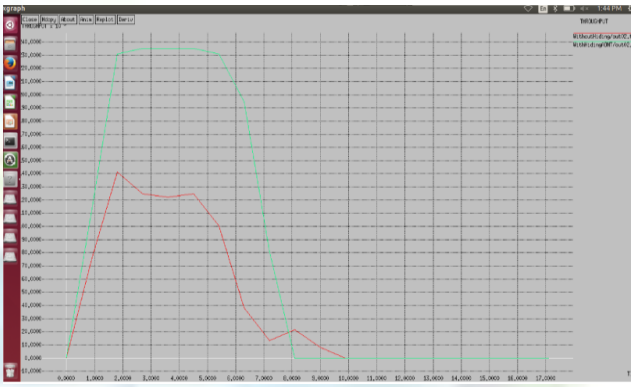

Fig 3: Throughput for packet hiding without packetloss scheme.

REFERENCES

1. P. Tague, M. Li, and R. Poovendran., "*Mitigation of control channel, jamming under node capture attacks*". IEEE Transactions on Computing, 8(9):1221–1234, 2009.
2. 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.
3. L. Lazos, S. Liu, and M. Krunz. "Mitigating *control-channel jamming attacks in multi-channel ad hoc networks*". In Proceedings of the 2nd ACM conference on wireless network security, pages 169–180, 2009.
4. O Goldreich. Foundations of cryptography: Basic applications, Cambrige University press 2005.
5. Damgard. "Commitment schemes and zero knowledge protocols",
6. Lecture notes in computer science, 1561:63-86.
7. Dilip Kumar D.P 1, H.Venugopal2. "Avoiding selective jam attack
8. by packet hiding method in wireless sensor network".
9. G. Noubir and G. Lin. "Low power DoS attacks in data wireless
10. LANs and countermeasures", ACM SIGMOBILE Mobile computing.

