Hiding Approach for Thwarting Attacks in Wireless Networks

Dr. S. Raja Ratna[1]
[1]Associate Professor, Department of Computer Science and Engineering,
V V College of Engineering, Tuticorin, India.
gracelinrr@yahoo.com
D. Merlin Gethsy[2]
[2]Assistant Professor, Department of Computer Science and Engineering,
V V College of Engineering, Tuticorin, India.
merlingethsy@gmail.com

Abstract

The open and shared nature of the wireless medium makes it easy for an adversary to launch a wireless jamming attack. Attacks can be of various types like Denial of Service, Distributed Denial of Service. The objective of denial-of-service attack is to make the server resource unavailable to the legitimate users. If zombies of attacker attack simultaneously it is called distributed denial-of-service attack. The idea here is to prevent the Ad-hoc network from DOS attack. An Ad-hoc network is an infrastructure-less, de-centralized network, consisting of a group of mobile wireless nodes, moving around freely and cooperating with each other in forwarding of packets. Normally jammers are considered outside the network, but this paper describes jammer to be inside the network which selects the packets of higher importance and attack them. Compromising a single node is enough to reveal all the network secrets and that compromised node acts as jammer. To prevent the network from jamming attack, the packets are hided and then transmitted. This paper describes a method for preventing Denial of service attack in the presence of jammers. A technique called Data Commitment-Concealing scheme has been proposed to prevent the classification of transmitted packets and hide the packet effectively.

Key words: *Ad-hoc, denial-of-service, zombies, distributed denial-of-service, jamming*

1. INTRODUCTION

Internet grows rapidly since it was created. Through the Internet, hosts can not only share their information, but also complete tasks cooperatively by contributing their computing resources. Moreover, an end host can easily join the network and communicate with any other host by exchanging packets. Internet were primarily built for frankness and scalability, and these features played a key role in the achievement of today's Internet However, attackers can also take these advantages to prevent legitimate users of a service from using that service by flooding messages to the corresponding server, which forms a Denial of Service (DOS) attack. Wireless networks are more borne to intentional or unintentional attacks than the wired based networks.

Network attacks are general nowadays. There are several types of important attacks, such as the worm, virus, Trojan horse and Denial of service, each of which causes crucial problems to usual business operations [4]. The DOS attacks usually cause considerable disruptions to computer networks.

A DOS attack can be regarded as an attempt of attackers to prevent legal users from gaining a normal network service. DOS attacks usually rely on the exploitation of a specific vulnerability in such a way that it results in a denial of the service. DOS ranks at the fourth place in the list of the most venomous attack classes against information systems. It can just flood packets to keep the server busy with processing packets

or cause congestion in the victim's network, so that the server might not have the ability to handle the packets from legitimate hosts or even cannot receive packets from them.

In order to deplete the victim's key resources (such as Bandwidth and CPU time), the attacker has to aggregate a big volume of malicious traffic. Most of the time, the attacker collects many (could be millions) of zombie machines or bots to flood packets simultaneously, which forms a Distributed Denial of Service attack. Network Security is becoming more and more important because huge volume of data is being exchanged across the internet. The security involves four important aspects: Confidentiality, message authentication, integrity and non–repudiation.

Normally jammers are considered under external threat model. In this paper, jammer is addressed as an internal threat model. Sophisticated adversary who is aware of network secrets and the implementation details of network protocols at any layer in the network stack has been considered. The adversary uses his internal knowledge for launching selective jamming attacks [8] in which messages of higher importance are targeted. For example, a jammer can target route-request/route-reply messages at the network 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 paper is organized as follows. In section 2 the related works are discussed. In section 3 the problem statement and the research contribution are discussed. In section 4 the data commitment-concealing scheme for hiding the data to prevent from attacker is discussed. In section 5 the results of the evaluated parameters are discussed. With section 6 the paper is concluded.

2. RELATED WORK

Liu et al. considered a smart jammer to optimize its jamming strategy [5]. At different layers in the network stack the jammer was assumed to target control messages. The authors proposed the SPREAD system, to mitigate smart jamming which is based on the idea of stochastic selection between collections of parallel protocols at each layer. The uncertainty introduced by this stochastic selection mitigated the selective ability of the jammer.

An 802.11-like wireless protocol called Slyfi was presented by Greenstein et al. that prevents the classification of packets by external observers. Slyfi protocol uses the encryption concept to hides all explicit identifiers from the transmitted packets (e.g., MAC layer header and payload). The identifiers are encrypted using the keys only known to the intended receivers [6] Selective jamming attacks have been experimentally implemented using software-defined radio engines [2], [4].

Thapa et al. studied selective jamming attacks against the rate-adaptation mechanism of 802.11 using selective jammer [2]. They showed in a point-to-point 802.11 communication only specific packets of higher importance are selected by selective jammers which reduce the rate of the communication to the minimum value of 1 Mbps, with relatively little effort (jamming of five to eight packets per second). The results were experimentally verified using the USRP2/GNU radio platform.

3. PROBLEM STATEMENT AND CONTRIBUTION

3.1 Problem Statement

Consider two nodes X and Y communicate via a wireless link as shown in Fig. 1 Within the communication range of both X and Y, there is a jamming node J. When node X transmits a packet *m* (consisting of header and payload) to Y, node J classifies m by receiving only the first few bytes of m. Jammer then corrupts the message m by adding extra bits before reception at Y. This paper addresses the problem of selective jamming and preventing the jammer from classifying the packet, thus preventing the jammer from performing selective jamming. The main objective is to transform a selective jammer to a random one.

3.2 Research Contribution:

In-order to prevent the jammer from classifying the packet and allowing it to reach the destination safely, the packet has to be hidden from the jammer. To mitigate such attacks, a technique called Data concealing has been proposed that prevents the classification of transmitted packets and hides the packet effectively. This technique relies on the joint consideration of cryptographic mechanisms with PHY-layer attributes.

4. PROPOSED DATA COMMITMENT-CONCEALING SCHEME

The proposed Data Commitment-Concealing scheme is used for preventing jamming attack which uses the combined concept of commitment Scheme, cryptographic puzzle generation and hiding between layers.

4.1 Commitment scheme

Commitment scheme is a cryptographic scheme employing symmetric cryptography which allows sender S to commit a value m, to the receiver R while keeping the data m hidden. It uses hiding property. For hiding the packet from the attacker, this concept uses a strong hiding scheme based on commitment. In cryptographic puzzle generation scheme the transmitted packets are temporarily hidden from the jammer using cryptographic puzzles. Consider sender S is transmitting the message m to receiver R. There is a puzzle generator function (PGF) at the sender side and a puzzle solver function at the receiver side.

4.2 Cryptographic Puzzle Generation

Consider a sender S wants to send a packet m to receiver R. The packet is encrypted with a randomly selected symmetric key k of a desirable length s. The key k is blinded using a cryptographic puzzle Q generated by the puzzle generation function at the sender side. Sender S uses the function commit ( ) to generate the pair (C, Q), where $C=E_k(\pi_1(m))$. Sender then sends the puzzle value to the receiver. The receiver R opens the commitment C using the function open ( ), using the key k which is obtained by solving the puzzle using puzzle solver at the receiver side.

For obtaining the strong hiding property, the packet which carries the puzzle value Q is formatted so that all the bit of Q are modulated and placed in the last few bits of the physical layer of the packet. To recover Q, any receiver including the jammer has to wait till the last bits of the packet are decoded. This helps to prevent the early disclosure of Q to the jammer. Both MAC and physical layers are used. To obtain strong hiding property a hiding sub-layer is placed between MAC layer and physical layer. This layer is used for formatting m before it is sent to the physical layer. Frame m consists of header, payload and CRC code as shown in Fig.2(a). CRC codes are used for error detection.

4.3 Hiding Sub-Layer:

The Fig.2 (b) explains the hiding sub-layer as follows, the frame m is permuted using the known permutation π_1 (m). After permutation the frame m is encrypted using random key k and produces the commitment value C. DES or AES symmetric encryption algorithm is used for encryption. Using pad function pad ( ), C is padded with pad bits and puzzle Q. Again it is permuted using the known permutation. The reason for permutation is to delay the reception of packet headers and to get random input for the encryption algorithm.

As shown in Fig.2(c) π_2 (C||pad(C) ||Q) enters into physical layer which is attached with the physical layer header of length y2. The frame carrying (C, Q) before passing the encoder has the length of (y+y1+y2+x). If the rate of the encoder is considered as r1, then the output of the encoder will be of 1/r1(y+y1+y2+x) where, y1 is the length of the pad bits padded to m, y2 is the header length added to physical layer, y is the length of the original frame m, x is the length of the puzzle Q.

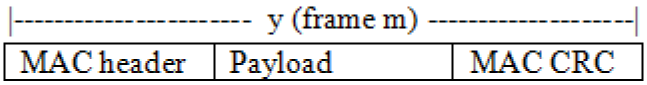


Fig. 2 (a) MAC layer

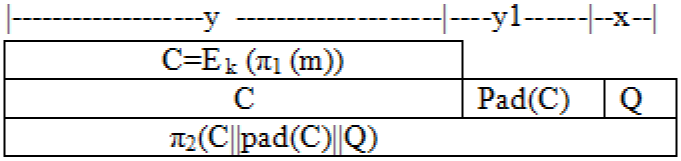

|------------------y -------------------|----y1------|--x--|
C=E$_k$ (π_1 (m))
C
Pad(C)
Q
π_2(C||pad(C)||Q)

Fig. 2 (b) Hiding sub-layer between MAC & Physical layer

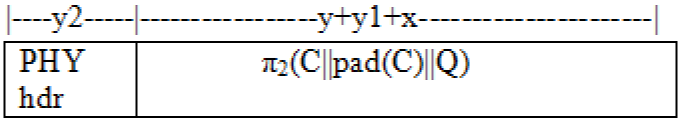


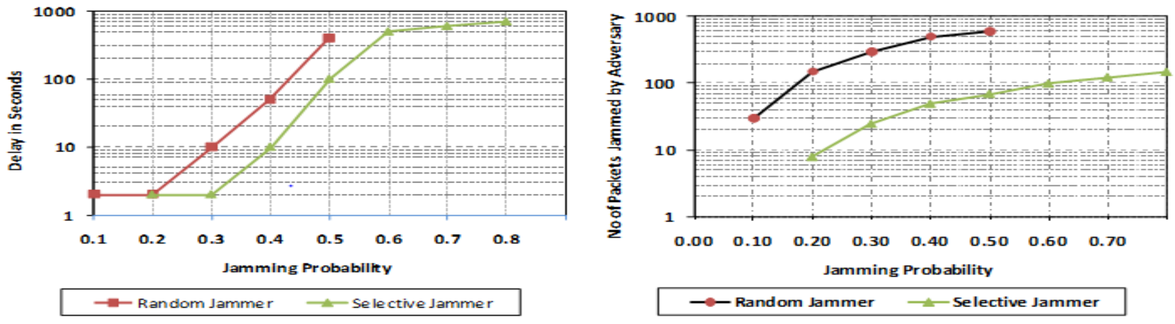
Fig. 2 (c) Physical layer

5. EXPERIMENTAL EVALUATION

A random topology of 50 Nodes are deployed with random movement in an area of 100 x 150 m^2, a 2 KB file is transferred between the sender node and receiver node connected via multiple hops. AODV protocol is used for finding the route data across the network. Selective jamming can attack both data packets and control packet, but in this paper selective jamming of data packet is considered.

The first set of experiment shows how selective jamming of data packets differs from random jamming of data packets. Delay represents the amount of time required to push all of the data bits into the communication channel.

The Fig. 3(a) shows the average delay D_A for completing the data transfer , as a function of jamming probability J_P, it shows that selective jamming of data packets grows several order of magnitude larger when compared to random jamming of data packets. The Fig. 3(b) shows the average number of packets jammed by the adversary J_A, as a function of jamming probability J_P. It is found that selective jamming of data packets is jammed for larger probability ratio when compared to random jamming of data packets.



(a) (b)

Fig. 3. For increasing jamming probability (a) Average Delay b) Number of packets jammed by adversary for random jammer and Selective jammer

The second set of experiment shows the comparative chart between cryptographic puzzle method and data concealing method. Cryptographic puzzle method deals with only puzzle generation method whereas data concealing method deals with both commitment scheme and puzzle generation scheme which more efficient than cryptographic schemes for hiding data from the jammer. The Fig. 4(a) show the average effective throughput, the throughput for data concealing method is higher when compared to cryptographic puzzle method. The Fig. 4(b) shows the number of packet jammed by the adversary between cryptographic puzzle method and data concealing method. It is found that the number of packets jammed in data concealing method is lesser when compared to cryptographic puzzle method.

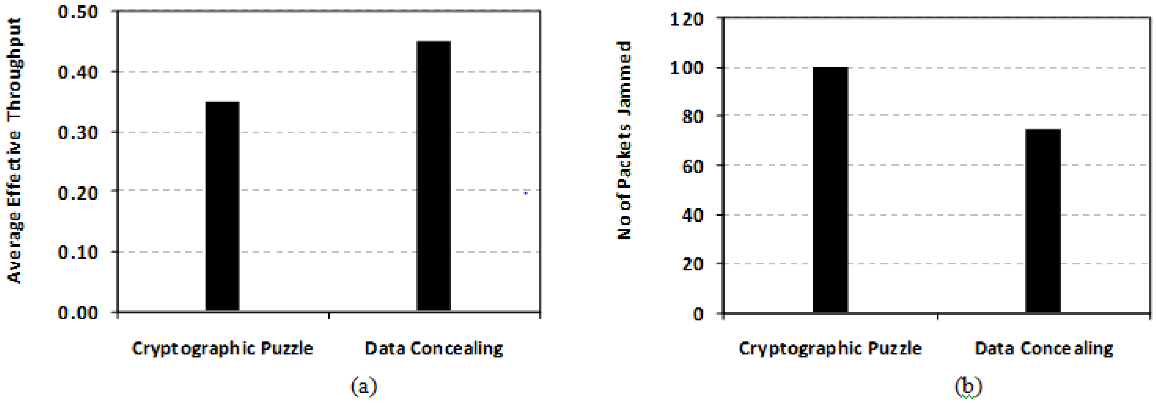


Fig. 4. For increasing jamming probability (a) Average Effective throughput b) Number of packets jammed by adversary using cryptographic puzzle and Data Concealing

6. CONCLUSION

This paper addresses jammer as an internal threat model which knows about network secrets and the protocols used. A technique called Data Commitment-Concealing scheme has been proposed to prevent the classification of packets and to hide the packet effectively from jammers. This technique relies on the joint consideration of cryptographic mechanisms with physical layer attributes. The data concealing method discussed in this paper effectively hides the packets from the attacker and transmits the data to the receiver efficiently. It is experimentally verified that this scheme provides better average throughput with lower number of packets jammed.

REFERENCES

[1] T. Dempsey, G. Sahin, Y. Morton, and C. Hopper, “Intelligent Sensing and Classification in Ad Hoc Networks: A Case Study,” IEEE Aerospace and Electronic Systems Magazine, vol. 24, no. 8, pp. 23-30, Aug. 2009.

[2] B. Thapa, G. Noubir, R. Rajaramanand and B. Sheng, “On the Robustness of IEEE802.11 Rate Adaptation Algorithms against Smart Jamming,” Proc. ACM Conf. Wireless Network Security (WiSec), 2011.

[3] D. Thuente and M. Acharya, “Intelligent Jamming in Wireless Networks with Applications to 802.11 b and Other Networks,” Proc. IEEE Military Comm. Conf. (MILCOM), 2006.

[4] M. Wilhelm, I. Martinovic, J. Schmitt, and V. Lenders, “Reactive Jamming in Wireless Networks: How Realistic Is the Threat,” Proc. ACM Conf. Wireless Network Security (WiSec), 2011.

[4] X. Liu, G. Noubir, and R. Sundaram, “Spread: Foiling Smart Jammers Using Multi-Layer Agility,” Proc. IEEE INFOCOM, pp. 2536-2540, 2007.

[5] B. Greenstein, D. Mccoy, J. Pang, T. Kohno, S. Seshan, and D. Wetherall, “Improving Wireless Privacy with an Identifier- Free Link Layer Protocol,” Proc. Int’l Conf.
Mobile Systems, Applications, and Services (MobiSys), 2008

[6] Y.W. Law, M. Palaniswami, L.V. Hoesel, J. Doumen, P. Hartel, and P. Havinga, “Energy-Efficient Link-Layer Jamming Attacks against WSN MAC Protocols,” ACM Trans. Sensor Networks, vol. 5, no. 1, pp. 1-38, 2009.

[7] T.X. Brown, J.E. James, and A. Sethi, “Jamming and Sensing of Encrypted Wireless Ad Hoc Networks,” Proc. ACM Int’l Symp. Mobile Ad Hoc Networking and Computing (MobiHoc), pp. 120-130, 2006.

[8] M. Cagalj, S. Capkun, and J.-P. Hubaux, “Wormhole-Based Anti- Jamming Techniques in Sensor Networks,” IEEE Trans. Mobile Computing, vol. 6, no. 1, pp. 100-114, Jan. 2007.

[9] A. Chan, X. Liu, G. Noubir, and B. Thapa, “Control Channel Jamming: Resilience and Identification of Traitors,” Proc. IEEE Int’l Symp. Information Theory (ISIT), 2007.

[10] D.Comer, Internetworking with TCP/IP : Principles, Protocols,and Architecture,Prentice Hall, 2006.

[11] G.Noubir and G.Lin, Low –power DoS attacks in data wireless LAN’s and countermeasures, ACM SIGMOBILE Mobile Computing and Communications review, 7(3):29-30, 2003.

[12] O.Goldreich, Foundations of Cryptography: Basic applications, Cambridge University Press, 2004.

[13] M.Gowsalya,V.Palanisamy,” Detection and prevention of congestion attacks and packet loss using piggyback methods in wireless network”, International Journal of Computer Applications (0095 – 8887), Volume 3, No. 3, 2012.

[14] G.Lin and G.Noubir, “On link layer Denial of service in data wireless LANs. Wireless communications and Mobile Computing, 5(3):273-284, May 2004.

[15] P. Yi, Y. Wu, F. Zou, and N. Liu, ”A Survey on Security in Wireless Mesh Networks”, *IETE Technical Review*, Vol. 27, No. 1, pp. 6-14, 2010.