International Journal of Modern Engineering Research (IJMER)
www.ijmer.com Vol.3, Issue.3, May-June. 2013 pp-1346-1349 ISSN: 2249-6645

AONT- Based Packet Hiding Method for Preventing Jamming Attacks

M.prasanthi, [1] G. Bala Raju[2]
[1]M.Tech, Sri Sunflower College of Engineering & Technology, Lankapalli
[2]Asst.Professor, Dept.of CSE, Sri Sunflower College of Engineering & Technology, Lankapalli

Abstract: *Wireless networks now enjoy widespread commercial implementation because of their ease of use, low cost and setup. However, since accessing wireless media is much easier than tapping a wired network, then security becomes a serious concern when implementing any wireless network. We consider a particular class of Denial of Service (DoS) attacks called jamming attacks. In the simplest form of jamming, the attacker interferes with the reception of messages by transmitting a continuous jamming signal, or several short jamming pulses. Jamming results in the loss of link reliability, increased energy consumption, extended packet delays and disruption of end-to-end routes. The use of distinct, dedicated communication links to transmit data and control traffic introduces a single point of failure for a denial of service attack, in that an adversary may be able to jam control channel traffic and prevent relevant data traffic. To prevent such jamming attacks, in this paper we propose a packet hiding method based on all- or- nothing transforms (AONT).*

Keywords: *AONT, Cipher text, DOS, Jammer.*

I. Introduction

The broadcast nature of wireless networks makes them particularly vulnerable to the radio interference, which prevents the normal communications. This interference or jamming can destroy the wireless transmission and may occur either by means of unintentional interference or collision at the receiver side or intentional attacks. The jamming attack can be easily launched since it can be implemented by simply listening to the open medium and broadcasting in the same frequency band as sensor networks.

In order to cope with this kind of Denial-Of- Service (DOS) style attack, many strategies and techniques have been developed. The traditional method is to use the sophisticated physical layer technologies such as- DSSS (Direct Sequence Spread Spectrum) and FHSS (Frequency Hopping Spread Spectrum), which have been widely used in military communication. However, it can be too costly for the energy and frequency constrained networks. So many kinds of evasion strategies have been researched, such as wormhole-based anti-jamming techniques [1], channel surfing [2] and timing channel [3].

This paper presents a packet hiding method based on AONT to prevent jamming attacks. Jamming attack is a kind of Denial of Service (DOS) attack, which prevents other nodes from using the channel to communicate by occupying the channel that they are communicating on. We define the jammer in wireless sensor networks as an entity who is purposefully trying to interfere with the physical transmission and reception of wireless communications. A typical scenario of jamming attack is shown in the figure 1. The normal nodes C and D has been jammed by the malicious node “X”, so the communications between the jammed nodes(C, D) and the normal nodes (A, B, E, H, I) are disrupted.

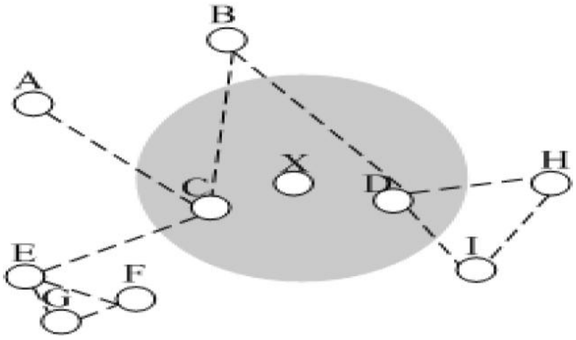

Figure 1: An example of Jamming Attack

II. Types of Jammers

Jammers are of five types based on the time of their activity and the mode of attacks:

- Continuous Jammers
- Impersonate Jammers
- Unsystematic Jammers
- Systematic Jammers
- Exacting Jammers

A. Continuous Jammers

The continuous jammers [4] transmit the jamming or attack signal into the medium at a constant rate. Since the jamming signal uses the medium or channel, the other users will not sense the medium to be free for their legitimate service. The packets transmitted by these type of jammers are random meaningless messages. The jammers are small electronic devices powered by a battery with the limited power resources. Hence after a considerable time, the jammer dries its battery power and thus the medium is retrieved from the attack. Even an energy efficient jammer could not last for a considerable time but still for a limited span, the jammer completely blocks the services in a network. The packets could be identified from the content it stores and thus the attacker. The route could be blocked to prevent the network from the attack.

B. Impersonate Jammers

Impersonate jammers [5] sends the packets which resemble the original packets. The network administrator would not try to suspect these packets and thus allows the packets into the network. Yet these jammers are not energy efficient and thus dry out soon after. The only advantage is that it evades the detection mechanisms for a longer period of time.

C. Unsystematic Jammers

Unsystematic jammers [5] are the foundation of energy efficient jammers. These type of jammers extended their life span by limiting the time of activity. Packets are sent from these jammers at a random time rather than continuously thus serving for a longer period. The jammers would alternate their activity time that is they would be on for certain period of time and thus switched on for a certain time. Conserving the power at regular intervals increased their lifetime, causing a threat to the entire network.

D. Systematic Jammers

Systematic jammers [6] are the intelligent jammers of all other types. Unlike the unsystematic jammers, they follow a strict order to be switched- on and off. These are highly energy efficient and the most significant in attacking the resources in the netwrok. This type of jammers waits for the sender and the receiver nodes to start the communication process and then gets activated. The mode of attack is simplified and then the attack becomes more vulnerable to the network. If there is no communication between the nodes, then the jammers remains idle, and conserving the energy. Moreover the packets sent over the medium are similar to the legal data packets raising no different pattern to awaken the defense mechanisms.

E. Exacting Jammers

Exacting jammers are considered to be the critical jammers which have to be spotted immediately before irrecoverable changes occur in the network. The exacting jammers determine the nature of the packet sent in between the nodes of a network. Unless those packets are of high importance [7], they are free to move. Packets such as route request or route response or a packet of either important data or control flow would readily be subjected to the jamming attack. The source of the jamming attack, being a part of the original network, defines the longer time for suspicion.

III. RELATED WORK

Continuous jamming has been used as a denial-of-service (DoS) attack against voice communication since the 1940s [8]. Recently, several alternative jamming strategies have been demonstrated [9], [10]. Intelligent attacks which target the transmission of specific packets were presented in [11], [12]. In [12], the authors consider an attacker who infers eminent packet transmissions based on timing information at the MAC layer.

In both [11], [12], real-time packet classification was considered beyond the capabilities of the adversary. Selectivity was achieved through inference from the control messages already transmitted. Channel-selective jamming attacks were considered in [13]. It was shown that targeting the control channel reduces the required power for performing a denial- of- service attack by several orders of magnitude. In [14], the authors proposed a randomized frequency hopping algorithm, to protect the control channel inside jammers. Finally, in [10], the authors proposed a frequency hopping anti-jamming technique that does not require the sharing of a secret hopping sequence, between the communicating parties.

IV. ALL- OR- NOTHING TRANSFORM

The concept of an All-or-Nothing Transform (AONT) was introduced by Rivest [15] to increase the cost of brute force attacks on block ciphers without changing the key length. As defined in [15], an AONT is an efficiently computable transformation f, mapping sequences of blocks (i.e., fixed length strings) to sequences of blocks, which has the following properties:

1. Given all of f(x1,x2,…….xn)= (y1,y2,…..yn), it is easy to compute x1,x2,……xn.
2. Given all but one of the blocks of the output, it is infeasible to find out any information about any of the original blocks xi.

An AONT itself does not perform any encryption, since there is no secret key information involved in it.. However, if its output is encrypted, block- by- block, with a block cipher, the resulting scheme will have the following interesting property- An adversary cannot and out any information about any block of the message without decrypting all the blocks of the cipher text. Now if the adversary attempts to do an exhaustive search for the key, he will need to perform n' decryptions before determining whether a given key is correct. Thus, the attack will be slowed down by a factor of n', without any change in the size of the secret key. This is particularly important in scenarios where the key length is of constrained to be insecure or marginally secure.

The use of AONT with encryption can be particularly useful for remotely keyed encryption i.e., applications where the part of the system that contains the keys is separate, and where bandwidth restrictions prevent us from sending the whole message from the insecure to the secure component [4]. An example of such a scenario would be the case where the keys are stored in the smartcard, and the user wishes to encrypt or decrypt large files. Through the use of AONT, we can completely eliminate any encryption components from the host system, and restrict such operations to the smartcard.

V. Proposed Method

In the proposed work, the packets are pre-processed by an AONT before transmission but remain unencrypted. The jammer cannot perform the packet classification until all 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. Recently Rivest motivated by different security concerns arising in the context of block ciphers, introduced an intriguing primitive called the All-Or-Nothing Transform (AONT). An AONT is an efficiently computable transformation "T" on strings such that

- For any string x, given *all* of T(x), one can efficiently recover "x"
- There exists some threshold such that any polynomial time adversery that learns all but bits of T(x) obtains no information about "X" (in a computational sense).

The AONT solves the problem of partial key exposure-rather than storing a secret key directly, we store the AONT applied to the secret key. If we can build an AONT, where the threshold value `is very small compared to the size of the output of the AONT, we obtain security against almost total exposure. Notice that this methodology applies to secret keys with arbitrary structure, and thus protects all the kinds of cryptographic systems. One can also consider AONT's that have a two-part output- a public output that doesn't need to be protected, and a secret output that has the exposure-resilience property stated above. Such a notion would also provide the kind of protection we try to achieve. The AONT has many other applications, as well, such as enhancing the security of block-ciphers and making the fixed-block size encryption schemes more efficient.

Figure 2 shows the proposed packet hiding method. The Sender transmits the message, which is divided into blocks of fixed size. These blocks are given as input to AONT. Then AONT encrypts these message blocks with a shared secret key and then sends to the receiver. Now the receiver decrypts these blocks with the same key, thus retrieves the original data.

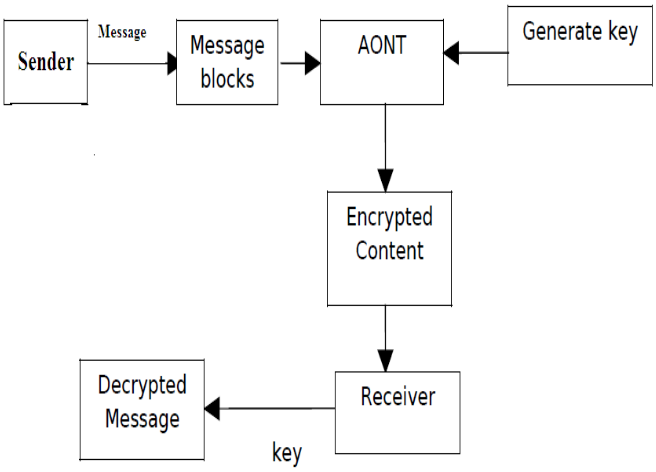

Figure 2: AONT- based packet hiding method

VI. Conclusion

Jamming attack is a kind of Denial of Service (DOS) attack, which prevents other nodes from using the channel to communicate by occupying the channel that they are communicating on. To prevent such attack, we propose a packet method based on All-or-Nothing Transform (AONT). An AONT itself does not perform any encryption, since there is no secret key information involved in it.. However, if its output is encrypted, block- by- block, with a block cipher, the resulting scheme will have the following interesting property- one must decrypt the entire cipher text before one can determine even one message block. This means that brute force searches against AONT encryption are slow down by a factor equal to the number of blocks in the cipher text.

REFERENCES

[1] Mario cagalj, srdjan capkun, jean hubaux, "Wormhole-Based Antijamming Techniques in Sensor Networks", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 6, NO. 1, JANUARY 2007.

[2] Wenyuan Xu , Wade Trappe, Yanyong Zhang, "Channel Surfing: Defending Wireless Sensor Networks from Interference", Cambridge, Massachusetts, USA, IPSN', 2007.

[3] Wenyuan Xu , Wade Trappe, Yanyong Zhang, "Anti-jamming Timing Channels for Wireless Networks", Alexandria, Virginia, USA, WiSec, 2008.

[4] G.Lin and G. Noubir."On link layer denial of service in data WirelessLANs".Wireless Communications and Mobile Computing, 5(3):273–284,May 2004.

[5] M. Wilhelm, I. Martinovic, J. Schmitt, and V. Lenders. "Reactivejamming in wireless networks: How realisticis the threat?" InProceedings of WiSec, 2011.

[6] W. Xu, T.Wood, W. Trappe, and Y. Zhang. "Channel surfing and spatial retreats: defenses against wireless denial of service". In Proceedings ofthe 3rd ACM workshop on Wireless security, pages 80–89, 2004.

[7] Alejandro Proano 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.

[8] M. Simon, J. Omura, R. Scholtz, and B. Levitt. Spread spectrum communications handbook. McGraw-Hill Companies, 1994.

[9] G. Noubir and G. Lin. Low-power DoS attacks in data wireless LANs and countermeasures. ACM SIGMOBILE Mobile Computing and Communications Review, 7(3):29–30, 2003.

[10] C. Po¨pper, M. Strasser, and S. Cˇ apkun. Jamming-resistant broadcast communication without shared keys. In Proceedings of the USENIX Security Symposium, 2009.

[11] 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 Transactions on Sensor Networks, 5(1):1–38, 2009.

[12] D. Thuente and M. Acharya. Intelligent jamming in wireless networks with applications to 802.11b and other networks. In Proceedings of the IEEE MILCOM, 2006.

[13] A. Chan, X. Liu, G. Noubir, and B. Thapa. Control channel jamming: Resilience and identification of traitors. In Proceedings of the IEEE ISIT, 2007.

[14] L. Lazos, S. Liu, and M. Krunz. Mitigating control-channel jamming attacks in multi-channel ad hoc networks. In Proceedings of the second ACM conference on wireless network security, pages 169–180, 2009.

[15] Ronald Rivest, "All- or- nothing encryption and the package transform", 4th international workshop on fast software encryption, pages 210- 218, 1997.