International Journal of Modern Trends in Engineering and Research
www.ijmter.com
e-ISSN No.:2349-9745, Date: 2-4 July, 2015

Implementation on Preventing Selective Jamming Attack Using Cryptographic Based Packet hiding method

Mr.Santosh B, Mahale[1], Prof.Prashant P.Rewagad[2]
[1]*ME CSE GHRIEM,Jalgaon,santosh.viit@gmail.com*
[2] *HOD CSE, GHRIEM, Jalgaon, prashantrewagad@gmail.com*

Abstract— The free ware nature of the with and without wired medium leaves it vulnerable to purpose intrusion attacks, typically can called as blocking or jamming. This on purpose intrusion with wireless transmissions can be used as a launch pad for mounting the various attacks like Denial-of-Service attacks (DOS) on wireless networks. Typically, jamming has been list out under an outside risk model. However, adversaries with internal knowledge of protocol specifications and network secrets can launch lowest level efforts jamming attacks that are difficult to identify and counter. It addresses the problem of selective jamming attacks in wireless networks. In these attacks, the challenger is on the go only for a less interval of time, selectively achieving messages of high importance. It illustrate the advantages of selective jamming in terms of network performance degradation and adversary effort by presenting analysis on network security, a selective attack on Transport Control Protocol and one on routing, in that selective jamming attacks can be launched by performing real-time packet classification at the physical layer. To mitigate these attacks, so that, three schemes that prevent real- time packet classification by combining cryptographic and primitives with physical-layer attributes.

Keywords- Modulation Schemes, DOS, Real time packet classification.

I. INTRODUCTION

Wireless networks rely on the continuous availability of the wireless medium to interconnect participating nodes. However, the open nature of this medium leaves it vulnerable to multiple security threats. Anyone with a transceiver can eavesdrop [1] on wireless transmissions, inject spurious messages, or jam legitimate ones. While eavesdropping and message injection can prevented using cryptographic methods, jamming attacks are much harder to counter. They have been shown to actualize severe Denial-of-Service (DoS) attacks against wireless networks [14], in the simplest form of jamming; the adversary interferes with the reception of messages by transmitting a continuous jamming signal [4], or several short jamming pulses [1].

1.1 Detection of Jamming

WLANs are built upon a shared medium that makes it easy to launch jamming attacks. These attacks can be easily accomplished by sending radio frequency signals that do not follow any MAC protocols. Detection of jamming attacks can be done in multiple ways. One of the most efficient ways is to jump channels. Because communication between two legitimate no des is done through a specific frequency, the frequency can be changed if necessary.

II . LITERATURE SURVEY

The various attacks on selective jamming attacks like Denial-of-Service attacks (DOS) on wireless networks. Typically, jamming has been list out under an outside risk model. However, adversaries with internal knowledge of protocol specifications and network [16] secrets can launch lowest level efforts jamming attacks that are difficult to identify and counter. It addresses the problem of selective jamming attacks in wireless networks.

To mitigate jamming attacks many hiding schemes were used. These are,

1. Real Time Packet Classification
2. Strong hiding commitment scheme
3. Cryptographic puzzle base scheme
4. All-or-nothing transmission

2.1 Real Time Packet Classification

At the Physical layer, a packet m is encoded, interleaved [1], and modulated before it is transmitted over the wireless channel. At the receiver, the signal is demodulated, de-interleaved and decoded to recover the original packet m. Nodes A and B communicate via a wireless link. Within the communication range of both A and B there is a jamming node J. When A transmits a packet m to B, node J classifies m by receiving only the first few bytes of m. J then corrupts m beyond recovery by interfering with its reception at B [1].

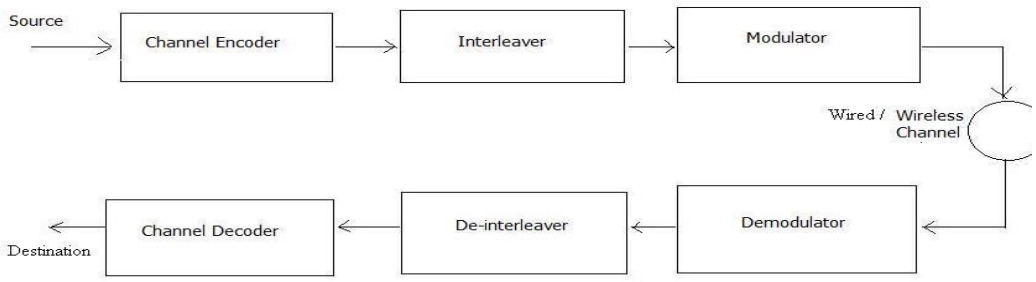


Figure 2.1: Block diagram of Proposed of Generic communication system.

The figure 2.1 shows the proposed architecture diagram of Real time Packet Classification process[1] ability in classifying a packet m depends on the implementation of the blocks in Fig. 2.1 The channel encoding block expands the original bit sequence m, adding necessary redundancy for protecting m against channel errors. For example, a α/β-block code may protect m from up to errors per block.

2.2. A Strong Hiding Commitment Scheme (SHCS)

It is based on symmetric cryptography. Assume that the sender has a packet for Receiver. First[1][2], S constructs commit message 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. Upon reception of d, any receiver R computes.

2.2 Cryptographic Puzzle Hiding Scheme(CPHS)

A strong hiding commitment scheme (SHCS), which is based on symmetric cryptography. Assume that the sender has a packet for Receiver. First [1][2], S constructs commit(message) the commitment function is an off-the-shelf symmetric encryption algorithm is a publicly known permutation.

III. PROPOSED WORK

It focuses on At the Physical layer, a packet m is encoded, interleaved [1], and modulated before it is transmitted over the wireless channel. At the receiver, the signal is demodulated, de-interleaved and decoded to recover the original packet m. Nodes A and B communicate via a wireless link. Within the communication range of both A and B there is a jamming node J. When A transmits a packet m to B, node J classifies m by receiving only the first few bytes of m. J then corrupts m beyond recovery by interfering with its reception at B[1].

3.1 Methods Used

There are various methods that are used for achieving strong security of system and hence it go through them in detail. So here using Real time classification for achieving strong hiding security. The figure 3.1 shows the proposed architecture diagram of Real time Packet Classification process[1] ability in classifying a packet m depends on the implementation of the blocks in Fig. 3.1 The channel encoding block expands the original bit sequence m, adding necessary redundancy for protecting m against channel errors.

For example, an α/β-block code may protect m from up to errors per block.

Alternatively, an α/β-rate convolution encoder with a constraint length of Lmax, and a free distance of e bits provides similar protection. For our purposes, it assumes that the rate of the encoder is α/β. At the next block, interleaving is applied to protect m from burst errors. For simplicity, consider a block interleaved that is defined by a matrix Ad×β.

3.2 Realization of a selective jamming attack

Impact of selective jamming on critical network functions. Our findings indicate at selecti jamming attacks lead to DoS with very low effort on behalf of the jammer.

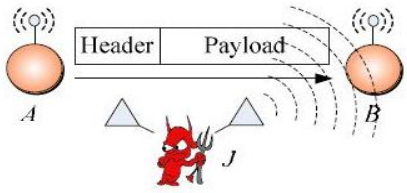


Figure 6.1 Realization of a selective jamming attack

An intuitive solution to selective jamming would be the encryption of transmitted packets (including headers) with a static key. However, for broadcast communications, this static decryption key must be known to all intended receivers and hence, is susceptible to compromise. An adversary in possession of the decryption key can start decrypting as early as the reception of the first cipher text block. For example, consider the cipher-block chaining (CBC) mode of encryption [7]. To encrypt a message m with a key k and an initialization vector IV, message m is split into x blocks m1, m2, mx, and each cipher text block ci, is generated as:

$$c_1 = IV,\ c_{i+1} = E_k(c_i \oplus m_i),\ i = 1, 2, \ldots,$$

x, (1)

Where E_k (m) denotes the encryption of m with key k. The plaintext m_i is recovered by:

$$m_i = c_i \oplus D_k (c_{i+1}), \quad i = 1, 2, \ldots,$$

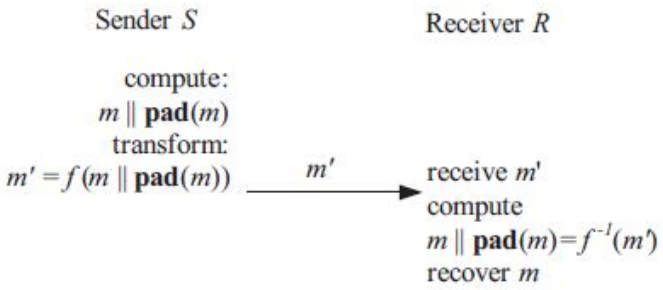
x. (2)

3.3 Algorithm

1. Symmetric encryption algorithm

2. Brute force attacks against block encryption algorithms

Algorithm Description



The AONT-based Hiding Scheme (AONT-HS).

3.4 RESULT

In the proposed work, in this section, here analyzed the effectiveness & comparison of all packets hiding method. Here have shown the effective throughput averaged over 100 different traces. So Observed that the PHSWPL is more effective than other hiding method. This method is required less computational overhead than AONT Because of base of hiding method.

CONCLUSION

As per the previous system, in selective jamming attacks generated a problem in LAN or wireless networks. Jammer attacks the importance message because of internal knowledge of network & its secrets. Here showed that the jammer could classify transmitted packets in real time by decoding the first few symbols of an ongoing transmission. It evaluated the impact of selective jamming attacks on network. Here show that a selective jammer can significantly impact performance with very low effort. Hence it analyzed the security of packet hiding schemes and quantified their effectiveness. Here I propose the packet hiding scheme without packet loss. In PHSPL, packets are sending with Header, Sequence ID and host name and the data is send to the selective host. That's why the packet loss is minimum. So the sender and receiver can communicate with each other securely. All the information about packet and data is in the header of packet. Hence the PHSPL is more effective over other real time classification methods.

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] B. Thapa, G. Noubir, R. Rajaramanand, and B. Sheng. On the robustness of IEEE802.11 rate adaptation algorithms against smart jamming. In *Proceedings of WiSec*, 2011.

[3] M. Wilhelm, I. Martinovic, J. Schmitt, V. Lenders, "Reactive jamming in wireless networks: How realistic is the

threat?", In Proceedings of WiSec, 2011.
[4] Y. Liu, P. Ning, H. Dai, and A. Liu. Randomized differential DSS: Jamming-resistant wireless broadcast communication. In *Proceedings of INFOCOM*, San Diego, 2010.
[5] SciEngines. Break DES in less than a single day. *http://www. sciengines.com*, 2010.
[6] C. P¨opper, M. Strasser, and S. Capkun. Jamming-resistant broadcast communication without shared keys. In *Proceedings of the USENIX Security Symposium*, 2009.
[7] 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 Sensors Networks*, 5(1):1–38, 2009.
[8] T. Dempsey, G. Sahin, Y. Morton, C. Hopper. "Intelligent sensing and Classification in ad hoc networks: a case study. Aerospace and Electronic Systems Magazine", IEEE, 24(8):23 -30, August 2009.
[9] P. Tague, M. Li, and R. Poovendran. Mitigation of control channel jamming under node capture attacks. IEEE Transactions on Mobile Computing, 8(9):1221–1234, 2009.
[10] K. Gaj and P. Chodowiec. FPGA and ASIC implementations of AES.Cryptographic Engineering, pages 235–294, 2009.
[11] M.Strasser, C.P'opper S.Capkun and M.Cagali.Jamming-resistant key of the establishment using uncoordinated frequency hopping in proceedings of IEEE Symposium on Survey and Privacy ,2008.
[12] B. Greenstein, D. Mccoy, J. Pang, T. Kohno, S. Seshan, and D. Wetherall. Improving wireless privacy with an identifier-free link layer protocol. In Proceedings of Mobole System, 2008.
[13] Cagalj, S. Capkun, and J.-P. Hubaux.Wormhole-based anti-jamming techniques in sensor networks. *IEEE Transactions on Mobile Computing*, 6(1):100–114, 2007.
[14] Schneier. Applied cryptography: protocols, algorithms, and source codein C. John Wiley & Sons, 2007.
[15] Thuente and M. Acharya. Intelligent jamming in wireless networks with applications to 802.11 b and other networks. In Proceedings of the IEEE Military Communications Conference MILCOM, 2006.
[16] 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.

