International Journal of Smart Sensor and Adhoc Network

Volume 3 | Issue 1 Article 7

October 2012

A SECURE PACKET HIDING TECHNIQUE FOR PREVENTING JAMMING ATTACKS

ANNAPOORNA B.R
CMRIT, Bangalore, India, annapoornabr@gmail.com

MRS.SHANTHI M. B
Dept of CSE, CMRIT, Bangalore, India, shanthimb@gmail.com

DR.JITENDRANATH MUNGARA
Dept of CSE & ISE, CMRIT, Bangalore, India, jmungara@gmail.com

A SECURE PACKET HIDING TECHNIQUE FOR PREVENTING JAMMING ATTACKS

ANNAPOORNA B.R.[1], MRS.SHANTHI M. B.[2], DR.JITENDRANATH MUNGARA[3]

[1]M.Tech CNE, CMRIT, Bangalore, India
[2]Asst. Prof., Dept of CSE, CMRIT, Bangalore, India
[3]Prof. & Dean, Dept of CSE & ISE, CMRIT, Bangalore, India

Abstract- Wireless Sensor Networks are exposed to serious security threat called jamming. This type of attacks with wireless transmission can be used as a catalyst for rising Denial-of-service attacks. This paper considers the problem of jamming under an internal threat model, where the attacker who is aware of all the network secrets and the details of implementation which results in the difficulty of detection. Jamming is broken down in to layers and this paper focuses on jamming at the Transport/Network layer. To overcome these attacks, we develop three schemes that prevent the attacker from attacking the packets. Then we evaluate the security of our schemes.

Keywords *- Jamming, DOS attacks, Wireless sensor Networks, Selective jamming, Packet classification, DSA, Encryption.*

I. INTRODUCTION

Wireless technologies have become increasingly popular in our everyday business and personal lives. It enables one or more devices to communicate without physical connections-without requiring network or peripheral cabling. As we know that wireless networks serve as the transport mechanism between devices and among devices. However, because of this wireless nature these are prone to multiple security threats in which one of the major serious security threat is jamming. Jamming can disrupt wireless transmission and can occur either unintentionally in the form of noise or interference at the receiver side. Jamming attacks may be viewed as a special case of Denial of service (DOS) attacks [1]. In simplest form of jamming, the attacker interferes with the set of frequency bands used for communication by transmitting a continuous jamming signal [2] or several short jamming pulses [3].

Normally Jamming attacks have been considered under an external threat model, but here we are considering jamming attacks under an internal threat model. Under an external threat model, jamming strategies transmits high power interference signals continuously or randomly [2] [4]. This type of strategies has several disadvantages. First, the attacker has to spend huge amount of energy in order to jam certain frequency bands. Second, these types of attacks are easy to detect because of continuous presence of unusually high interference levels. [3], [4], [6].

A well known countermeasure against this type of jamming attacks are spread spectrum techniques such as frequency hopping, direct sequence spread spectrum and chirp spread spectrum [5]. With respect to these entire techniques one thing that is common is that they rely on secret codes that are user between the communicating parties.

In this paper, we deal with the problem of jamming under an internal threat model. Here the attacker who is aware of network secrets and the implementation details of all the layers of network protocols in the network stack. The attacker uses his internal knowledge for launching selective jamming attacks in which high importance messages are targeted. For example, a jammer can target TCP acknowledgments in a TCP session or target route request/reply messages at the routing layer.

II. RELATED WORK

Jamming problem has been addressed under various threat models. The impact of external selective jammer targeting various control packets at the MAC layer is studied in the paper [7] by Thuente. Selective jamming attack is based on protocol semantics, where they considered several packet identifiers for encrypted packets such as packet size, signal sensing and timing information of different protocols. Unification of packet characteristics like minimum length and inter packet timing was used in order to prevent selectivity.

In [8], attempts to make use of protocols at various layers to get three advantages: targeted jamming, jamming gain, and reduced probability of detection. In targeted jamming, it may jam particular nodes, flows or links. Here the attacker may be interested in specific parts of the network and attacking those regions can lead to further jamming gains. Where as in reduced probability of detection, the sufferer network may not be aware of jamming countermeasures. Selective jamming attacks have been experimentally implemented using software defined radio engines [9]. USRP2-based jamming

platform called RFReact was implemented by Wilhelm [9] that enables selective and reactive jamming. We develop three schemes that prevent jamming attacks; they are Strong Hiding Commitment Scheme, Cryptographic Puzzle Hiding Scheme and All or Nothing Transformation.

In Strong Hiding Commitment Scheme we use DES [10] algorithm to encrypt packets where single secret key is used between sender and receiver. The major disadvantage is, the attacker can easily retrieve the packets based on brute force attacks so we need to provide more security for the packets. In Cryptographic puzzle Hiding Scheme, where each packet is attached with the puzzle and encrypted. We specify the time limit for the solution of the puzzle. If puzzle is not solved within the time limit there may be dropping of packets and also there is a delay in receiving the packets. In All or Nothing Transformation, before sending the packets to the receiver the binary information is represented in matrix form. The jammer can launch a brute force attack to capture the information in the packets.

III. PROPOSED SYSTEM

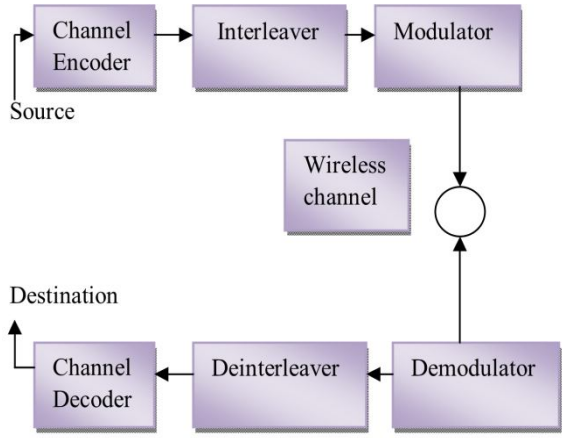


Figure 1: System architecture for packet hiding methods

At the physical layer, packet from the source is encoded, interleaved and then modulated before it is transmitted over the wireless channel. At the destination, the information is demodulated, de-interleaved and then it is decoded to obtain the original packet. The channel encoder adds the extra bits in order to make the transmission more robust and also it protect against channel errors. Interleaving block takes a sequence of symbols/data and arranges them in different order to protect from burst errors, where as modulator modulates these symbols into waveforms for transmission of these packets over the wireless channel.

In order to obtain the original information, the packets are then passed to demodulator where it extracts the original information bearing signal from a modulated wave. The deinterleaver block arranges the interleaved data in to original form and deinterleaved bits are passed through the decoder. Channel decoder converts the encoded information in to original sequence and then the packets are passed to the destination.

A. Strong Hiding Commitment Scheme (SHCS)

Strong Hiding Commitment Scheme which is based on asymmetric cryptography. The main goal is to satisfy the strong hiding property by keeping the computation overhead to a minimum. A commitment scheme allows an entity S, to commit to a chosen value, to another entity V while keeping that value hidden to others. Commitment scheme must satisfy the two properties:

- Binding: Deliver the committed value to the receiver, here the sender cannot alter the value once it is committed
- Hiding: The receiver cannot see the message until he gets the key, after receiving the key receiver verifies that it is indeed the message to which the sender is committed.

Here the role of the committer is implicated by the transmitting node or the sender, whereas role of the verifier is implicated by any receiver including the attacker.

Consider that sender S has a packet m for the transmission for R. First, before transmission S constructs

$$(C,d) = \text{commit}(m)$$
$$C = E_k(\pi_1(m)) \text{ and } d=k$$

Where E_k the commitment function is an asymmetric encryption algorithm (eg. DSA or RSA [11]), π_1 is a publicly known permutation and k is a randomly selected key. At the receiver side, upon receiving d the receiver R computes $m = \pi_1^{-1}(D_k(C))$, where π_1^{-1} is the inverse permutation of π_1 and also it verifies the signature which is attached to the packets. For reducing the overhead of SHCS, value d called decommitment value i.e. decryption key k which is carried in the same packet with the committed value c. This reduces the burden of carrying the extra packet header which is needed for transmitting d.

B. Cryptographic Puzzle Hiding Scheme (CPHS)

The main idea behind this scheme is to solve for the puzzle at the receiver side by executing a pre defined set of computations before the receiver extracts the information. The time required for solving the puzzle to obtain the solution depends on the ability of the solver and its hardness. Here the main advantage of this scheme is, security does not depend on physical layer parameters.

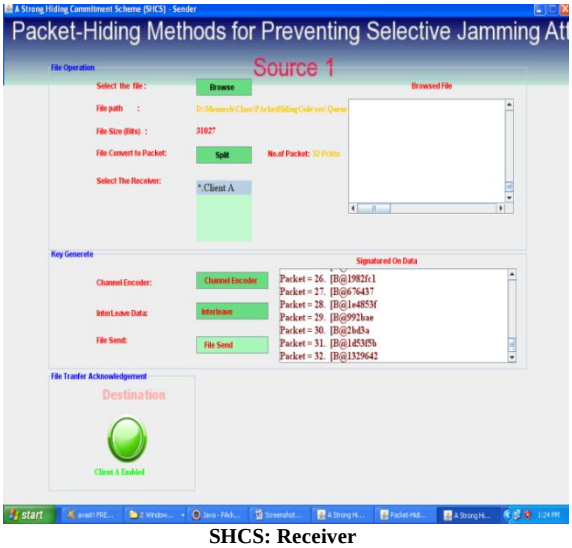
Sender S have a block of packets $m_1, m_2 .. m_n$ for transmission purpose. The sender selects a symmetric key k of some length, then S generates a puzzle P = puzzle(k, t_p), where t_p is the time required for

obtaining the solution of the puzzle and it is measured in units of time, and puzzle() specifies the puzzle generator function. After generating the puzzle P, the sender attaches the puzzle for block of packets and sends (C,P) where $C= E_k (\pi_1(m))$. At the receiver side, the receiver solves the received puzzle P' and then computes $m' = \pi_1^{-1}(D_{k'} (C'))$. We can also send the same data to 'N' number of receivers with the same attached puzzle. If m' is meaningful the receiver accepts the message or it discards m'.

IV RESULTS SHCS:

At the sender side, based on the content random keys are generated then before sending the data to the receiver we have to establish a connection with queue and then using DSA we encrypt the data and attaches a signature for each packets. Queue monitors each packet, whereas at the receiver side we use public keys for decrypting and we verify the signature attached to the packets. By comparing SHCS using DES with respect to DSA we can prove that it provides higher security

SHCS: Sender



SHCS: Receiver

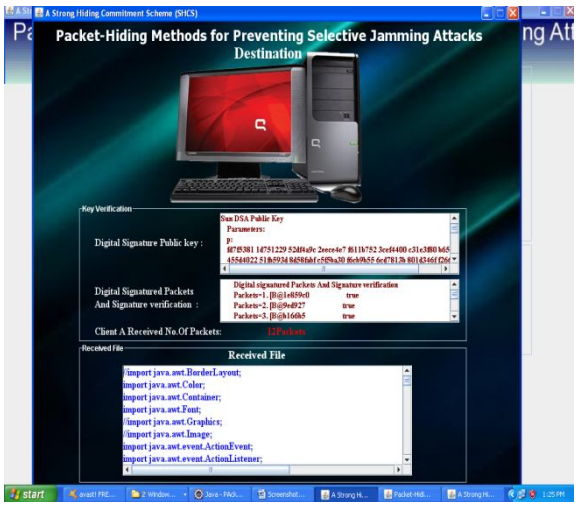


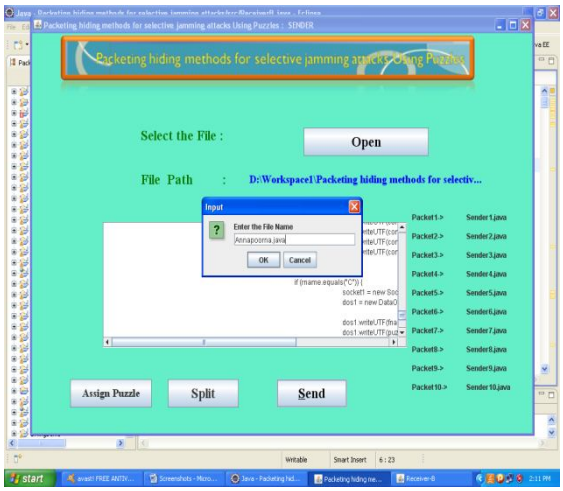
Table 1: Strong Hiding Commitment Scheme

Sender	Attached Signature	Queue	Signature Verified/ Receiver
Packet 1	Packet 1 = [B@le859e0	No attack	Allow
Packet 2	Packet 2 = [B@9ed927	No attack	Allow
Packet 3	Packet 3 = [B@b166b5	No attack	Allow

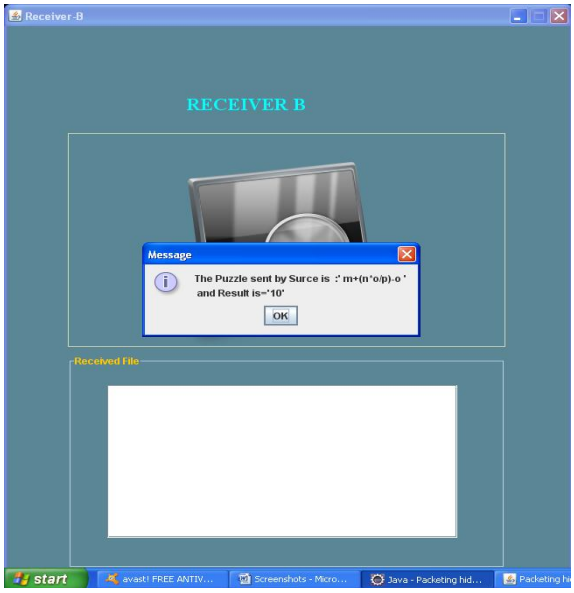
CPHS:

In CPHS, sender before sending any data to the receiver he attaches a puzzle to a block of packets and then encrypt the data with the puzzle where as at the receiver side receiver solves the puzzle with in a specific time limit. By comparing CPHS with existing method, we can achieve time efficiency and also we may overcome the dropping of packets.

CPHS: Sender



CPHS: Receiver



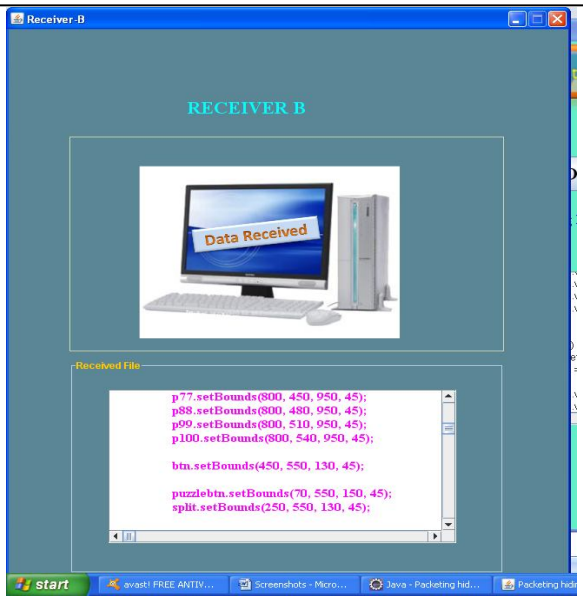


Table 2: Cryptographic Puzzle Hiding Scheme

Source end	Attaching puzzle	Receiver end
G1	G1 || m+(n*o/p) - o	G1
G2	G2 || m+(n*o/p) - o	G2
G3	G1 || m+(n*o/p) - o	G3

*G1, G2, G3: Group of packets

V. CONCLUSION

In this paper we addressed the problem of selective jamming attacks under an internal threat model, where the attacker is a part of the network who is aware of network secrets and also the implementation details. In order to overcome these kinds of attacks we develop three schemes that combine cryptographic primitives such as strong hiding commitment scheme, cryptographic puzzle hiding scheme and all or nothing transformations. We analyze the security of above mentioned schemes and through simulation we can achieve the higher throughput by analyzing the comparative study of these schemes.

REFERENCES

[1] A.D. Wood and J.A.Stankovic, "Denial of Service in Sensor networks",computer, vol.35, no.10, pp. 54-62,2002

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

[3] G.Noubir, and G.Lin,"Low Power DOS Attacks in Data Wireless LANs and Countermeasures," in proc.ACM MobiHoc, 2003

[4] 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

[5] R.A.Poisel.Modern Communications Jamming principles and techniques. Artech House Publishers,2006

[6] W.Xu, W.Trappe,Y.Zhang and T.Wood. Channel surfing and spatial retreats defense against wireless denial of service. In proceedings of the 3rd ACM workshop on wireless security, pages 80-89,2004

[7] D.Thuente and M.Acharya. Intelligent jamming in wireless networks with applications to 802.11b and other networks. In proceedings of the IEEE Military Communications Conference MILCOM, 2006.

[8] T.X.Brown, J.E.James, and A.Sethi. jamming and sensing of encrypted wireless adhoc networks.In proceedings of MobiHoc, pages 120-130 ,2006

[9] M.Wilhelm, I.Martinovic, J.Schmitt and V.Lenders. Reactive jamming in wireless networks: How realistic is the threat? In proceedings of WiSec,2011.

[10] D.Stinson. Cryptography:theory and practice.CRC press,2006

[11] Ravneet kaur and Amandeep Kaur. Digital Signature, in International Conference on Computing Sciences, 2011

[12] Ashish Kumar, Sachin Kumar Gupta, Shubham Singh."Packet Hiding Methods for Preventing Selective Jamming Attacks", in International Journal of Computational Engineering Research, Vol 3, Issue 1, January 2013.