Volume 3, Issue 3, March 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

SHCS Technique Defined for Packet Hiding Methods in Wireless Networks

Bharath J[1#]
M.Tech Student,
Department of CSE, EWIT, VTU,
Bangalore, India

Mr. Rajashekar S A[2]
[#]Assistant Professor
Department of CSE, EWIT, VTU,
Bangalore, India

Abstract— Due to their nature wireless networks are vulnerable to denial of service (DoS) attack (any event that diminishes or eliminates a networks capacity to perform its expected function) Jamming attacks are one of the most urgent threats harming the dependability of wireless communication. Jamming attacks may be viewed as a special case of Denial of service (DoS) attacks. With the internal knowledge of protocol specifications and network secrets can launch low-effort jamming attacks that are difficult to detect and counter. An adversary masks the events that the sensor network should detect by jamming an appropriate subset of the nodes. In this paper, we concentrate on the problem of selective jamming attacks in wireless networks. We develop schemes that prevent real-time packet classification by combining cryptographic primitives.

Keywords— wireless networks, Jamming attacks, encryption.

I. INTRODUCTION

Wireless networks now enjoy widespread commercial Implementation because of their low cost, ease of use and setup. However, since accessing wireless media is much easier than tapping a wired network, security becomes a serious concern when implementing any wireless network. We consider a particular class of Denial of Service (DoS) attacks called jamming. In the simplest form of jamming, the adversary interferes with the reception of messages by transmitting a continuous jamming signal, or several short jamming pulses. Jamming results in a loss of link reliability, increased energy consumption, extended packet delays and disruption of end-to-end routes. The use of distinct, dedicated communication channels 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.

Jamming strategies under the external threat model include the continuous or random transmission of high power interference signals. With the knowledge of network protocols, the adversary targets the specific packets of high priority by launching selective jamming attacks. To perform selective jamming, the adversary must be capable of classifying transmitted packets in real time, and corrupting them before the end of their transmission. Packet classification can be performed by receiving just a few bytes of a packet. The paper is organized as follows. In section 2 the related works are discussed. In section 3 the contribution over the encryption are discussed. In section 4 the results of the evaluated parameters are discussed. With section 5 the paper is concluded.

II. RELATED WORK

J. E. James and A. Sethi in their paper proposed the encryption technique taken place in the wireless networks [1]. O.Goldreich [2] in his proposed paper discusses about the basic applications of the cryptography and their encryption decryption formulas. G.Lin and G.Noubir in their paper proposed discusses about the denial of service attacks [3]. Brown illustrated the feasibility of selective jamming based on protocol semantics [1]. They considered several packet identifiers for encrypted packets such as packet size, precise timing information of different protocols. Lazos [4] proposed an algorithm to protect the control channel from inside jammers In the short paper work proposed by M.Wilhelm and I.Martinovic, J.Schmitt and V.Lenders the “Reactive jamming in the wireless networks: How realistic is the threat?” the jamming attacks, principles and the selective packet hiding techniques are referred [5].

III. OUR CONTRIBUTION

In this proposed work we propose two new methodologies to send data between the server and numerous clients in the secure manner. First the data encryption technique is handled by the RSA Algorithm. Secondly the encrypted text is transfer over the network .For packet hiding technique A Strong Hiding Commitment Scheme (SHCS) is implemented

3.1 Packet Classification

This section describes how adversary classifies the packet in real time before the actual packet is transmitted to destination. At the Physical layer, a packet k is encoded, interleaved, and modulated before transmitting. At the receiver, the signal is demodulated, de-interleaved and decoded to recover the original packet m. Nodes C and D communicate via a wireless link.

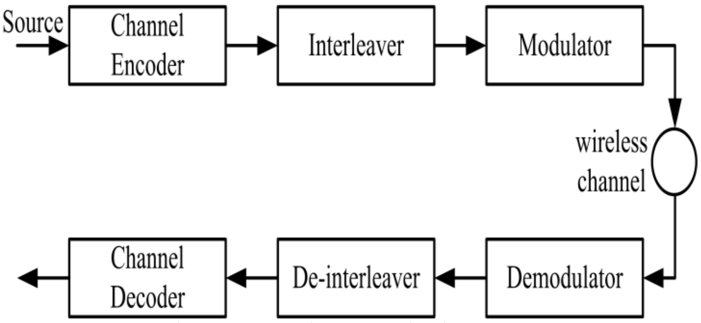

Figure 1: Generic communication system

3.2 Strong hiding commitment scheme :

Main impetus is to satisfy the strong hiding property while keeping the computation and the communication overhead to a minimum. The proposed SHCS requires the joint consideration of the MAC and PHY layers. To reduce the overhead the de-commitment value or the decryption key value is done in the same packet in which the encryption is taken place.

In cryptography, a commitment scheme allows one to commit to a chosen value (or chosen statement) while keeping it hidden to others, with the ability to reveal the committed value later. Commitment schemes are designed so that a party cannot change the value or statement after they have committed to it: that is, commitment schemes are binding. Commitment schemes have important applications in a number of cryptographic protocols including secure coin flipping, zero-knowledge proofs, and secure computation [2].

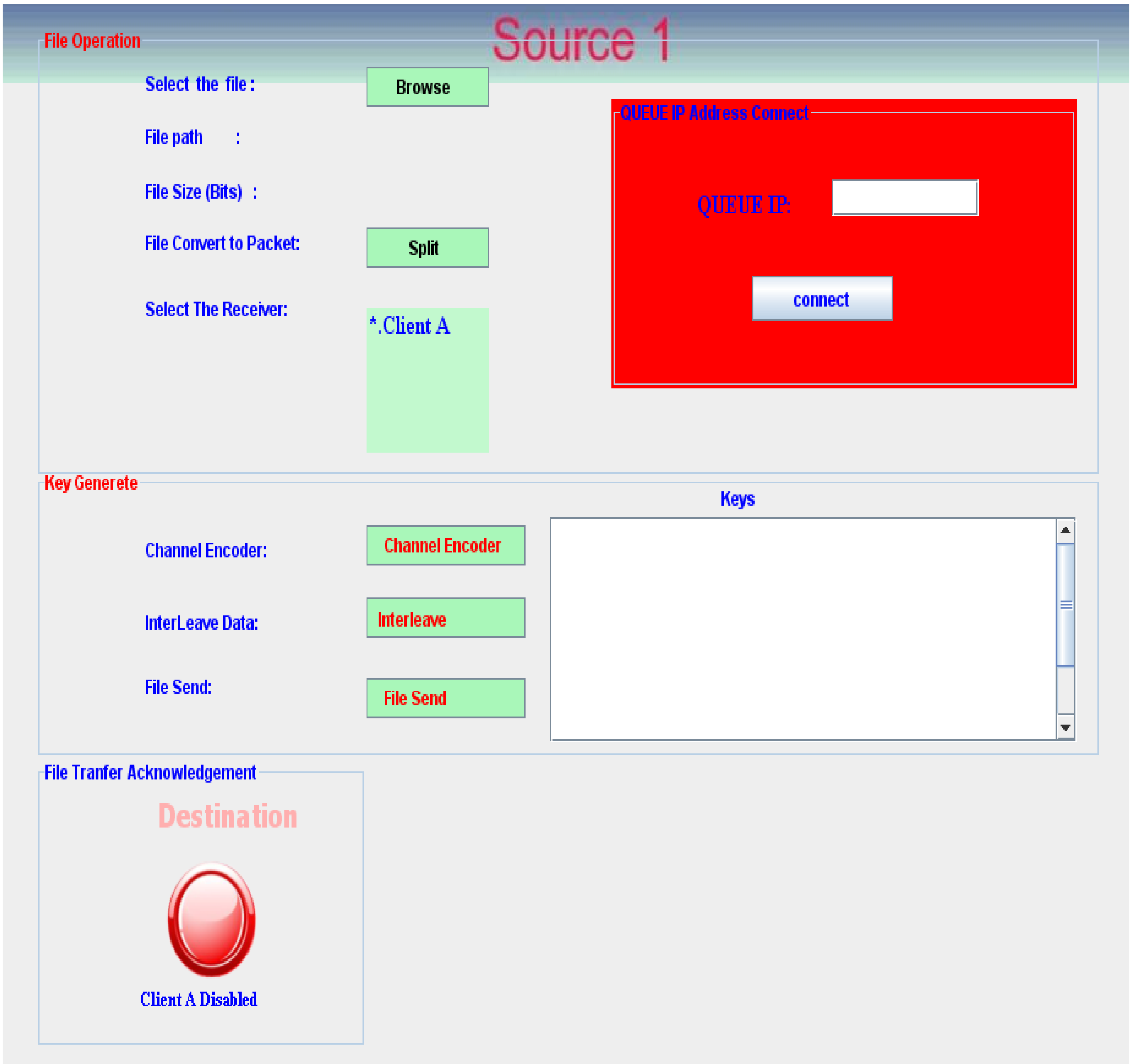

Fig 2: Sender

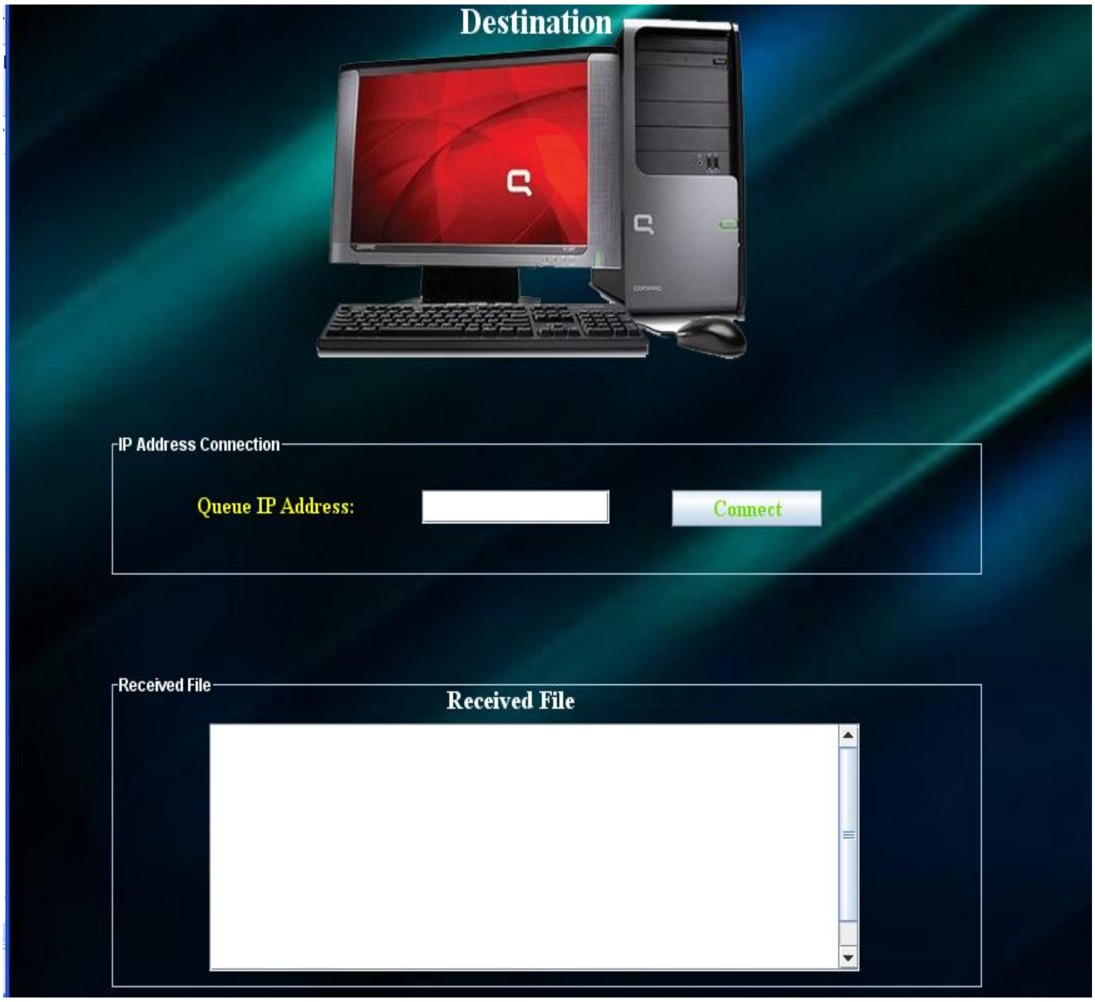

Fig 3: Receiver

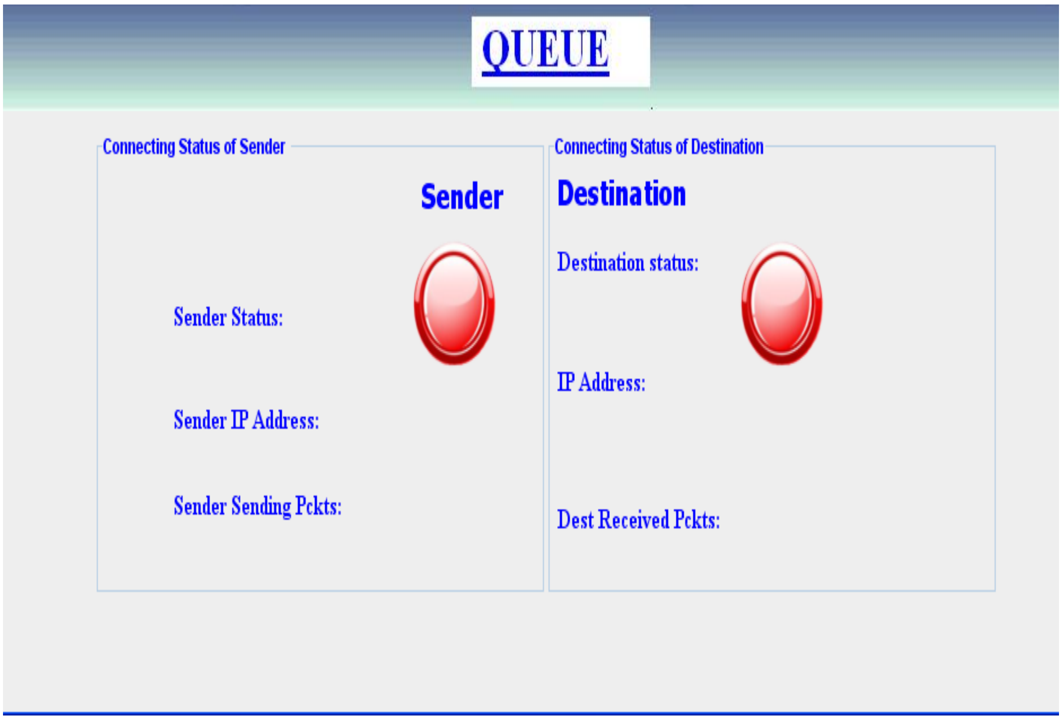

Fig 4: Queue

IV. CONCLUSION

We addressed the problem of selective jamming attacks in wireless networks. We showed that an adversary can exploit its knowledge of the protocol implementation to increase the impact of his attack at a significantly lower energy cost. We illustrated the feasibility of selective jamming attacks by performing real time packet classification. We also maintain the strong hiding scheme that provides the packet from loss and stored in the buffer. The congestion control is maintained in this paper by following the sequential number ID of the packets. In the wireless network, the confidentiality of the data is more important aspect and is maintained.

ACKNOWLEDGMENT

Special thanks to East West Institute of Technology for helping us in our work and supporting the research. Visvesvaraya Technological research centre are also helping us in this work.

REFERENCES

[1] T.X.Brown, J.E.James and A.Sethi , Jamming ans sensing of encrypted wireless ad hoc networks . In proceedings of Mobihoc, pages 120-130,

[2] Oded Goldreich (2001). Foundations of Cryptography: Volume 1, Basic Tools, (draft available from author's site). Cambridge University Press. ISBN 0-521-79172-3. (See also http://www.wisdom.weizmann.ac.il/~oded/foc-book.html).

[3] 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.

[4] 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

[5] M.Wilhelm, I.Martinovic , J.Schmitt, and V.Lenders. Reactive Jamming in Wireless Networks: How realistic is the threat? In proceddings of Wisec, 2011.