August, 2014

Encryption Techniques in Packet Hiding Methods to Prevent Jamming Attacks in Wireless Network

Rashmi B. Dhamannavar
Dr. Rashmi M. Jogdand

ISSN:0975-9646

Encryption Techniques in Packet Hiding Methods to Prevent Jamming Attacks in Wireless Network

Rashmi B.Dhamannavar[1], Dr.Rashmi M.Jogdand[2]

[1, 2] *Department of Computer Science and Engineering,* [1,2VTU] *University*

KLS Gogte Institute of Technology, Udyambag, Belgaum, Karnataka, India

***Abstract*—Wireless Networks are becoming an increasingly important technology that is bringing the world closer together. In this type of network environment there could be more chances of attacks. The packets cannot be easily transferred over the network. It affects network performance degrade. While eavesdropping and message injection can be prevented using cryptographic methods, jamming attacks are much harder to counter. They have been shown to actualize severe Denial-of-Service (DoS) attacks against networks. In Simplest form adversary blocks the packets that are transmitted over wireless network. Typically, jamming attacks has been considered under an external threat model, in which the jammer is not part of the network. To overcome the above problem of network traffic and performance in this paper we have considered a packet hiding methods that can be securely transmit packets over the network. We are addressing the problem of jamming attacks under internal threat model and two schemes are proposed that prevent real-time packet classification of packets by combining hiding scheme based on cryptographic primitives.**

***Keywords*—Selective Jamming, Denial-of-Service, Wireless Networks, Packet Classification.**

I. INTRODUCTION

Wireless networks are computer networks that are not connected by cables of any kind. Wireless System enables wireless connectivity to the Internet via radio waves rather than wires on a personals home computer, smartphone, laptops or similar mobile device. The use of a wireless network makes enterprises to avoid the costly process of introducing cables into buildings or as a connection between different equipment locations. The bases for wireless systems are radio-waves; it means an implementation that takes place at the physical level of network structure. In the computing world, the term wireless can be used as ambiguous, since it may refer to several different wireless technologies. Wireless Networks are becoming an increasingly important technology that is bringing the world closer together. Wireless Networks are used in every area, such as agriculture, education, pharmaceuticals, manufacturing, military, transportation and research. Therefore, the importance of Wireless Networks security is significant. **S**ecurity is one of the critical attributes of any communication network. Various attacks were reported over the last many years.

Wireless networks are highly sensitive to Denial of Service (DoS) attacks [2-3]. A Denial of Service (DoS) attack can be characterized as an attack with the purpose of preventing legitimate users from using a specified network resource such as a website, web service, or computer system. The wireless communication medium is a broadcast channel, exposing physical layer of wireless communication to jamming [4]. Past research has mostly focused on defending voice communication using spread spectrum techniques [5]. The SS techniques provide bit-level protection by spreading bits according to a secret pseudo-noise (PN) code, known only to the communicating parties. Such approach spreads the signal into a very large frequency band and makes a jammer with limited energy resources unable to afford jamming the entire band. These methods only protect wireless transmissions under the external threat model. Non-continuous jamming only results in a graceful degradation of the voice quality. Therefore, this approach is effective to protect voice communication against jamming.

II. LITRETURE SURVEY

Timothy et.al [6] address problem of an attacker disrupting an encrypted victim wireless ad hoc network through jamming. Jamming is broken down into layers and this paper focuses on jamming at the Transport/Network layer. Jamming at this layer exploits AODV and TCP protocols and is shown to be very effective in simulated and real networks when it can sense victim packet types, but the encryption is assumed to mask the entire header and contents of the packet so that only packet size, timing, and sequence is available to the attacker for sensing. A sensor is developed that consists of four components. The first is a probabilistic model of the sizes and inter-packet timing of different packet types. The second is a historical method for detecting known protocol sequences that is used to develop the probabilistic models, the third is an active jamming mechanism to force the victim network to produce known sequences for the historical analyser, and the fourth is the online classifier that makes packet type classification decisions. The method is tested on live data and found that for many packet types the classification is highly reliable. The relative roles of size, timing, and sequence are discussed along with the implications for making networks more secure.

M. Cagalj et.al [7] Due to their very nature, wireless sensor networks are probably the most vulnerable category of wireless networks to “radio channel jamming”-based Denial-of-Service (DoS) attacks: An adversary can easily mask the events that the sensor network should detect by stealthily jamming an appropriate subset of the nodes; in this way, he prevents them to report what they are sensing to the network operator. Therefore, in spite of the fact that an event is sensed by one or several nodes (and the sensor network is otherwise fully connected), the network operator cannot be informed on time. This paper showed how the

sensor nodes can exploit channel diversity in order to establish wormholes out of the jammed region, through which an alarm can be transmitted to the network operator. Three solutions are proposed: the first is based on wired pairs of sensors, the second relies on frequency hopping, and the third is based on a novel concept called uncoordinated channel hopping.

Loukas Lazos et.al [8] addresses the problem of control-channel jamming attacks in multi-channel ad hoc networks. Deviating from the traditional view that sees jamming attacks as physical-layer vulnerability, we consider a sophisticated adversary who exploits knowledge of the protocol mechanics along with cryptographic quantities extracted from compromised nodes to maximize the impact of his attack on higher-layer functions. This paper proposes new security metrics that quantify the ability of the adversary to deny access to the control channel, and the overall delay incurred in re-establishing the control channel. They also proposed a randomized distributed scheme that allows nodes to establish a new control channel using frequency hopping. Our method differs from classic frequency hopping in that no two nodes share the same hopping sequence, thus mitigating the impact of node compromise. Furthermore, a compromised node is uniquely identified through its hop sequence, leading to its isolation from any future information regarding the frequency location of the control channel.

III. PROPOSED SYSTEM

The problem of jamming under an internal threat model has been considered. Adversary who is aware of network secrets and the implementation details of network protocols at any layer in the network stack has been designed. The adversary exploits the internal knowledge for launching selective jamming attacks in which specific messages of "high importance" are targeted. A jammer can target route-request/route-reply messages at the routing layer to prevent route discovery, or target TCP acknowledgments in a TCP session to severely degrade the throughput of an end-to-end flow. To address this problem we proposed two schemes that provide encryption techniques to hide the packets from jammer. And packets are delivered to receiver and with confidentiality without any packet loss.

A. Network module

The network consists of a collection of nodes connected via wireless links. Nodes may communicate directly if they are within communication range, or indirectly via multiple hops. Nodes communicate both in unicast mode and broadcast mode. Communications can be either unencrypted or encrypted. For encrypted broadcast communications, symmetric keys are shared among all intended receivers. These keys are established using pre-shared pair wise keys or asymmetric cryptography.

B. Adversary Module

Adversary is in control of the communication medium and can jam messages at any part of the network of his choosing. The adversary can operate in full-duplex mode, thus being able to receive and transmit simultaneously. This can be achieved, for example, with the use of multi-radio transceivers. Adversary is equipped with directional antennas that enable the reception of a signal from one node and jamming of the same signal at another. It is assumed that the adversary can pro-actively jam a number of bits just below the ECC capability early in the transmission. When the adversary is introduced, the data packets from the node cannot be reached at receiver.

C. Real time packet classification

At the Physical layer, a packet m is encoded, interleaved, 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.

D. Commitment scheme based Strong hiding

Strong hiding Commitment scheme is based on symmetric cryptography. It provides strong hiding property while keeping the computation and communication overhead to a minimum. SHCS module is to be implemented. First the cryptographic keys are to be generated using any cryptographic algorithm like DES. Then the data is divided into packets and these packets are encrypted using the newly created key. Then some bits are added with the encrypted data as padding process to hide the identity of the data. Now the data is permutated and transferred to the destination node. The cryptographic key is refreshed periodically to hide the key from the jammer node.

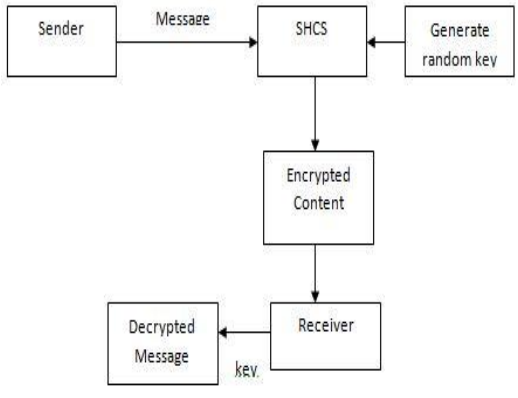

Fig 2: Module Diagram of Strong Hiding Commitment Scheme

Padding and Permutation are two functions that are applied in message. First, the message is divided into several packets, and each packet is encrypted with random key values. This key value is changed frequently to keep the key values secret from the adversaries. The next step is padding. Here some bits are added to the encrypted data to modulate the data. Finally, the data is permuted and send to

the destination. Here adversary tries to block the packets but fails to block because packets encrypted.

E. Hiding scheme based Cryptographic puzzle

Cryptographic puzzles are primitives originally suggested by Merkle as a method for establishing a secret over an insecure channel. They find a wide range of applications from preventing DoS attacks to providing broadcast authentication and key secure schemes.

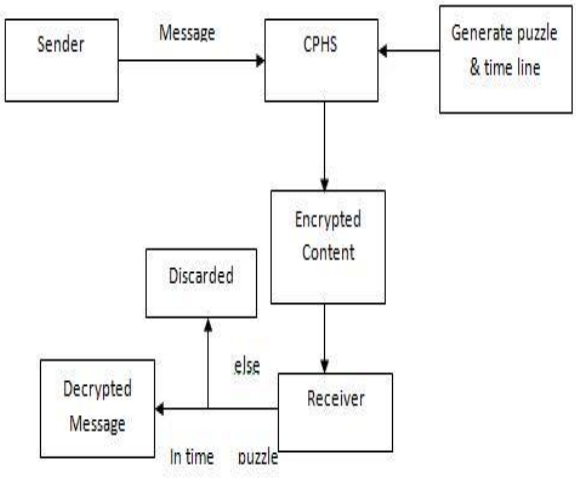

Fig 3: Module diagram of hiding based on cryptographic puzzle

In hiding scheme based on cryptographic puzzle functions called time lock puzzle is used. The main idea behind such puzzles is to force the recipient of a puzzle execute a pre-defined set of computations before he is able to extract a secret of interest. The time required for obtaining the solution of a puzzle depends on its hardness and the computational ability of the solver. The advantage of the puzzle based scheme is that its security does not rely on the PHY layer parameters.

IV. IMPLEMENTATION

In this paper, we have implemented Client server model. We used Java Swing for designing GUI. In this paper we have developed a client server application, which could be deployed in network, where client can send data to server and server receive the data in secure manner. We studied the preventive jamming attacks under two special cases such as Cryptographic Puzzles, Strong Hiding Commitment Schemes.

When a sender wants to send a data to receiver, sender encrypts the data and sends in secure manner. There are two techniques used to for hiding the data, which are Commitment Scheme based on strong hiding, hiding based on Cryptographic puzzle. The packet hiding techniques is followed to send data by avoiding jamming attack.

A. Implementation of Commitment scheme based on strong hiding

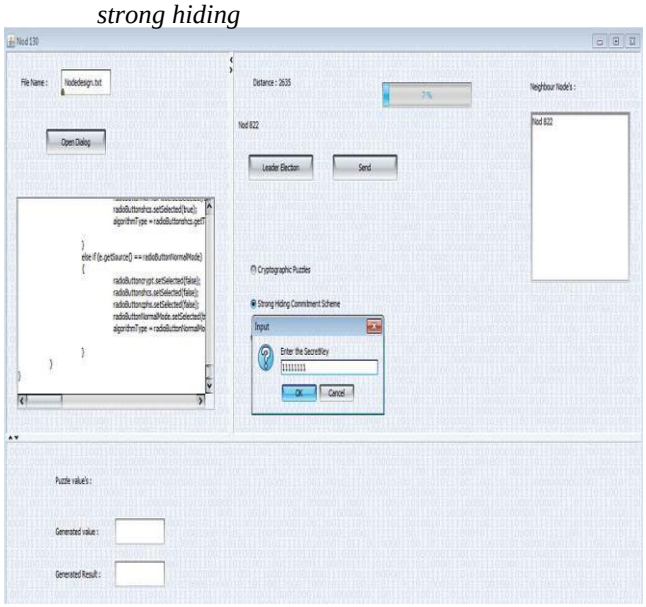

Fig 4: Node selecting Commitment scheme based on strong hiding

First Nodes are initialized. Two or more nodes are initialized and depending upon mobility one node will be selected as leader node. Other nodes act like neighbour node and here file will be uploaded and node will select SHCS, here it will ask for secrete key.

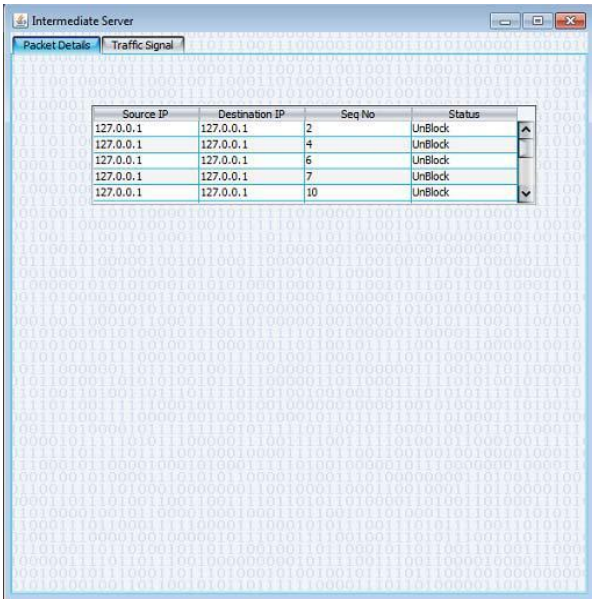

Fig 5: Intermediate Server

Intermediate Server which acts like normal node and it will receive the packets that are randomly sent from sender and transfer it to receive. When packets are sent in normal mode, intermediate severer will ask whether to block the packets or send it normally.

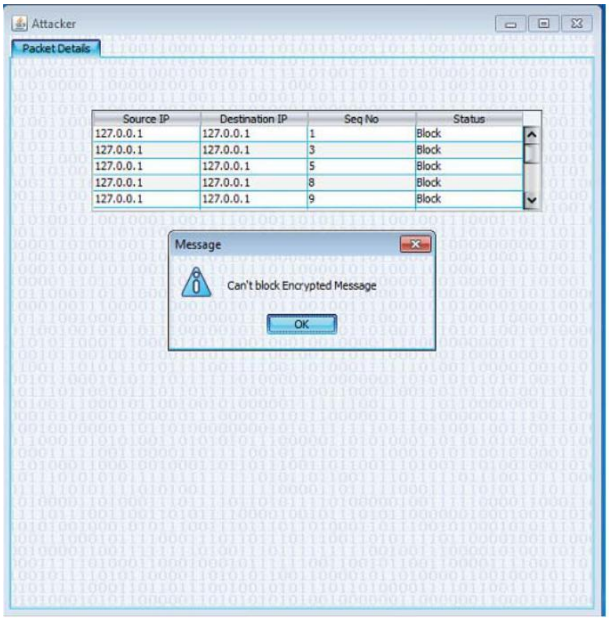

Fig 6: Attacker

Attacker will block the packets. Here packets are randomly send to intermediate server and attacker. Attacker tries to block the packets but he cannot block the packets, because packets are encrypted and they are securely received by receiver. Attacker can block the packets in normal mode.

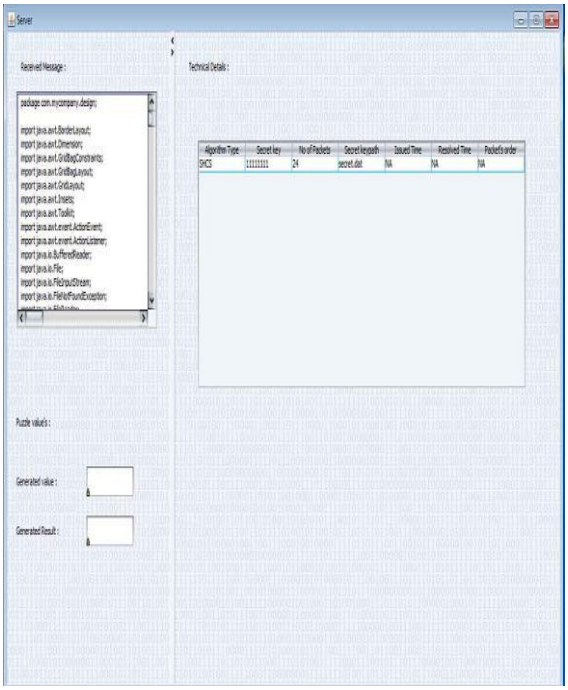

Fig 7: Server displaying message that is decrypting using strong hiding

Here it acts like receiver and waiting for data. Once the packets are sent, in receiver side ask for decryption of secret key, legitimate receiver will only know key and using that key it will decrypt the message.

B. Implementation of Hiding based on cryptographic puzzle

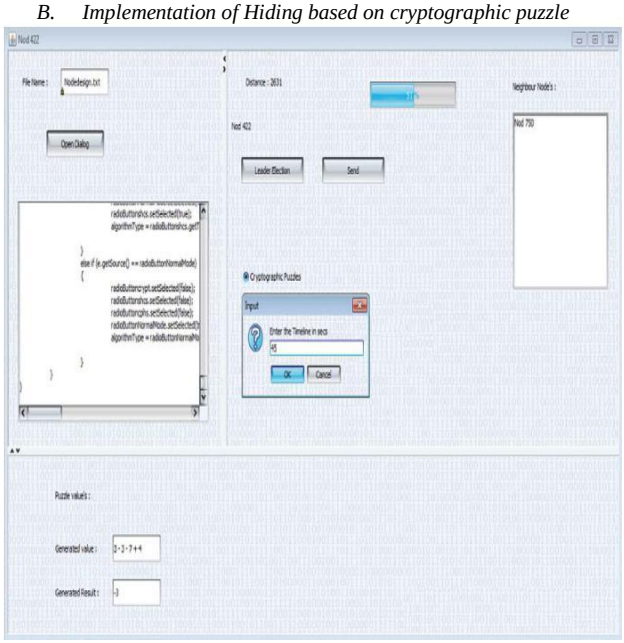

Fig 8: Node selecting hiding scheme based on cryptographic puzzle

Here node will select the cryptographic puzzle hiding schemes, that time puzzle will be generated and ask for timeline to solve the puzzle and send it receiver.

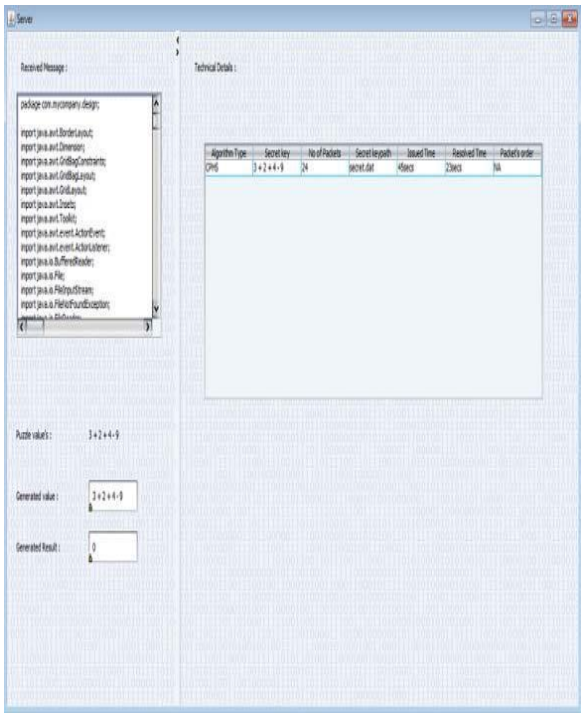

Fig 11: Server displaying message that is decrypting using cryptographic puzzle

Receiver will solve the puzzle within timeline. After solving puzzle only receiver will get the original message. If receiver will not solve the puzzle with in timeline then timeline will expire.

V. CONCLUSIONS

The problem of selective jamming attacks under internal threat model is considered. Here jammer is part of the network under attack, thus being aware of the protocol specifications and shared network secrets. To avoid packet classification in wireless transmission we proposed two schemes such as commitment scheme based on strong hiding and hiding based on cryptographic puzzle. These two schemes prevent the jammer from blocking the packets that is transmitted over wireless network so that the data reaches the receiver without any inaccuracies.

ACKNOWLEDGMENT

I give my sincere feelings of thankfulness to Dr.Rashmi M.Jogdand for her valuable guidance, support and encouragement which helped me a lot to write this paper and also other faculty members of KLS Gogte institute of Technology, Belgaum for their valuable suggestions and comments that helped to improve the quality of article.

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] Singh, Kirat Pal, Shivani Parmar, and Dilip Kumar. "Design of High Performance MIPS Cryptography Processor." International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness. Springer Berlin Heidelberg, 2013.

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

[3] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt. Spread Spectrum Communications Handbook. McGraw-Hill, 2001.
Y. Desmedt. Broadcast anti-jamming systems. Computer Networks,35(2-3):223–236, February 2001

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

[5] T. X. Brown, J. E. James, and A. Sethi. Jamming and sensing of encrypted wireless ad hoc networks. In Proceedings of MobiHoc, pages120–130, 2006.

[6] M. Cagalj, S. Capkun, and J.-P. Hubaux. Wormhole-based antijamming techniques in sensor networks. IEEE Transactions on Mobile Computing, 6(1):100–114, 2007.

[7] L. Lazos, S. Liu, and M. Krunz. Mitigating control-channel jamming attacks in multi-channel ad hoc networks. In Proceedings of the 2ndACM conference on wireless network security, pages 169–180, 2009.