IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727
PP 00-00
www.iosrjournals.org

Maximizing the Performance and Reliability of Wireless Network by Preventing Jamming Attacks

B. Mahalakshmi[1], S.V. Shri Bharathi[2], W. Lydia Shammi[3]

[1]*(Cse Department, New Prince Shri Bhavani College of engineering and Technology/ Anna University,India)*
[2]*(Cse Department, New Prince Shri Bhavani College of engineering and Technology/ Anna University,India)*
[3]*(Cse Department, New Prince Shri Bhavani College of engineering and Technology/ Anna University,India)*

Abstract: *Wireless networks are computer networks that are not connected by cables of any kind. It enables the wireless connectivity to the Internet via radiowaves. So it is more sensitive to the Denial-of-Service attacks. This paper proposes a Strong Hiding Commitment schemes, Cryptographic Puzzles Hiding Schemes, and wormholes for sending the message in wireless network safely even if the attacker is present, and also alerts the other nodes about the presence of jammer. Thus, it improves the performance and reliability of wireless sensor networks.*

Keywords: *Cryptographic puzzles, Denial-of- Service attack, Strong hiding schemes, Wormholes*

I. Introduction

Wireless networks rely on the uninterrupted availailability 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 on wireless transmissions, inject spurious messages, or jam legitimate ones. While eaves- dropping and message injection can be prevented using cryptographic methods, jamming attacks a remuch harder to counter. They have been shown to actualize severe Denial-of-Service (DoS) attacks against wireless networks. 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. Typically, jamming attacks ha v e been considered under an exterior threat model, in which the jammer is not part of the network. In almost every case, jamming causes a denial of service type attack to either sender or receiver. The easiest form of jamming a wireless network communication is to continually transmit useless data to the node where the server becomes overloaded. Most people have no idea if a jamming signal is in use. It appears as if there is no service. This attack makes the network resource unavailable to its legitimate users. The existing system is based on Spread Spectrum (SS). This technique mainly focused on an external threat model. In broadcast communication, if an attacker present within the network can easily eavesdrop the message sent by any node. In selective jamming attack, the attacker always tries to block the message sent by its target node and it leads to the Denial-of-Service attack. In this paper, main focus is to prevent selective jamming attack in an internal threat model. A wormhole[11] is used to generate an alarm to indicate the presence of jammer to all access point in the network. Presence of any jammer is detected a method called packet hiding [12] is used to transmit message through the network. This method is based on the technique called Strong Hiding Commitment Scheme(SHCS) [12]. Alejandro Proano and LoukasLazos [12] proposed a paper based on this technique. Wormhole based anti-jamming concept along is included in the newly proposed method for eliminating DoS attack.

II. Problem Statement

Consider the scenario depicted where 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 apacket m to B, node J classifies m by receivingonly the first few bytes o f m. J then corrupts m beyond recovery by interfering with its reception at B. We address the problem of preventing the jamming node from classifying m in real time, thus mitigating J 's ability to perform selective jamming. In this, Spread Spectrum technique provides bit-level protection by spreading bits according to asecret pseudo noise (PN) code. That is known only to the communicating parties. Thismethod can only protect the wireless networks under an external threat model. We know thatthe communication within the wireless network is done through the broadcastcommunication. So, this is vulnerable under an internal threat model. All intended receiversmust know about the secrets used to protect transmissions. Another one drawback iscompromise of a single receiver. So, the sender needs to reveal relevant cryptographicinformation to its receiver. A packet hiding technique is introduced for sending messagesamong nodes within the wireless network [4].

III. Proposed System

A solution to the selective jamming attack in the wireless network would be the encryption ofpacket that is going to send. Here encryption is applied to the attributes except destination. Itmeans that we hide the packet from attacker. The encryption is applied only to the attributesexcept destination. That is why, during broadcasting there is no need for intermediatedecryption. Each node checks the IP address of incoming packet. If it is sent for thatparticular node it will decrypt otherwise just forwarded to the next node .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 preshared 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. 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.

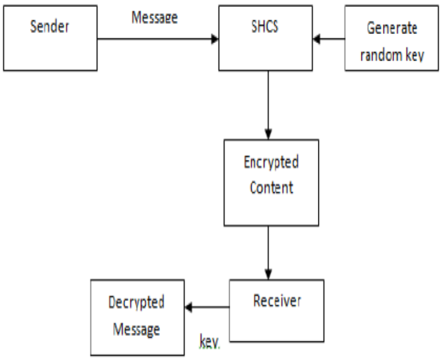


Fig 1: Module Diagram of Strong Hiding Commitment Scheme

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. 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.

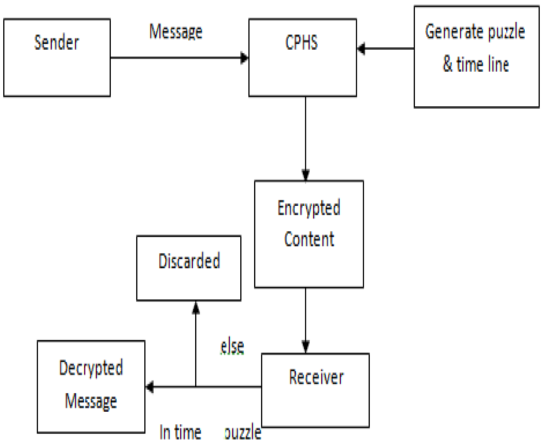


Fig 2: Module diagram of hiding based on cryptographic puzzle

One question arises here is that, how the node can identify that a particular node is a jammer. The answer for this question is that a node which receives repeated acknowledgements for the same message or another situation is that the packet is held by a node in the network for along time (not because of high network traffic) or if any node that violates the rules in aarticular network region. Then the access point can identify that the particular node is a jammer.In this situation, the wormhole concept is newly encorporated. The access point then turns into a wormhole. This wormhole then prevents the jamming activity of particular jammer. By this method, all other nodes within that network can understand information about the jammer. Next time when they send a message, they can select another path for transmitting message or transmit through the same path, but must apply the packet hiding technique.The packet can also be send through a shortest path between source and destination. Any algorithm for finding the shortest path between a source and destination can be used. In wireless network, it is possible to find the path by analyzing the range of nodes. Figure 2 shows a process flow, which describes the overall working of this concept when weimplement it as practical. Simulation of this proposed technique can be done by performing operations shown in theprocess flow. Node Creation module creates the nodes in wireless network. When we create a node we must specify the range of that particular node, because it is essential for the calculation of shortest path. Nodes can move from one position to another position. Suppose if one node is selected as a jammer, then the source send packet after applying SHCS technique and transmit through shortest path between source and destination.The application of this concept arises when we require a secure communication such as emergency response operations, military, or police networks or safety-secret business operations. Just take an example, in emergency response operations like after a naturaldisaster, adhoc networks could be used for real-time safety feedback. In this situation, the usual network may be damaged. Emergency rescue groups might rely upon the adhoc networks for communication within that affected place.

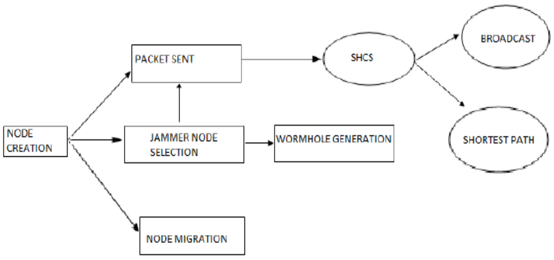


Fig 3: Process flow

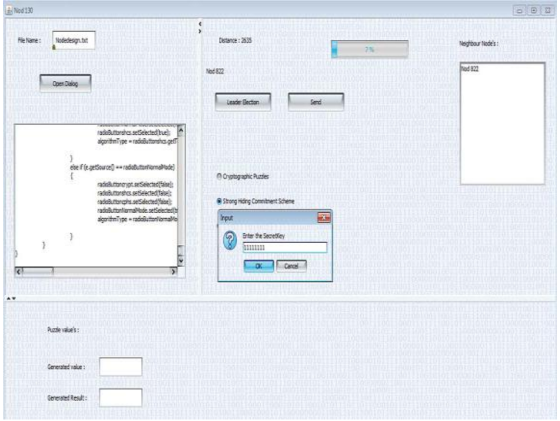
The packet can also be send through a shortest path between source and destination. Any algorithm for finding the shortest path between a source and destination can be used. In wireless network, it is possible to find the path by analyzing the range of nodes. Figure 3shows a process flow, which describes the overall working of this concept when weimplement it as practical. Simulation of this proposed technique can be done by performing operations shown in the process flow. Node creation module creates the nodes in wireless network. When we create a node we must specify the range of that particular node, because it is essential for the calculation of shortest path. Nodes can move from one position to another position. Suppose if one node is selected as a jammer, then the source send packet after applying SHCS technique and transmit through shortest path between source and destination.

The application of this concept arises when we require a secure communication such as emergency response operations, military, or police networks or safety-secret business operations. Just take an example, in emergency response operations like after a naturaldisaster, adhoc networks could be used for real-time safety feedback. In this situation, the usual network may be damaged. Emergency rescue groups might rely upon the adhoc networks for communication within that affected place.

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



File Name : Nodedesign.txt

```
                radioButtonshcs.setSelected(true);
                algorithmType = radioButtonshcs.getT
            }
            else if (e.getSource() == radioButtonNormalMode)
            {
                radioButtoncrypt.setSelected(false);
                radioButtonshcs.setSelected(false);
                radioButtonqphs.setSelected(false);
                radioButtonNormalMode.setSelected(t
                algorithmType = radioButtonNormalMo
            }
        }
}
```

Distance : 2635

Nod 822

○ Cryptographic Puzzles

● Strong Hiding Commitment Scheme

Enter the SecretKey: 11111111

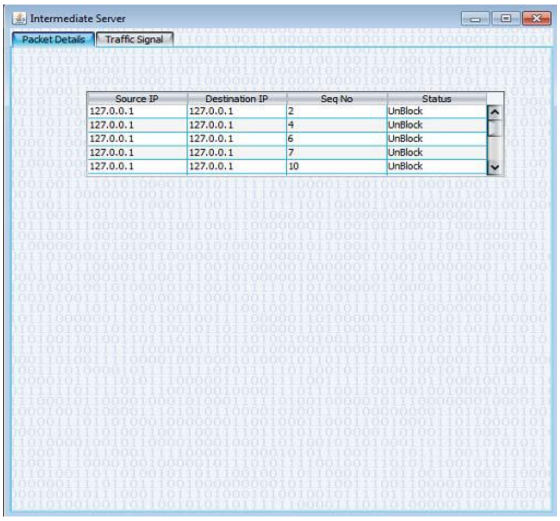
Neighbour Node's : Nod 822

Puzzle value's :

Generated value :

Generated Result :

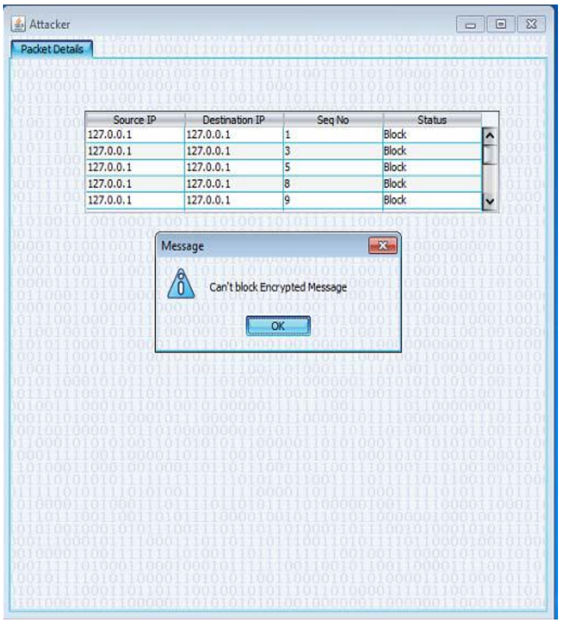
Fig 4: Node selecting Commitment scheme based on strong hiding



Source IP	Destination IP	Seq No	Status
127.0.0.1	127.0.0.1	2	UnBlock
127.0.0.1	127.0.0.1	4	UnBlock
127.0.0.1	127.0.0.1	6	UnBlock
127.0.0.1	127.0.0.1	7	UnBlock
127.0.0.1	127.0.0.1	10	UnBlock

Fig 5: Intermediate Server

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.

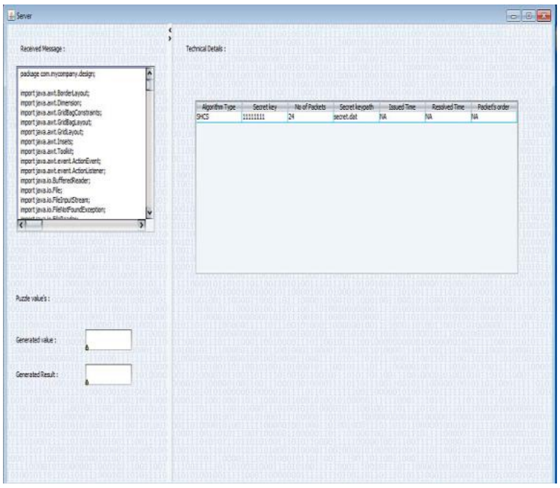


Source IP	Destination IP	Seq No	Status
127.0.0.1	127.0.0.1	1	Block
127.0.0.1	127.0.0.1	3	Block
127.0.0.1	127.0.0.1	5	Block
127.0.0.1	127.0.0.1	8	Block
127.0.0.1	127.0.0.1	9	Block

Can't block Encrypted Message

Fig 6: AttackerIntermediate

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.



Received Message :

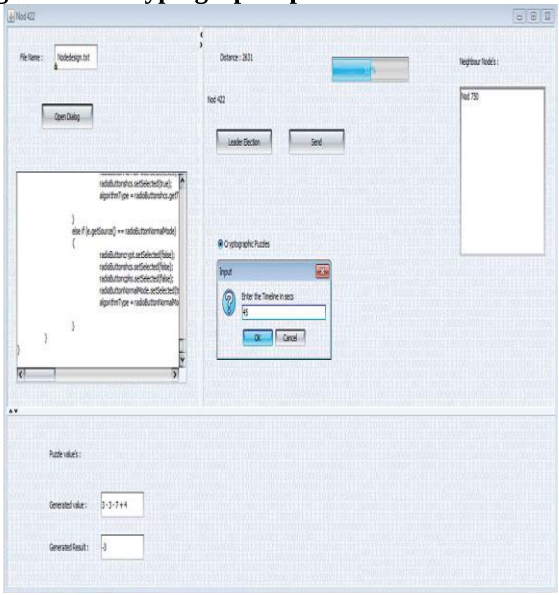
```
package com.mycompany.design;

import java.awt.BorderLayout;
import java.awt.Dimension;
import java.awt.GridBagConstraints;
import java.awt.GridBagLayout;
import java.awt.GridLayout;
import java.awt.Insets;
import java.awt.Toolkit;
import java.awt.event.ActionEvent;
import java.awt.event.ActionListener;
import java.io.BufferedReader;
import java.io.File;
import java.io.FileInputStream;
import java.io.FileNotFoundException;
```

Algorithm Type	Secret key	No of Packets	Secret keypath	Issued Time	Resolved Time	Packet's order
SHCS	11111111	24	secret.dat	NA	NA	NA

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

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.

B. Implementation of Hiding based on cryptographic puzzle



File Name : Nodedesign.txt

Distance : 2631

Nod 422

Nod 750

● Cryptographic Puzzles

Enter the Timeline in secs: 45

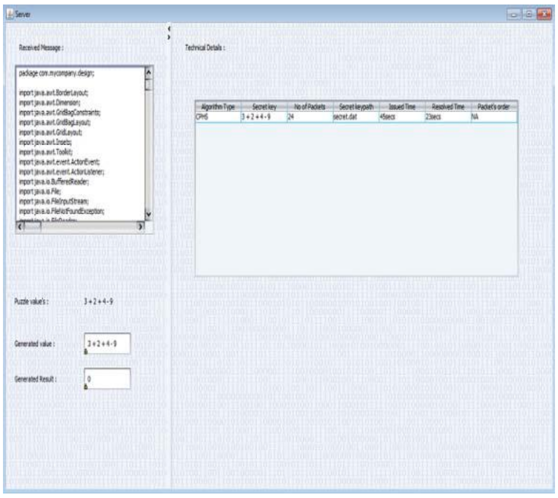
```
                radioButtonshcs.setSelected(true);
                algorithmType = radioButtonshcs.getT
            }
            else if (e.getSource() == radioButtonNormalMode)
            {
                radioButtoncrypt.setSelected(false);
                radioButtonshcs.setSelected(false);
                radioButtoncphs.setSelected(false);
                radioButtonNormalMode.setSelected(t
                algorithmType = radioButtonNormalMo
            }
        }
}
```

Generated value : 3-3-7+4

Generated Result : -3

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.



Received Message :

```
package com.mycompany.design;

import java.awt.BorderLayout;
import java.awt.Dimension;
import java.awt.GridBagConstraints;
import java.awt.GridBagLayout;
import java.awt.GridLayout;
import java.awt.Insets;
import java.awt.Toolkit;
import java.awt.event.ActionEvent;
import java.awt.event.ActionListener;
import java.io.BufferedReader;
import java.io.File;
import java.io.FileInputStream;
import java.io.FileNotFoundException;
```

Technical Details :

Algorithm Type	Secret key	No of Packets	Secret keypath	Issued Time	Resolved Time	Packet's order
CPHS	3+2+4-9	24	secret.dat	45secs	23secs	NA

Puzzle value's : 3+2+4-9

Generated value : 3+2+4-9

Generated Result : 0

Fig 9: Server displaying message that is decrypting using cryptographicpuzzle

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. Wormhole Implementation

Wormholes can be used as a reactive defense mechanism. After receiving repeated acknowledgements, the source becomes the wormhole and sends the information regardingthe jammer to all other nodes. This wormhole, then prevent the jamming activity of particularjammer. By this method, all other nodes within that network can understand the informationabout the jammer.

VI. Shortest Path Implementation

Using the communication ranges between nodes, the shortest distance is calculated. A routingtable is maintained to store the distance between nodes in a network. Updations are possibleto the table whenever necessary

VII. Conclusion

In this paper, a technique is proposed for sending message in wireless network even if anattacker is present. It also described the technique wormholes, which will alert all other nodesabout the presence of a jammer. Here the packet sends through the shortest path betweensender and receiver. After including wormholes and shortest path concept the performance ofpacket hiding method improved. This technique is very effective in emergency responseoperations, military, police networks etc. It improves the performance and reliability ofwireless networks.

References

[1]. T.X. Brown, J.E. James, and A. Sethi, "Jamming and Sensing of Encrypted Wireless Ad Hoc Networks," Proc. ACM Int'l Symp. Mobile Ad Hoc Networking and Computing (MobiHoc), pp. 120-130,2006.

[2]. M. Cagalj, S. Capkun, and J.-P.Hubaux, "Wormhole-Based Anti- Jamming Techniques in Sensor Networks," IEEE Trans. Mobile Computing, vol. 6, no. 1, pp. 100-114, Jan.2007.

[3]. A. Chan, X. Liu, G. Noubir, and B. Thapa, "Control Channel Jamming: Resilience and Identification of Traitors," Proc. IEEE Int'l Symp. Information Theory (ISIT), 2007.

[4]. W. Xu, W. Trappe and Y. Zhang, "Anti-Jamming Timing Channels for Wireless Networks," Proc. ACM Conf .Wireless Network Security (WiSec), pp. 203-213, 2008.

[5]. R. Rivest, "All-or-Nothing Encryption and the Package Trans- form," Proc . Int'l Workshop Fast Software Encryption, pp. 210-218,1997.

[6]. R. Rivest, A. Shamir, and D . Wagner, "Time Lock Puzzles and Timed-Release Crypto," technical report, Massachusetts Inst. of Technology, 1996.

[7]. P. Tague, M. Li, and R. Poovendran, "Mitigation of Control Channel Jamming under Node Capture Attacks," IEEE Trans.Mobile Computing, vol. 8, no. 9, pp. 1221-1234, Sept. 2009

[8]. A. Juels and J. Brainard, "Client Puzzles: A Cryptographic Countermeasure against Connection Depletion Attacks," Proc. Network and Distributed System Security Symp. (NDSS), pp. 151-165, 1999

[9]. A.D.Wood and J.A. Stankovic, "Denial of service in sensor networks," Computer, vol. 35, no. 10, pp. 54-62, oct. 2002.

[10]. J. McCune, E.Shi, A.Perrig, and M.K.Reiter, "Detection of Denial-of-message attacks on sensor networks broadcasts", Proc. IEEE symp. Security and Privacy, May 2005.

[11]. Mario Cagalj, SrdjanCapkun, Jean-PierroHubau "Wormhole-Based Anti jamming Techniques in sensor networks", IEEE Transactions on mobile computing, vol. 6, no. 1, Jan 2007.

[12]. AlejandroProano and LoukasLazos, “Packet-Hiding methods for preventing Selective Jamming Attack”, IEEE Transactions on dependable and secure computing, vol. 9, no. 1,Feb-2012.

[13]. I.Akyildiz,W.Su,Y.Sankarasubramaniam, and E.Cayirci, “A Survey on Sensor Networks,” IEEE Comm. Magazine, vol. 40, no, 8, 2002.

[14]. K. Gaj and P. Chodowiec, “ FPGA and ASIC Implementations of AES”,Cryptographic Engineering, pp. 235-294 , Springer, 2009.

[15]. O. Goldreich, “Foundations of Cryptography: Basic Applications”, Cambridge Univ. Press,2004.

[16]. W.Xu,W.Trappe,Y.Zhang, and T.Wood, “The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks”, proc. MobiHoc ’05, pp.46-57, 2005.

[17]. B. Schneier, “Applied Cryptography: Protocols, Algorithms, and Source Code in C”, 2007. International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.3, May 2014 105

[18]. W. Xu, T. Wood, W. Trappe, and Y. Zhang, “Channel Surfing and Spatial Retreats: Defenses against Wireless Denial of Service,”Proc. Third ACM Workshop Wireless Security, pp. 80-89,2004.