OPTIMIZING EFFICIENT AND RELIABLE PACKET TRANSMISSION OVER WIRELESS NETWORKS

Bamuli Swapna, Suresh Kumar Mandala
Assistant professor, Assistant professor
Department of computer science and Artificial intelligence, Department of computer science and Artificial intelligence,
SR University, Warangal-506371, Telangana, SR University, Warangal-506371, Telangana

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, smart phone, 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. JAMMING ATTACKS

The DNS is a hierarchical tree structure whose root node is known as the root domain. A label in a DNS name directly corresponds with a node in the DNS tree structure. A label is an alphanumeric string that uniquely identifies that node from its brothers. Labels are connected together with a dot notation, ".", and a DNS name containing multiple labels represents its path along the tree to the root. Labels are written from left to right. Only one zero length labels are allowed and is reserved for the root of the tree. This is commonly referred to as the root zone. Due to the root label being zero length, all FQDNs end in a dot [RFC 1034].A study into DoS attacks and defense was done by Raymond and Mid kiff (2008). Since WSNs are used in monitoring medical uses, homeland security, industrial automation, and military applications, security of WSNs must be guaranteed. Defeating many threats of DoS attacks on WSNs can be done by encryption and authentication, but some other techniques still need to be found to prevent from special DoS attacks, especially Denial of Sleep attacks, which are still critical threats in WSNs.

A. 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 nodes is done through a specific frequency, the frequency can be changed if necessary. While a jammer is attacking the wireless network, there are other effective ways to continue legitimate communication in the network. Engaging the jammer on the jammed channel and continuing communication in another channel was introduced. When the nodes detected the jamming in the wireless network, they jumped to another channel to continue legitimate communication. In the experiments, both 10 and 20 nodes experiments were done, and in both scenarios, after channels were jumped, the network resumes communications as normal. In both scenarios, the amount of packets dropped reduced immediately. The research concluded that channel jumping will decrease the throughput of the network. Also, it was easier to detect jamming through intermitted channel jumping. Concluded, channel jumping was a superior method of combating network interference, rather than changing network protocols. The research concluded that channel jumping will decrease the throughput of the network.

Also, it was easier to detect jamming through intermitted channel jumping. Concluded, channel jumping was a superior method of combating network interference, rather than changing network protocols. In order to prevent from multi-channel jamming attacks, a cross-layer jamming detection method was developed. Cross-layer jamming detection is a tree-based approach. A jamming detection algorithm was utilized in all legitimate nodes; when the communication process began, all the nodes had the ability to report jamming attacks in different layers, and only the reports which were generated by nodes with jamming detection algorithm were accepted by the system in order to avoid error. Research was also done about multi-channel jamming attacks. The difference from the jamming detection algorithm was that it focused on network restoration and design of traffic rerouting.

B. Algorithm

1. Symmetric encryption algorithm
2. Brute force attacks against block encryption algorithms.

We propose a solution based on all-Or- Nothing Transformations (AONT) that introduces a modest communication and computation overhead. Such transformations were originally proposed by Rivest to slow down brute force attacks against block encryption algorithms. An AONT serves as a publicly known and completely invertible pre-processing step to a plaintext before it is passed to an ordinary block encryption algorithm

1. Algorithm Description

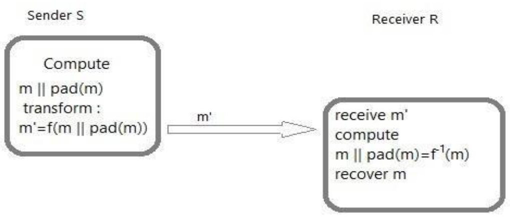


Fig.1. the AONT-based Hiding Scheme (AONT-HS)

C. The Package Transform

In the package transform, given a message m, and a random key k′, the output pseudo-messages are computed as follows: m'i = mi ⊕ Ek' (i), for i=1, 2, 3 ....,x m'x+1 = k' ⊕ e1 ⊕ e2 ⊕ e3 ⊕ ....⊕ ex ,

Where ei = Ek0 (m'i ⊕ i), for i = 1, 2, ..., x, and k0 is a fixed publicly-known encryption key. With the reception of all pseudo-messages message m is recovered as follows:

k' = m'x+1 ⊕ e1 ⊕ e2 ⊕ e3 ⊕.................. ⊕ ex , mi = m'i ⊕ Ek' (i) , for i=1,2,3..........,x,

Note that if any m'i is unknown, any value of k′ is possible, because the corresponding ei is not known. Hence, Ek' (i) cannot be recovered for any i, making it infeasible to obtain any of the mi.

D. Hiding Sub layer Details

AONT-HS is implemented at the hiding sub layer residing between the MAC and the PHY layers. In the first step, m is padded by applying function pad () to adjust the frame length so that no padding is needed at the PHY layer, and the length of m becomes a multiple of the length of the pseudo-messages m′ i. This will ensure that all bits of the transmitted packet are part of the AONT. In the next step, m||pad (m) is partitioned to x blocks, and the AONT f is applied. Message m′ is delivered to the PHY layer. At the receiver, the inverse transformation f−1 is applied to obtain m||pad (m). The padded bits are removed and the original message m is recovered. The steps of AONT-HS are shown in Fig.1.

1. Architecture

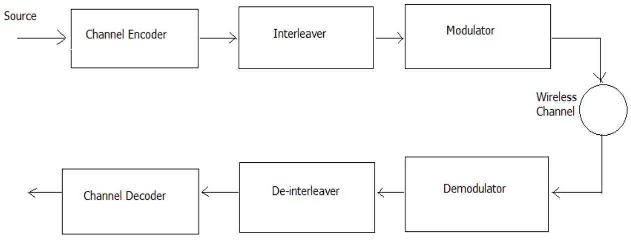


Fig.2. Architecture.

E. Types of Jammer

Continuous blocking has been used as a denial-of-service (DoS) attack against voice communication since the 1940s. Recently, several alternative jamming strategies have been Categorized jammers into four models, (a) a constant jammer that continuously emits noise, (b) a deceptive jammer that continuously broadcasts fabricated messages or replays old ones, (c) a random jammer that alternates between periods of continuous jamming and inactivity, and (d) a reactive jammer who jams only when transmission activity is detected.

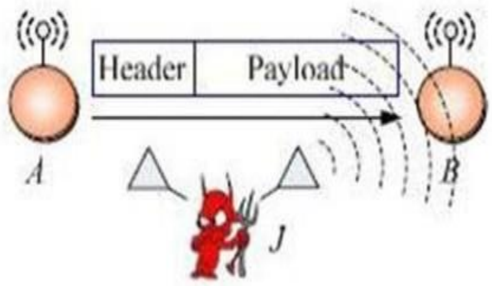


Fig.3.Realization of a selective jamming attack

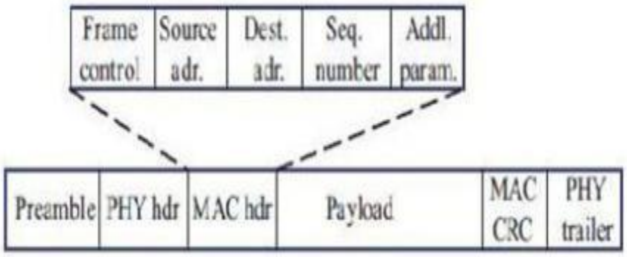


Fig.4. A generic frame format for a wireless network

A. Constant jammer

The constant jammer continually emits a radio signal. It has implemented a constant jammer using two types of devices. The first type of device to use is a waveform generator which continuously sends a radio signal. The second type of device it used is a normal wireless device. In this author, it will focus on the second type, which it built on the MICA2 Mote platform. This constant jammer continuously sends out random bits to the channel without following any MAC layer etiquette. Specifically, the constant jammer does not wait for the channel to become idle before transmitting. If the underlying MAC protocol determines whether a channel is idle or not by comparing the signal strength measurement with a fixed threshold, which is usually lower than the signal strength generated by the constant jammer, a constant jammer can effectively prevent legitimate sources from getting hold of channel and sending packets

B. Deceptive jammer

Instead of sending out random bits, the deceptive jammer constantly injects regular packets to the channel without any gap between subsequent packet transmissions. As a result, a normal communicator will be received into believing there is a legitimate packet and will be duped to remain in the receive state. For example, in Tiny OS, if a preamble is detected, a node remains in the receive mode, regardless of whether that node has a packet to send or not. Hence, even if a node has packets to send, it cannot switch to the send state because a constant stream of incoming packets will be detected. Further, it also observe that it is adequate for the jammer to only send a continuous stream of preamble bits (0xAA in Tiny OS) rather than entire packets.

C. Random jammer

Instead of sending out a radio signal continuously, a random jammer alternates between sleeping and jamming. Specifically, after jamming for tj units of time, it turns on its radio, and enters a sleeping mode. It will resume jamming after sleeping for ts time. tj and ts can be either random or fixed values. During its jamming phase, it can either behave like a constant jammer or a deceptive jammer. Throughout this art hour, this random jammer will operate as a constant jammer during jamming. The distinction between this model and the previous two models lies in the fact that this model tries to take energy conservation into consideration, which is especially important for those jammers that do not have unlimited power supply. By adjusting the distribution governing the values of tj and ts, it can achieve various levels of tradeoff between energy efficiency and jamming effectiveness.

D. Reactive jammer

The three models discussed above are active jammers in the sense that they try to block the channel irrespective of the traffic pattern on the channel. Active jammers are usually effective because they keep the channel busy all the time. These methods are relatively easy to detect. An alternative approach to jamming wireless communication is to employ a reactive strategy. For the reactive jammer, it takes the view point that it is not necessary to jam the channel when nobody is communicating. Instead, the jammer stays quiet when the channel is idle, but starts transmitting a radio signal as soon as it senses activity on the channel. As a result, a reactive jammer targets the reception of a message. It would like to point out that a reactive jammer does not necessarily conserve energy because the jammer's radio must continuously be on in order to sense the channel. The primary advantage for a reactive jammer, however, is that it may be harder to detect.

III. PROBLEM FORMULATION

A. Existing System

Jamming attacks are much harder to counter and more security problems. 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 jamming attacks have been considered under an external threat model, in which the jammer is not part of the network. Under this model, jamming strategies include the continuous or random transmission of high power interference signals.

B. Proposed System

In this paper, we address the problem of jamming under an internal threat model. We consider a sophisticated adversary who is aware of network secrets and the implementation details of network protocols at any layer in the network stack. The adversary exploits his internal knowledge for launching selective jamming attacks in which specific messages of "high importance" are targeted. For example, 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 launch selective jamming attacks, the adversary must be capable of implementing a "classify-then-jam" strategy before the completion of a wireless transmission. Such strategy can be actualized either by classifying transmitted packets using protocol semantics, or by decoding packets on the fly. In the latter method, the jammer may decode the first few bits of a packet for recovering useful packet identifiers such as packet type, source and destination address. After classification, the adversary must induce a sufficient number of bit errors so that the packet cannot be recovered at the receiver. Selective jamming requires an intimate knowledge of the physical (PHY) layer, as well as of the specifics of upper layers.

C. Modules

1. Network module
2. Real Time Packet Classification
3. Selective Jamming Module
4. Strong Hiding Commitment Scheme (SHCS)
5. Cryptographic Puzzle Hiding Scheme (CPHS)

1. Network module

We address the problem of preventing the jamming node from classifying m in real time, thus mitigating J's ability to perform selective jamming. 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.

2. Real Time Packet Classification

Consider the generic communication system depicted in Fig.5 at the PHY 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 inter leaved, and decoded, to recover the original packet. Moreover, even if the encryption key of a hiding scheme were to remain secret, the static portions of a transmitted packet could potentially lead to packet classification. This is because for computationally-efficient encryption methods such as block encryption, the encryption of a prefix plaintext with the same key yields a static cipher text prefix. Hence, an adversary who is aware of the underlying protocol specifics (structure of the frame) can use the static cipher text portions of a transmitted packet to classify it.

3. Selective Jamming Module

We illustrate the impact of selective jamming attacks on the network performance. Implement selective jamming attacks in two multi-hop wireless network scenarios. In the first scenario, the attacker targeted a TCP connection established over a multi-hop wireless route. In the second scenario, the jammer targeted network-layer control messages transmitted during the route establishment process 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.

4. Strong Hiding Commitment Scheme (SHCS)

We propose a strong hiding commitment scheme (SHCS), which is based on symmetric cryptography. Our main motivation is to satisfy the strong hiding property while keeping the computation and communication overhead to a minimum.

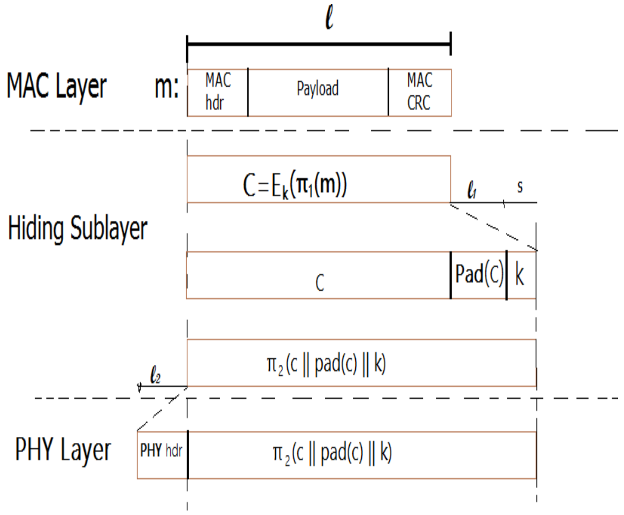


Fig.5. Processing at the hiding sub layer.

The computation overhead of SHCS is one symmetric encryption at the sender and one symmetric decryption at the receiver. Because the header information is permuted as a trailer and encrypted, all receivers in the vicinity of a sender must receive the entire packet and decrypt it, before the packet type and destination can be determined. However, in wireless protocols such as 802.11, the complete packet is received at the MAC layer before it is decided if the packet must be discarded or be further processed. If some parts of the MAC header are deemed not to be useful information to the jammer, they can remain unencrypted in the header of the packet, thus\ avoiding the decryption operation at the receiver.

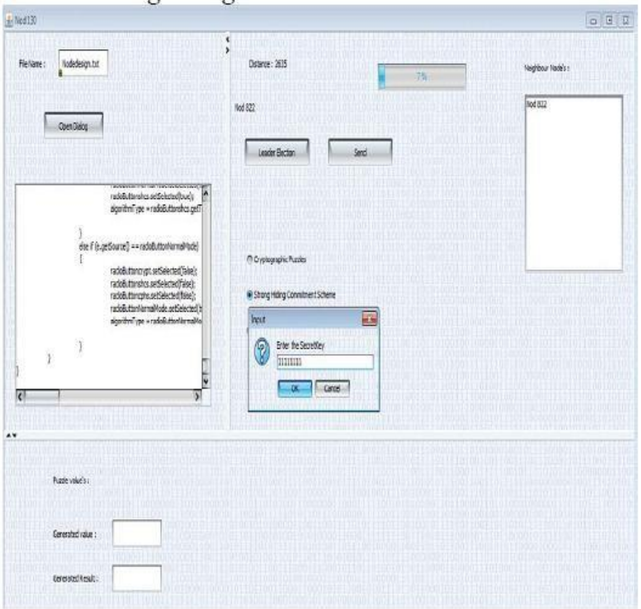
5. Cryptographic Puzzle Hiding Scheme (CPHS)

We present a packet hiding scheme based on cryptographic puzzles. 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. However, it has higher computation and communication overhead we consider several puzzle schemes as the basis for CPHS. For each scheme, we analyze the implementation details which impact security and performance. 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 escrow schemes.

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

Distance : 2635

7%

Neighbour Node's :

Nod 822

Nod 822

```
        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
    }
  }
}
```

○ Cryptographic Puzzles

● Strong Hiding Commitment Scheme

Enter the SecretKey
11111111

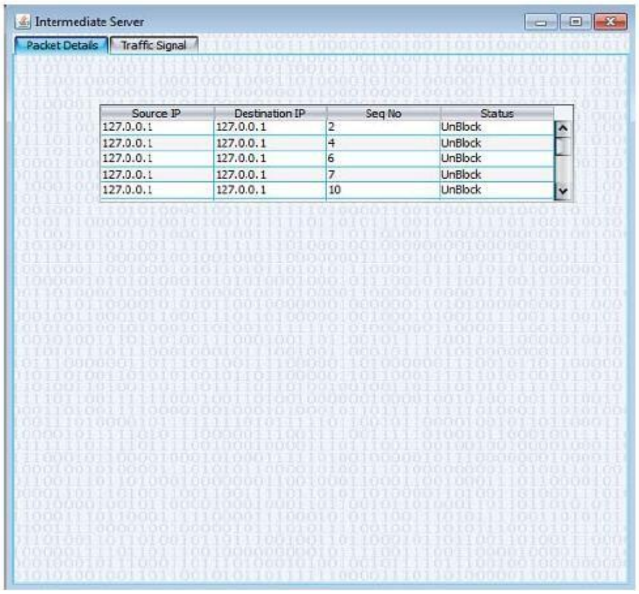
Puzzle value's :

Generated value :

Generated Result :

Fig.6. Node selecting Commitment scheme based on strong hiding.

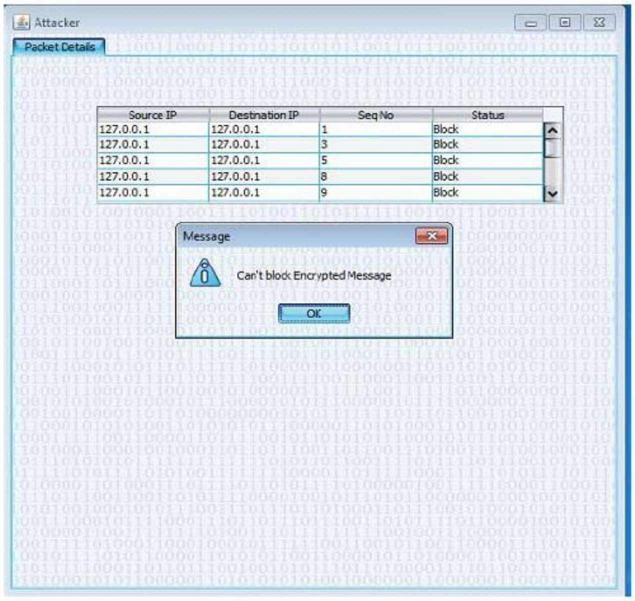
First Nodes are initialized. Two or more nodes are initialized and depending upon mobility one node will be selected as leader node. Other nodes act like neighbor node and here file will be uploaded and node will select SHCS, here it will ask for secrete key.



Source IP	Destination IP	Seq No	Status
127.0.0.1	127.0.0.1	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.7. 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.

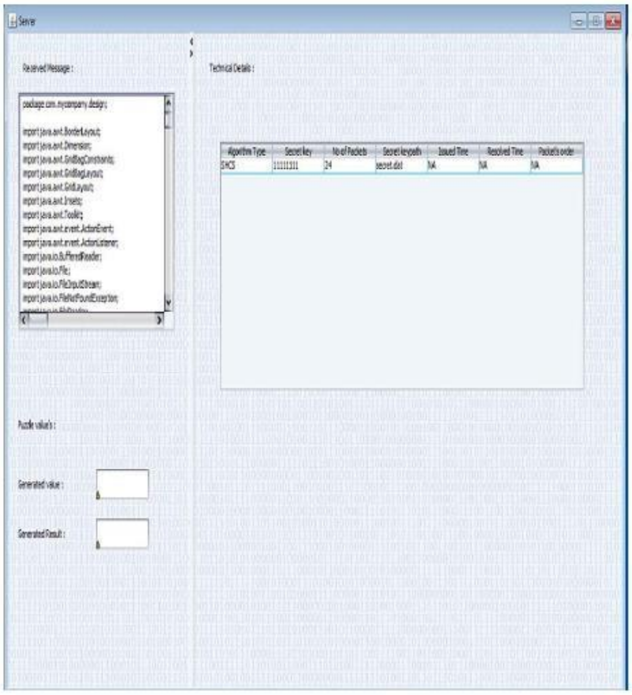


Source IP	Destination IP	Seq No	Status
127.0.0.1	127.0.0.1	1	Block
127.0.0.1	127.0.0.1	3	Block
127.0.0.1	127.0.0.1	5	Block
127.0.0.1	127.0.0.1	8	Block
127.0.0.1	127.0.0.1	9	Block

Can't block Encrypted Message

Fig.8. 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.



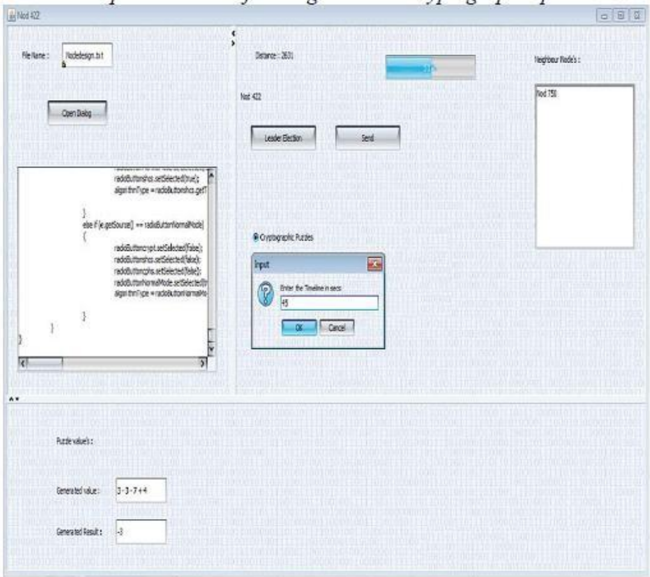
```
package com.mycompany.design;

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.9. 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



File Name : Nodedesign.txt

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

Neighbour Node's : Nod 750

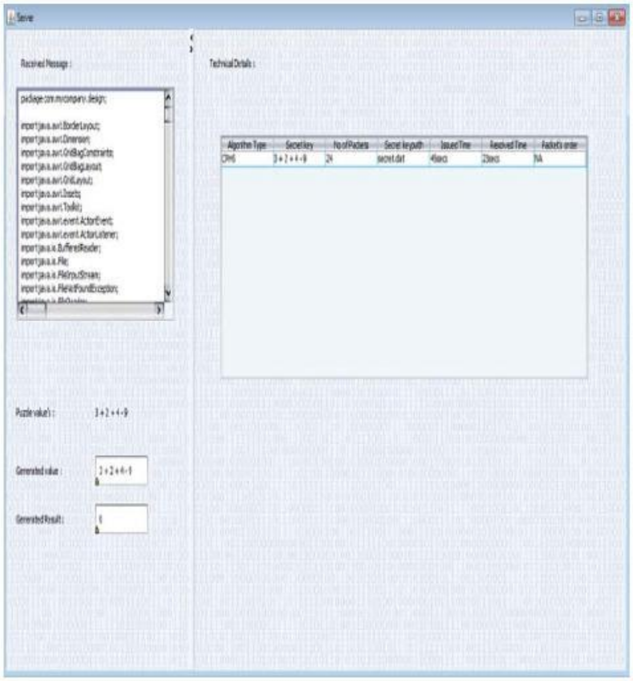
Enter the Timeline in secs: 45

Generated value : 3-3-7+4

Generated Result : -3

Fig.10. 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.



```
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
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.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. CONCLUSION

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.

VI. REFERENCES

[1] Rashmi B.Dhamannavar, Dr.Rashmi M.Jogdand, “Encryption Techniques in Packet Hiding Methods to Prevent Jamming Attacks in Wireless Network”, International Journal of Computer Science and Information Technologies, Vol. 5 (4) , 2014, 4981-4985.
[2] 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.
[3] 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.

[4] wireless lans and countermeasures. Mobile Computing and Communications Review,7(3):29–30, 2003.

[5] 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.

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

[7] 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.

[8] 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.

[9] 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.