Analyzing the Efficiency of the Packet Hiding Methods based on the Strong Hiding Commitment Scheme (SHCS)

K.J Eldho
Asst.Professor & Research Scholar, Department of Computer Science
Don Bosco College, Sulthan Bathery

ABSTRACT

This research describes about analyze the packet hiding methods. These methods are efficiently hiding the data packets while transferring in the network Medias. To protect the system from the unauthorized users, unauthorized programs, threaten the confidential matters and confirm the system availability to the legal users. Our need of network security has broken into two needs. One is the need of information security and other is the need of computer security. On internet or any network of an organization, thousands of important information is exchanged daily. This information can be misused by attackers. The information security is needed for the following given reasons. In my project, a single text file is the input of the system. In this project analysis of packet hiding methods, there are three types of transferring data are performed. In this I have analysis of the result manually. I have taken different sizes of file. This file is included in packet hiding methods. I calculate encryption times of the different files and different methods. Here different outputs are obtained.

1. INTRODUCTION

Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority.

2. NETWORK SECURITTY ISSUES

The networks are computer networks, both public and private, that are used every day to conduct transactions and communications among businesses, government agencies and individuals. The networks are comprised of "nodes", which are "client" terminals (individual user PCs), and one or more "servers" and/or "host" computers. They are linked by communication systems, some of which might be private, such as within a company and others which might be open to public access. The obvious example of a network system that open to public access is the Internet, but many private networks also utilize publicly-accessible communications. Today, most companies' host computers can be accessed by their employees whether in their offices over a private communications network, or from their homes or hotel rooms while on the road through normal telephone lines.

Network security involves all activities that organizations, enterprises, and institutions undertake to protect the value and ongoing usability of assets and the integrity and continuity of operations. An effective network security strategy requires identifying threats and then choosing the most effective set of tools to combat them.

Security management for networks is different for all kinds of situations. A home or small office may only require basic security while large businesses may require high-maintenance and advanced software and hardware to prevent malicious attacks from hacking and spamming.

3. ENCRYPTION AND DECRYPTION PROCEDURES:

Wireless networks rely on the uninterrupted availability 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 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 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 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. However, adopting an “always-on” strategy has several disadvantages. First, the adversary has to expend a significant amount of energy to jam frequency bands of interest. Second, the continuous presence of unusually high interference levels makes this type of attacks easy to detect.

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. There are many Encryption and Decryption techniques are available here used only, two techniques they are Strong Hiding Commitment Scheme (SHCS) and All Or Nothing Transformations (AONT). These techniques will see on literature survey part.

4. PROBLEM DESCRIPTION

PROBLEM DEFINITION

Nodes A and B communicate via Network. 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. Here address the problem of preventing the jamming node from classifying m in real time, thus mitigating J’s ability to perform selective jamming.

Aim

This project describes about analyze the packet hiding methods. These methods are efficiently hiding the data packets while transferring in the network Medias.

Objectives

The following specific objectives will be pursued in order to achieve the aim above.

1. Analyze the packets in the efficient way.
2. Analyzing packets are hiding use the above mentioned packet hiding methods ie) SHCS, AONT and No Packet hiding Method.

Analyze the packet hiding methods and find the efficient hiding method. The three packet hiding methods are going to compare effectively by using the different file transmission methods. And the result will be compared.

5. REQUIREMENTS OF THE PROLEMS ANALYSIS

In this project analysis of packet hiding methods, there are three types of transferring data are performed. In this I have analysis of the result manually. I have taken different sizes of file. This file is included in packet hiding methods. I calculate encryption times of the different files and different methods. Here different outputs are obtained.To protect the system from the unauthorized users, unauthorized programs, threaten the confidential matters and confirm the system availability to the legal users. Our need of network security has broken into two needs.

- To protect the secret information users on the net only. No other person should see or access it.
- To protect the information from unwanted editing, accidently or intentionally by unauthorized users.
- To protect the information from loss and make it to be delivered to its destination properly.
- The loss of data will be compared in the effective methods which I am comparing.

6. PROBLEM DESIGN INPUT OF THE PROBLEM

In my project, a single text file is the input of the system. A file is transferred from the sender to receiver and required processes are performed in this intermediate time and the data packets are safely send to the receiver. Safety and time is the main research things that I am comparing in my research. The file should reach the receiver safely and without losing any data.

Output of the Problem

Using effective techniques to hide the data packets effectively and secure the data packets. While the data is transmission, there is any data loss and error should not be occur. While the data is transmission, there is any data loss and error should not be occurring. Analyze the packet hiding methods and find the efficient hiding method. The three packet hiding methods are going to compare effectively by using the different file transmission methods. And the result will be compared. Based on the result the final result will be concluded.

Process of the problem

The processing steps of the system should be defined clearly. What is the algorithm to be used and should clearly understand the every step of the algorithm. In my project analysis of packet hiding methods. There are three algorithms that are compared here.

Feasibility Analysis:

The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of the system.

7. PROBLEM DESCRIPTION

Systems design is the process of defining the architecture, components, modules, interfaces, and data for a system to satisfy specified requirements. One could see it as the application of systems theory to product development. There is some overlap with the disciplines of systems analysis, systems architecture and systems engineering. Safety and time is the main research things that I am comparing in my research. The file should reach the receiver safely and without losing any data. This research describes about analyze the packet hiding methods. These methods are efficiently hiding the data packets while transferring in the network Medias. To protect the system from the unauthorized users, unauthorized programs, threaten the confidential matters and confirm the system availability to the legal users. Our need of network security has broken into two needs. One is the need of information security and other is the need of computer security. On internet or any network of an organization, thousands of important information is exchanged daily.

MODULATION

Modulation is the process that modulates the signal into suitable wave form across the communication channel. Typical modulation techniques are Binary Phase Shift Keying (BPSK) and Quadrature Amplitude Modulation (QAM). This module can implement in physical level only. So I am going to only study this module not implement.

DESIGN DETAILS:

There are two systems are available. One is sender and another one is receiver. Here one file can be send to the receiver. The file contains the original data. The file can be met to the following phases.

8. SYSTEM DESIGN

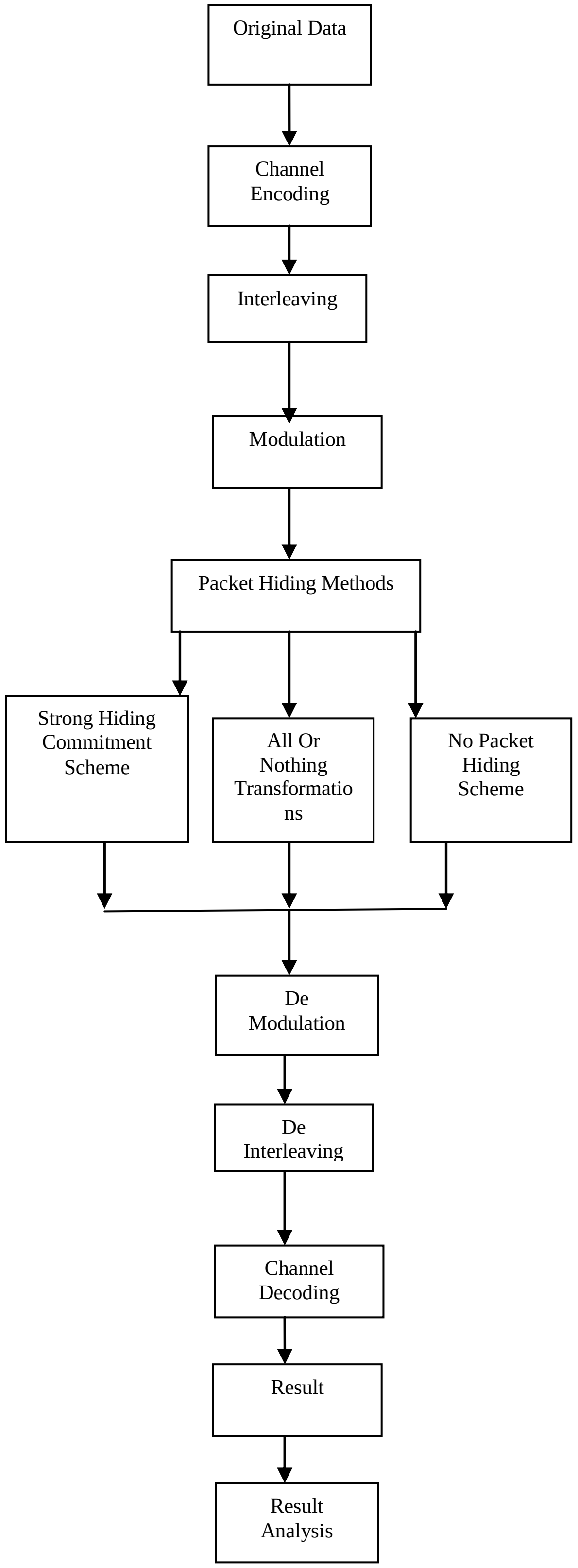


Fig 1.System Design

9. PACKET HIDING METHODS

In packet hiding methods module I am going to implement two methods. These are

- Strong Commitment Hiding Scheme(SHCS)
- All Or Nothing Transformations(AONT)

Strong Hiding Commitment Scheme

A commitment scheme is a two phase interactive protocol defined as a triple {X, M, E}. Set X = {A, V} denotes two probabilistic polynomial-time interactive parties, where A is known as the committer and V as the verifier; set M denotes the message space Set E = {(ti, fi)} denotes the events occurring at protocol stages ti (i = 1, 2), as per functions fi (i = 1, 2). During commitment stage t1,A uses a commitment function f1 = commit()During commitment stage t2, B uses a commitment function f2=open(). This is based on symmetric cryptography. Satisfy the strong hiding property while keeping the computation and communication overhead to minimum.

If the sender S has a packet m for R

- (c,d)=commit(m)
  - Where $C=E_k(\text{л}(m))$, d=k
- $m=\text{л}_1^{-1}(D_k(C))$

Where л_1^{-1} - denotes inverse permutation of л_1

By this algorithm the original message can be encrypted using the standard encryption algorithm in the sender side. Then the message can be transmitted in the communication channel, now the message cannot be opened by the hacker. At last the receiver side the message can be decrypted and get the original message.

All or Nothing Transformations

In cryptography, an all-or-nothing transform (AONT), also known as an all-or-nothing protocol, is an encryption mode which allows the data to be understood only if all of it is known AONTs are not encryption, but frequently make use of symmetric ciphers and may be applied before encryption. In AONT there are two methods are available, one is linear AONT and another one is package transform. I am going to implement only the package transform. In package transform the following steps are important.

Given a message m, and a random key k' the output pseudo messages are computed as

$$m'_i = m_i \oplus Ek'(i), \text{ for } i = 1, 2, \ldots, x$$

$$m'_{x+1} = k' \oplus e1 \oplus e2 \oplus \cdot \cdot \cdot \oplus ex,$$

$$\text{where } ei = Ek_0(m'_i \oplus i), \text{ for } i = 1, 2, \ldots, x,$$

With the reception of all pseudo messages, message m is recovered as

$$k' = m'_{x+1} \oplus e1 \oplus e2 \oplus \cdot \cdot \cdot \oplus ex,$$

$$m_i = m'_i \oplus Ek'(i), \text{ for } i = 1, 2, \ldots, x.$$

In the above algorithm shows that, with the original message some padding message are added in the sender side, then the message can be transmitted in the communication media. Meanwhile if the attacker opens the message, it cannot be opened. Finally in the sender side the padding message can be removed and get the original message.

No Packet hiding method

Here, the original message can be sent to the receiver. There is any packet hiding method is not used. While the data transmitted in the communication channel the hacker easily get the original message. This is the normal way of data transmission. Here data security is very poor.

De Modulation

Demodulation is the act of extracting the original information-bearing signal from a modulated carrier wave. A demodulator is an electronic circuit (or computer program in a software-defined radio) that is used to recover the information content from the modulated carrier wave. These terms are traditionally used in connection with radio receivers, but many other systems use many kinds of demodulators. Another common one is in a modem, which is a contraction of the terms modulator/demodulator.

De Interleaving

De interleaving is the process of reverse process of interleaving. In de interleaving the repeated bits are removed and get the original bit. Then these bits are sending to the channel decoding process.

Channel Decoding

In this channel Decoding process ASCII value bits are converted into the original user friendly characters. This is also the reverse process of channel encoding. This is the last process of file transferring. As per this process total file (i.e sending file) is change into this original format.

Problem Implementation

For the implementation of the project, Analysis of project hiding methods, Java 1.6 have used as the front end and there is no back end tool. Using the above system design this project was implemented. By this the above mentioned all the modules are implemented successfully.

For implement this project I have created server and client program. From the server one text file is send to the client. This file meets the following phases.

Channel encoding:

This is the first step of sender side. Here expands the original bit sequence of the message m. The original text will be converted into equivalent ASCII values and the values goes to the next step. In this project the file's characters are converted into equivalent ASCII values. In java to convert the integer ASCII value in to equivalent binary value integer to binary function is used.

Interleaving:

Binary values are collapses into repeated bit, this process is protect bits against the burst error while the bits travel in the communication channel. To implement this process, in java I have used in simple java statements. This process is also act the sender side.

Modulation:

Modulation is the process that modulates the signal into suitable wave form across the communication channel. Typical modulation techniques are Binary Phase Shift Keying (BPSK) and Quadrature Amplitude Modulation (QAM). This module can implement in physical level only. So I have put this as a study module.

Strong Hiding Commitment Scheme

If the sender S has a packet m for R

- $(C,d)=commit(m)$
  - Where $C=E_k(л(m))$, $d=k$
- $m=л_1^{-1}(D_k(C))$

Where $л_1^{-1}$ - denotes inverse permutation of $л_1$

By this algorithm the original message can be encrypted using the standard encryption algorithm in the sender side. Then the message can be transmitted in the communication channel, now the message cannot be opened by the hacker. At last the receiver side the message can be decrypted and get the original message. To implement this algorithm first message is fit into MAC layer format. The MAC layer format is given below

Ref: Y. Liu, P. Ning, H. Dai, and A. Liu. Randomized differential DSSS: Jamming-resistant wireless broadcast communication. In Proceedings of INFOCOM, San Diego, 2010

MAC Layer format

MAC Header	Payload	MAC CRC

MAC layer format

MAC Header format

MAC Header format

From the above figures shows that MAC Layer format and the MAC header format. In MAC layer contains MAC Header, Payload and MAC CRC information. In MAC Header contains the Frame control, source address, Destination address, Sequence number and the additional pram. Payload is the message packet and MAC CRC is the error checking code.

For implement MAC layer I have put the class MAC frame and the Mac header. The program use these classes take the necessary information. Then commit the message using the function commit (). To perform the commit () function I have encrypt the message using the Data Encryption Standard (DES) algorithm. I have implemented using the function encrypts (). This process is acted in the sender side. In the receiver side decommit () function is used to decommit the message and decrypt() is used to decrypt the message.

All or Nothing Transformations (AONT)

Given a message m, and a random key k' the output pseudo messages are computed as

$m'i = mi \oplus Ek'(i)$, for $i = 1, 2, \ldots, x$

$m'x+1 = k' \oplus e1 \oplus e2 \oplus \cdot \cdot \cdot \oplus ex$,

Where $ei = Ek0(m'i \oplus i)$, for $i = 1, 2, \ldots, x$,

With the reception of all pseudo messages, message m is recovered as

$k' = m'x+1 \oplus e1 \oplus e2 \oplus \cdot \cdot \cdot \oplus ex$,

$mi = m'i \oplus Ek'(i)$, for $i = 1, 2, \ldots, x$.

In the above algorithm shows that, with the original message some padding message are added in the sender side, then the message can be transmitted in the communication media. Mean while if the attacker open the message, it cannot be opened. Finally in the sender side the padding message can be removed and get the original message. For implement this we have to convert the data into MAC layer format. From the MAC layer format pay load field is taken and process it for hiding the data.

Ref: B. Greenstein, D. Mccoy, J. Pang, T. Kohno, S. Seshan, and D. Wetherall. Improving wireless privacy with an identifier-free link layer protocol. In Proceedings of MobiSys, 2008.

No Packet hiding method

Here, the original message can be sent to the receiver. There is any packet hiding method is not used. While the data transmitted in the communication channel the hacker easily get the original message. This is the normal way of data transmission. Here data security is very poor. This is a ordinary data transmission method, as per this method original data is transmitted without using any encryption and packet hiding methods. In this transmission I have implemented easily.

De Modulation

Demodulation is the act of extracting the original information-bearing signal from a modulated carrier wave. A demodulator is an electronic circuit (or computer program in a software-defined radio) that is used to recover the information content from the modulated carrier wave. These terms are traditionally used in connection with radio receivers, but many other systems use many kinds of demodulators. Another common one is in a modem, which is a contraction of the terms modulator/demodulator.

De interleaving

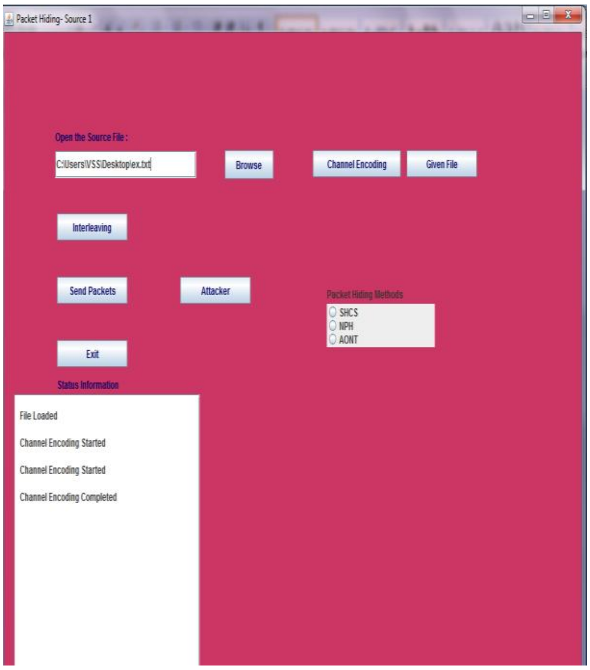
De interleaving is the process of reverse process of interleaving. In de interleaving the repeated bits are removed and get the original bit. Then this bits are send to the channel decoding process. I have implemented this process using simple java build in functions.

Channel Decoding

In this channel Decoding process ASCII value bits are converted into the original user friendly characters. This is also the reverse process of channel encoding. This is the last process of file transferring. As per this process total file (i.e sending file) is change into this original format. To implement this process integer to string conversion function is used. Here one queue is created. In this queue file's characters are stored. Then the stores characters are involved in these transformations. At last we get the original characters.

10. PERFORMANCE ANALYSIS CHANNEL ENCODING:

In the first module of my project is channel encoding. In this, original file's characters are converted into equivalent ASCII value then it is converted in to its binary form. Before that I have to create the source and destination systems i.e) server and the client, so I have created the two forms using Java platforms. This form contains one text area, text field and required command buttons. The following window is the source form and its components. Ref:Capkun, and J.-P. Hubaux. Wormhole-based anti jamming techniques in sensor networks. IEEE Transactions on Mobile Computing, 6(1):100–114, 2007



C:\Users\VSS\Desktop\ex.txt

File Loaded

Channel Encoding Started

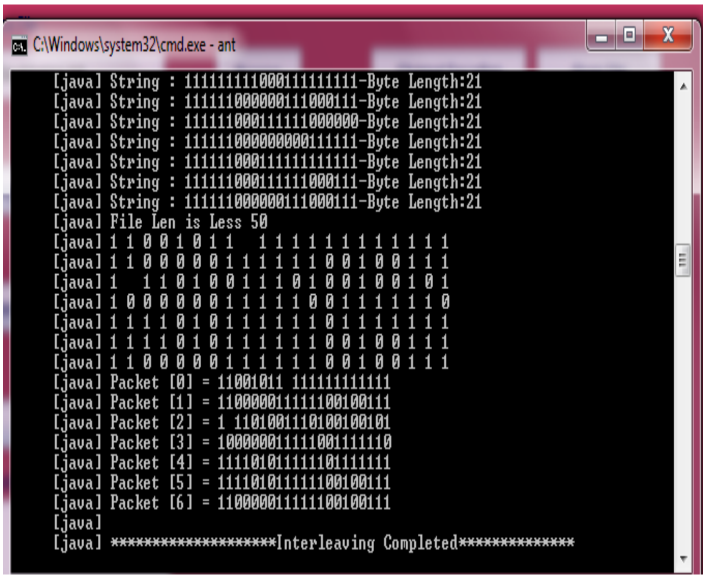
Channel Encoding Started

Channel Encoding Completed

Fig 2. Channel Encoding

Here I have selected using the browse button select the one file and choose the button encoding. Then

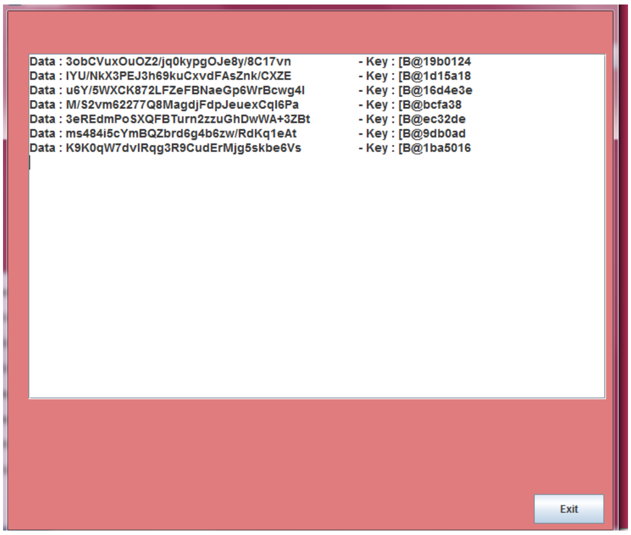
Interleaving is the process that performs repeat the binary bits for avoid the channel error during packet transmission. For that in the source form



```
     [java] String : 111111111000111111111-Byte Length:21
     [java] String : 111111000000111000111-Byte Length:21
     [java] String : 111111000111111000000-Byte Length:21
     [java] String : 111111000000000111111-Byte Length:21
     [java] String : 111111000111111111111-Byte Length:21
     [java] String : 111111000111111000111-Byte Length:21
     [java] String : 111111000000111000111-Byte Length:21
     [java] File Len is Less 50
     [java] 1 1 0 0 1 0 1 1   1 1 1 1 1 1 1 1 1 1 1 1
     [java] 1 1 0 0 0 0 0 1 1 1 1 1 1 0 0 1 0 0 1 1 1
     [java] 1   1 1 0 1 0 0 1 1 1 0 1 0 0 1 0 0 1 0 1
     [java] 1 0 0 0 0 0 0 1 1 1 1 1 0 0 1 1 1 1 1 1 0
     [java] 1 1 1 1 0 1 0 1 1 1 1 1 1 0 1 1 1 1 1 1 1
     [java] 1 1 1 1 0 1 0 1 1 1 1 1 1 0 0 1 0 0 1 1 1
     [java] 1 1 0 0 0 0 0 1 1 1 1 1 1 0 0 1 0 0 1 1 1
     [java] Packet [0] = 11001011 111111111111
     [java] Packet [1] = 110000011111100100111
     [java] Packet [2] = 1 11010011101001001O1
     [java] Packet [3] = 100000011111001111110
     [java] Packet [4] = 111101011111101111111
     [java] Packet [5] = 111101011111100100111
     [java] Packet [6] = 110000011111100100111
     [java]
     [java] ********************Interleaving Completed**************
```

Fig 3.Interleaving Process

Strong hiding commitment scheme

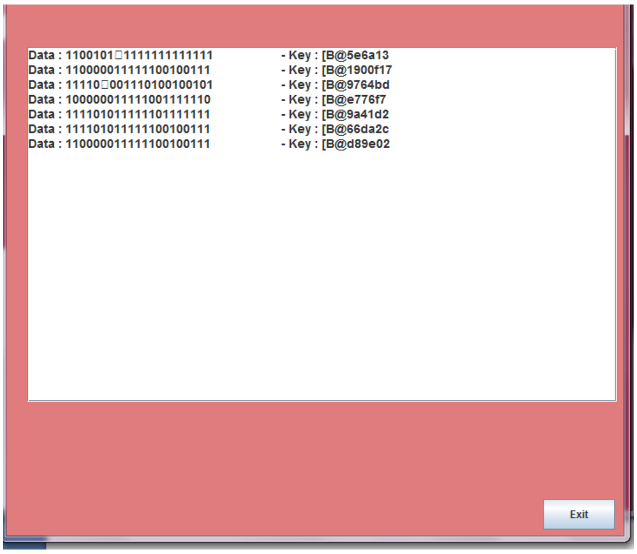


```
Data : 3obCVuxOuOZ2/jq0kypgOJe8y/8C17vn          - Key : [B@19b0124
Data : IYU/NkX3PEJ3h69kuCxvdFAsZnk/CXZE          - Key : [B@1d15a18
Data : u6Y/5WXCK872LFZeFBNaeGp6WrBcwg4l          - Key : [B@16d4e3e
Data : M/S2vm62277Q8MagdjFdpJeuexCql6Pa          - Key : [B@bcfa38
Data : 3eREdmPoSXQFBTurn2zzuGhDwWA+3ZBt          - Key : [B@ec32de
Data : ms484i5cYmBQZbrd6g4b6zw/RdKq1eAt          - Key : [B@9db0ad
Data : K9K0qW7dvlRqg3R9CudErMjg5skbe6Vs          - Key : [B@1ba5016
```

Fig 4. Strong Hiding Commitment Scheme

All or Nothing Transformations

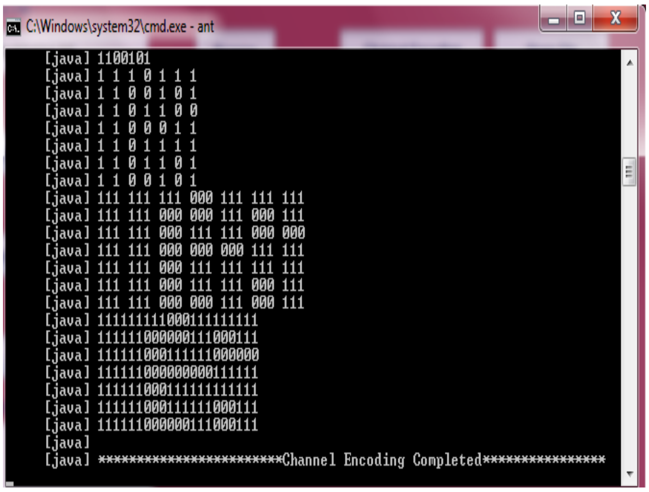
By this packet hiding method packet's serial number is encrypted but not encrypts the message. To get the original message all the packet information's are required. So the hackers are not easily hacking the data. As per this algorithm Decrypted data and the secret key is send to the receiver. In the receiver side get the encrypted data and key, then get the original message. The following figure shows that the encrypted message and the corresponding key.



```
Data : 1100101□1111111111111          - Key : [B@5e6a13
Data : 11000001111100100111           - Key : [B@1900f17
Data : 11110□001110100100101          - Key : [B@9764bd
Data : 10000001111001111110           - Key : [B@e776f7
Data : 11110101111101111111           - Key : [B@9a41d2
Data : 11110101111100100111           - Key : [B@66da2c
Data : 11000001111100100111           - Key : [B@d89e02
```

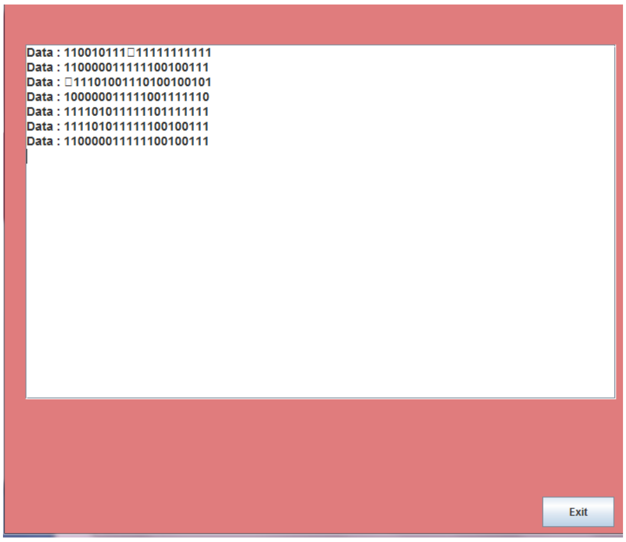
Fig 5.All Or Nothing Transformation

No Packet hiding Method



```
[java] 1100101
[java] 1 1 1 0 1 1 1
[java] 1 1 0 0 1 0 1
[java] 1 1 0 1 1 0 0
[java] 1 1 0 0 0 1 1
[java] 1 1 0 1 1 1 1
[java] 1 1 0 1 1 0 1
[java] 1 1 0 0 1 0 1
[java] 111 111 111 000 111 111 111
[java] 111 111 000 000 111 000 111
[java] 111 111 000 111 111 000 000
[java] 111 111 000 000 000 111 111
[java] 111 111 000 111 111 111 111
[java] 111 111 000 111 111 000 111
[java] 111 111 000 000 111 000 111
[java] 111111111000111111111
[java] 111111000000111000111
[java] 111111000111111000000
[java] 111111000000000111111
[java] 111111000111111111111
[java] 111111000111111000111
[java] 111111000000111000111
[java]
[java] ***********************Channel Encoding Completed****************
```

In this module packets are transferring without any packet hiding methods. So the following figure shows that data only and that is without encryption. It is just the binary form of the original data, so the hacker easily hack this.



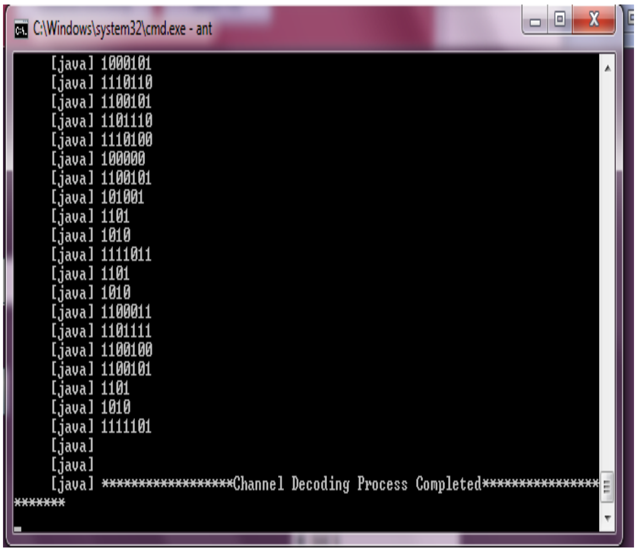
```
Data : 110010111□11111111111
Data : 11000001111100100111
Data : □11101001110100100101
Data : 10000001111001111110
Data : 11110101111101111111
Data : 11110101111100100111
Data : 11000001111100100111
```

Fig 6. No packet Hiding Method

De interleaving

De interleaving is the process that is the reverse process of interleaving. Here the repeated bits are removed and get the original binary bits.

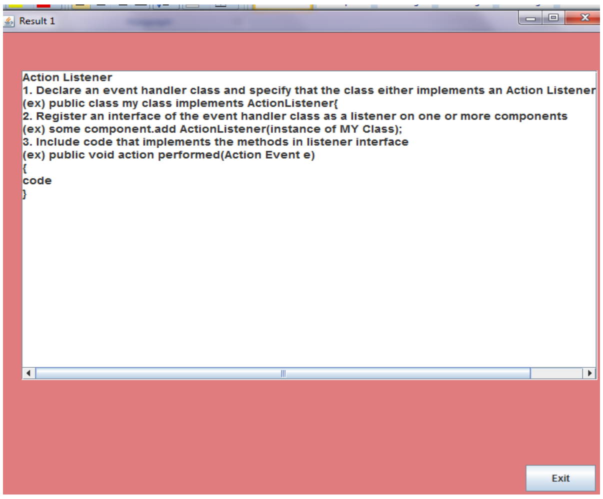
Channel Decoding



```
     [java] 1000101
     [java] 1110110
     [java] 1100101
     [java] 1101110
     [java] 1110100
     [java] 100000
     [java] 1100101
     [java] 101001
     [java] 1101
     [java] 1010
     [java] 1111011
     [java] 1101
     [java] 1010
     [java] 1100011
     [java] 1101111
     [java] 1100100
     [java] 1100101
     [java] 1101
     [java] 1010
     [java] 1111101
     [java]
     [java]
     [java] *****************Channel Decoding Process Completed***************
*******
```

Fig 7 Channel Decoding Process

In this channel encoding binary bits are converted in to original character's bits and it is stored in text file. At last If we click the result button the stored file display in the screen. The following window is the example testing file. The secure transmission performed between the sender and the receiver. Using the above methods the intermediate nodes cannot get the original file except the No packet hiding method.



```
Action Listener
1. Declare an event handler class and specify that the class either implements an Action Listener
(ex) public class my class implements ActionListener{
2. Register an interface of the event handler class as a listener on one or more components
(ex) some component.add ActionListener(instance of MY Class);
3. Include code that implements the methods in listener interface
(ex) public void action performed(Action Event e)
{
code
}
```

Fig 8 Channel Decoding Process

11. RESULT ANALYSIS

In this project analysis of packet hiding methods, there are three types of transferring data are performed. In this I have analysis of the result manually. I have taken different sizes of file. This file is included in packet hiding methods. I calculate encryption times of the different files and different methods. Here different outputs are obtained. The following table shows that this observation result.

Table 1

File size/methods	4283	466	139
SHCS	25	8	2
NPH	7	2	0.5
AONT	18	5	1

The following chat shows the different encryption time and the efficiency of the packet hiding methods.

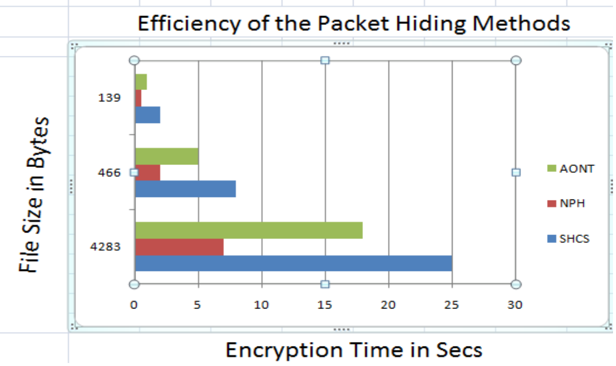


Figure 9 Result analysis

The above chart shows that three different size of files are taken for testing. (i.e 139,466 an4283 KB). In 139 kb, SHCS is taken to 2 seconds, NPH is 0.5 secs and AONT is 1 secs. In 466 KB , SHCS is taken to 8 secs, NPH is 2 secs and AONT is 5 secs. In 4282 KB SHCS is taken to 25 secs, NPH is 7 secs and AONT is 8 secs. In the above techniques SHCS is efficient technique compare to others. This technique is taken to more time for encryption. So this algorithm is efficient than others. No Packet hiding method is poor throughput compare others.

12. CONCLUSION

In this work entitled on "ANALYSING THE EFFICIENCY OF THE PACKET HIDING METHODS BASED ON THE STRONG HIDING COMMITMENT SCHEME (SHCS) I have done Analysis of Packet Hiding Methods implemented by the methods Strong Hiding Commitment Scheme, All Or Nothing Transformations and No packet Hiding Method. Taken the different results then analysis of those results successfully. In this Research work I have concluded that, the best hiding method is "Strong Hiding Commitment Scheme" and the poor transmission method is "No packet hiding". The average transmission method is All Or Nothing Transmission based on the output I have got through my research. The SHCS can be used for secure and fast data transmission. So that the method is concluded as the best by comparing the other two file transmission methods.

13. FUTURE ENHANCEMENT

In the future, will focus on implement the packet hiding methods in wireless network. The effective of the packet hiding method will be more on future. In this Project just only a simulation, here physical layers models such as Modulation and Demodulation have not implemented. Those layers will be implemented in future. More packet hiding methods will be introduced in future.

14. REFERENCES

[1] T. X. Brown, J. E. James, and A. Sethi. Jamming and sensing of encrypted wireless ad hoc networks. In Proceedings of MobiHoc, pages 120–130, 2006.

[2] B. Thapa, G. Noubir, R. Rajaramanand, and B. Sheng. On the robustness of IEEE802.11 rate adaptation algorithms against smart jamming. In Proceedings of WiSec, 2011.

[3] M. Wilhelm, I. Martinovic, J. Schmitt, and V. Lenders. Reactive jamming in wireless networks: How realistic is the threat? In Proceedings of WiSec, 2011.B. Thapa, G. Noubir, R. Rajaramanand, and B. Sheng. On the robustness of IEEE802.11 rate adaptation algorithms against smart jamming. In Proceedings of WiSec, 2011.

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

[5] A. Chan, X. Liu, G. Noubir, and B. Thapa. Control channel jamming: Resilience and identification of traitors. In Proceedings of ISIT, 2007.

[6] T. Dempsey, G. Sahin, Y. Morton, and C. Hopper. Intelligent sensing and lassification in ad hoc networks: a case study. Aerospace and Electronic Systems Magazine, IEEE, 24(8):23–30, August 2009.

[7] Y. Desmedt. Broadcast anti-jamming systems. Computer Networks, 35(2-3):223–236, February 2001.

[8] K. Gaj and P. Chodowiec. FPGA and ASIC implementations of AES. Cryptographic Engineering, pages 235–294, 2009.

[9] O. Goldreich. Foundations of cryptography: Basic applications. Cambridge University Press, 2004.

[10] B. Greenstein, D. Mccoy, J. Pang, T. Kohno, S. Seshan, and D. Wetherall. Improving wireless privacy with an identifier-free link layer protocol. In Proceedings of MobiSys, 2008.

[11] IEEE. IEEE 802.11 standard. http://standards.ieee.org/getieee802/

[12] download/802.11-2007.pdf, 2007.

[13] Y. W. Law, M. Palaniswami, L. V. Hoesel, J. Doumen, P. Hartel, and P. Havinga. Energy-efficient link-layer jamming attacks against WSN MAC protocols. ACMTransactions on Sensors Networks, 5(1):1–38, 2009.

[14] 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.

[15] 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.

[16] X. Liu, G. Noubir, and R. Sundaram. Spread: Foiling smart jammers using multi-layer agility. In Proceedings of INFOCOM, pages 2536–2540, 2007.

[17] Y. Liu, P. Ning, H. Dai, and A. Liu. Randomized differential DSSS: Jamming-resistant wireless broadcast communication. In Proceedings of INFOCOM, San Diego, 2010.

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

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

AUTHOR

K J Eldho Working as an Asst.Professor in Don Bosco College Sulthan Bathery Wayanad. He is pursuing his P hD in Bharathiyar university Coimbatore.