A Novel Technique of Security Improvement in Ad-hoc Network by using FTP

Dr. Preeti Gulia
Assistant Professor, Department of Computer Science and Applications,
Maharshi Dayanand University, Rohtak, Haryana, India.

Orcid: 0000-0001-8535-4016

Reena
Student, Department of Computer Science and Applications,
Maharshi Dayanand University, Rohtak, Haryana, India.

Orcid: 0000-0003-0218-0634

Abstract

In this era of technology, use of Ad-hoc network is increasing day by day. There are several threats to AD-HOC based network. In this paper, the role of AD-HOC in communication has been discussed as well as the security threats from hacker during file transmission. The main focus in the research is the security of data in a file. Here in this paper, the traditional security mechanisms with their loop holes are also discussed. The proposed work would definitely reduce the probability of data theft. Content of packets has been replaced by corresponding small strings in order to reduce size of packet to be transmitted on network. In this paper, Research has been done that if there is secure transmission then speed of data transfer gets degraded.

Keywords: Security, network, FTP, Ad-hoc network, Hacker.

INTRODUCTION

Ad hoc network is considered as a network which is compositions of different type of devices that are communicating to one other in direct way. Several ad hoc networks are considered as local area networks in which computers and different other devices have been enabled to transfer data in direct way to one another instead of transferring through a centralized access point [20]. In case of Ad- hoc, network does not need any router. It does not need any wireless base station [1], [6]. This network is established for single session only. If someone wants to share file in multiple computers then he could set more than one hop ad hoc network that can be used to transfer information on more than one node. It is created to solve specific problem. It becomes permanent network if someone is going to establish such network for longer period.

The Wireless networks are getting popularity since 1970. In several decades a lot of researches have been developed on Ad Hoc Network. The Ad hoc networks are playing an important role in case of martial applications & many researches like global mobile information program. This is useful in case of programs that are related to near digital radio. There can be new spaces of industrial & commercial applications for those networks which are based on wireless Ad Hoc. The fast development of internet has made communication a useful factor for Computation. In recent era of mobile devices usually we stay online. It is compulsory to make network cost effective & very fast to stay online all time [1], [11].

File Transfer Protocol (FTP) is an application level protocol used to transfer files securely. FTP can be considered a protocol that is dependent on an Internet Protocol [9].

FTP client has supported downloading of those files on Internet from computers which are known as FTP servers. The FTP means a File Transfer Protocol technology that is a FTP clients making & servers which are able to upload & download file on computer networks. FTP client is considered as software in a graphical user interface that is providing many options in to support and handle activity of files transmission.

LITERATURE SURVEY

According to Yet-Chun Hu, [1] Wormhole attack can be performed even if attacker is not compromising hosts & even if each transmission is providing authenticity as well as confidentiality.

As per C. Sanchez-Avil [2] et.al they made comparison of performance among recent AES, DES & T-DES for various micro controllers has been implemented , & displaying recent AES is having cost of computer of same order as compared to one needed by traditional DES based system.

Susan [3] et. al tells the Security field is fast moving career. They defined group of skills that are needed by Network Security as skills of network security which focus on practices of business & legal foundations. They also discussed the aims at attack recognition and network optimization with active learning exercises.

Neetu Setia [4] said there are several security & attack aspects of cryptographic methods. They have been discussed in dominant issues of protection from different attacks. Their bench represents considered latest cryptographic based algorithms that are finding suitable adjustment in case of security. At the part of their research Cryptography Tool has been used as simulator for conducting experiments & in order to get result.

According to Zhang [5] et.al packet payload are generally used to identify attacks at application level. He has focused on attacks that are at application level. He also represents current condition of network problem finding, & focused on importance of payload based finding based research using present issue, & proposed appropriate ways to find payload relevant attacks. In these situations ways are classified in a detection phase & a training phase.

Ahmed M. Al [6] identifying & summarizing security concerns with solutions are mandatory in Wireless Local Area Network. Present paper checks & summarizes such security issues & solutions. Security issues within WLAN world are classified into physical & logical broadly.

Punita Meel [7] tells it is better to use basic mathematics behind AES algorithm which is used in case of security system used in communication because Advanced Encryption Standard is providing better security. They stated that there is less complexity in implementation. It is considered the most efficient as well as strongest algorithms in present time.

Scott Wolchok [8] described how 48 hours of that system goes live and how they had gained election server control. District held a unique public trial before deploying system in usual election. It is done in mock election at the time when anyone was called to attempt to check its security.

As per Sumedha Kaushik, and Ankur Singhal [9] Network Security Using Cryptographic Techniques are presently in use of large organizations. Network Security is concerned with all hardware & software functions, operational procedures, accountability, characteristics, features, measures, and access control & administrative & management policy needed to give an acceptable level of protection for Hardware & Software, & information in a network.

According to Jason V. Chang [10] small amount of computer hackers have been caught. Issue is that many companies that are victims, hides such issues from public because of publicity that is negative. So this article proposes that a urgent reporting need imposed by Congress that forces companies in order to disclose intrusions would be salient to issue of computer hacking in many regards.

Dr. Mazin Sameer Al-Hakeem [11] Development of Fast Reliable Secure File Transfer Protocol has been performed. In this research author is developing a reliable file transfer protocol which is based on UDP for fast performance but reliable & secure protocol such as TCP. It is known as FRS-FTP.

Sharad Pratap Singh [12] FTP has been configured as per security requirements to transfer file. Additional process overhead in FTPs such as encryption affects its performance. They discussed the security configuration & performance analysis of FTP server.

As per Lidong Zhou [13] Ad hoc networks are not relying on fixed infrastructure unlike traditional mobile wireless networks. Hosts depend on one other in order to keep network inter connected. The Military tactical & several other security-sensitive operations are main software of ad hoc networks however there is a trend to use ad hoc based networks.

As per Aaditya Jain [14] there are few new types of honey pots that are base of recently proposed models. His paper explains honey pot technology. Its categorization is dependent on different factors. Tools for network security deal within recording capture & analysis of events related to network in order to find evidential data related to source of attacks on security.

LIMITATIONS OF EXISTING RESEARCH

There were several limitations in last research work and here in this paper we would remove the limitations of previous researches. The objective of existing researches was to secure Ad Hoc Networks. Some research deal with development of Fast Reliable Secure File Transfer Protocol.

Securing Wireless and Security configuration & performance analysis of FTP server has been also proposed in traditional system. Advance Trends in Network Security within Honeypot and Wormhole Attacks within Wireless Networks were discussed in some research. Some explains Wireless LAN Security analyzed structure.

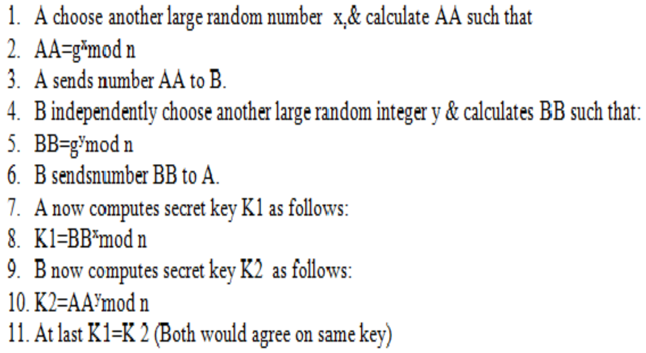
Some of researchers discussed security & attack aspects of cryptographic techniques. Some presented fundamental mathematics behind AES algorithm. Many researchers focused on application level attacks like Attacking Washington Voting System & Scott Wolchok Security etc. Research on Lightweight Hidden Services Network Security Using Cryptographic Techniques is also done.

Here in our research, we have developed the file server as well as file receiver. The socket programming has been used to implement it. More over the study is made on the limitation of existing researches. In our research we have tried to minimize the limitations of traditional security system.

In this paper we use the **Diffie–Hellman key exchange** Which is a important method of strongly conversation cryptographic keys of public direct was one of the first public key procedure as in beginning conceptualized by Ralph &

named after Whitfield Diffie and Martin Hellman is one of original practical examples of public key exchange execute within area of cryptography [19].

Let us assume that A & B need to concur upon to be used for encrypting /decrypting messages that would be conversation between them. So steps are as:-Firstly A & B agrees on two large prime numbers, n & g.



1. A choose another large random number x,& calculate AA such that
2. $AA=g^x mod n$
3. A sends number AA to B.
4. B independently choose another large random integer y & calculates BB such that:
5. $BB=g^y mod n$
6. B sendsnumber BB to A.
7. A now computes secret key K1 as follows:
8. $K1=BB^x mod n$
9. B now computes secret key K2 as follows:
10. $K2=AA^y mod n$
11. At last K1=K 2 (Both would agree on same key)

Figure 1: Algorithm for Key Exchange

PROPOSED WORK

Proposed work focuses on the reduction of packet size in order to reduce the probability of congestion and to secure network from packet dropping attack as shown in figure 2. It is better than previous protocol enhancement as in focuses more than the network era & growing packet transfer ratio. Because power is deliver symmetric & traffic load is dispersed over network so we have to put minimum load on the network during packet transmission.

Step of proposed work

1. Development of Secure File server using Socket Programming.
2. Development of Secure File Client using socket programming.
3. Enabling encrypted data transmission among File Server and File Client
4. The transmission would not be done from standard FTP protocol. Here we are using TCP based transmission mechanism with user defined port.
5. During Transmission a particular key would be used at both ends to make information understandable.
6. The transmission would be made during specific time slot initiated by client.

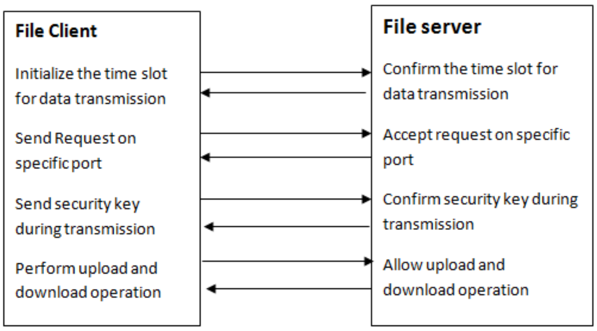

File Client
Initialize the time slot for data transmission
Send Request on specific port
Send security key during transmission
Perform upload and download operation
File server
Confirm the time slot for data transmission
Accept request on specific port
Confirm security key during transmission
Allow upload and download operation

Figure 2: Proposed Model

RESULTS

Server Side Implementation

In this research, we have developed a server application as well as client application in Netbeans IDE. As shown in following figure:

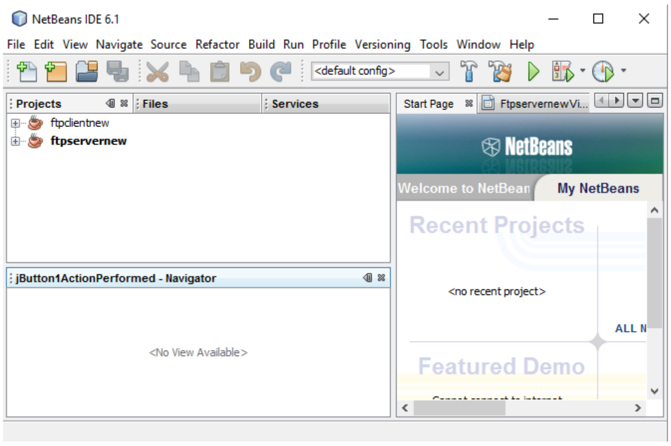
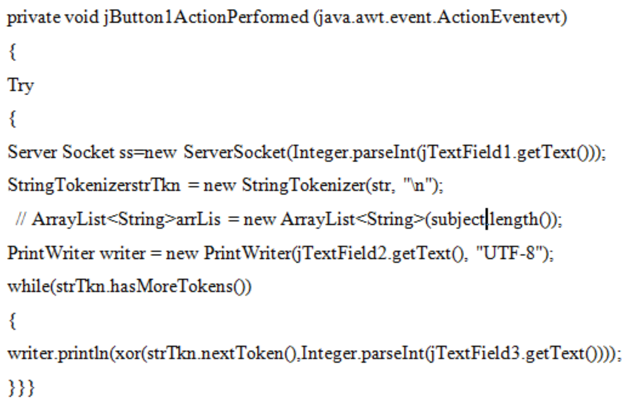


Figure 3: Server Side Implementation

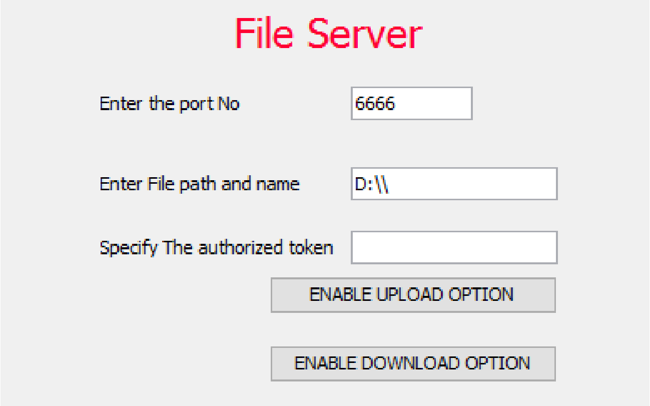
In server side we have made designing & written code to enable download option & disable downloads option.



```
private void jButton1ActionPerfomed (java.awt.event.ActionEventevt)
{
Try
{
Server Socket ss=new ServerSocket(Integer.parseInt(jTextField1.getText()));
StringTokenizerstrTkn = new StringTokenizer(str, "\n");
 // ArrayList<String>arrLis = new ArrayList<String>(subjectlength());
PrintWriter writer = new PrintWriter(jTextField2.getText(), "UTF-8");
while(strTkn.hasMoreTokens())
{
writer.println(xor(strTkn.nextToken(),Integer.parseInt(jTextField3.getText())));
}}}
```

Figure 4: Code for Enable Upload Option

Following is design view of server side application, Here we have to specify port no, file path, & token (to decode data)



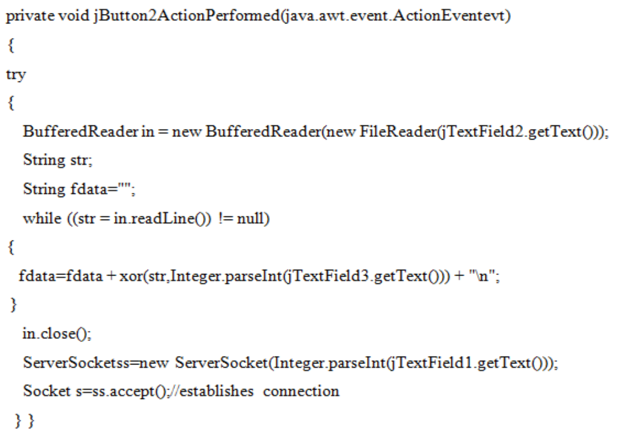
File Server

Enter the port No: 6666

Enter File path and name: D:\\

Specify The authorized token:

Figure 5: Design view of server side application

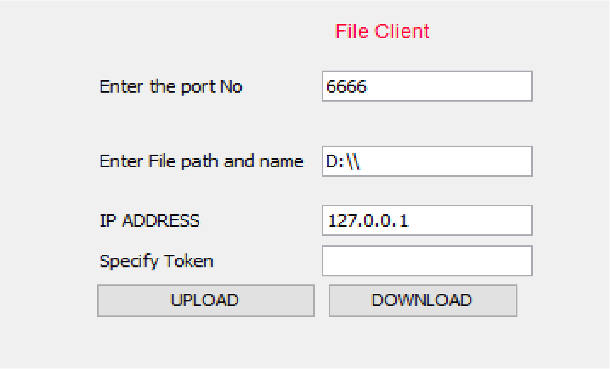


```
private void jButton2ActionPerformed(java.awt.event.ActionEventevt)
{
try
{
  BufferedReader in = new BufferedReader(new FileReader(jTextField2.getText()));
  String str;
  String fdata="";
  while ((str = in.readLine()) != null)
{
 fdata=fdata + xor(str,Integer.parseInt(jTextField3.getText())) + "\n";
}
  in.close();
  ServerSocketss=new ServerSocket(Integer.parseInt(jTextField1.getText()));
  Socket s=ss.accept();//establishes  connection
 } }
```

Figure 6: Code for Enable Download Option

Client Side Implementation

Following is design view for file client in order to upload&download data. Here we have to specify port no, file path, IP address of server & token (to encode data).



File Client

Enter the port No: 6666

Enter File path and name: D:\\

IP ADDRESS: 127.0.0.1

Specify Token:

Figure 7: Code to implement upload on client side

CONCLUSION & FUTURE SCOPE

This research is useful for security of contents & services over AD HOC network. Our research would restrict unauthentic access of digital data & dropping of service would not be allowed. It would result in smooth working. File transmission would not be done from standard FTP protocol. Here TCP based transmission mechanisms have been defined with user defined port.

The transfer file data has been captured from file using Java file handling and write that data on socket and sent to the server. The receiver would capture the information using TCP based communication and data would be written to the remote server using java file handling code on receiver end. Security of File transfer protocol server would definitely reduce chances of miss happening in AD HOC Network.

REFERENCES

[1] Yet-Chun Hu “Attacks within Wireless Networks” International Journal of Engineering Science & Technology (IJEST) ISSN : 0975-5462 Vol. 3 No. 4 April 2006

[2] C. Sanchez-Avila analyzed structure & design International Journal of Engineering Science & Technology Vol. 8 No 2007

[3] Susan Darshan Lal “Destruction Security field is a new & fast moving career” International Journal of Advance Research in Computer Science & Management Studies on 2008

[4] Neetu Settia “security & attack aspects of cryptographic techniques Current Activity & Future Directions “ Acm Sigcomm Computer Communication Review, 28(3):5–26, July 2008

[5] Zhang “Application level attacks”, IEEE New York 2009

[6] Ahmed M. Al Naamany “Wireless LAN Security Overview” in 2006

[7] Punita Meelu “ fundamental mathematics behind AES algorithm” in 2009

[8] Scott Wolchok , Attacking Washington, D.C.Internet Voting System ,2010

[9] Sumedha Kaushik, Ankur Singhal “Network Security Using Cryptographic Techniques” in 2012

[10] Jason V. Chang,” computer hacking making”, Journal of Zhejiang University-SCIENCE, 2012

[11] Dr. Mazin Sameer Al-Hakeem, " Development of Fast Reliable Secure File Transfer Protocol ", Journal of Zhejiang University-SCIENCE , 2013

[12] Sharad Pratap Singh, " security configuration &

performance analysis of ftp server", intelligent Computing, Networking, & Informatics Advances in Intelligent Systems & Computing ,2014

[13] Lidong Zhou Ali Jalooli, Rafidah MdNoor,Rashid Hafeez Khokhar, Jaime Lloret, " Securing Ad Hoc Networks", Wireless Networks , Springer ,2015

[14] Aaditya Jain, "Advance Trends in Network Security within Honey pot & its Comparative Study within other Techniques" ,December 2015

[15] Sonu MadhuViswanatham, "Review Paper on Securing Wireless", IEEE, 2016

[16] Lian, S., Liu, Z., Ren, Z., Wang, H.: "Secure advanced video coding based on selective encryption algorithms". IEEE Trans. Consume. Electron. 2006

[17] Lian, S., Liu, Z., Ren, Z., Wang, H.: "Commutative encryption & watermarking in video compression" IEEE Trans. Circuits Syst. Video Technol.2007

[18] Logic Bomb: Hacker's Encyclopedia (1997)

[19] https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange

[20] https://www.techopedia.com/definition/5868/ad-hoc-network.