Advances in Computational Sciences and Technology
ISSN 0973-6107 Volume 10, Number 5 (2017) pp. 1417-1426

http://www.ripublication.com

Review of Security in AD-HOC Networks Using FTP

Ms. Reena

Department of Computer Science & Applications, MDU, Rohtak, India

Dr. Preeti Gulia

Department of Computer Science & Applications, MDU, Rohtak, India

Abstract

This is era of development of mobile devices. It has become must to stay online every time. Furthermore it is must to develop communication faster in military operations. It is also useful in case of environment disaster. Existing infrastructure would be destroyed it is probable. In this research, our focus would be on security of Ad-hoc networks using File Transfer Protocol. Here we had elaborated traditional hacking mechanism used by hackers in order to access data in unauthentic manner. In this paper, we have discussed existing research. After considering the loop holes in existing researches we proposed a new approach for FTP security in Ad Hoc Network.

Keywords: Ad-Hoc Network, FTP, Security, Network

1. INTRODUCTION

Ad Hoc is generally used for those that have been developed on fly for specific purpose. Mobile network of Ad hoc network is considered as a wireless mobile system node with self-organizes in temporary network topologies. From several decades there are many of research on Wireless Ad Hoc Network. In military applications Ad hoc networks have played a significant role.

Story of wireless ad hoc networks can be considered back to packet radio based Defense Advanced Research Project Agency networks that was indulge in adaptive radio networks application. We can say that Ad hoc networks was playing significant role in military applications. It has been also useful in related research efforts. In this paper, our main focus is on security of Ad-Hoc network using FTP against hackers

attack. Also we have tried to elaborate traditional hacking scheme using ftp password for hacking. In this paper, we have considered existing research and proposed an algorithm along with flowchart for FTP security in Ad Hoc Network. FTP means File Transfer Protocol technology which is a making FTP clients & servers able to download and upload file on computer networks. An FTP client is considered as software within a graphical user interface which is providing different options in order to support the handle the activity of files transmission .When a connection is established client could be able choose to send and get copies of files. In order to connect with FTP server usually client requires a username & password that has been set by administrator of server. FTP client is supporting downloading of files across Internet from computers that are known *FTP servers*. Several public FTP archives are following a convention for that is accepting a username of anonymous. FTP is allowing user to transfer files between two computers on Internet. FTP is considered as a simple network protocol which is based on Internet Protocol.

2. LITERATURE REVIEW

Many researchers as well as several testers have identified & summarize these security concerns & their solutions. These researchers have focused on security. Some papers are discussed in this section.

Sonu [20] has defined that security exploit is application that has been developed to take benefit of a known weakness. Some samples of security exploits are SQL injection and Cross Site Scripting. Other issues are Cross Site Request Forgery that is abusing security.

Aaditya Jain [19] has defined network system security is most popular & fastest Information Technologies in different organizations. Several tools for network security are dealing within capture, recording & analysis of network events in order to discover evidential information about source of security attacks. This paper discusses about honeypot technology within its classification based on various factors. Paper also throws light on some new types of honey pots within recently proposed models based on it.

Lidong Zhou [18] defines Ad hoc networks are considered as latest wireless networking paradigm that has been used for mobile hosts.

Sharad Pratap [17] Singh has defined that File Transfer Protocol is to transmit files to clients over networks. There are needs that are considered important while file transfers & these are Authentication, Integrity & Confidentiality. This research paper is comparing both FTPS & FTP on Linux & Windows server.

Dr. Mazin Sameer Al-Hakeem[16] make research in order to make file transfer protocol which should be based on UDP as a high speed, more reliable & secure protocol & that is generally referred as Fast Reliable Secure File Transfer Protocol.

Jason V. Chang [15] wrote that incidences of computer hacking is increasing over years. This article represents a small amount of computer hackers are caught & prosecuted.

Andriy Panchenko[14] has defined Hidden services are mechanisms that have been designed in order to give network services and preserving anonymity for server identity.

Michigan[13] has defined Wireless communication is going to develop inroads into several facets of society. Objective of this article was to check security issues within recent wireless networks.

Zhang[12] et.al discussed about application level attacks. In their paper they explored how packet payload should be utilized to check application level attacks.

Susan [10] et.al has written that Security field is recent moving career. In this paper he wrote on security stabilizes course material. It also reduced worry of hacking.

Neetu Settia [11] ET. Al in her paper discussed about security and attack in case of cryptographic techniques. They represented issues of security with different type of attacks.

C. Sanchez-Avila [9] et.al in their paper makes analysis of structure & design of Rijndael cipher. They remarked its pros and cons.

The analysis of existing approaches shows that in previous researches several mechanisms have been developed to improve cryptographic technique such as AES, DES and T-DES. Purpose of this article was to examine security & privacy issues within some new & emerging types of wireless networks, & attempt to identify directions for future research**.**

2.1 Summary of Literature Review

Table 1 : Review of Security Issues in Ad-hoc Network

Year	Author	Title	**Work done**	**Limitations**
2016 [20]	Sonu	Review Paper on Securing Wireless	Research is capable to be used through FTP, HTTP, PHP, SSH, Telnet. They are common in website and hacking.	This research provides no solution for sql injections and denial of services

2015 [19]	Aaditya Jain	Advance Trends in Network Security within Honey pot & its Comparative Study within other Techniques	Analysis of events of network in order to find evidential data for source of security attacks.	This research does not make any discussion related to Ad Hoc Based network.
2015 [18]	Lidong Zhou	Securing Ad Hoc Networks	Wireless networks ad hoc networks is not relying on fixed infrastructure.	This research provides no solution for denial of services
2014[17]	Sharad Pratap Singh	security configuration & performance analysis of ftp server	Research is providing two techniques to transfer file. First is anonymous method & second is password authentication technique.	This research is focused on FTP only. Security of other protocol such as telnet, http is not discussed here
2013[16]	Dr. Mazin Sameer Al-Hakeem	Development of Fast Reliable Secure File Transfer Protocol	This research enforces reliability issue using cryptographic hash checksum and to tackle security issue	This research is focused on FTP only. Security of other protocol such as telnet, http is not discussed here
2012[15]	Jason V. Chang	computer hacking making	This research found that small percentage of computer hackers are detected & prosecuted.	This research is focused on network hacker only. They do not discuss Cryptanalyst.
2011[14]	Andriy Panchenko	Lightweight Hidden Services	Instead of securing identity of server secret services is helping for resisting censorship.	This research is focused on lightweight and hidden services what about heavy weighted services
2010[13]	Michigan dear born	security & privacy in emerging wireless networks article	While within past wireless communication was highly restricted to first with last data transmission.	This research does not make any discussion related to Ad Hoc Based network.
2009	Zhang	focused on	It represents recent status	This research only

[12]		application level attacks	of anomaly detection. Research also focused on benefit of payload based detection.	focused on application level layer attacks. What if attack is made on different layer
2008[11]	Neetu Settia	Discussed security & attack aspects of cryptographic techniques	Bench focused on modern cryptographic algorithms. Objective is to find for best compromise in network security.	This research is focused on cryptographic techniques only. Threats such as ping of death are not discussed here.
2008[10]	Susan	Security field is a new & fast moving career	It is defining the group of skills that are needed by Network Security analysts.	Does not influence the network security in case of denial of services
2007[9]	C. Sanchez-Avila	analyzed structure & design	This research focused on cost of AES Based research	This research is focused on cryptographic techniques only. Threats such as ping of death are not discussed here.
2006[6]	Yet-Chun Hu	Attacks within Wireless Networks	This research focused on Wormhole attack. This attack is possible even if attacker has not compromised any hosts.	Threat from wormhole attack

3. PROPOSED WORK

In this research, we design & analyze a new server side module & client side module to transfer multimedia contents for Ad-Hoc Network and also propose a novel Key independent & fast & selective video encryption technique for confidentiality of video stream delivered over Ad-Hoc Network to end user. To design easy to use graphical user interface for Ad-Hoc Network. The steps are described below:-

Step 1 Development of Secure File server using Socket programming.
Step 2 Development of Secure File Client using socket programming.
Step 3 Enabling encrypted data transmission among File Server & File Client.
Step 4 Transmission would not be done from standard FTP protocol.

Step 5 During Transmission a particular key would be used & both end to make information understandable.
Step 6 Transmission would be made during specific time slot initiated by client.

We are considering well known asymmetric key cryptography algorithm RSA [1]. Let us assume that A (Server) & B (Receiver) want to agree upon a key to be used for encrypting /decrypting messages that would be exchanged between them. So steps are as:- Firstly A & B agree on two large prime numbers, n & g. These two numbers need not be secret. They could use some insecure channel to agree on them.

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

3.1 Encryption Steps:-

Step 1 Sender would Encrypt plain text using Secret Picture (Sender's private key) & generate cipher text using Data Encryption Standard.

Step 2 Sender would take Secret Picture, encrypt it using Covered Picture (Receiver's public key) & get encrypted picture using RSA algorithm.

Step 3 Sender would place cipher text & encrypted picture into a digital envelope & send it to receiver.

The flow chart is described below for Encryption:-

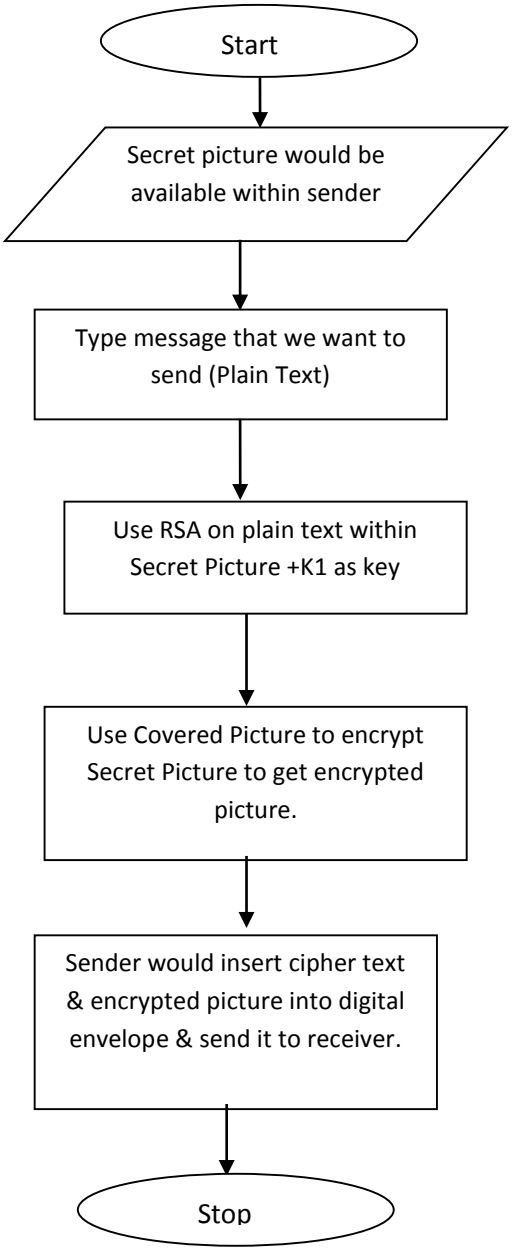

Fig 1: Flow Chart for Encryption Process

3.2 Decryption Steps:-

The Decryption of the picture will be reverse of the above steps.

Step 1 Digital envelope will be received by the receiver.

Step 2 Receiver will open the digital envelope, get the encrypted picture, decrypt it using its own Key Picture using RSA algorithm and get the Secret Picture.

Step 3 Receiver will use the Secret Picture to get plain text from cipher text using Data Encryption Standard.

Step 4 Receiver will get plain text.

The flow chart is described below for Decryption:-

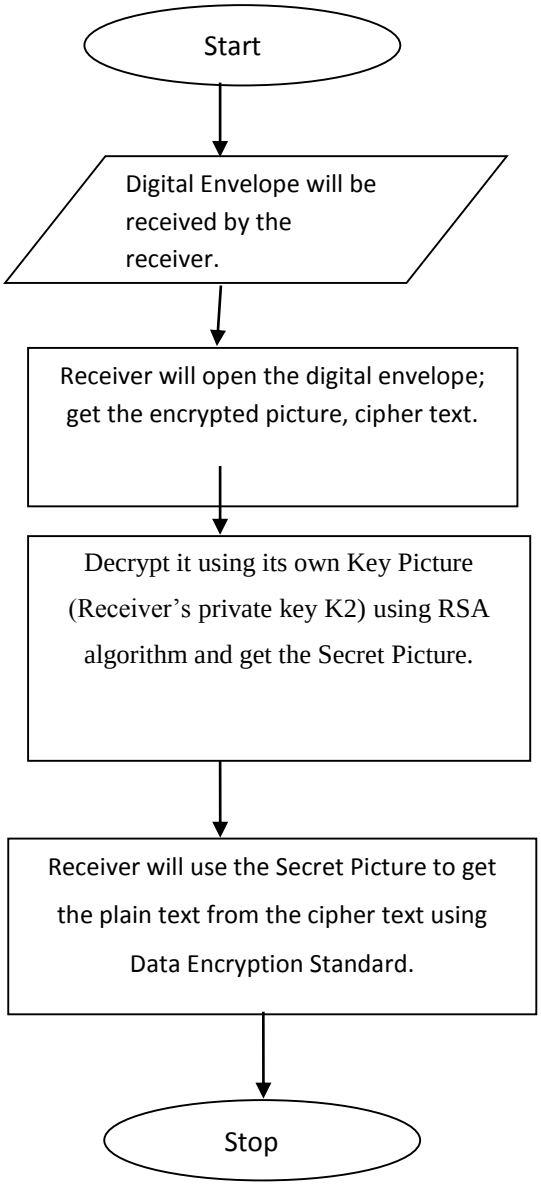

Fig 2: Flow chart for the decryption process

4 CONCLUSION & SCOPE OF RESEARCH

This research is useful for security of contents & services over Ad-Hoc network. Our research would restrict unauthentic access of multimedia data & dropping of service would not be allowed. It would result in smooth working. Security of File transfer

protocol server would definitely reduce chances of miss happening in AD HOC Network.

REFERENCE

[1] Rivest, R.; Shamir, A.; Adleman, L. (February *1978).* "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems" *(PDF).* Communications of the ACM. ***21*** *(2): 120–126.* doi*:*10.1145/359340.359342

[2] Hafner, Katie; Markoff, John (1991). Cyberpunk: Outlaws & Hackers on Computer Frontier. New York: Simon & Schuster. ISBN 0-671-68322-5.

[3] Sterling, Bruce (1992). Hacker Crackdown. Bantam. ISBN 0-553-08058-X.

[4] Slatalla, Michelle; Joshua Quittner (1995). Masters of Deception: Gang That Ruled Cyberspace. HarperCollins. ISBN 0-06-017030-1.

[5] Logik Bomb: Hacker's Encyclopedia (1997)

[6] Yet-Chun Hu "Attacks within wireless Networks" International Journal of Engineering Science & Technology (IJEST) ISSD : 0975-5462 Vol. 3 No. 4 April 2006

[7] Lian, S., Liu, Z., Ren, Z., Wang, H.: Secure advanced video coding based on selective encryp-tion algorithms. IEEE Trans. Consum. Electron. **52**(2), 621–629 (2006)

[8] Lian, S., Liu, Z., Ren, Z., Wang, H.: Commutative encryption & watermarking in video compression. IEEE Trans. Circuits Syst. Video Technol. **17**(6), 774–778 (2007)

[9] C. Sanchez- Avila analyzed structure & design international journal of Engineering Science & Technology Vol. 8 No. 2007

[10] Susan Darshan Lal Destruction Security field is a new & fast moving career international journal of Advance Research in computer Science & Management Studies on 2008

[11] Neetu Settia Discussed Security & Attack Aspects of cryptographic techniques current activity &Future Direction Acm Sigcomm Computer Communication Review, 28(3):5-26,july 2008

[12] Zhang focused on application level attacks, pp.137-144. IEEE Press, New York 2009

[13] Michigan dear born.: security & privacy in emerging wireless networks article(2010)

[14] Andriy Panchenko, " Lightweight Hidden Services", IET Communication, 2011, Vol.6,Iss.15,pp.2287-229

[15] Jason V. Chang," Computer Hacking Making", 2012 Journal of Zhejiang University-SCIENCE C (Computer & Electronics)

[16] Dr. Mazin Sameer AI- Hakeem , "Development of Fast Reliable secure File Transfer Protocol", Journal of Zhejiang University- SCIENCE C (Computer & Electronics),2013 15(7):pp489-513

[17] Sharad Pratap Singh, "Security Configuration & Performance analysis of FTP Server", intelligent Computing, Networking, & Informatics Advances in Intelligent System & Computing Vol. 243,2014,pp 45-56

[18] Lidong Zhou Ali Jalooli, Rafidah Md Noor ,Rashid Hafeez Khokhar , Jaime Lioret,"Securing Ad Hoc Networks", Wireless Networks, 2015, Springer

[19] Additya Jain, "Advance trends in network Security within Honey pot & its Comparative Study within other techniques, Volume 18, Issue 6, December 2015, pp 879-895

[20] Sonu Madhu Viswanatham,"Review Paper on Securing Wireless", IEEE, IET Netw. 2016, Vol. 3, Iss. 2, pp.150-159