© UNIVERSAL RESEARCH REPORTS | REFEREED | PEER REVIEWED
ISSN : 2348 - 5612 | Volume : 04 , Issue : 09 | October - December 2017

A REVIEW OF SECURITY ISSUES IN AD-HOC NETWORK BASED DATA TRANSMISSION

[1]Ritu Malik, [2]Esha Bansal
[1]Research Scholar, Department of CSA, CRSU Jind, ritumalik430@gmail.com
[2]Assistant Professor, Department of CSA, CRSU Jind, eshabansal2006@gmail.com

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 network in communication as well as the security threats from hacker during file transmission has been studied. The security of data in a file is a major concern. AD-HOC networks allow information to route from different path after old routes are destroyed. AD-HOC network leads to development of new kind of algorithms to route information.

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

ISSN : 2348-5612 © URR
9 770234 856124

[1] INTRODUCTION

AD-HOC network is considered as a network which is a composition of different type of devices that are communicating with one other directly. 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. Usually AD-HOC network does not need any router and any wireless base station.

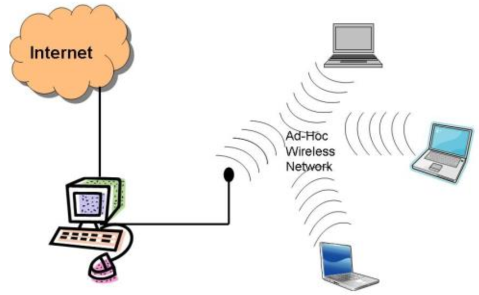

Fig. 1 Ad Hoc Network

This network is established for single session only. Administrator could set multiple hop ad hoc networks that could be used for the transmission of information on multiple nodes. 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.

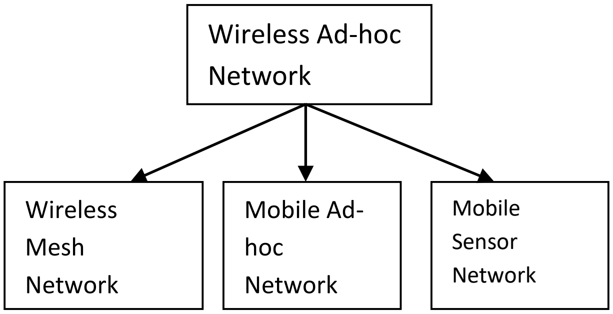

Fig. 2 Classification of Wireless AD-HOC Network

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.

[2] SECURITY ISSUES IN AD-HOC NETWORK

Third party provides data & infrastructure management in AD-HOC network so security of Network is biggest concern. There is a risk in providing sensitive data to AD-HOC Network service provider. Any security breach could result in customer or business loss so vendors provide protection to accounts. In following graph the different type of attack on routing are discussed. There are two types of attack on routing that are passive attack and active attack. The passive attack is further classified as Eavesdropping and Routing Information hiding

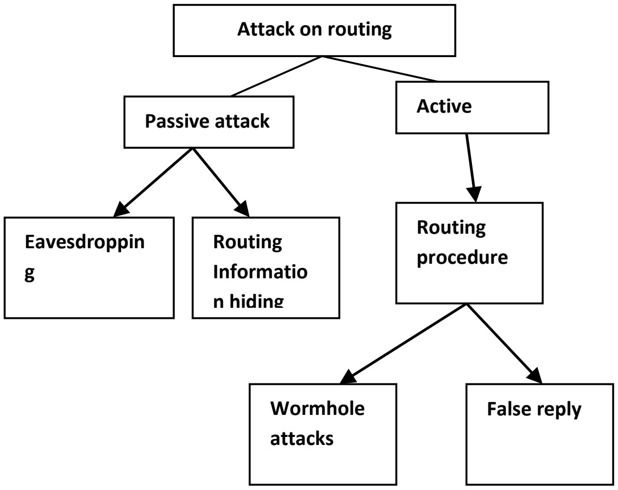

Fig. 3 Attack on routing

Attack on routing

1. Passive attack

A passive attack generally checks data which has been not converted traffic & would checks for sensitive information & clear-text passwords which could be used with in different types of attacks. Passive attacks comprise of traffic analysis, decrypting on weekly basis encrypted traffic, monitoring of unprotected communications & capturing validated information as passwords that user enter to login.

a. Eavesdropping

In case of Eavesdropping there is unauthorized real-time interception of communication like phone call, instant message, fax transmission or videoconference. Eavesdrop came into existence from practice of standing. Customer cannot switch from one service provider to another quickly so he is dependent on service provider for service. Customer management interface is usually accessible on network in case of various public AD-HOC Network service. Data security should be considered in network because data is frequently transferred over Internet. Basic mechanisms to protect data over AD-HOC Network are data auditing, data access control, data authentication & data authorization.

b. Routing information hiding: The data is hidden during routing process in this case

2. Active Attack

In active attack, attacker tries to break into safe systems. It is generally done through Trojan horses or worms. Such attacks include the theft of data. These attacks also try to circumvent in order to insert malicious code.

Routing procedure: The Routing protocol confirms the communication of routers. It disseminates the information that allows data to check routes among multiple nodes on network. Generally a routing algorithm confirms the particular option of route. Every router is attached to it directly that has priori idea of networks.

i Wormhole attacks: Wireless sensor networks could be destabilized by Wormhole attacks. Attacker receives packets at a location in the network in a typical wormhole attack.

ii False Reply: The attacker performs the feedback of invalid data in such attack.

[3] LITERATURE REVIEW

Several researches have been come in existence. Here in this section the existing relevant research have been discussed.

As per Yet-Chun Hu, [16] Wormhole attack can be attempted even if attacker is not compromising hosts & even if each transmission is providing authenticity as well as confidentiality.

As per C. Sanchez-Avil et.al [3] comparative analysis of performance of various algorithms as AES, DES & T-DES on micro controllers was made. On analysis they concluded that AES is having cost of computer of same order as compared to one needed by traditional DES based system.

As per Susan et. Al [11] the Security field is fast moving career. They defined group of skills that are needed for Network Security .They discussed the aims at attack recognition and network optimization with active learning exercises.

As per Neetu Setia [9] there are several security & attack aspects of cryptographic methods. They have discussed technique of protection from different attacks. They considered latest cryptographic based algorithms that are finding suitable place in providing security. They used Cryptography Tool as simulator for conducting experiments & in order to get results.

According to Zhang et. al [17] packet payload is generally used to identify attacks at application level. They have focused on attacks that are at application level. They also represented current condition of network problem finding, & focused on importance of payload based research using present issue, & proposed appropriate ways to find payload relevant attacks. In these situations they suggested ways in a detection phase & training phase.

As per Ahmed M. Al [1] identification & summarization was made for security concerns with solutions that are mandatory in Wireless Local Area Network. They summarized issues related to security & there expected solutions thereof. They classified security issues into physical & logical issues broadly.

As per Punita Meelu [10] it is better to use basic mathematics behind AES algorithm which is used in case of security system used in communication, as the existing cryptographic technology is providing better security. He stated that there is less complexity in its implementation. It is considered the most efficient as well as strongest algorithm in present time.

As per Scott Wolchok [12] the system that goes lives and gained election server control. District held a unique public trial before deploying that system in usual election. It is done in mock election at time when anybody from public was called to attempt to check its security.

As per Sumedha Kaushik, and Ankur Singhal [13] discussed was made Network Security Using Cryptographic Techniques that are used by huge organizations. The Network Security is related to all hardware & software functions. It is also related to operational procedures, characteristics, features, accountability, measures, and access control & administrative & management policy. These policies are required to provide an acceptable level of protection for Hardware & Software, & information in a network.

As per Jason V. Chang [5] 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 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.

As per Dr. Mazin Sameer Al-Hakeem [4] 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.

As per Sharad Pratap Singh [14] 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 [8] 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 [2] there are few new types of honey pots. 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.

Existing ADHOC network has been secured using cryptography**.**

Cryptography consists of converting plain text to cipher text and cipher text to plain text. The process of converting plain text to cipher is known as encryption and process of converting cipher text to plain is known as decryption.

Encryption is the process of encoding a message or information in such a way that only authorized parties can access. Encrypted data is called cipher text and unencrypted data is called plaintext. A key is required to perform encryption and decryption during data transmission over ADHOC network.

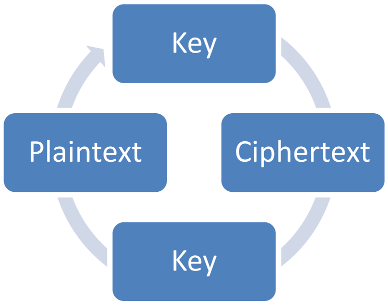

Fig. 4 Encryption and decryption cycle

Two types of encryption exist asymmetric key encryption and symmetric key encryption. The basic requirement for the encryption is as follow:

- Confidentiality**:** It identifies that only participants should be able to access message.
- Integrity**:** Content of message should not be changed. If this has been altered, then this has been called type of modification attack.
- Non-repudiation**:** There has been situation where sender converts content of message & after that he refuses that he had not sent message.
- Authentication: Both sender & receiver has to prove credentials to every other.

[4] CONCLUSION

There are several limitations in traditional research work. The objective of traditional researches was to secure AD-HOC Networks. Some of researchers discussed security & attack aspects of cryptographic techniques. 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. This paper represents the limitation of traditional researches. Thus the loop holes of existing researches could be considered. It is base for the development new AD-HOC based security model.

Reference

1. Ahmed M. Al Naamany "Wireless LAN Security Overview" in 2006
2. Aaditya Jain, "Advance Trends in Network Security within Honey pot & its Comparative Study within other Techniques" ,December 2015
3. C. Sanchez-Avila analyzed structure & design International Journal of Engineering Science & Technology Vol. 8 No 2007
4. Dr. Mazin Sameer Al-Hakeem, " Development of Fast Reliable Secure File Transfer Protocol ", Journal of Zhejiang University-SCIENCE , 2013
5. Jason V. Chang," computer hacking making", Journal of Zhejiang University-SCIENCE, 2012
6. Lidong Zhou Ali Jalooli, Rafidah MdNoor,Rashid Hafeez Khokhar, Jaime Lloret, " Securing AD-HOC Networks", Wireless Networks , Springer ,2015
7. Lian, S., Liu, Z., Ren, Z., Wang, H.: "Secure advanced video coding based on selective encryption algorithms". IEEE Trans. Consume. Electron. 2006
8. Lian, S., Liu, Z., Ren, Z., Wang, H.: "Commutative encryption & watermarking in video compression" IEEE Trans. Circuits Syst. Video Technol.2007
9. Neetu Settia "security & attack aspects of cryptographic techniques Current Activity & Future Directions " Acm Sigcomm Computer Communication Review, 28(3):5–26, July 2008
10. Punita Meelu " fundamental mathematics behind AES algorithm" in 2009
11. Susan Darshan Lal "Destruction Security field is a new & fast moving career" International Journal of Advance Research in Computer Science & Management Studies on 2008
12. Scott Wolchok , Attacking Washington, D.C.Internet Voting System ,2010
13. Sumedha Kaushik, Ankur Singhal "Network Security Using Cryptographic Techniques" in 2012
14. Sharad Pratap Singh, " security configuration & performance analysis of ftp server", intelligent Computing, Networking, &

Informatics Advances in Intelligent Systems & Computing ,2014

15. Sonu MadhuViswanatham, “Review Paper on Securing Wireless”, IEEE, 2016
16. Yet-Chun Hu “Attacks within Wireless Networks” International Journal of Engineering Science & Technology (IJEST) ISSN : 0975-5462 Vol. 3 No. 4 April 2006
17. Zhang “Application level attacks”, IEEE New York 2009