© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 06 Issue: 06 | 10 | October-December 2015

ENHANCED SECURITY IN ADHOC NETWORK USING TCP/IP BASED TECHNOLOGY

[1]Shokeen , [2]Swati Gupta

Abstract: The rapid growth of Internet has made communication an integrated and highly important factor of computing. In today's society with the development of mobile devices it has become important to stay online all the time. After the ad hoc network has been established the nodes that connect the network might move, say for example that one military squad is under heavy attack and has to escape. In ad hoc networks nodes should be able to move freely and the information should be routed through new paths after old ones have been broken, the network should also be able to handled clustering. The advent of ad hoc network has given birth to new kinds of routing algorithms and new security threats.

Keywords: AD HOC Network, Hacker, TCP/IP, PORT, SOCKET, CRYPTOGRAPHY.

[1] Introduction

"Ad Hoc" is actually a Latin phrase that means "for this purpose." It is often used to describe solutions that are developed on-the-fly for a specific purpose. In computer networking, an ad hoc network refers to a network connection established for a single session and does not require a router or a wireless base station.

For example, if you need to transfer a file to your friend's laptop, you might create an ad hoc network between your computer and his laptop to transfer the file. This may be done using an Ethernet crossover cable, or the computers' wireless cards to communicate with each other. If you need to share files with more than one computer, you could set up a mutli-hop ad hoc network, which can transfer data over multiple nodes. Basically, an ad hoc network is a temporary network connection created for a specific purpose (such as transferring data from one computer to another). If the network is set up for a longer period of time, it is just a plain old local area network (LAN).

[2] WIRELESS AD-HOC NETWORK

Research on Wireless Ad Hoc Networks has been ongoing for decades. The history of

wireless ad hoc networks can be traced back to the Defense Advanced Research Project Agency (DAPRPA) packet radio networks (PRNet), which evolved into the survivable adaptive radio networks (SURAD) program. Ad hoc networks have play an important role in military applications and related research efforts, for example, the global mobile information systems (GloMo) program and the near-term digital radio (NTDR) program. Recent years have seen a new spate of industrial and commercial applications for wireless ad hoc networks, as viable communication equipment and portable computers become more compact and available. Since their emergence in 1970's, wireless networks have become increasingly popular in the communication industry. These networks provide mobile users with ubiquitous computing capability and information access regardless of the users' location. There are currently two variations of mobile wireless networks: infrastructure and infrastructure less networks. The infrastructure networks have fixed and wired

gateways or the fixed Base-Stations which are connected to other Base-Stations through wires. Each node is within the range of a Base-Station. A "Hand-off" occurs as mobile host travels out of range of one Base-Station and into the range of another and thus, mobile host is able to continue communication seamlessly throughout the network. Example applications of this type include wireless local area networks and Mobile Phone. The other type of wireless network, infrastructureless networks, is knows as Mobile Ad-hoc Networks (MANET). These networks have no fixed routers, every node could be router. All nodes are capable of movement and can be connected dynamically in arbitrary manner.

[3] SECURITY ISSUES IN AD HOC NETWORK

Security is an important thing for all kinds of networks including the Wireless Ad Hoc Networks. It is obviously to see that the security issues for Wireless Ad Hoc Networks are difficult than the ones for fixed networks. This is due to system constraints in mobile devices as well as frequent topology changes in the Wireless networks. Here, system constraints include low-power, small memory and bandwidth, and low battery power.

Mobility of relaying nodes and the fragility or routes turn Wireless Ad-hoc Network architecture into highly hazardous architectures. No entity is ensured to be present at every time and it is then impossible to rely on a centralized architecture that could realize network structure or even authentication. The people who consider the Mobile Ad hoc Networks are not a flawed architecture, while we cannot see it used in practice is only because most of its applications are in military are totally wrong. It is true that Mobile Ad hoc Networks come from the military. But perhaps those persons forgot one of the most important things: the Security! Everybody knows that the core requirement for military applications dealing with trust and security! That is to say, security is the most important issue for ad hoc networks, especially for those security sensitive applications.

As we have mentioned before, in Mobile Ad-hoc Networks, security is difficult to implement because of the networks constrains and the rapidly topology changes. After investigation, we found that there are two kinds of security related problems in the Mobile Ad-hoc Networks.

[4] OBJECTIVE OF RESEARCH

1. Researcher proposes to design and analyze a new server side module and client side module to transfer multimedia contents for Ad-Hoc Network.
2. Researcher also proposes a novel Key independent and fast & selective video Encryption Technique for Confidentiality of video stream delivered over Ad-Hoc Network to end user.
3. Deployment & Integration of above two techniques simultaneously for providing Confidentiality & Authentication of Video Delivered or received over self Deployed Ad-Hoc Network for Video on Demand Service.
4. To enhance the network security of Digital Data by adding New Security Mechanisms
5. Research proposes to design easy to use graphical user interface for Ad-Hoc Network.

[5] DESIGN METHODOLOGY

Socket Programming

The endpoint in an inter process communication is called a socket, or a network socket for disambiguation. Since most communication between computers is based on the Internet Protocol, an almost equivalent term is *Internet socket*. The data transmission between two sockets is organized by communications protocols, usually implemented in the operating system of the participating computers. Application programs write to and read from these sockets. Therefore, network programming is essential for socket programming.

Client server Model

It is possible for two network applications to begin simultaneously, but it is impractical to require it. Therefore, it makes sense to design communicating network applications to perform complementary network operations in sequence, rather than simultaneously. The server executes first and waits to receive; the client executes second and sends the first network packet to the server. After initial contact, either the client or the server is capable of sending and receiving data.

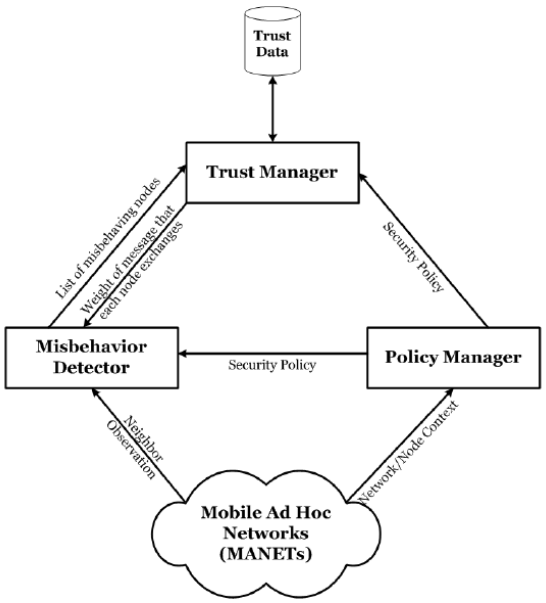
IP4 addresses:

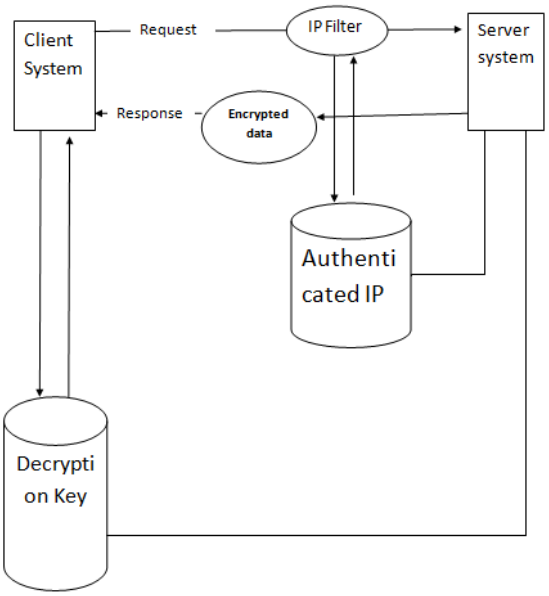
IP4 addresses are 32 bits long. They are expressed commonly in what is known as dotted decimal notation. Each of the four bytes which makes up the 32 address are expressed as an integer value (0 – 255) and separated by a dot. For example, 138.23.44.2 is an example of an IP4 address in dotted decimal notation. There are conversion functions which convert a 32 bit address into a dotted decimal string and vice versa. Often times though the IP address is represented by a domain name, for example, hill.ucr.edu. Several functions described later will allow you to convert from one form to another (Magic provided by DNS!).The importance of IP addresses follows from the fact that each host on the Internet has a unique IP address. Thus, although the Internet is made up of many networks of networks with many different types of architectures and transport mediums, it is the IP address which provides a cohesive structure so that at least theoretically, (there are routing issues involved as well), any two hosts on the Internet can communicate with each other.

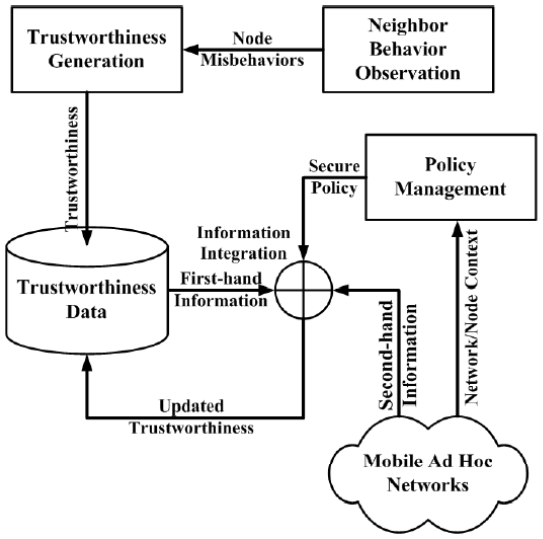
Port

Sockets are UNIQUELY identified by Internet address, end-to-end protocol, and port number. That is why when a socket is first created it is vital to match it with a valid IP address and a port number. In our labs we will basically be working with TCP sockets. Ports are software objects to multiplex data between different applications. When a host receives a packet, it travels up the protocol stack and finally reaches the application layer. Now consider a user running an ftp client, a telnet client, and a web browser concurrently. To which application should the packet be delivered? Well part of the packet contains a value holding a port number, and it is this number which determines to which application the packet should be delivered.So when a client first tries to contact a server, which port number should the client specify? For many common services, standard port numbers are defined.

[6] EXISTING RESEARCH







[7] Data flow diagram of Proposed Model

[7] CONCLUSION

Ad hoc network is a temporary network connection created for a specific purpose so the security of such system is must. There are several mechanisms to enhance the security of Ad hoc Network but they have some limitations.
Our proposed system will overcome the previous limitation and enhance the security.

REFERENCE

1. C.Siva Ram Murthy and B.Smanoj, " Ad Hoc Wireless Networks – Architectures and Protocols", Pearson Education, 2004.
2. Feng Zhao and Leonidas Guibas, "Wireless Sensor Networks", Morgan Kaufman Publishers, 2004.
3. C.K.Toh, "Ad Hoc Mobile Wireless Networks", Pearson Education, 2002.
4. Thomas Krag and Sebastin Buettrich, "Wireless Mesh Networking", O'Reilly Publishers, 2007.
5. Agi, I., Gong, L.: An empirical study of secure mpeg video transmissions. In:

Proceedings of the Symposium on Network and Distributed System Security, pp. 137–144. IEEE Press, New York (1996)

6. Baugher, M., McGrew, D., Naslund, M., Carrara, E., Norrman, K.: The secure real-time trans-port protocol (SRTP) (2004)
7. Bergeron, C., Lamy-Bergot, C.: Complaint selective encryption for h.264/avc video streams. In: IEEE 7th Workshop on Multimedia Signal Processing, pp. 1–4 (2005). doi: 10.1109/ MMSP.2005.248641
8. Cheng, H., Li, X.: Partial encryption of compressed images and videos. IEEE Trans. Signal Process. **48**(8), 2439–2451 (2000). doi: 10.1109/78.852023
9. Chiaraluce, F., Ciccarelli, L., Gambi, E., Pierleoni, P., Reginelli, M.: A new chaotic algorithm for video encryption. IEEE Trans. Consum. Electron. **48**(4), 838–844 (2002)
10. Li, S., Zheng, X., Mou, X., Cai, Y.: Chaotic encryption scheme for real-time digital video. In: Real-Time Imaging VI. Proceedings of SPIE, vol. 4666, pp. 149–160 (2002)
11. 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)
12. Lian, S., Liu, Z., Ren, Z., Wang, H.: Commutative encryption and watermarking in video compression. IEEE Trans. Circuits Syst. Video Technol. **17**(6), 774–778 (2007)
13. Logik Bomb: Hacker's Encyclopedia (1997)
14. Hafner, Katie; Markoff, John (1991). Cyberpunk: Outlaws and Hackers on the Computer Frontier. New York: Simon & Schuster. ISBN 0-671-68322-5.
15. Sterling, Bruce (1992). The Hacker Crackdown. Bantam. ISBN 0-553-08058-X.
16. Slatalla, Michelle; Joshua Quittner (1995). Masters of Deception: The Gang That Ruled Cyberspace. HarperCollins. ISBN 0-06-017030-1.
17. Dreyfus, Suelette (1997). Underground: Tales of Hacking, Madness and Obsession on the Electronic Frontier. Mandarin. ISBN 1-86330-595-5.
18. Verton, Dan (2002). The Hacker Diaries : Confessions of Teenage Hackers. McGraw-Hill Osborne Media. ISBN 0-07-222364-2.
19. Thomas, Douglas (2002). Hacker Culture. University of Minnesota Press. ISBN 0-8166-3345-2.
20. Taylor, Paul A. (1999). Hackers: Crime in the Digital Sublime. Routledge. ISBN 978-0-415-18072-6.
21. Levy, Steven (2002). Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age. Penguin. ISBN 0-14-024432-8.
22. Ventre, Daniel (2009). Information Warfare. Wiley - ISTE. ISBN 978-1-84821-094-3.
23. Bhushan Lal Sahu,Rajesh Tiwari, Journal of Advanced Research in Computer Science and Software Engineering 2(9) (2012) 33-37.