International Journal of Computer Networks and Communications Security

VOL. 4, NO. 8, AUGUST 2016, 237–241
Available online at: www.ijcncs.org
E-ISSN 2308-9830 (Online) / ISSN 2410-0595 (Print)

Security framework against Denial of Service Attacks in Wireless Mesh Network Networks

SANDEEP DALAL[1] and SEEMA DEVI[2]

[1, 2] Department of Computer Science and Applications, Maharshi Dayanand University, Rohtak, Haryana, India

ABSTRACT

Any type of computer network, a wireless network to connect network nodes uses wireless data connection. Wireless networking are a way by which the houses, telecommunication network and enterprise (business) started in a building wiring installations to avoid costly process, or as a connection between various devices in places. Within a relatively small area of wireless personal area network interconnect devices within reach of a person is usually. For example, both Bluetooth radios and a laptop for an invisible infrared light provides a headset each. ZigBee are also supports application. General Wi-Fi (2010) is becoming as a variety of consumer electronic device designers to integrate Wi- Fi start. A hacker is someone who exploits and vulnerabilities within a computer network or computer system is looking for. Such a hacker gain, as opposed to the challenge or can be induced by a multitude of reasons. Everywhere that often underground hackers group has evolved and these days they are well known in the community known as computers.

Keywords: *Transmitter, Framework, Cryptography, Cellular, Telecommunications.*

1 INTRODUCTION

Any type of computer network, a wireless network to connect network nodes uses wireless data connection. Wireless networking is a way by which the houses, telecommunication network and enterprise (business) started in a building wiring installations to avoid costly process or as a connection between several devices in places.

Wireless telecommunications networks are usually applied using radio communications are administered. The implementation of the physical layer of OSI model network infrastructure (layer) takes place. Example of wireless networks, cell phone networks and local Wi- Fi network includes temporal microwave network.

Computer very often are connected to the wireless network using link

- Terrestrial microwave– Earth- based transmitter and receiver, such as satellite dishes, temporal microwave communication uses. Terrestrial microwave are low gigahertz range which limits all communications within the vision. Relay stations are about 48 kilometers (30 miles) distinct in distance.
- Communication satellites – Satellites, Microwave, Radio waves which are not deflected by the Earth's atmosphere through dialogue. Satellites are usually geosynchronous orbit above the equator, 35,400 kilometers (22,000 miles), within the space within posted. These Earth-orbiting systems and receiving voice, data, and are capable of relaying television signals.
- PCS and Cellular systems are using various radio communications technologies. System covers the area divided into various geographical regions. Each field to relay calls from one area to the next area a low-power transmitter or radio relay antenna for the devices.
- Radio & spread spectrum technology – Wireless local area network access High-frequency radio digital cellular and a Low-frequency radio technology similar techniques. The use of spread spectrum wireless LAN technology in a limited area to enable communication between multiple devices. IEEE 802.11 Wi-Fi open standards wireless

radio-wave technology is known as a common flavor.

2 DENIAL OF SERVICE ATTACK (DOS)

A Denial-of-Service (DoS) attack a machine or network resources such as temporary or inexplicit interrupt or suspended services of a host connected to the Internet as their aim is an attempt to make unavailable to users.

A Distributed Denial-of-Service (DDoS) attack is where often multiple sources thousands of unique IP address. Shop or business of the parties to enter into a valid state, not disrupting the normal operations or business or a store entrance, a group of people rush to the gate and is consistent.

DoS attacks are often banks, credit card payment gateways on the target host, as high-profile web servers are the perpetrators of the crime sites or services

. Revenge, blackmail or other motives behind the attacks may be active.

2.1 Attack Tools

Wide arrays of programs are used to launch DoS attacks. In cases such as my doom malware tool embedded systems and have begun their attack without the knowledge of the owner. Stacheldraht is a classic example of the DOS device. This is a multi-layered structure where the attacker operators, which is the system that zombie agent , which in turn issue orders to facilitate DDoS attacks are patched to connect to a customer uses the program uses. Agents are compromised by the attacker through operators automated routine use programs that accepts remote connections on the remote host targets to exploit vulnerabilities. Each handler can control thousand agents.

2.2 Denial- of -service Level

DOS L2 (possibly DDoS) attack which blocks a safety net for the goal of the network is due to the introduction of the section from which the attack began. Distributed attacks or IP header modifications (depending on the type of behavior that the security) completely block it from Internet to attack the network, but without the system in case of accident.

2.3 Distributed attacks

A Distributed Denial of Service (DDoS) Attack occurred when multiple system flood the bandwidth or resources of an objective system generally one or more web servers.[8] Such attacks constantly compromised systems (for example, a botnet) traffic is a result of flooding in the target system.

In order to achieve a botnet owner without the knowledge of the program is a network of zombie computers.[13] When a connection to the server is overloaded with new connections can no longer be accepted. A distributed denial- of-service attacks are major advantage of using an attacker than a machine can generate more attack traffic.

Multiple attack machines are hard to stop an attack and the behavior of each attack machine making it difficult to traces and off can be stealthier. These challenges cause the attackers to gain the security apparatus.

2.4 Denial-of-Service (DoS) Level II

DOS Level 2 (possibly DDoS) attack which blocks a safety net for the goal of the network segment in which the origin of the attack would mean a launch. In distributed attack or IP header alteration (depending on the type of security behavior). The attack networks completely block the Internet, but without a system crash.

3 THE PROPOSED IMPLEMENTATION

The data transmissions between two bases are united by communications protocols generally applied to the operating system of the participating systems. Application programs are writing and read from these bases. Thus socket programming is required for network programming. In an embed-process communication endpoint of a socket or a network socket is called illumination. Communication between computers is based on Internet Protocol. Internet socket is roughly equal duration.

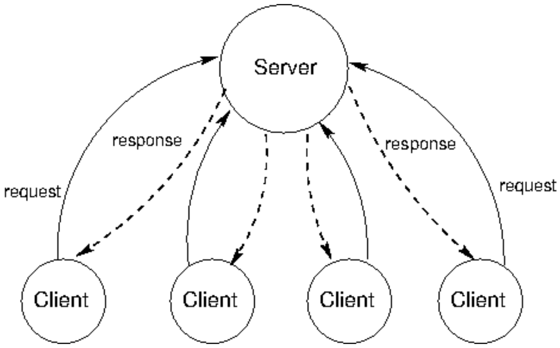


Fig. 1. Data Transmission between client and server

Cryptography (only the message as plain text) is the process of converting plain text into cipher text using the encryption process. Encryption is a process of transforming radical data called plaintext or clear text into a form that perform to be arbitrary and obscure which is called cipher text. That radical text cannot be understood by a person or a computer. (Executable code) is called Plain text or clear text. After transformation into cipher text, then it is impossible until it is decrypted by the human as well as machine to process the text.

2.5 Symmetric Cryptography

Symmetric key cryptography is as the saying goes secret key cryptography or private key cryptography. Both encryption and decryption of messages issued for the same key between sender and receiver. As there is only one key between them, also known as the secret key and to maintain the security of the communication must be kept secret.

Both parties have the same key and the decision to carry out the transmission and it should not be known to others. The use of this key cipher text converted to plain text in the sender end and reverse action in another end. In this way original message is received by the receiver.

4 SIMULATION AND RESULT

Simulation Environment

The following environment was taken to simulate the proposed protocol.

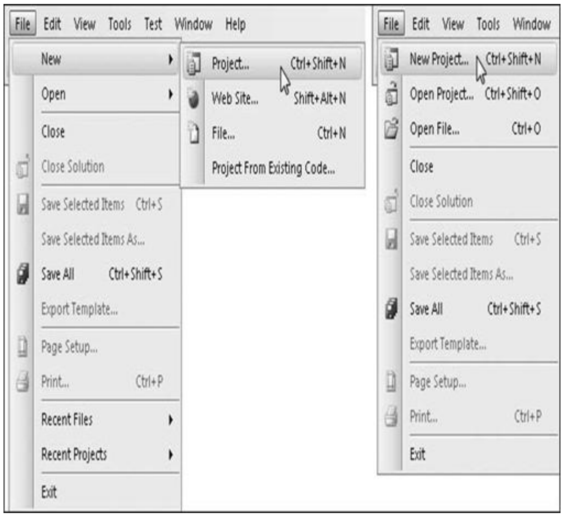
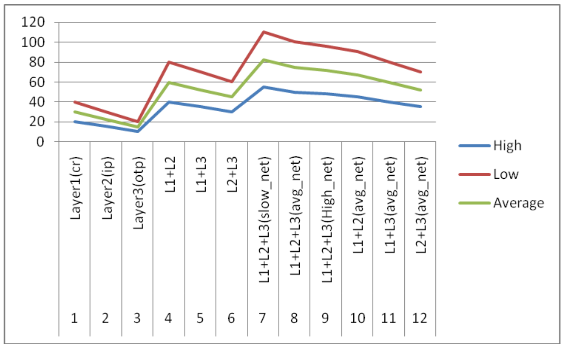


Fig. 2. In VS, select the Visual C# node in Project types pane of the window, and console application n project type in the Templates pane

Table 1: Data within case of Fiber optics

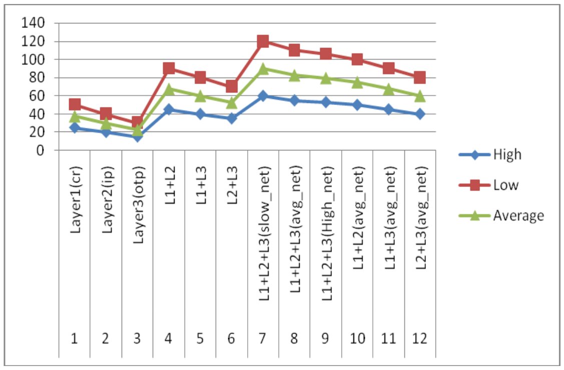
Sno	Security_Level	H	L	Avg
1	Layer1(cr)	20	40	30
2	Layer2(ip)	15	30	22.5
3	Layer3(otp)	10	20	15
4	L1+L2	40	80	60
5	L1+L3	35	70	52.5
6	L2+L3	30	60	45
7	L1+L2+L3(slow_net)	55	110	82.5
8	L1+L2+L3(avg_net)	50	100	75
9	L1+L2+L3(High_net)	48	96	72
10	L1+L2(avg_net)	45	90	67.5
11	L1+L3(avg_net)	40	80	60
12	L2+L3(avg_net)	35	70	52.5



Graph. 1. Analysis of transmission speed of packet within case of Fiber optics

Table 2: Data within case of Coaxial Cable

Sn.	Security_Level	H	L	Avg
1	Layer1(cr)	25	50	37.5
2	Layer2(ip)	20	40	30
3	Layer3(otp)	15	30	22.5
4	L1+L2	45	90	67.5
5	L1+L3	40	80	60
6	L2+L3	35	70	52.5
7	L1+L2+L3(slow_net)	60	120	90
8	L1+L2+L3(avg_net)	55	110	82.5
9	L1+L2+L3(High_net)	53	106	79.5
10	L1+L2(avg_net)	50	100	75
11	L1+L3(avg_net)	45	90	67.5
12	L2+L3(avg_net)	40	80	60



Graph. 2. Analysis of transmission speed of packet within case of Coaxial Cable.

5 CONCLUSIONS

AD-HOC Network security is the issue of the day demand. Implementation of the proposed ad hoc network security is enhanced.

Data transmission could be made more secure from hacker to by encrypting data on sender side and decrypt it on client side. To demonstrate this we need to merge two technologies. And on the part of .net play its best role to develop GUI interface to make system easy to operate by user

I. Socket Programming

II. Data Encryption.

Our security system will first prevent hacker to access data within unauthorized way and the way they use the data to understand the hacker will be able to restrict.

6 REFERENCES

[1] David Pointcheval, Olivier Blazy, New Smooth Projective Hash Functions and One-Round Authenticated Key Exchange(18_22 august 2013, Santa Barbara, California, USA), Springer-Verlag, LNCS 8042, pages 449_475.

[2] David Pointcheval, Olivier Blazy, Effcient UC-Secure Authenticated Key-Exchange for Algebraic Languages(26 February - 1 March 2013, Nara, Japan)), 16th International Conference on Practice and Theory in Public-Key Cryptography (PKC '13)Springer-Verlag, Kaoru Kurosawa Ed., Springer-Verlag, 2013.

[3] David Pointcheval, Password-based Authenticated Key Exchange. (21-23 may 2012, Darmstadt, Germany)Springer-Verlag, LNCS 7293, pages 390-397.

[4] David Pointcheval, Michel Abdalla, Contributory Password-Authenticated Group Key Exchange with Join Capability, (February 14-18, 2011, San Francisco, CA, USA), A. Kiayias Ed. Springer-Verlag, LNCS 6558, pages 142-160.

[5] David Pointcheval, Xavier Boyen, Strong Cryptography from Weak Secrets, (3 – 6 may 2010, Stellenbosch, South Africa), D. Bernstein and T. Lange Eds., Springer-Verlag, LNCS 6055, pages 297–315.

[6] David Pointcheval, Michel Abdalla, Flexible Group Key Exchange with On-Demand Computation of Subgroup Keys, (3-6 May 2010, Stellenbosch, South Africa)), D. Bernstein and T. Lange Eds., Springer-Verlag, LNCS 6055, pages 351-368.

[7] David Pointcheval, Michel Abdalla, Distributed Public-Key Cryptography from Weak Secrets, (18_20 march 2009, Irvine, CA,

USA), S. Jarecki and G. Tsudik Eds. Springer-Verlag, LNCS 5443, pages 139_159.

[8] David Pointcheval, Michel Abdalla, Password-Authenticated Group Key Agreement with Adaptive Security and Contributiveness, (21 – 25 june 2009, Gammarth, Tunisia) B. Preneel Ed., Springer-Verlag, LNCS 5580, pages 254–271.

[9] Rafael Álvarez, Leandro Tortosa, Analysis and design of a secure key exchange scheme, Information Sciences 179 (2009) , Elsevier

[10] David Pointcheval, Michel Abdalla, Anonymous and Transparent Gateway-based Password-Authenticated Key Exchange , December 2–4, 2008, Hong-Kong, China – M. Franklin, L. Hui and D. Wong Eds. Springer-Verlag, LNCS 5339, pages 133–148.

[11] Emmanuel Bresson, Olivier Chevassut, and David Pointcheval, Provably-Secure Authenticated Group Diffie-Hellman Key Exchange, ACM Transactions on Information and System Security, Vol. 10, No. 3. August 2007.

[12] Kumar Mangipudi, Rajendra Katti, A Secure Identification and Key agreement protocol with user Anonymity (SIKA), journal homepage: www.elsevier.com/locate/cose, Computers & security 25(2006) 420 – 425.

[13] Chin-Chen Chang, Jung-San Lee, An anonymous voting mechanism based on the key exchange protocol, journal homepage: www.elsevier.com/locate/cose, Computers & security 25(2006) 307– 314.

[14] Tseng, Y.M., 2005, Weakness in simple authenticated key agreement scheme, Electronics. Letters 36 (1) pp. 48–49.