© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 07 | July – September 2016
Paper is available at www.jrps.in | Email : info@jrps.in

IMPLEMENTATION OF WIRELESS NETWORK FROM DENIAL OF SERVICE

[1]Mukesh Kumar, Research Scholar, Department of CSE, CBS group of Institutions Jhajhar
[2]Pooja Dhankhar , assistant professor, Department of CSE, CBS group of institutions jhajhar

9 772278 684800 03
© iJRPS International Journal for Research Publication & Seminar

Abstract: A wireless network is any type of computer network that uses wireless data connections for connecting network nodes. Wireless networking is a method by which homes, telecommunications networks & enterprise (business) installations avoid costly process of introducing cables into a building, or as a connection between various equipment locations. Wireless personal area networks (WPANs) interconnect devices within a relatively small area, that is generally within a person's reach. For example, both Bluetooth radio & invisible infrared light provides a WPAN for interconnecting a headset to a laptop. ZigBee also supports WPAN applications. Wi-Fi PANs are becoming commonplace (2010) as equipment designers start to integrate Wi-Fi into a variety of consumer electronic devices. A hacker is somebody who exploits & seek weaknesses within a computer network or computer system. A hacker can be motivated by a multitude of reasons, such as profit, challenge or protest. grouping that has evolved everywhere hackers is often referred to as computer underground & these days they are well known community.

Keyword: transmitter, Communications, Framework, Cryptography, Cellular, telecommunications, equipment

[1] Introduction

A wireless network is any type of computer network that uses wireless data connections for connecting network nodes. Wireless networking is a method by which homes, telecommunications networks & enterprise (business) installations avoid costly process of introducing cables into a building, or as a connection between various equipment locations. Wireless telecommunications networks are generally implemented & administered using radio communication. This implementation takes place at physical level (layer) of OSI model network structure. Examples of wireless networks include cell phone networks, Wi-Fi local networks & terrestrial microwave networks.

Computers are very often connected to networks using wireless links

- Terrestrial microwave – Terrestrial microwave communication uses Earth-based transmitters & receivers resembling satellite dishes. Terrestrial microwaves are within low gigahertz range, which limits all communications to line-of-sight. Relay stations are spaced approximately 48 km (30 mi) apart.
- Communications satellites – Satellites communicate via microwave radio waves, which are not deflected by Earth's atmosphere. satellites are stationed within space, typically within geosynchronous orbit 35,400 km (22,000 mi) above equator. These Earth-orbiting systems are capable of receiving & relaying voice, data, & TV signals.
- Cellular & PCS systems use several radio communications technologies. systems divide region covered into multiple geographic areas. Each area has a low-power transmitter or radio relay antenna device to relay calls from one area to next area.
- Radio & spread spectrum technologies – Wireless local area networks use a high-frequency radio technology similar to digital cellular & a low-frequency radio technology. Wireless LANs use spread spectrum technology to enable communication between multiple devices within a

limited area. IEEE 802.11 defines a common flavor of open-standards wireless radio-wave technology known as Wifi.

[2] Service attacks in wireless mesh network

1. Passive Attack

A **passive attack generally** checks the data which is not converted traffic & will 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 weakly basis encrypted traffic, monitoring of unprotected communications & capturing validated information as passwords that user enter to login. Passive interception of network operations usually enables adversaries to view upcoming actions. Passive attacks usually result with in information disclosure or data files to an attacker. And all this can be done without knowledge of operator.

2. Active Attack

In an **active attack** attacker generally attempts to crack or breakdown into secured systems. This could be performed through worms/viruses/stealth/Trojan horses. Active attacks consist of steal information & attempts to circumvent to introduce malicious code. Such harmful attacks are mounted within contrast to a network backbone, digitally breach an enclave, then this will exploit information within transit or attack an authorized remote client operator when an attempt to connect to an enclave. Active attacks would result within discovery/dissemination of information data files and manipulation of client data.

3. Distributed Attack

A **distributed attack** would require opposition introduced code, such as a back-door program or Trojan horse attacks, to a *trusted* component or software which are later be distributed to many other client companies & users. Distribution of harmful attacks focus on spiteful manipulation of software or hardware at factory or during distribution. And this type of harmful attacks introduce spiteful programing code such as back door to a module to gain unauthorized access to information or to a system function that would work at a later date.

4. Insider Attack

An **insider attack** includes somebody from inside, such as a discontented operative, attacking on network that generate Insider harmful attacks may be spiteful or not spiteful. Malicious insiders intentionally steal, eavesdrop or damage confidential or valuable data; that will use information within a falsified manner; or deny access to other authorized users. No malicious harmful attacks characteristically result from inattentiveness, lack of knowledge, or intentional circumvention of security for such reasons as executing a process.

5. Close-in Attack

The **close-in attack** includes somebody attempting to get physically/connected close to network data, components & systems within order to learn more about a network Close-in harmful attacks consist of regular checking of individuals attaining close physical proximity to networks, systems, or facilities for purpose of altering, denying access to information or gathering. Close physical closeness is attained through furtive/secret entry into network system, this may be open access, or any other type, or both. One of most popular form of close within attack is **social engineering** within which a social engineering attack achieved, attacker compromises network or system through social communication with an individual, through an electronic mail message or phone. Various ways or tricks can be used by individual to revealing information about security of company. Important information which victim reveals to hacker would be used within a subsequent attack within order to gain unlawful means of access to network.

6. Phishing Attack

In phishing attack hacker or devil prepare a fake web site that looks exactly like a popular site such as any bank i.e. PNB, YES BANK, ICICI or paypal. In phishing hacker then sends an e-mail message which try to trick user into clicking a link that leads to fake site (i.e. the design of site will be similar to original site.). When user try to log on site with their own account information, hacker records password & username & then hacker tries that information on real site to steal information.

7. Hijack attack

In hijack attack, a hacker establishes a session between victim & another individual & then disconnects other individual from communication. Victim still believe that he was talking to original or authentic person & by mistake send private information to hacker.

8. Spoof attack

In a spoof attack, hacker changes source address of packets over network & hacker sends packets so that they create illusion that packets are coming from authorized source. And by these attempt hackers try to bypass victim's firewall settings.

9. Buffer overflow

A buffer overflow massive attack is when attacker sends information within massive quantity to any program than is estimated. In most cases this could be used when attacker try to gaining administrative access to system within a shell or CMD (command prompt).

10. Exploit attack

This is also one type of attack; within which attacker knows of a security problem within an OS (operating system) or a particular of software application & influences that knowledge by exploiting defenselessness.

11. Password attack

In this category of attacks attacker tries to crack passwords stored within a password-protected file or a remote network account database. A dictionary attack hackers use a word list file, which is generally a list of possible passwords of users. A brute-force every possible combination of characters is tried by attacker.

[3] THE PROPOSED IMPLEMENTATION

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. 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*.

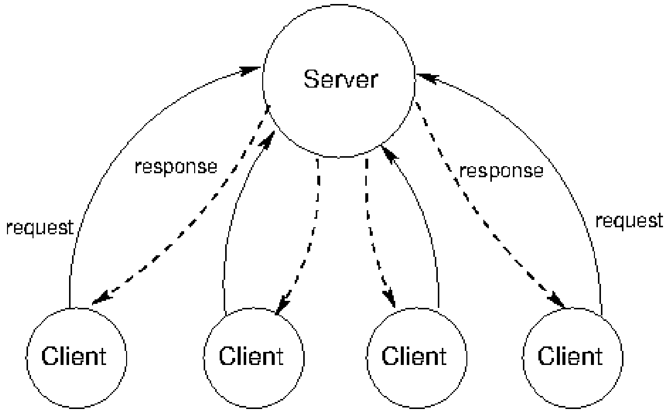


Fig 4 Data Transmission between client and server

Cryptography is the process of converting plaintext (ordinary text, just as message) using process encryption into cipher text using process decryption. Encryption is a method of transforming original data, called plaintext or clear text, into a form that appears to be random and unreadable, which is called cipher text. That text can be understood by a person by a computer. (executable code) is called Plain text or clear text. After transformation into cipher text, then it is impossible to process this text by human as well as machine until it is decrypted.

Symmetric Cryptography

Symmetric key cryptography is also called as secret key cryptography or private key cryptography. In this a single key isused for both encryption and decryption of messages between sender and receiver. It is also known as secret key as there is only single key between two of them and it must be kept secret to maintain the security of communication. Both parties must decide a single key and carry out transmission and it must not be known to others. At sender end the plain text get converted to cipher text using this key and reverse action is performed at 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.

Hardware used:

- Model : HP Pavilion dv4 Notebook PC
- Processor : Intel(R) Core (TM) i3 CPU M 350 @ 2.27 GHz
- Installed Memory : 2.00 GB
- System Type : 32 bit operating System

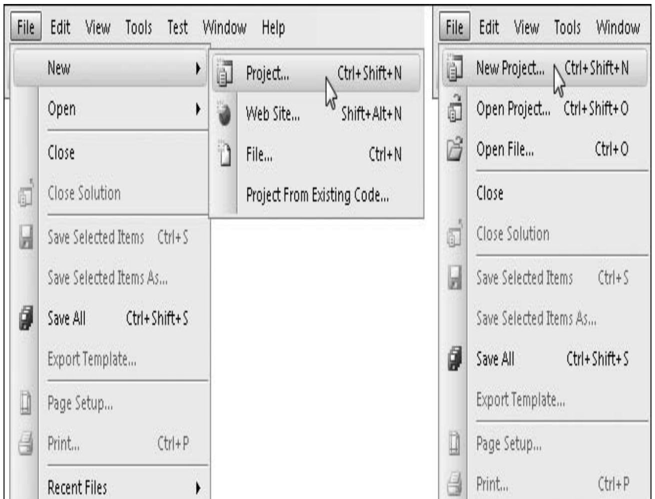
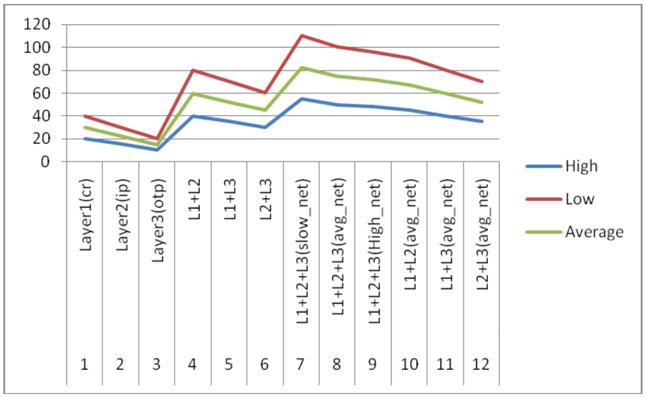


Fig 5 In VS, select the Visual C# node in the Project Types pane of the window that appears, and the Console Application project type in the Templates pane

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

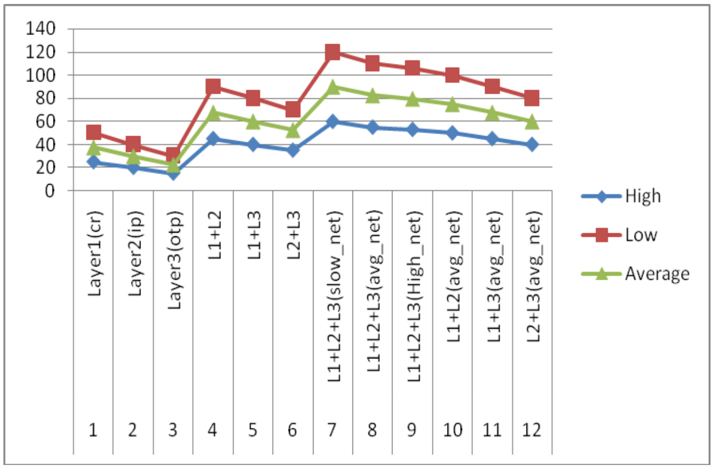
Table 1 Data within case of Fiber optics



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

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

Table 2 Data within case of Coaxial Cable



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

[5] CONCLUSION

Issue of ADHOC Network security is the demand of day. The proposed implementation has enhanced the security of ADHOC Network. Data transmission could be made more sercure from hacker to by encrypting data on sender side and decrypt it on client side. To perform 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.

[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.