Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 5, May 2017, pg.423 – 429

Security Architecture against Denial of Service Attacks in Wireless Mesh Network

Swati Singla[1], Deepika Dhingra[2]

[1,2]Department of Computer Science and Engineering, Om Group of Institution
Swati.singla1993@gmail.com[1]
Dhingra.deepika17711@gmail.com[2]

Abstract— The mesh client are frequently laptop, cell phone and other wireless devices patch the mesh routers forward traffic to and from the gateway which may, but need not, be connected to the Internet. The coverage area of the radio nodes functional as a single network is sometimes called a mesh cloud. Approach to this mesh cloud is dependent on the radio nodes working in harmony with each other to produce a radio network. A mesh network is reliable and extends redundancy. In this work, the data transmissions between two bases are joined by communications protocol mostly applied to the operating system of the participating system. Application programs are writing and read from these bases. Thus socket programming is required for network programming. The paper has presented the common algorithmic model for preventive communication route. This paper generates a preventive path while performing the data transfer and communication. The objective of work is to reduce communication delay and data loss.
Keywords— "Wireless mesh network","WMNs","DOS","DDOS","Network Socket".

1. INTRODUCTION

In any type of Computer network, a wireless network to connect to a network using the wireless data connection. A Wireless telecommunication network is normally applied using radio communication are administered. The execution of the physical layer of OSI model network infrastructure (layer) takes place. Example of wireless network, cell phone network and local Wi- Fi network include temporal microwave network [1].

The mesh client is a great deal of laptop, cell phone, and other wireless devices patch the mesh router onward traffic to the gateway which may, but need not, be connected to the Internet. The coverage area of the radio node working as a single network is sometimes called mesh cloud. Access code to this mesh cloud is dependent on the radio node working in harmony with each other to make a radio network. A mesh network is dependable and offers redundancy. When one node can no longer operate, the rest of the node can still communicate with each other, directly one or more intermediate node. The Wireless mesh network can self-form and self-heal. The Wireless mesh networks can be implemented with various wireless technologies including 802.11, 802.15, 802.16, cellular technologies and need not be controlled to any one technology or protocol.

DENIAL OF SERVICE ATTACK (DoS)

A Denial-of-Service (DoS) attack a machine or network resources such as temporary or suspended services of a host connected to the Internet as their aim is an attempt to make unavailable to the user [2].

A Distributed Denial-of-Service (DDoS) where is attack source is more than one thousands of unique IP address. Shop or business of the parties to enter into a valid state, not disrupting the normal operation or business or a store entrance, a group of people rush to the gate and is consistent [3].

DoS attack is often banks, credit card payment gateway on the target host, as a high-profile web server are the perpetrator of the crime site or service, Revenge, blackmail or another motive behind the attack may be active [4].

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 attack or IP header modification (depending on the type of behavior that the security) completely block it from the Internet to attack the network, but without the system in case of accident

Distributed attacks

A Distributed Denial of Service (DDoS) Attack occurred when multiple systems flood the bandwidth of an accusative systems generally one or more web server..Such attack constantly compromised systems (for example, a botnet) traffic is a result of flooding in the target system [3].
In order to achieve a botnet owner without the knowledge of the program is a network of zombie computer. When a connection to the server is overloaded with a new connection can no longer be accepted. A distributed denial- of-service attack is a 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.

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. The attack networks completely block the Internet, but without a system crash [2].

2. Objective

To identify the Denial of Service (DOS) attack in wireless mesh network and generate a preventive path while performing the data transfer and communication. The Objective of work is to reduce the communication delay and data loss.

3. PROPOSED WORK

Methods/Statistical Analysis: In this work, 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. The paper has presented the common algorithmic model for preventive communication route

Findings: Here we have discussed that the wifi network and Denial of services attack. DoS attacks are often bank, credit card payment gateway on the target host, as high-profile web servers are the culprit of the crime sites. 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 the sender side and decrypt it on the client side. To demonstrate this we need to merge two technologies on the part of .net play its best role to develop GUI interface to make the system easy to operate by the user. The paper has explored the model and the associated work stages in detail.

Cryptography is the process of converting plaintext into cipher text using the encryption process. Encryption is a process of transforming base data called plain text or clear text into a form that executes to be arbitrary and obscure which is called

cipher text. That base 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 [5].

Symmetric Cryptography:
Symmetric key cryptography is 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 [8].

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 at the sender end and revert action in another end. In this way, the original message is received by the receiver.

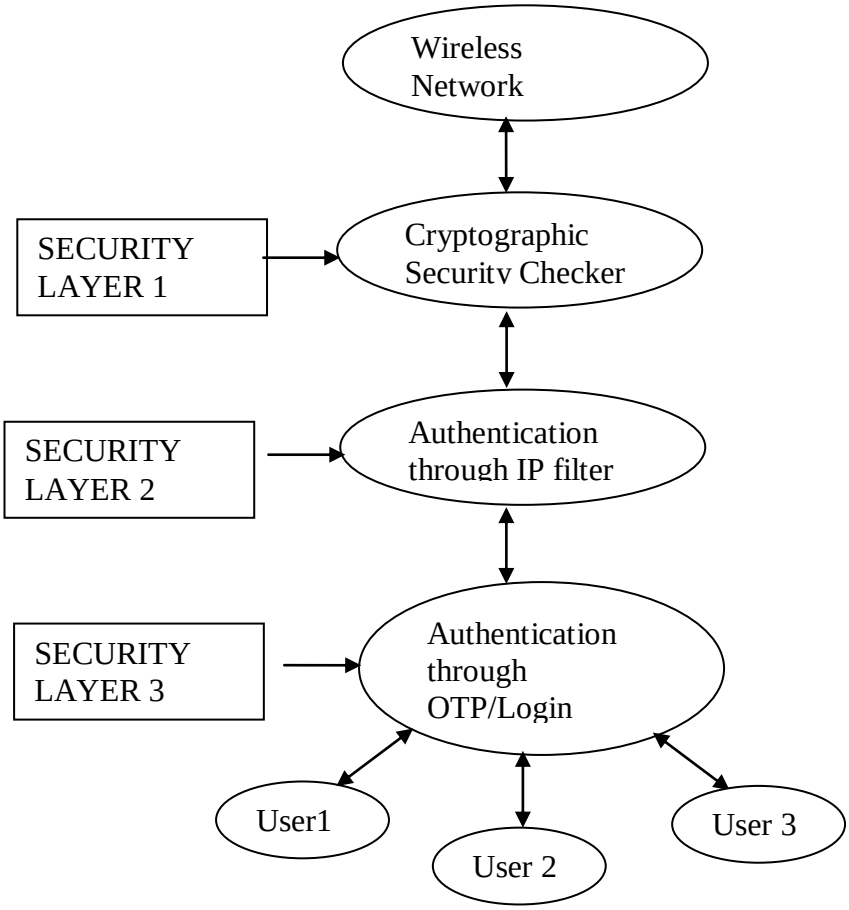

Fig 1 Triple Layer Security

4. Result

Data Analysis work: - We have made the reading of packet transmission time in different cases such as fiber optic, coaxial, twisted pair cable**.**

S no	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 in case of Fiber Optics

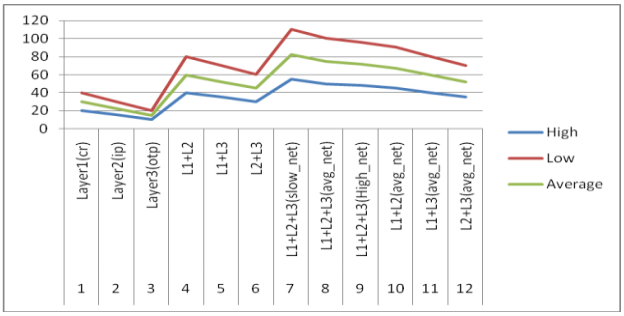

Fig 2 Analysis of transmission speed of packet in case of Fiber Optics

S no.	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 in case of Coaxial Cable

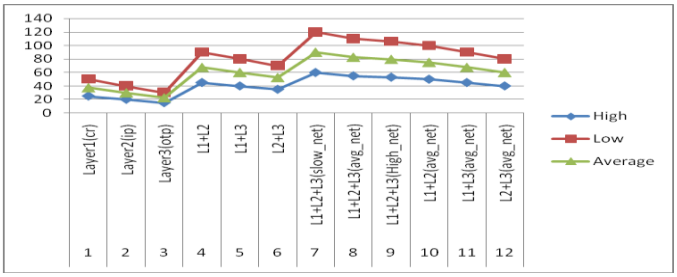

Fig 3 Analysis of transmission speed of packet in case of Coaxial Cable

S no	Security Level	H	L	Avg
1	Layer1(cr)	30	60	45
2	Layer2(ip)	25	50	37.5
3	Layer3(otp)	20	40	30
4	L1+L2	50	100	75
5	L1+L3	45	90	67.5
6	L2+L3	40	80	60
7	L1+L2+L3(slow_net)	65	130	97.5
8	L1+L2+L3(avg_net)	60	120	90
9	L1+L2+L3(High_net)	58	116	87
10	L1+L2(avg_net)	55	110	82.5
11	L1+L3(avg_net)	50	100	75
12	L2+L3(avg_net)	45	90	67.5

Table 3 Data in case of Twisted Cable

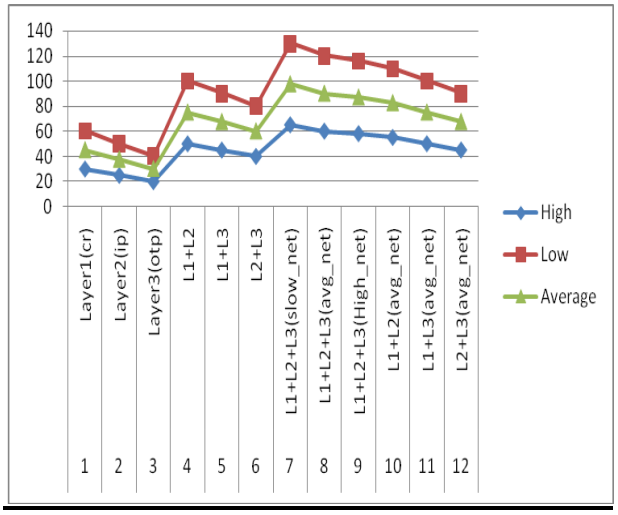

Fig 4 Analysis of transmission speed of packet in case of Twisted Cable

5. FUTURE SCOPE & CONCLUSION

AD-HOC Networking has been still evolving but its benefits are enormous. AD-HOC Networking provides excellent support for amazing infrastructures, applications & services such as shared resource pool, broad network base, reduced this cost or rapid elasticity of network to handle varying customers' demands as well as AD-HOC network computing various service & deployment models that have been part of main the reason for adopting this computing system. Thus this makes network computing open shared system volatile to security breaches & other challenges. So there has been a need to focus on solutions to various challenges to maintain dependence level of organization for deploying AD-HOC Networking without any hesitation & also need of technical support for elastic scalability to serve ever pressing demand the customer. Hacking has both its benefits & a risk this also concludes that hacking has been an important aspect of the computer world. This deals with both sides of being good & bad. Ethical hacking plays a vital role in maintaining & saving a lot of secret data, whereas malicious hacking could destroy everything. What all depends has been intention of a hacker. This has been almost impossible to fill gap btw ethical & malicious hacking as the human mind cannot be conquered, but security measures could be tightened.

REFERENCES

[1] Fahad T. Bin Muhaya, King Saud University Fazl-e-Hadi Atif Naseer, "Selfish Node Detection in Wireless Mesh Networks".
[2] Haggerty J, Shi Q, Merabti M. Early "Detection and prevention of denial-of-service attacks": A novel mechanism with propagated traced-back attack blocking. IEEE Journal on Selected Areas in Communications. 2005.
[3] Dongwon Seo & Heejo Lee "Probabilistic Filter Scheduling against Distributed Denial-of-Service Attacks" 25 March 2011..pp. 89-105.
[4] David Pointcheval, Michel Abdalla, Contributory Password-Authenticated Group Key Exchange with Join Capability, S A. Kiayias Ed. Springer-Verlag, LNCS 6558, 18 Feb 2011. pp. 142-160.
[5] 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 & Theory within Public-Key Cryptography (PKC '13)Springer-Verlag, Kaoru Kurosawa Ed., Springer-Verlag, 2013
[6]. M.Imani Bing He, S M.E.Rajabi M.Naderi "Vulnerabilities in network layer at Wireless Mesh Networks (WMNs)'.International Conference on Educational and Network Technology.

[7] David Pointcheval, Olivier Blazy, "New Smooth Projective Hash Functions & One-Round Authenticated Key Exchange", Santa Barbara, California, 18 Aug 2013.pp.449-475.
[8] Pointcheval D,Boyen X, *Strong Cryptography from Weak Secrets*, (Stellenbosch, South Africa), D. Bernstein and T. Lange Eds., Springer-Verlag , pp. 297–315.
[9] Raghav Mathur, Vishnu Sharma and Shruti Agarwal published their research titled "Solving Security Issues in Mobile Computing using Cryptography Techniques".

