INTERNATIONAL JOURNAL
FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

www.ijraset.com

Call: ◯08813907089 | E-mail ID: ijraset@gmail.com

Implementation of Security of Wireless Mess Network from Denial of Service Attack

Navpreet Kaur
Computer Network

Abstract: A wireless mesh network is a communications network made up of radio nodes organized in a mesh topology. It is also a form of wireless ad hoc network. Wireless mesh networks often consist of mesh clients, mesh routers & gateways. In our research we have discussed security issues related to Wireless Network. After that we will study of Existing Security loop holes within wireless mesh based distributed network environment. The objective of research is to develop system to make Warless mesh network secure form denial of service attack.
Keyboard: Ad Hoc, Fibber optics, Co-axial cable, Wireless Cable.

I. INTRODUCTION

A. Wireless Mesh Network

The web clients are a lot laptops, cell phones and extra wireless devices while web router to fore traffic to & from gateways which may, but need not, be connected to Internet. Coverage area of radio nodes working as a single network [3]is sometimes called a mesh cloud. Way in to this mesh cloud is reliant on radio nodes effective in harmony within all other to build a radio network.
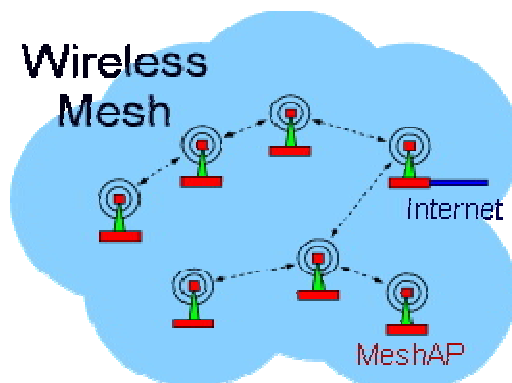

Fig: 1 Wireless Mesh Network [16]

II. DENIAL OF SERVICE ATTACK

A. Types of Attack

Five types of attacks are as follow:
1) Passive Attack
2) Active Attack
3) Distributed Attack
4) Insider Attack
5) Close in Attack

Now we would discuss above harmful attacks with in detail one by one.

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. Passive interception of network operations usually enables adversaries to view upcoming actions. Passive attacks usually result within information disclosure or data files to attacker. & all this can be done without knowledge of operator

Mesh networks might involve either fixed or mobile devices. Conclusion are as modifies as statement needs, for cash in point in difficult environments such as emergency situations, tunnels, oil rigs, battlefield surveillance, high-speed mobile-video applications on board public transport or real-time racing-car telemetry. An important possible application for wireless mesh networks is VoIP. By using a Quality of Service scheme, wireless mesh might support local telephone calls to be routed through mesh.
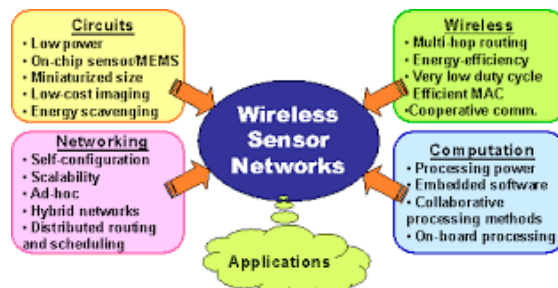Some current applications

Fig: 2 application f wireless network [17]

III. TOOLS & TECHNOLOGY

A. Addressesing Schemes

Generally IP4 addresses are 32 bits long. They are expressed commonly in what is known as dotted decimal notation. Each of four bytes which makes up 32 address are expressed as an integer value (0 – 255) & 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 & vice versa. Often times though IP address is represented by a domain name, for example, hill.ucr.edu. Many functions explained later would allow user to change from one form to another. Importance of IP addresses follows from fact that each host on Internet has a unique IP address.

IV. JAVA SOCKET PROGRAMMING

Programming of Java Socket has been used for communication applications running on different JRE.
Java Socket programming could be connection-oriented or connection-less.
Socket &Server Socket classes are used for connection-oriented socket programming &Datagram Socket & Datagram Packet classes are used for connection-less socket programming.
The client in socket programming must know two information:
A. IP Address of Server, and
B. Port number.
C. Conclusion
Due to number of dissimilar problems versions & minor differences within these, we set out particular problem that we are addressing within this dissertation. problem had been key contract btw both communicating parties within case of symmetric key cryptography.
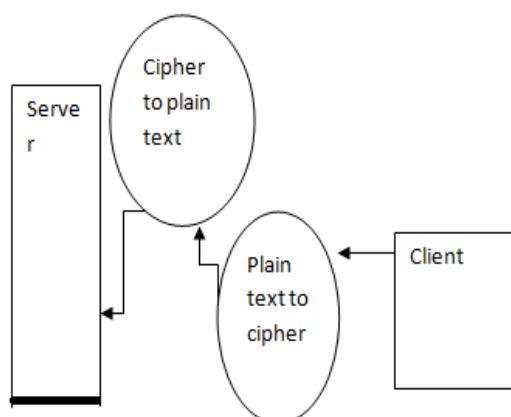

Fig 3 Secure Client Server Communications

V. CLIENT SERVER COMMUNICATION

It is possible for two network applications to begin simultaneously, but it is impractical to require it. It made sense to develop communicating applications to make complementary network operations in sequence, instead of simultaneously.

A. Port

Sockets [22] are UNIQUELY identified by Internet address, end-to-end protocol, & port number. That is why when a socket is first created it is vital to match it within a valid IP address & a port number. Ports are software objects to multiplex data between different applications. Now consider a user running an ftp client, a telnet client, & a web browser concurrently.
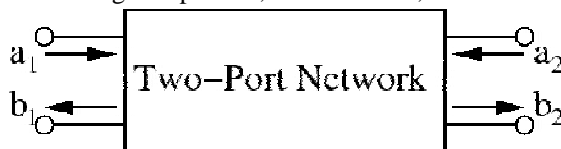

FIG 4 port network [17]

VI. PROPOSED WORK

Here we are using IP filter to reject unauthenticated transmission of packets from server to client.

Here we have to enhance network security by customizing existing encryption techniques.

To study loopholes of existing security mechanisms & enhance security of network.

To program own socket server & corresponding client to prevent unauthentic access during data transmission.

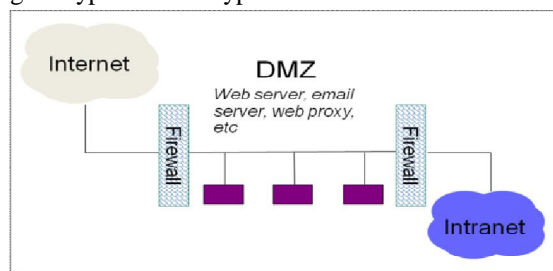To make use of more complex key during encryption & decryption.

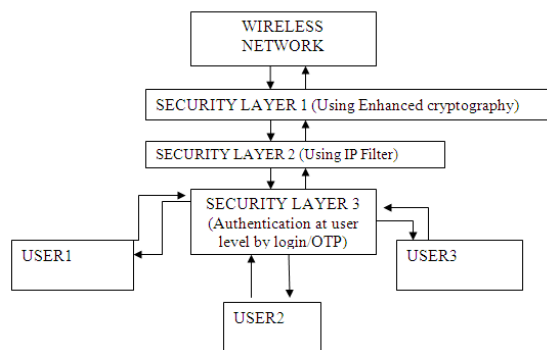Fig 5 Firewall within internet & Intranet

Fig. 6 Triple Layer Security

A. XOR operation

The bit wise xor operation returns 1 if there is any change in bit and it returns 0 if there is no chance in bit

A	B	A XOR B
0	0	0
0	1	1
1	0	1
1	1	0

Table 1 Role of xor during encryption

VII.   IMPLEMENTATION

Create a new application project by selecting File New Project in java

It is often easier to demonstrate code by running it as part of a Windows application than through a console window or via a command prompt. You could do this using user interface building blocks to piece together a user interface.

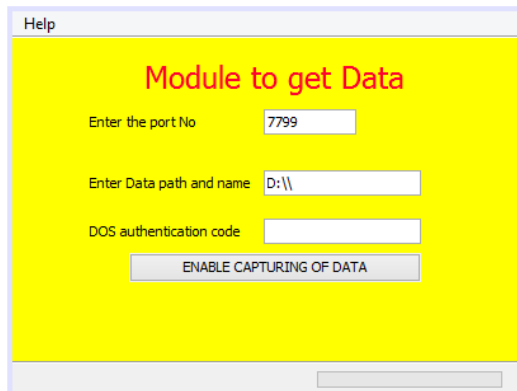Create a new project of type Forms Application

Fig : .7Module to get data

Module to send data using particular port and at particular Location using Specific DOS authentication code.
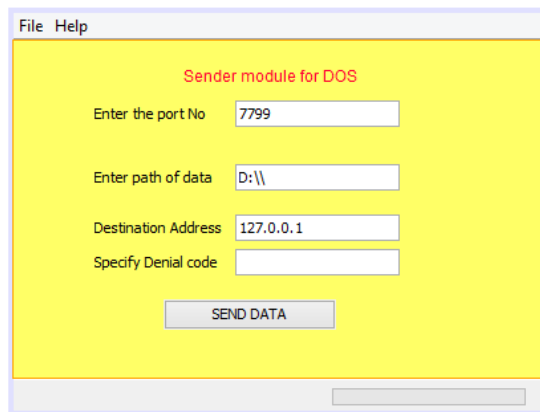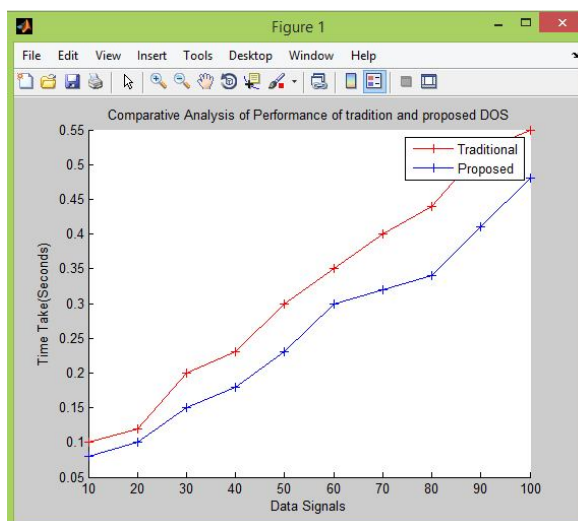

Fig: 7Sender modules for DOS

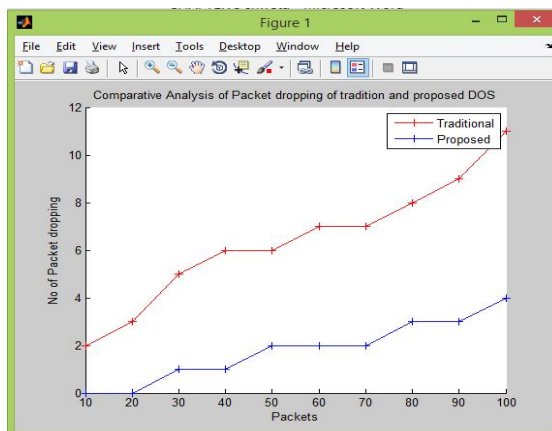Fig: 8Comparative analysis of performance of tradition and proposed DOS

Fig: 9 Comparative Analysis of Packet dropping by DOS

VIII. CONCLUSION

Wireless Mesh Network security is basic requirement during data communication. We made Implementation to enhance network security. Data transmission could be made more secure from hacker to by encrypting data on sender side & decrypt[8] it on client side. But encryption cannot stop denial of service. As it does not matter what is actual data for hacker, he had to just destroy service so that no one could access it. Here we restrict unauthentic dropping of packets using our proposed model.

REFERENCES

[1]   POOJA SHARMA (2005) "performance analysis of secure wireless meshes networks" International Journal of Research in Science and Technology (IJRST) 2013, Vol. No. 3, Issue No. IV, Oct-Dec

[2]   Khaled M. Elleithy(2005) "Denial of Service Attack Technique": Analysis, Implementation and Comparison Computer Science & Information Technology Faculty Publications) 2005, Vol. No. 5, Issue No. IV, Oct-Dec

[3]   Yanchao Zhang, Member (2006) "arsa: an attack-resilient security architecture for multihop wireless mesh networks" ieee journal on selected areas in communications, vol. 24, no. 10, october 2006 multihop wireless mesh networks (wmns) are

[4]   Saman Taghavi Zargar (2008) "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks ") 2008 , Vol. No. 6, Issue No. IV, Oct-jan

[5]   Monika Denial (2010)" of Service Attacks in Wireless Mesh Networks International" Journal of Computer Science and Information Technologies, Vol. 3 (3) , 2012,4516-4522

[6]   Mewada Shivlal (2012)" Performance Analysis of Secure Wireless Mesh Networks "Research Journal of Recent Sciences Vol. 1(3), 80-85, March (2012)

[7]   Lakshmi Santana, Depth Nandiraju,(2012)" Active Cache Based Defense against Does Attacks in Wireless Mesh Network'' Research Journal of Recent Sciences Vol. 1(5), 30-85, june (2012)

[8]   Anil Kumar Gankotiya1 (2013)" Sahil Seth Attacks and their Counter Measures in Wireless Mesh Networks" 2013, Vol. No. 9, Issue No. IV, Feb-Dec

[9]   Joydeep Roy (2014) "Design of Smart Universal Remote using Mobile for Home Automation" Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 5, Ver. VIII (Sep – Oct. 2014),

[10] BOTEZATU, N[icolae](2015) "denial of service resistant mac for wireless mesh networks" international daaam symposium, volume 22, no. 1, issn 1726-9679 isbn 978-3-901509-83-4, editor b. Katalinic, published by daaam international, vienna, austria, eu, 2011

[11] Priya Maidamwar(2016)" a survey on security issues to detect wormhole attack in wireless sensor network" international journal on adhoc networking systems (ijans) vol. 2, no. 4, october 2012

[12] Elsevier B.V.(2017) All rights reserved. capability of self-organization in WMNs reduces complexity of network Journal of Computer Engineering (ISSN: 2278-8727, Volume 14 Issue 4, Ver. VIII (Sep – Oct. 2017),

[13] Res.J.Recent Sci Performance Analysis of Secure Wireless Mesh Networks Research Journal of Recent Sciences Vol. 1(3), 80-85, March (2012) Anil Kumar Gankotiya Attacks and their Counter Measures in Wireless Mesh Networks

[14] Mewada Shivlal and Singh Performance Analysis of Secure Wireless Mesh Networks Research Journal of Recent Sciences Vol. 1(3), 80-85, March (2012)

[15] Priya Maidamwar a survey on security issues to detect wormhole attack in wireless sensor network international journal on adhoc networking systems (ijans) vol. 2, no. 4, october 2012

[16] http://www.surfability.com/images/meshAP.gif

[17] https://encrypted tbn0.gstatic.com/images?q=tbn:ANd9GcRsn_Jbsb84bo_DMeyDAdh7uCWtIdiBD1NZaucfGeM6sZF2z7Z3

[18] http://www.iue.tuwien.ac.at/phd/vitanov/img568.png

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 ○ (24*7 Support on Whatsapp)