© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 08 Issue: 03 | April - June 2017
Paper is available at www.jrps.in | Email : info@jrps.in

# ENHANCEMENT OF SECURITY AGAINST DENIAL OF SERVICE ATTACKS IN WIRELESS MESH NETWORK

Shweta Nijhawan, M.Tech Student, Department of computer science & engineering
BPS Mahila Vishwavidyalaya Khanpur Kalan (Sonipat)

**ABSTRACT:** 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 Internet as their aim is an attempt to restrict users. Distributed Denial-of-Service attack is where often multiple sources thousands of unique IP address. Shop or business of parties to enter into a valid state, not disrupting normal operations or business or a store entrance, a group of people rush to gate & is consistent. DoS attacks are often banks, credit card payment gateways on target host, as high-profile web servers are perpetrators of crime sites or services. Here in our research we would enhance security against Denial of service attack in wireless mesh network.

ISSN : 2278-6848 03
9 772278 684800
© International Journal for Research Publication and Seminar

**Keywords:** DOS, DDOS, WMN, Cryptography, Networking, Hackers

## [1] WIRELESS MESH NETWORK

A **wireless mesh network** (**WMN**)[4, 7] is a communications network made up of radio nodes organized in a mesh[7] topology. It is a type of wireless ad hoc network.[1] Wireless mesh networks often consist of mesh clients, mesh routers & gateways. Mesh clients are often laptops, cell phones & other wireless devices while mesh routers forward traffic to & from gateways that may, but need not, be connected to Internet. Coverage area of radio nodes working as a single network is sometimes known as a mesh cloud. Access to this mesh cloud is dependent on radio nodes working in harmony with each other to create a radio network. A mesh network is reliable & offers redundancy. When one node could no longer operate, rest of nodes could still communicate with each other, directly or through one or more intermediate nodes. Wireless mesh networks[7] could self form & self heal. Wireless mesh networks could be implemented with various wireless technologies including 802.11, 802.15, 802.16, cellular technologies & need not be restricted to any one technology or protocol.

## [2] DENIAL OF SERVICE ATTACK (DOS)

A Denial-of-Service (DoS) attack[3] a machine or network resources such as temporary or inexplicit interrupt or suspended services of a host connected to Internet as their aim is an attempt to make unavailable to users.

A Distributed Denial-of-Service (DDoS) attack[3] is where often multiple sources thousands of unique IP address. Shop or business of parties to enter into a valid state, not disrupting normal operations[14] or business or a store entrance, a group of people rush to gate & is consistent.

DoS attacks[13] are often banks, credit card payment gateways on target host, as high-profile web servers are perpetrators of crime sites or services

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

### *Attack Tools[3]*

Wide arrays of programs are used to launch DoS attacks. In cases such as my doom malw are tool embedded systems & have begun their attack without knowledge of owner. Stacheldraht is a classic example of DOS device. This is a multi-layered structure where

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 08 Issue: 03 | April - June 2017
Paper is available at www.jrps.in | Email : info@jrps.in

attacker operators, that is system that zombie agent , that in turn issue orders to facilitate DDoS attacks are patched to connect to a customer uses program uses. Agents are compromised[11, 16] by attacker through operators automated routine use programs that accepts remote connections on remote host targets to exploit vulnerabilities. Each handler could control thousand agents.

***Denial- of -service Level***

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

***Distributed attacks[8]***

A Distributed Denial of Service[2] (DDoS) Attack occurred when multiple system flood bandwidth or resources of objective system one or more web servers. These attacks constantly compromised systems traffic is a result of flooding in target system.

In order to achieve a bot net owner without knowledge of program is a network of zombie computers.[13] When a connection to server is overloaded with new connections could no longer be accepted. Distributed[8] denial of service attacks are major advantage of using an attacker than a machine could generate more attack traffic.

Multiple attack machines are hard to stop an attack & behaviour of each attack machine making it difficult to traces & off could be stealthier. These challenges cause attackers to gain security apparatus.

***Denial-of-Service (DoS) Level II***

DOS Level 2 (possibly DDoS) attack[9] that blocks a safety net for goal of network segment in which origin of attack would mean a launch. In distributed10] attack or IP header alteration depending on type of security[5] behaviour. attack networks completely block Internet, but without a system crash.

## [3] TOOLS & TECHNOLOGY

**Hardware requirement**

1. CPU (ABOVE 1GHZ)
2. RAM (1 GB)
3. HARDDISK (10GB FREE SPACE)
4. MONITOR
5. KEYBOARD
6. MOUSE

**Software Requirement**

1. Windows 7
2. Java development kit
3. Matlab

## [4] SOCKET PROGRAMMING IN JAVA

Socket programming is used for communication between applications running on different JRE. 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. client in socket programming must know two information IP Address of Server & Port number.

***Socket class***

A socket is simply an endpoint for communications between machines. Socket class could be used to create a socket.

### Important methods

| Method | Description |
|---|---|
| 1) public InputStream getInputStream() | returns InputStream attached with this socket. |
| 2) public OutputStream getOutputStream() | returns OutputStream attached with this socket. |
| 3) public synchronized void close() | closes this socket |

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 08 Issue: 03 | April - June 2017
Paper is available at www.jrps.in | Email : info@jrps.in

***ServerSocket class***

The ServerSocket class could be used to create a server socket. This object is used to establish communication with clients.

## Important methods

| Method | Description |
|---|---|
| 1) public Socket accept() | returns socket & establish a connection between server & client. |
| 2) public synchronized void close() | closes server socket. |

## *Example of Socket Programming*

Let's see a simple of socket programming in that client sends a text & server receives it.

**File: MyServer.java**

```
import java.io.*;

import java.net.*;

public class MyServer {

public static void main(String[] args){

try{

ServerSocket ss=new ServerSocket(6666)
;

Socket s=ss.accept();//establishes connecti
on

DataInputStream dis=new DataInputStrea
m(s.getInputStream());

String  str=(String)dis.readUTF();

System.out.println("message= "+str);

ss.close();

}catch(Exception e){System.out.println(e)
;}  }}
```

**File: MyClient.java**

```
import java.io.*;

import java.net.*;

public class MyClient

{

public static void main(String[] args)

{

try

{

Socket s=new Socket("localhost",6666);

DataOutputStream dout=new DataOutput
Stream(s.getOutputStream());

dout.writeUTF("Hello Server");

dout.flush();

dout.close();

s.close();

}

catch(Exception e)

{

System.out.println(e);

}  } }
```

To execute this program open two command prompts & execute each program at each command prompt as displayed in below figure.

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 08 Issue: 03 | April - June 2017
Paper is available at www.jrps.in | Email : info@jrps.in

```
C:\new>javac MyServer.java

C:\new>java MyServer
message= Hello Server

C:\new>
```

**Fig.1 Execution of server**

After running client application, a message would be displayed on server console.

```
C:\new>javac MyClient.java

C:\new>java MyClient

C:\new>
```

**Fig.2 Execution of Client**

## Socket Programming (Read-Write both side)

In this example, client[11] would write first to server then server would receive & print text. Then server would write to client[14] & client would receive & print text. step goes on.

**File: MyServer.java**

```
import java.net.*;

import java.io.*;

class MyServer{

public static void main(String args[])thro
ws Exception{

ServerSocket ss=new ServerSocket(3333)
;

Socket s=ss.accept();

DataInputStream din=new DataInputStrea
m(s.getInputStream());

DataOutputStream dout=new DataOutput
Stream(s.getOutputStream());

BufferedReader br=new BufferedReader(
new InputStreamReader(System.in));

String str="",str2="";

while(!str.equals("stop")){

str=din.readUTF();

System.out.println("client says: "+str);

str2=br.readLine();

dout.writeUTF(str2);

dout.flush();

}din.close();

s.close();

ss.close();

}}
```

**File: MyClient.java**

```
import java.net.*;

import java.io.*;

class MyClient{

public static void main(String args[])thro
ws Exception{

Socket s=new Socket("localhost",3333);

DataInputStream din=new DataInputStrea
m(s.getInputStream());

DataOutputStream dout=new DataOutput
Stream(s.getOutputStream());

BufferedReader br=new BufferedReader(
new InputStreamReader(System.in));

String str="",str2="";
```

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 08 Issue: 03 | April - June 2017
Paper is available at www.jrps.in | Email : info@jrps.in

```
while(!str.equals("stop")){
str=br.readLine();
dout.writeUTF(str);
dout.flush();
str2=din.readUTF();
System.out.println("Server says: "+str2);
}  dout.close();
s.close();
}}
```

## [5] PROPOSED MODEL

In this research we have used socket programming in java to make a protocol. Commutative encryption[10,11,12] & watermarking in video compression. We would develop client server model so that data sent from client to serve[10]r could not we hacked or dropped by hacker as we have used our own protocol[1] to restrict unauthentic access from hacker[16].

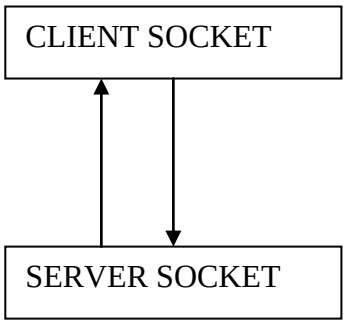
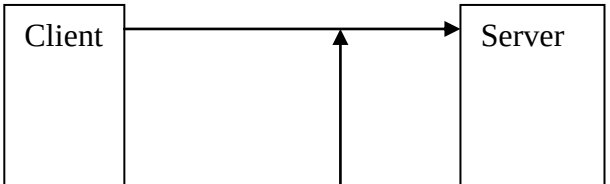



**Fig 3** Client server socket communication

This model would create a separate layer for data transmission & hacker[15] would not be capable to access data on wireless network without application layer required on client.



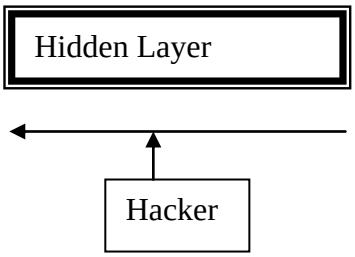




**Fig 4** Proposed Model

## [6] CONCLUSIONS

Wireless Mesh Network security[5] is basic requirement during data communication[12]. We made Implementation to enhance network security[8].
Data transmission could be made more secure from hacker[14] to by encrypting[18] 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[16], he has to just destroy service so that no one could access it. Here we restrict unauthentic dropping of packets using our proposed model.

## Reference

1. B.SOUJANYA "STUDY OF ROUTING PROTOCOLS IN MOBILE AD-HOC NETWORKS"International Journal of Engineering Science and Technology (IJEST) ISSN : 0975-5462 Vol. 3 No. 4 April 2011
2. Khemapech, I. Duncan and A. Miller A Survey of Wireless Sensor Networks Technology in 2004
3. Darshan Lal Meena Destruction DENIAL OF SERVICE ATTACKS International Journal of Advance Research in Computer Science and Management Studies on 2014
4. Aleksi Penttinen Research On Ad Hoc Networking: Current Activity And Future Directions Acm Sigcomm Computer Communication Review, 28(3):5–26, July 1998.
5. B.SOUJANYA* Feng Zhao & Leonidas Guibas, "Wireless Sensor

Networks", Morgan Kaufman Publishers, 2004.
6. C.K.Toh, "Ad Hoc Mobile Wireless Networks", Pearson Education, 2002.
7. Thomas Krag & Sebastin Buettrich, "Wireless Mesh Networking", O'Reilly Publishers, 2007.
8. Agi, I., Gong, L.: An empirical study of secure mpeg video transmissions. In: Proceedings of Symposium on Network & Distributed System Security, pp. 137–144. IEEE Press, New York (1996)
9. Baugher, M., McGrew, D., Naslund, M., Carrara, E., Norrman, K.: secure real-time trans-port protocol (SRTP) (2004)
10. 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
11. Cheng, H., Li, X.: Partial encryption of compressed images & videos. IEEE Trans. Signal Process. **48**(8), 2439–2451 (2000). doi: 10.1109/78.852023
12. 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)
13. 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)
14. 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)
15. Lian, S., Liu, Z., Ren, Z., Wang, H.: Commutative encryption & watermarking in video compression. IEEE Trans. Circuits Syst. Video Technol. **17**(6), 774–778 (2007)
16. Logik Bomb: Hacker's Encyclopedia (1997)