Secure Routing Packet Transmission

Manjula. M
M. Tech (CE),
Dept. of CSE
SJBIT, Bengaluru
sowmya.jsm@gmail.com

Mrs. Pavithra. G.S
Asso. Professor
Dept. of CSE
SJBIT, Bengaluru
pavi.pgs@gmail.com

Abstract— The Secure Routing Packet Transmission is the one which can be used to send or transmit the message or packets which contain some sensitive data in the network. Network is a medium which can consists of routers and network devices. In network there may be a chance of modifying the files by the attacker, but in our approach we age removing the attackers in other words we are removing the untrusted nodes. By generating the frequency to each and every nodes and by using the NDP protocol we can remove untrusted nodes and the shortest path is choosed based on frequency of all the nodes from source to destination, each time the frequency will be randomly generated so that same route will not select. The route will be selected based on shortest path.

After successful transmission of file from source to destination, the file will be safely stored in destination folder.

Index term- *Secure Routing, Wireless communication, Packet fragmentation, IP References, NDP, Shortest path Routing.*

*****

I. INTRODUCTION

Transmission of packets or file in network is highly vulnerable to attackers or third party. In Network weather it is wired or wireless there may be chance of existing attackers. So the sensitive data may be corrupted or taken by the attackers. Networks are of types 1) Personal Area Network, 2) Local Area Network, 3) Metropolitan Area Network or, 4) Wide Area Network. A personal area network (PAN) is a computer network organized around an individual person. Personal area networks typically involve a mobile computer, a cell phone and or a handheld computing device such as a PDA. You can use these networks to transfer files including email and calendar appointments, digital photos and music. Personal area networks can be constructed with cables or be wireless. A Local Area network (LAN) is a computer network that spans a relatively small area. Most often, a LAN is confined to a single room, building or group of buildings, however, one LAN can be connected to other LANs over any distance via telephone lines and radio waves. A system of LANs connected in this way is called a *wide-area network (WAN).* Metropolitan Area Network, a data network designed for a town or city. In terms of geographic breadth, Man’s are larger than local-area network, but smaller than wide area networks. Man’s are usually characterized by very high-speed connections using fiber optical cable or other digital media.

All these network uses Nodes, Transmitter, Receiver, Routers etc.. In this paper we proposed the concept of secure transmission of packets. To do this we developed and application, in this application first module is user login. If the user is valid then he or she can choose file and can send the file in network. A node is a point of intersection/connection within a network. In an environment where all devices are accessible through the network, these devices are all considered nodes. The concept of nodes works on several levels, but the big-picture view defines nodes as the major centers through which Internet traffic is typically routed. The idea of nodes was popularized with the adoption of packet-switching theory and the concept of distributed networks. In this context, nodes were gateways that could receive, store and send information along different routes through a distributed network. Each node was given an equal standing within the network.

An IP (Internet Protocol) address is a unique identifier for a node or host connection on an IP network. An IP address is a 32 bit binary number usually represented as 4 decimal values, each representing 8 bits, in the range 0 to 255 (known as octets) separated by decimal points. This is known as "dotted decimal" notation.

Example: 140.179.220.200

It is sometimes useful to view the values in their binary form.

140 .179 .220 .200
10001100.10110011.11011100.11001000

Every IP address consists of two parts, one identifying the network and one identifying the node. The Class of the address and the subnet mask determine which part belongs to the network address and which part belongs to the node address.

Consider a text file for ex: ABC.txt, this file is choosed and get selected and the file gets into fragmented packets. File will be fragmented as packets based on file size. If the file size is less then number of packets fragmented is less. If the file size is large then the numbers of fragmented packets are more. Each packet will have its own size based on content. Later the Packets are send in network. In network each nodes will have its own node numbers. For each node respective random frequency will be generated. These frequencies will be generated randomly. And for each node respective IP Address is generated. Using this IP Reference we can find weather the node is trusted or not. To do this we are adopting Neighbour Distance Protocol, the trusted nodes will have IP References but other untrusted nodes will not have IP references and get disconnected in network so that packets are not transmitted through untrusted nodes. Later the Source and Destination will be choosed and the route will be set between source and destination, the route will be selected based on shortest path between source and destination. So the route is set only through the trusted nodes because already untrusted nodes are get disconnected from the link. Each packet is transmitted by each node and reaches destination successfully, so successfully all the packets gets merged and forms files in the destination.

II. PROPOSED SYSTEM

Through this paper we are presented a new routing protocol for secure routing in wireless networks, this new routing protocol will not support link failures and route breaks occur frequently. Here we are adding frequency for nodes these frequencies are support for secure routing nodes. However, the protocol routing is done by frequencies of trusted nodes. Our approach consists of an extension to the routing protocol. In proposed system we are generating the frequency to all the nodes, all the nodes will have its own frequency so by using these frequency the path will get selected. The file should chooses by the user only, file choosing concept is implemented here so the selected file will get choosed and file fragmented and also number of packets created depends on file size. Everything will be displayed to user through update message. In the proposed concept every nodes will have its own IP addresses. Using IP References we can find the trusted nodes and untrusted nodes. All the trusted nodes will have its own IP References and all the untrusted nodes doesn't have any IP address.

Neighbor distance protocol support to remove untrusted nodes links in routing time, and trusted and untrusted nodes identified by TCP internet address reference. So while deciding shortest path, the route will selects through trusted nodes only. The untrusted nodes are removed from the network. Each and every details of shortest path selection, details of trusted nodes and untrusted nodes are stored and displayed through update message. So by analyzing the update message we can conclude the result of secure routing. Also after reaching the destination securely the packets gets merged and forms file structure and stored in specific directory.

All the packets are transmitted through selected path, in this path all the packets are passed through each nodes, finally the packets will reaches the destination system and these packets are get converted into file. The converted file which was received in destination system is same as that of file selected by user to send through network, because in our proposed system we removed link failure, untrusted nodes so everything is perfect in network so the file received to destination system without any damages or corrupt.

Multipath Routing Algorithm

```
Step 1: Start
Step 2:  Connect pubic network Con.Connect (IP)
Step 3: Find the all Network nodes
Step 4: Visibility $\tau$ (i,j)= $\tau$0
            If “Is the best path found?”
Step 5: Analyze the path then Print “Final path”
Step 6: Send file via Final path
Step 7: Close network Connection
            Con.Close ();
Step 8: End of Algorithm
```

EXPERIMENTAL RESULTS

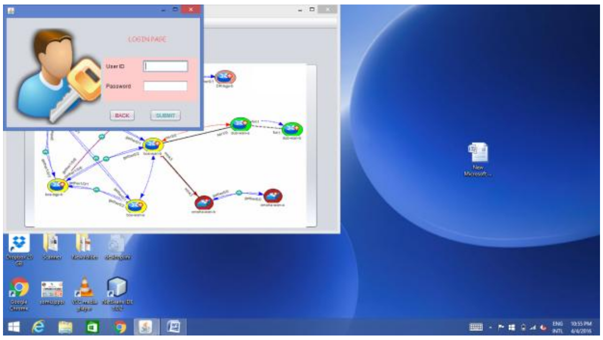
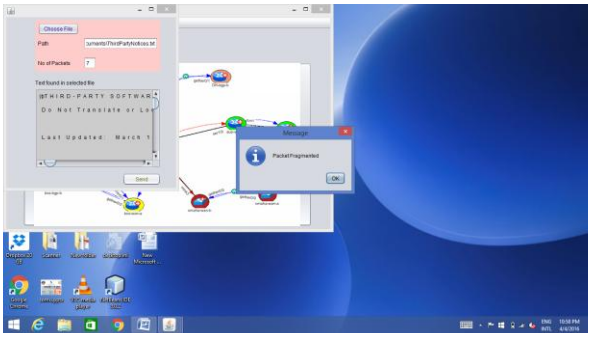


Fig 1: Login to the Packet Transmission

Login to the packet transmission by user name and password to transmission begins. To secure packet transmission, user name and password has been given.



Path: cuments\ThirdPartyNotices.txt

No of Packets: 7

Text found in selected file

THIRD-PARTY SOFTWAR

Do Not Translate or Lo

Last Updated March 1

Message: Packet Fragmented

Fig 2: Packet Fragmentation

Select the file or choose the file which is divided into packets and these packets are fragmented and it shows packet fragmented successful.

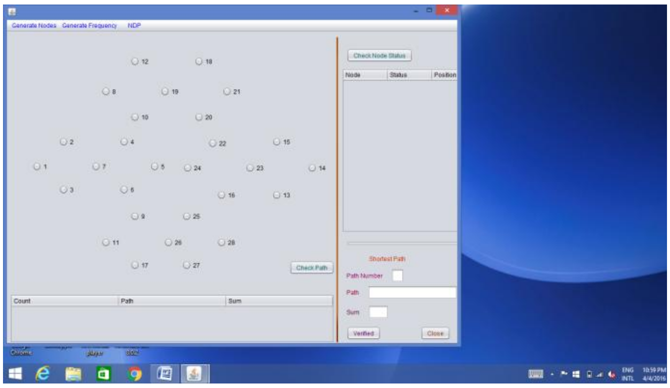
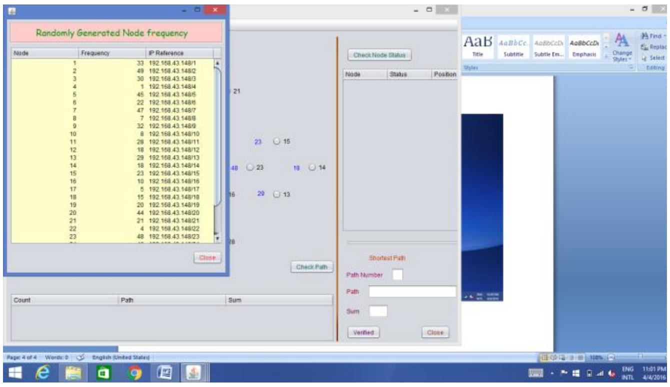


Fig 3: Generate nodes

Generate the nodes to be fragmented and these nodes are combination of both trusted and untrusted nodes.



Randomly Generated Node frequency

Node	Frequency	IP Reference
1	33	192.168.43.148/1
2	49	192.168.43.148/2
3	30	192.168.43.148/3
4	1	192.168.43.148/4
5	45	192.168.43.148/5
6	22	192.168.43.148/6
7	47	192.168.43.148/7
8	7	192.168.43.148/8
9	32	192.168.43.148/9
10	8	192.168.43.148/10
11	28	192.168.43.148/11
12	18	192.168.43.148/12
13	29	192.168.43.148/13
14	18	192.168.43.148/14
15	23	192.168.43.148/15
16	10	192.168.43.148/16
17	5	192.168.43.148/17
18	15	192.168.43.148/18
19	20	192.168.43.148/19
20	44	192.168.43.148/20
21	21	192.168.43.148/21
22	4	192.168.43.148/22
23	48	192.168.43.148/23

Fig 4: Frequency Generation

Generate the frequency for every node and generate the IP address for each node.

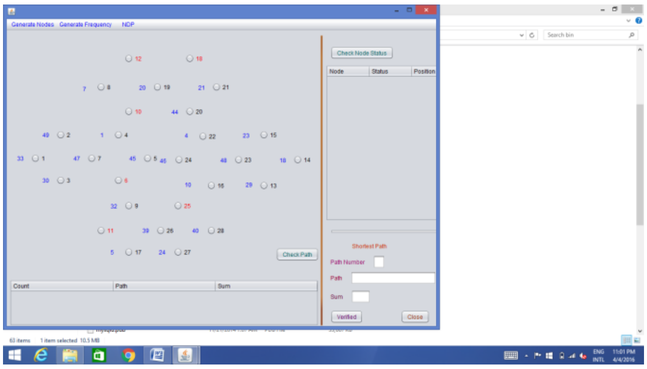
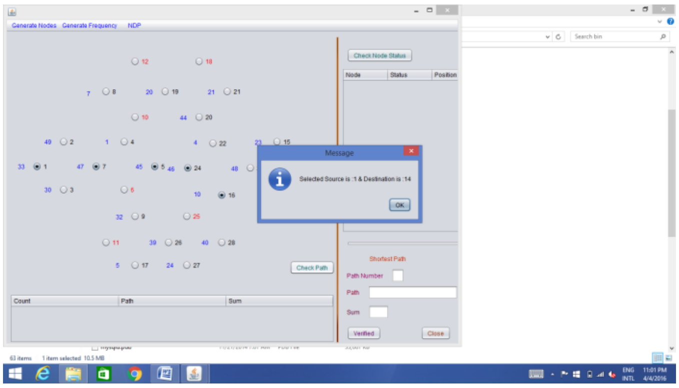


Fig 5: Untrusted node Detection

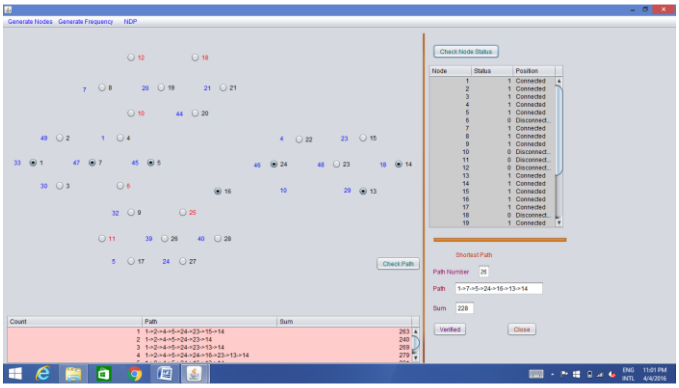
Nodes which is generated before is a combination of both trusted and untrusted nodes. Detection of untrusted nodes which indicates in red, remove those untrusted nodes.



Message: Selected Source is :1 & Destination is :14

Fig 6: Path and Destination

Select the path and destination where packet transmission where it has been saved.



Node	Status	Position
1	1	Connected
2	1	Connected
3	1	Connected
4	1	Connected
5	1	Connected
6	0	Disconnect...
7	1	Connected
8	1	Connected
9	1	Connected
10	0	Disconnect...
11	0	Disconnect...
12	0	Disconnect...
13	1	Connected
14	1	Connected
15	1	Connected
16	1	Connected
17	1	Connected
18	0	Disconnect...
19	1	Connected

Shortest Path

Path Number: 26

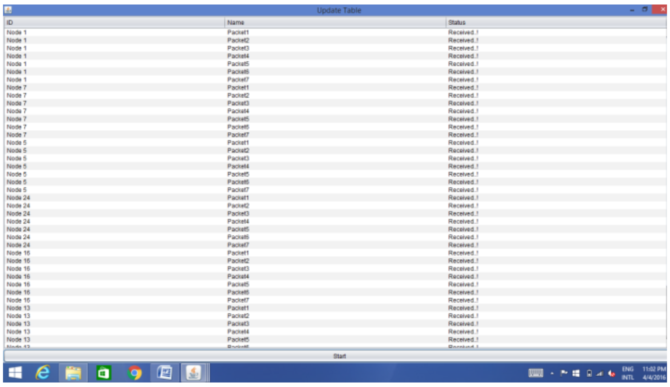
Path: 1->7->5->24->16->13->14

Sum: 228

Count	Path	Sum
1	1->2->4->5->24->23->15->14	263
2	1->2->4->5->24->23->14	240
3	1->2->4->5->24->23->13->14	269
4	1->2->4->5->24->24->16->23->13->14	279

Fig 7: Message Display

Display the updated message in the screen after removed of untrusted nodes.



Update Table

ID	Name	Status
Node 1	Packet1	Received..!
Node 1	Packet2	Received..!
Node 1	Packet3	Received..!
Node 1	Packet4	Received..!
Node 1	Packet5	Received..!
Node 1	Packet6	Received..!
Node 1	Packet7	Received..!
Node 7	Packet1	Received..!
Node 7	Packet2	Received..!
Node 7	Packet3	Received..!
Node 7	Packet4	Received..!
Node 7	Packet5	Received..!
Node 7	Packet6	Received..!
Node 7	Packet7	Received..!
Node 5	Packet1	Received..!
Node 5	Packet2	Received..!
Node 5	Packet3	Received..!
Node 5	Packet4	Received..!
Node 5	Packet5	Received..!
Node 5	Packet6	Received..!
Node 5	Packet7	Received..!
Node 24	Packet1	Received..!
Node 24	Packet2	Received..!
Node 24	Packet3	Received..!
Node 24	Packet4	Received..!
Node 24	Packet5	Received..!
Node 24	Packet6	Received..!
Node 24	Packet7	Received..!
Node 16	Packet1	Received..!
Node 16	Packet2	Received..!
Node 16	Packet3	Received..!
Node 16	Packet4	Received..!
Node 16	Packet5	Received..!
Node 16	Packet6	Received..!
Node 16	Packet7	Received..!
Node 13	Packet1	Received..!
Node 13	Packet2	Received..!
Node 13	Packet3	Received..!
Node 13	Packet4	Received..!
Node 13	Packet5	Received..!
Node 13	Packet6	Received..!

Fig 8: Output Results

The packet is received to the output destination and the result is shown.

CONCLUSION

By this we can conclude that the message which was transmitted in the form of packets are securely reaches the destination system through network. All the nodes in the networks are made as trusted nodes and the untrusted nodes are removed from the network so that there is no concept of packet loss or packet misuse and all. All the information's about routing packet, trusted nodes, untrusted nodes, frequency and IP address are all stored in memory. In our approach we are using mysql database to store the data. So everything is preserved securely in database.

"Secure Routing Packet Transmission" as name suggests packets are securely transmitted in network. This method can be used to transmit the sensitive file securely in network system. All the functionality and results are stored and displayed by update message. In destination system the file is stored in specific directory, the user can open and read this file using the system.

FUTURE WORK

It mainly based on deployment of this concept in real time process and to increase the performance and efficiency.Also the work will be planned for encryption of file before sending through network, and decryption of filewill be done the receiver side so that we can add furthermore security in the network.

ACKNOWLEDGMENT

I express my deep sense of gratitude to the **SJBIT Institute of Technology**, Bangalore for providing us an opportunity to carry out my project in a prestigious organization.
I would also like to thank my internal guide **Mrs. Pavithra G**.**S** Assoc. Professor, CSE, SJBIT Institute of Technology, Bangalore for her guidance and support.

REFERENCES

[1] Justin Deng, Siheng Wu, Kenny Sun "A Comparison of RIP, OSPF and EIGRP Routing Protocols based on OPNET", 2014.

[2] Pankaj Rakheja, Prabhjot Kaur, Anjali Gupta, Aditi Sharma, "Performance Analysis of RIP, OSPF, IGRP and EIGRP Routing Protocols in a Network". Retrieved on June 18, 2012.

[3] Jaehyun Park "Shortest Path Algorithms" Stanford University, June 29, 2015.

[4] Joydeep Chandra, Ingo Scholtes , Niloy Ganguly and Frank Schweitzer "A Tunable Mechanism for Identifying Trusted Nodes in Large Scale Distributed Networks" Indian Institute of Technology, Kharagpur, India, 2012

[5] Idris M. Atakli, Hongbing Hu, Yu Chen, Wei-Shinn Ku, Zhou Su "Malicious Node Detection in Wireless Sensor Networks using Weighted Trust Evaluation", SpringSim, 2008