A Path Confusion Algorithm to Prevent Intrusion

Ramesh[1], Senthil Kumaran[2], Shiny Angel[3]
[1,2]Student, [3]Assistant professor
SRM University,Chennai

***Abstract* - Intrusion has become a major threat in this modern age, to prevent intrusion several intrusion detection systems and techniques has been developed. Our paper also focuses on network security and we came up with a new and innovative solution to tackle the problem. In this paper our primary focus is to confuse the intruder by creating multiple paths and send the data safely from one end to the other end, Thereby minimizing the chances of intrusion and enable users to transfer data without the fear of being hacked.**

***Keywords* - Intrusion, Routing Tables, Client/Server and Encryption**

I. INTRODUCTION

Intrusion occurs due to different reasons. The main ones are unethical behaviors, mostly successful due to trusted security mechanism failures or shortcomings. There is the need to have a look at it all for possible lead to improvements. This will result in improved security measures and ultimately lead to more secure computing environment. Extensive literature review on the subject matter was performed. The relevant documents obtained were qualitatively analyzed for convergence, and relevant details were extracted, using inductive approach. It is true that the benefits of this research could not be entirely determined. This overview could also serve as indicator of or pointer to a research area or be a rider to a more detail research into certain aspects of network security.

II. DEFINING THE METHODOLOGY

The system is peer to peer network developed for the sending and receiving data. A peer to peer network is a powerful tool which allows individuals to interact with each other and share their resources. They thus help in bridging the geographical boundaries separating these users and create a truly global village. The developers of the system feel that it is high time that a peer to peer network is developed which is dedicated to the secure transmission. We hope that this project will provide to its users the benefits of peer to peer networks and facilitate in bringing together the global Open Source community and the Indian Open Source Community It aims to replace the existing peer to peer networks by providing an enhancement over their existing features. Thus, it is a self- contained peer to peer tool for secure data transmission The main function of this system is to allow its users to share their resources over the internet. It also allows the users to interact with each other via a chat client that will be integrated in the tool. The users can also post blogs on a website, where they can post code snippets etc. and others can comment on their posts.

III. CONSTRUCTION OF THE RULES

The data is transferred from sender to receiver. To send the data from one end to the other end first the user should have the IP address of the receiver after that the required data to be transferred is located from the user's computer and then it is sent to the receiver's end. First the connection is established between the two ends and request is made from sender's port to the receiver's socket and when the connection is accepted the data packets are sent. Suppose if there is any delay in connection or any failure occurred during packet sending the sender is notified and the packet is sent again. To establish a secure connection we use multi-path algorithm where multiple virtual paths are created and it is like one port is accessing multiple sockets at a time and this causes the attacker to be confused while the data is sent securely from sender end to the receiver end through this path confusion algorithm.

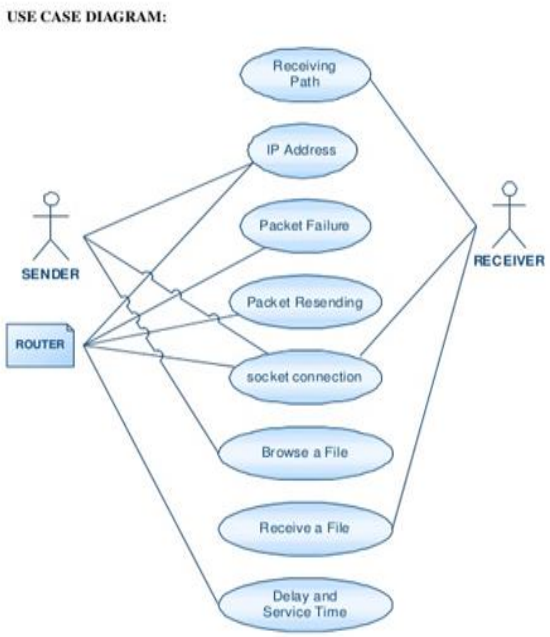

Fig.1.1 Establishing connection between sender and receiver

The above use case diagram shows how the connection is established.First the sender will send request and receiver has to accept the request.then the router tracks the delay time,service time,packet failure and socker connection.Then the sender browses the necessary file to be sent to the receiver and that file is sent to the receiver and the receive will accept that file.

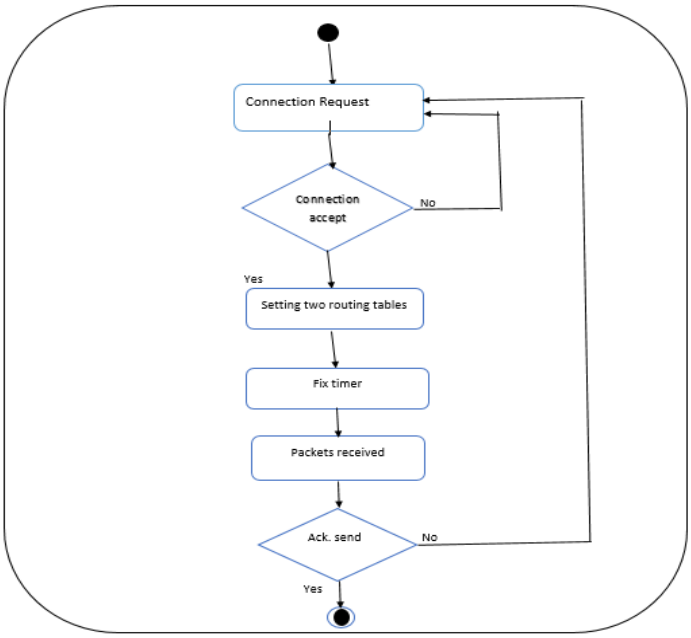

Fig.1.2 Activity diagram

In the above diagram we can see how the connection is established .First the connection request is sent to the receiver. If the receiver accepts the connection request the connection will be established. If the user failed to accept the connection the step is repeated till the user accepts the connection then the data transmission will start and the packets will be sent from the sender's end. The routing tables are used to keep in-track of the received data.

Two routing tables are used. The first routing table is used to track the duplicate data and the second routing table is used for tracking the original data. A timer is used to determine the data transfer rate and if the connection is idle for a period of time then the connection is terminated and notification is sent to the user and packets transfer are stopped. The main goal is to send duplicate data equivalent to the original data thereby confusing the attacker by projecting multiple paths. If the attacker chooses a random path the chances of hacking the data are less the data is split into several parts and sent through different paths and so it is difficult to decode the full information in that particular time-span. If the attacker chooses the path that contains the duplicate data by the time the attacker decodes the duplicate data the original had been sent to the receiver.

IV. WORKING MODEL OF THE SYSTEM

The proposed system is that the sender sends requests to the receiver. After the receiver accepts the requests then connection is established. In Some paths duplicate data are sent and in some path original data are sent to confuse the hackers. Each time a random path is selected and the data is sent through that path. Random selection algorithm is used to choose a random path and send the data through that path, so hackers would be confused in which path the data will come by the time the hacker figures out the path the would have been sent to the receiver .We include encryption to encrypt the data for secure transmission which provides more security. Each time a different path is selected to send the data. Same paths are not used continually. Two routing table are fixed. The front routing table is used to confuse the hackers which shows duplicate data are received by the receiver. Each duplicate data and correct data are of the same size. After the hacker hacks that path to identify that was duplicate data. In the back routing table the information of the path and the real data is identified and the receiver can access the correct data. An intrusion detection system may be used at the back routing table to monitor the data transfer.

A timer is fixed to monitor the amount of time taken to receive the data at the receiver's end. If the time exceeds the data transfer is stopped. Suppose if the receiver fails to send the acknowledgement the transfer will be stopped till the receiver sends the acknowledgement. If the receiver does not receive the data in that particular path then the sender has to decide whether to send the data in that particular path or block that path. The major merits of our system is that it is more secured because the main focus is to secure the data through the path and to provide a three tier security through encryption techniques. The receiver receives the file and checks if the file is correct,

Then the receiver will send the acknowledgement to the sender. Each time multiple connection are given by the sender each connection each data was send. Many paths are used to send duplicate data and only one path is used to send original data. If the attacker wants to hack correct data choose correct path then only know about the data. Each time each path is used to send the data. May be original path used by the duplicate data. Next time duplicate data path is used by the original data. The process will take place vice-versa after receiving data then only the receiver knows that was original data and then the receiver will send the acknowledgement to the sender that the data is received. If the receiver wants additional set of data then the receiver should send a request to the sender to access that information

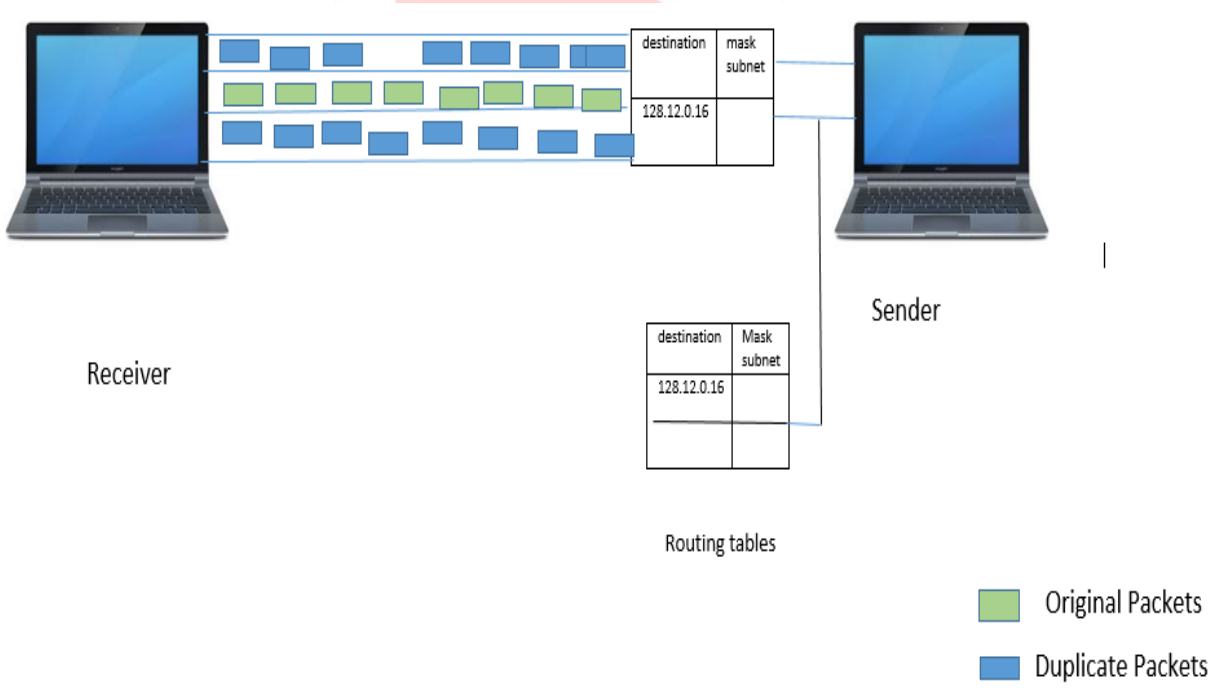

Fig.1.3 Original data is send only in one path but duplicate data simultaneously send to multiple path with same size

V. CONCLUSION

Every system has its own merits and demerits. In this paper we propose a new and innovative idea in the field of network security to help the users to protect their valuable data and we would like to create a safer environment where the users can feel secured about their data being comprehended by hackers. Our future enhancements are increase the speed of data transfer and bandwidth reduction. We also plan to reduce the load.

VI. ACKNOWLEDGEMENT

We would like to thank our guide and mentor Mrs T.S SHINY ANGEL and our parents and our dear friends for constantly encouraging us to believe in our dreams and motivated us to achieve greater heights. And I would like to thank the entire software engineering department in SRM UNIVERSITY for believing in our work and constantly supported our work.

REFERENCE

[1] Scarfone, Karen; Mell, Peter (February 2007). "Guide to Intrusion Detection and Prevention Systems (IDPS)". *Computer Security Resource Center* (National Institute of Standards and Technology) (800–94). Retrieved 1 January 2010.

[2] nitin.; Mattord, verma (2008). *Principles of Information Security*. Course Technology. pp. 290–301. ISBN 978-1-4239-0177-8.

[3] *A Guide to Building Dependable Distributed Systems*. New York: John Wiley & Sons. pp. 387–388. ISBN 978-0-471-38922-4.

[4] Anderson, James P., "Computer Security Threat Monitoring and Surveillance," Washing, PA, James P. Anderson Co., 1980.

[5] Denning, Dorothy E., "An Intrusion Detection Model," Proceedings of the Seventh IEEE Symposium on Security and Privacy, May 1986, pages 119–131

[6] Lunt, Teresa F., "IDES: An Intelligent System for Detecting Intruders," Proceedings of the Symposium on Computer Security; Threats, and Countermeasures; Rome, Italy, November 22–23, 1990, pages 110–121.

[7] Lunt, Teresa F., "Detecting Intruders in Computer Systems," 1993 Conference on Auditing and Computer Technology, SRI International

[8] Sebring, Michael M., and Whitehurst, R. Alan., "Expert Systems in Intrusion Detection: A Case Study," The 11th National Computer Security Conference, October, 1988