International Journal of Computer
Science and Engineering (IJCSE)
ISSN 2278-9960
Vol. 2, Issue 4, Sep 2013, 91-102
© IASET

International Academy of Science, Engineering and Technology
Connecting Researchers; Nurturing Innovations

AN INTEGRATED PROTOCOL FOR DETECTION AND AVOIDANCE OF DENIAL OF SERVICE ATTACKS ON MPLS

S. VENKATA RAJU[1], P. PREMCHAND[2] & A. GOVARDHAN[3]

[1]Research Scholar, Department of Computer Science and Engineering, University College of Engineering(Autonomous), Osmania University, Hyderabad, Andhra Pradesh, India

[2]Professor and Dean, Department of Computer Science and Engineering, University College of Engineering(Autonomous), Osmania University, Hyderabad, Andhra Pradesh, India

[3]Professor, School of Information Technology, Jawaharlal Nehru Technological University Hyderabad, Kukatpally, Hyderabad, India

ABSTRACT

In MPLS, unwanted traffic and malicious effect of different nodes leads the network to an erroneous network, resulting in lower efficiency. One of the main causes of erroneous network is Denial of Service (DoS) attacks. Generally the DoS attack harms the network system both in the domain of hardware and software. This paper presents an integrated protocol for detecting and avoiding the DoS attacks based on time, and bandwidth. In this protocol, the data is grouped and analyzed to detect the variety of attacks present in the network. For individual attack detection, an individual solution is presented. Finally, all the solutions are integrated and applied to the network so that every attack can be prevented. Both forward and backward checking is enabled to detect flood attack, SYN flood attack, ICMP flood attack, starvation attack.

KEYWORDS: Denail of Service, Detection, Integrated System, MPLS Networks

INTRODUCTION

Multi-Protocol Label Switching (MPLS)

Recently communication has grown rapidly in a client server model [1]. Multi-protocol Label Switching (MPLS) is a broadband technique which, supports and strengthens IP services. MPLS includes Label Edge Router (LER), which is responsible for attaching appropriate labels on the packet. LER are of two types and they are ingress or egress router. A label is a signature to transmit data in the network.

The labeled packets are forwarded or routed through the path known as Label Switch Path (LSP). During transmission, the final LER is responsible for removing label from the packets. [2] MPLS is a connection oriented technique. MPLS provides reliable services according to the customer demands and profit goals and network requirements. [3]. It works at the second layer and a third layer of the network. [4]

MPLS networks consist of more than one client and more service providers. A node can do the work of source, destination, and routers. There are a lot of switching devices, routers, multiplexures and demultiplexures. A node can operates multiple works. The different switch level path follows different protocols to transmit their message to the next node. A switch can transmit a message in any direction in the networks.

The data packet used in the transmission system carries required information and some extra bit of data. The extra amount data provides a proper direction to reach the destination, while ciphering of data provides a secure way for transmissions and other extra bits are added for multiple purposes such as error detection, probability of failure detection etc.

Denial of Service (DoS) Attacks

The resources of hosts and network are consumed maliciously through worms and denial of service (DoS) attacks. In addition to this, resources can also be consumed unnecessarily through traffic transmitted by misconfigured hosts and servers. Denial-of-service attack is an explicit attack caused by the attackers with the intention of preventing legitimate users from utilizing the resource and service. DoS attacks may accomplish in two ways such as crashing the services and flooding the services. Some of the operations of DoS attacks are (i) Consumption of computational resources like bandwidth, processor time or disk space, (ii) Interrupting configuration information such as routing information, (iii) Distracting physical network components and state information and (iv) Obstructing the communication media between the legitimate users and the victim [8].

Various forms of DoS attack are listed include [7] Internet Control Message Protocol (ICMP) Flood, SYN Flood, Teardrop attacks, Distributed denial of service attack (DDoS) and Nuke attacks.

In our other work [5], a swarm based algorithm is given for error detection and in the second work [6], grouping and categorize of errors with complementary solution is given. To detect the problem of Denial of Service and catagorise it as well as to give proper solution of those attacks, this method proposes an integrated system of protocols to detect, catagorise and prevent Denial of Service attack. This paper is grouping the data and analyzing these data to detect the variety of attack present in the network. For individual detection, there is a individual solution present in the network. At last all the protocols are integrated and applied to the network so that every attack can be prevented.

RELATED WORKS

Raman Singh and Amandeep Verma [9] have proposed a Dynamic Bandwidth Assignment Approach Under DDoS Flood Attack. The main objective of their approach is sustaining the server. Their approach had examined the traffic flow of legitimate user IP considering traffic volume. And then the traffic is categorized into two broad categories as genuine traffic and malicious traffic. The bandwidth allocated according to the traffic category. By achieving this, the hosts can provide services even when the server is under attack. Though the approach is simple, it degrades the system performance.

Chien-Min Su et al. [11] have proposed a Fuzzy Collision Danger Domain known as FCDD. Their technique have effectively established a ship collision avoidance decision system, and a Fuzzy Monitoring System (FMS). The main objective is navigation safety. They have analyzed the ship collision avoidance decision and provide optimal maneuver advice when a ship is in risk of collision. This method only one type of regions and one group of networks only. This should generalize to a number of applications.

The technology threat avoidance theory (TTAT) is proposed by Huigang Liang and Yajiong Xue in [12]. They have proposed this theory considering a huge amount of of theories and the relevant literature in psychology, health psychology, information systems, management, marketing, and finance. TTAT considering the scenario of avoiding threats in the perspective Information Technology (IT) user. The theory describes the avoidance behavior as a dynamic positive feedback loop. The loop encompass of two cognitive processes, threat appraisal and coping appraisal. In the process of threat appraisal, users will perceive an IT threat if they believe that they are susceptible to malicious IT and that the negative consequences are severe. The threat perception leads to coping appraisal, in which users assess the degree to which the IT threat can be avoided by taking safeguarding measures based on perceived effectiveness and costs of the safeguarding measure and self efficacy of taking the safeguarding measure. However, their TTAT does not focus on the present data sets present and easy to retrieve.

PROBLEM AND PROPOSED METHODOLOGY

Problem Definition

MPLS networks are widely used throughout the world in internet, mobile networks. Unwanted traffic and malicious effect of different nodes leads the network to an erroneous network, which is resulting in lower efficiency. One of the main causes of erroneous network is denial of service attacks. Generally the denial of service harms the network system both in the domain of hardware and software. A few types of DOS attack present in the network are ICMP flood, SYN flood, Teardrop attacks [7], Unintentional denial of service, Distributed attack [7], Asymmetry of resource utilization in starvation attacks and Nuke attacks [7] .

The first solution [5], which is for the enhancement of MPLS network through a swarm based algorithm, is described. In the previous paper [6] it is proposed to group the errors through fault detection. In this paper the solution is specified for a certain set of attacks based on time, and bandwidth. Both forward and backward checking is enabling the proposal to detect flood attack, SYN flood attack, ICMP flood attack, starvation attack. This type of errors needs to be expanded in a broader way. Denial of service attacks required to be solved through a good detection technique.

Proposed Methodology

The proposed methodology focuses DoS attacks and defines them in sub-domains.

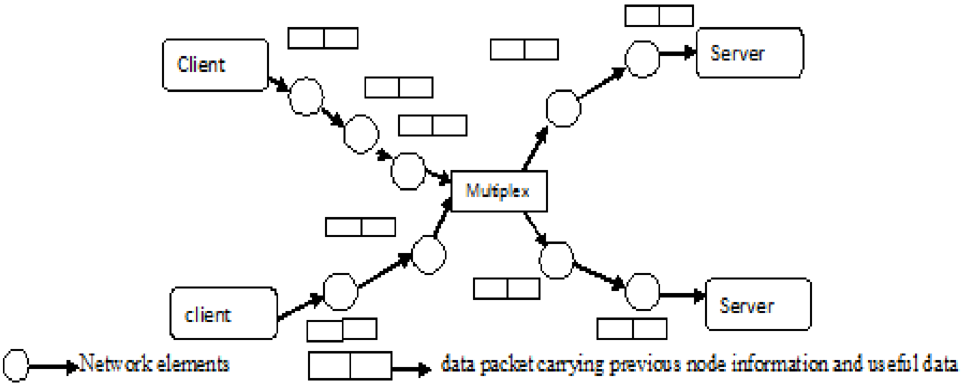

Client
Server
Multiplex
client
Server
Network elements
data packet carrying previous node information and useful data

Figure 1: Showing the Architecture of MPLS Network

This proposal focuses on the generation of data packet number. The data packet number consists of the sender's ID as well as the randomly generated packet number which is generated by the sender node (n_s). The data packet number is having extra bits, which are indicating the expected number responses from the specific receiver node (n_r). So that receiver nodes (n_r) can identify the sender node (n_s) and the number of data packets it serves to the specific node sener node (n_s) at different time. For the priority detection it is taking a ratio useful response generated to the total no of request send. This information is sent to every receiver node (n_r) (where the sender wants response) with the ratio by the sender (n_s). The data packet number, it gives the information about the sender. The data packet carries the a time variable in it. The total numbers of data packets at some time duration, with its usefulness generates the priority (p) at the receiving node (n_r). The receiver node (n_s) keeps the track of total requests through grouping the received data packets details in a sender based scenario.

The sender node (n_s) generates a data packet. The sender keeps the required information like current time, senders address, and useful data packet ratio and sends it to destination node (n_r) through long range data transmission systems. Procedure for Detection of bandwidth and delay is given in the previous paper [5]. Every data packet is given a unique ID number which is a combination of packet number [PN], number of responses required at sender (n_s) and last traveled nodes

ID (n_{r-1}). After getting a data packet a node, which may be a end receiver (n_s) or intermediate node (n_i) first verifies the destination. Then it examines the information available in it.

There are some data tables at the receiver node (n_r) and intermediate node (n_i). These data tables detect which type of attack it is facing. The data table stores the values like priority (p). Previously send data packet numbers (PN). The number of data packets required at a different time is analyzed according to the sender's address (n_s) at the receiver node (n_r). The sender's data packet carries the sender's address, useful data packet ratio (u_{dp}) of the sender node (n_s), the dependency value of the sender's node (NS) at certain times. The receiver node (n_r) detects the dependency ratio (d_s) through the ratio of the dependency number of nodes and total no of dependent nodes from all the request nodes. The receiver node (n_r) or the intermediate node (n_i) decides the priority (p) of the data packet, taking the average of dependency ratio (d_s), useful data packet ratio (u_{dp}). The sender has a data table. If a specific node (n_s) is sending a lot of ping packets without having high priority value then it is detected as ICMP flood. At this time the receiver has to stop its operation for a random time of period. If a lot of requests come for a certain data, having a high dependency value then it is treated as SYN flood. At this time receiver tries to get the original senders through sending a separate acknowledgement data packet. Distributed attack is detected through bandwidth factor. If the bandwidth factor is more than 0.95 then it is treated as distributed attack. A field checking table is present at receiver node. It just tracks the data packet fields. If the data is missing then the receiver (n_r) sends an acknowledgement to the sender node and prohibits more transmission from that sender node (n_s). This is the method for teardrop prohibition. For nuke attack detection this method proposes a data table present at intermediate nodes. This table stores the first senders ID, the time of the first time the first sender sends the request and total responses comes for the service from the final receiver. In long time if no response comes then it is treated as nuke attack. At this time the current node prohibits further transmission of data packet having the same address.

Procedure for Numbering the Data Packet

Generally, the entire field of a data packet in a network is sent as a character array. So it is proposed to make a character array for producing a unique number for every data packet. Every node has a node ID having X alphanumeric characters. The number of the data packet is also an alpha numeric. Suppose it is of N characters. The nodes which are also the part of the network are having X alphanumeric characters in their ID. Here the values of X and N was determined at the time of initialization of the network. The size (value) of X depends upon the number of the nodes present in the network. The value of N depends upon the amount of data packets required to send. Suppose X_1 is the last node travelled nodes ID. When a sender wants to get some data from any node, it will calculate the number of data to be received from the specific node. Suppose the amount is A number of data needed for this request. Considering all the above cases the data packet number will be AXN.

The following algorithm is given below-

```
String dataPacketnumber (){
        Random X= (string) new random (). ToString;
        Random N=new Random;
        Int A=getTotalReamiained ();
        String datapacketNum=null;
        datapacketNum=datapacketNum. Concate (A);
        datapacketNum=datapacketNum. Concrete (X);

        datapacketNum=datapacketNum. Concate (N);

        Return datapacketNum;

    }
```

Estimation of Available Bandwidth

The available bandwidth is determined based on the channel status and idle periods of the shared wireless media. As the transmission and reception of the data packets from other nodes affects the channel status, this method takes neighbor nodes behavior into consideration. The idle time (IT_i) consists of number of idle periods for the period of examining time interval and each node sums up all the idle periods in order to estimate the aggregate idle time. [13]

The ideal ratio δ for every time period t is computed using Eq (1)

$$\delta = IT_i / t \tag{1}$$

Thus the available bandwidth BW is given in Eq (2)

$$BW = \delta * B_c \tag{2}$$

Where B_c = raw channel bandwidth

Time Taken in Travel through the Medium

The time is estimated based on the time of receiving (T_1) the data packet at the node (n_{i+1}) and sending time (T_2) of previous node (n_i) is given in Eq.6.

$$\text{Travelling Time (TT)} = T_1\,(n_{i+1}) - T_2\,(Ni) \tag{3}$$

Here, T_1 (n_{i+1}) is the receiving time of the node (n_{i+1}), T_2 (n_i) is sending time of the previous node (n_i).

Details About Data Packet

The data packets are mainly divided into two parts. One part is for carrying the data; the other part is for information at the current node (n_i). The information present at the current node (n_i) is about the bandwidth available and current time (Ti) and the delay (Di) till the current node (ni). The method of calculation of bandwidth, delay is given in our previous paper [5].

Table 1: Showing Data Packet for Transmission

Available Bandwidth	Current Time	Number Of Dependent Nodes	Sender's Address(Ns)	Useful Data Packet Ratio	Data	Destination

Flood Attack Detection and Avoidance

For the flood attack detection the following table is present. The required scenarios are given below.

Table 2: Showing Table for Detection of Flood Attack

Sender's id	Timer1 (TR1)	Required Data (RD1)	Total Data send (DS)	Timer2 (TR2)	Required data (RD2)	Status

The receiver compares the required data numbers (RD2 and RD2). A transmission time calculation method is given above. The difference between the timer1 (TR1) and timer2 (TR2) is the standard transmission time (TT) given above. When the receiver (n_r) gets the data packet, it first checks whether any previous request present with the same sender's (n_s) address or not. If there is any record present then it checks the difference between required data at timer1 and required data at timer2 (RD2-RD1) is equal to total data send (DS) or not. If it is nearer to equal then the transmission is considered as attack free transmission. If there is more present, the attack is treated as flood attack. When a flood attack is detected, the receiver node (n_r) black listed the sender node (n_s) and does not accept any more data packet from that node. If the node (n_s) is detected as safe node (not producing any attack). It is further processed for the priority checking and further data transmission.

SYN Flood Attacks

Any node forged sender's address to attack through SYN flood attack. For this type of attack this method proposes an acknowledgement based attack detection technology. When a receiver gets a request data packet it has to send the acknowledgement to the node, from where it receives the acknowledgement. The acknowledgement data packet carries a data packet number and the first sender address in it. After receiving of any acknowledgement, nodes find the data packet belongs to itself or not. The below table is formed to detect the SYN flood.

Table 3: Showing the Parameters for SYN Flood and a Nuke Attack at Intermediate Detection

Data Packet Number Received	Data Packet Number Send	Timer-11	Acknowledgement Received (Yes/No)	Acknowledgement Send (Yes/No)	Timer-12
………………..	………………..	……	………………	………………..	……

When an intermediate node receives an acknowledgement; it first checks whether the sender's address matches with it. If the node is not the first generator of the request then it is sent to the previous node from it gets the data packet. When the data packet reaches the first sender, it verifies whether the request belongs to it. If the sender node finds the data packet is not belonging to it, then it informs all other nodes that SYN attack is there in the network.

Details of Acknowledgement Packet

The acknowledgement packet carries a data packet number, sender's address (act as the final destination for the acknowledgement packet), and the node address who sends the acknowledgement packet.

Table 4: Showing the Acknowledgement Data Packet

Data Packet Number	Sender's Address (Who Sends the Acknowledgement)	Receiver's Address (The First Sender)

Detection of Nuke Attack

When a node receives a data packet it checks whether the destination address matches with it. If the final address matches with the nodes with own ID then it is treated as receiver node or it will treated as intermediate node. Except the receiver (n_r) and sender (n_s) all other nodes are treated as intermediate node (n_i). Intermediated nodes are affected by nuke attack. Nuke attack is a waste of time and energy. To act against nuke attack, the nodes which are acting as intermediate node are keeping a table which is having the details of data packets processed through it and the intermediate node generates attack information in the network. The detail of data checking is given in table-3. If an intermediate node is not getting any acknowledgement of a certain sender's data packet within a standard time which is equal to time transmission

(TT) then the intermediate node declares a nuke attack in the network. At this time the intermediate node prohibits more transmission from the specific sender node (n_s) to another node in the MPLS network.

Priority Calculation Method

For the priority check-in, this method considers three parameters. The definition of parameters is already described. The priority is detected as P= d_s+u_{dp} (4)

Where d_s= data required for own service of the intermediate node (n_i), U_{dp}= useful data packet.

Where u_{dp}=total input of data packets/ total useful output of data packets (5)

$_s$= dependency ratio= total no of depend node on the sender (n_s)/total no of dependent on the specific node (n_r) (6)

Total no of dependent on receiver= $\sum_{i=0}^{n} \textit{dependent on}$ node (n_i) , where n is the total no of nodes communicating with the node (n_r) (7)

Asymmetry Research Utilization (Starvation Attack)

For starvation attack avoidance this method purposes the priority based data service. Further transmission of data packets and processing of the data packets; the intermediate nodes and end nodes use priority. To better use the available bandwidth this method uses priority based data transmission. Priority detection technique is already devolved. When a number of requests are coming to the receiver node (n_r) or the intermediate node (n_i) the priority based data transmission is done on the basis of the following table which is given in figure-5. The table consists of fields which having information about priority and data packet number. The Numbers of data packets send over a limited bandwidth line determined by the ratio of bandwidth to transmit one data packet to the total bandwidth available at the links.

Table 5: Showing Starvation Attack Avoidance Table Present at Receiver and Intermediate Nodes

Data Packet Number	Priority	Status (Send/ Discard)

ICMP Flood Detection

ICMP flood is the attack, which is caused when a number of nodes serve for a specific sender node having the same priority. This can be detected from the previous table 5 given. If the number of equal priority is more than the number of data packets the sender can serve, then the node is detected as an ICMP flood attack. At this time the node tries to shutdown itself for a random period of time.

To detect the number of requests the receiver node (n_r) can serve is given by

N= available bandwidth (BW)/ bandwidth required for single data packet transmission (BW (n)) (8)

Here N should be greater than or equal to the number of nodes having equal priority.

Data Table Present at the Sender Node for Detection of Black Holes

When a node sends any data packet to any node it is keeping the track of sending information. It starts a timer waits for the standard time to get the acknowledgement from the next node. The table is given below.

Table 6: Showing the Table Present at the Node for Sending Information

Data Packet Number	Transmitting (Sending) Time	Expected Time For Acknowledgement Receive	Status

If the node is getting any acknowledgement at a certain time distant then it is called to be attacked by the black hole. So black hole detection is a forward detection. It is detected at the previous node (n_{r-1}).

SIMULATION RESULTS

We simulated the design of our Integrated Protocol for Detection and Avoidance of Denial of Service Attacks in MPLS Networks (IPDA-DoS) with Network Simulator (NS-2) [14]. We consider the simulation topology given in Figure 2. The topology consists of 18 nodes.Different link bandwidth and delay are set for the all the links. We compared our results with the normal Attack strategy withour any detection technique.

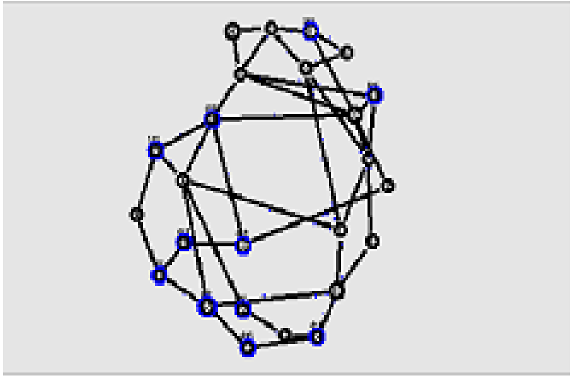


Figure 2: Simulation Topology

RESULTS

Based on Attackers: The number of attackers performing DDoS attacks is varied from as 1 to 4 and the performance is evaluated in terms of Attacked data, End-to-End delay and packet loss.

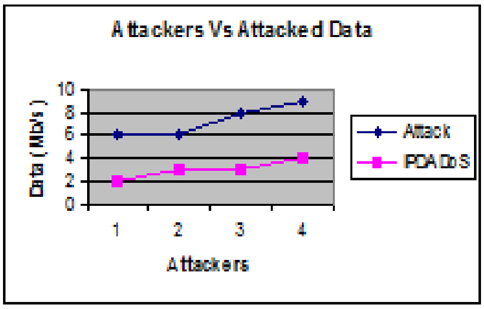


Figure 3: Attackers Vs Attack Bandwidth

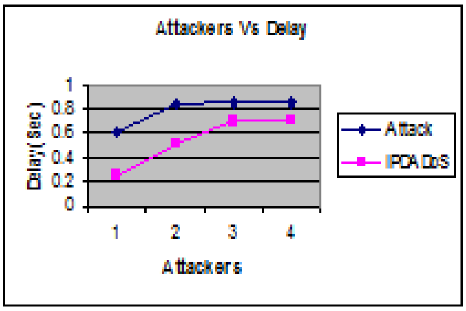


Figure 4: Attackers Vs Delay

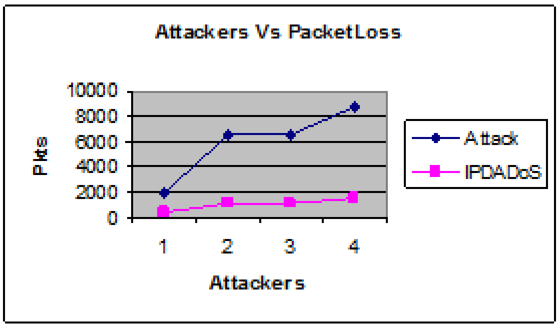


Figure 5: Attackers Vs Packet Loss

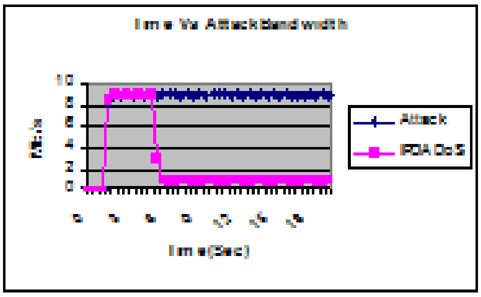
Figure 3 shows the fraction attacked data when the number of attackers is increased from 1 to 4. It is trivial that the increase of attackers results in more attacked data and packet loss. From figure 3, we can see that the attacked data of our proposed IPDADoS is 58% less than the normal attack scenario.

From figure 5, we can see that the proposed IPDADoS reduced the packet loss to 75% when compared to the attack Scenario.

From figure 4, we can see that the delay of our proposed IPDADoS is 32% less than the existing attack Scenario.

Based on Time

In our second experiment we analysis the metrics based on the time.



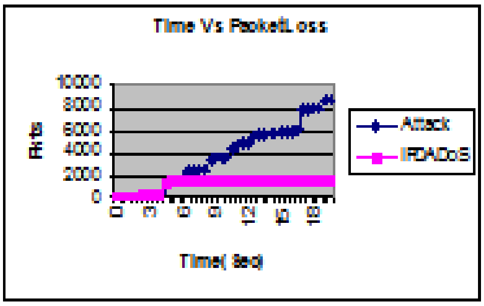


Figure 6: Time Vs Attack Bandwidth

Figure 7: Time Vs Packet Loss

From figure 6, we can see that the attack Bandwidth of our proposed IPDADoS is less than the existing Normal attack scenario. From figure 7, we can see that the packet loss of our proposed IPDADoS is less than the existing Normal Attack Scenario.

CONCLUSIONS

In this paper, an Integrated Protocol for Detection and Avoidance of DoS attacks in MPLS networks has been proposed. While most of the previous works focuse only on distributed DoS attack,.this paper describres about the sub domain of DoS attacks. The protocol can able to detect the errors like ICMP flood, SYN flood, Distributed attack, Asymmetry of resource utilization in starvation attacks, Nuke, Teardrop attacks. This protocol can detect attacks in both UDP and TCP transmissions. Different module for different types of attack detection provides the facility of attack detection of a single type at a single time. It is the user’s choice to choose the detection method for a specific type of attack. Simulation results show that the proposed protocol reduces the fraction of attacked data and packet loss. This approach can be more improvised adding more error detection techniques and adding effort to detect the errors from a single data table.

REFERENCES

1. XiboWang, Zhen Zhang,” Design of Embedded WEB Remote Monitoring System Based on mC/OS-II Operating System”, International Journal of Intelligent Engineering and Systems, Vol.5, No.1, 2012

2. Muhammad Kamran and Adnan Noor Mian, “Multiple Fault Tolerance in MPLS Network using Open Source Network Simulator”, Proceedings of the 4th International Conference on Open-Source Systems and Technologies (ICOSST ‘10), 2010

3. Jong Tae Park, Senior Member, IEEE, Jae Wook Nah, and Wee Hyuk Lee,” Dynamic Path Management with Resilience Constraints under Multiple Link Failures in MPLS/GMPLS Networks”, IEEE Transactions on Dependable and Secure Computing, Vol. 5, No. 3, 2008

4. Eusebi Calle,” Enhanced fault recovery methods for protected traffic services in GMPLS networks”, Universitat de Girona, February 2004

5. Venkata Raju S, Dr. Govardhan A and Dr.Premchand, “Swarm based Fault Tolerant Routing in MPLS Networks”, International Review on Computers and Software (IRECOS), March 2013, Vol. 8. n. 3, pp. 770-778

6. Venkata Raju S, Dr. Govardhan A and Dr.Premchand, ”Fault Detection and Grouping of Errors in MPLS Networks”, Accepted for publication in Journal of Theoretical and Applied Information Technology,

7. Jouravlev, I., "Mitigating Denial-Of-Service Attacks On VoIP Environment", The International Journal of Applied Management and Technology, pp-183-223, 2008

8. Felipe Huici, Mark Handley” An Edge-to-Edge Filtering Architecture Against DoS”, 200X ACM

9. Amandeep Verma, Raman Singh,“A Dynamic Bandwidth Assignment Approach Under DDoS Flood Attack**”,** Journal of Advances In Information Technology, VOL. 3, NO. 2, MAY 2012

10. Munish Sharma and Anuradha, “Network Intrusion Detection System for Denial of Service Attack based on Misuse Detection” , IJCEM International Journal of Computational Engineering & Management, Vol. 12, April 2011

11. Chien-Min Su, Ki-Yin Chang, and Chih-Yung Cheng,” Fuzzy Decision On Optimal Collision Avoidance Measures For Ships In Vessel Traffic Service”, Journal of Marine Science and Technology, Vol. 20, No. 1, pp. 38-48 2012

12. Huigang Liang, Yajiong Xue,” Avoidance of Information Technology Threats: A Theoretical Perspective”, Liang & Xue/Avoidance of IT Threats,2009

13. Noureddine Kettaf, Hafid Abouaissa, Thang Vuduong† and Pascal Lorenz,” A Cross layer Admission Control On-demand Routing Protocol for QoS Applications”, IJCSNS International Journal of Computer Science and Network Security, VOL.6 No.9B, September 2006

14. Network Simulator, http://www.isi.edu/nsnam/ns

AUTHOR’S DETAILS

Venkata Raju Sagiraju is Pursuing Ph.D in Computer Sciences and Engineering from Osmania University, Hyderabad, India. He obtained his Bachelor’s degree in Biomedical Engineering and Masters degree in Computer Sciences and Engineering from Osmania University College of Engineering, Hyderabad. His career began as a Customer Support Engineer and further served as Lecturer in GIOE and as Assistant Professor in Osmania University. Currently, he is working as Director of Shubh Soft Solutions Pvt Ltd, Hyderabad, India, where he created the customer support team and was responsible for all pre/post sales technical support and he is serving as Professional Services Consultant to Juniper Networks. He has published 10+ research papers at national and international level as well as being awarded with the young scientist fellowship from Andhra Pradesh Council of Science and Technology (APCOST), India. He is a fully qualified Juniper and Brocade Networking and Solutions Architect and holds the recognized highest level certifications which include Juniper Networks Certified Internet Expert (JNCIE#151) and Brocade Distinguished Architect (BDA#19).

Dr. Govardhan Aliseri obtained his Bachelors degree in Computer Science and Engineering from Osmania University College of Engineering,Hyderabad in 1992 and M.Tech from Jawaharlal Nehru University(JNU), Delhi in 1994 and he earned his Ph.D from Jawaharlal Nehru Technological University, Hyderabad (JNTUH) in 2003. Currently he is working as Director of Evaluation and Professor in JNTUH, Hyderabad. He joined Jawaharlal Nehru Technological University in the year 1994 as an Asst.Prof, became Associate Professor in 1999 and Professor in 2006. He is a member for Standing Committee for Academic Senate, JNT University Hyderabad and Academic Advisory Committee (AAC), UGC-Academic Staff College, JNT University Hyderabad. He has guided 100+ M.Tech projects. He has 100+ research publications at International/National Journals and Conferences. He is a Member on the Editorial Boards for International Journal of Emerging Technologies and Applications in Engineering Technology and Sciences , International Journal of Computer Applications in Engineering, Technology and Sciences , International Journal of Advanced Computing , International Journal of Data Engineering and Computer Science , International Journal of Computational Intelligence and Information Security and Technical Committee & Editorial Review Board, World Academy of Science, Engineering and Technology. He has been listed as one among the Top Three Faculty in JNTU Hyderabad made by Outlook Survey for the year 2008.

Dr. Premchand Parvataneni obtained his Bachelor’s degree in Electrical Engineering and Masters Degree from Andhra University, Visakhapatnam, India and he earned his Ph.D from Andhra University. Currently, he is working as Dean, faculty of Engineering, Osmania University, Hyderabad. He joined as Lecturer in Andhra University in the year 1985 and further joined as Associate Professor at Osmania University in 1991 and became Professor in 1999. He served as the Director for AICTE, New Delhi during the years 1998 and 1999. He also served at various roles in improving academics which include Addl. Controller of examinations, Chairman for Board of Studies and Head of Computer Sciences Department in Osmania University, Hyderabad. He has guided 100+ M.Tech projects. He has 100+ research publications at International/National Journals and Conferences.