www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 6 Issue 3 March 2017, Page No. 20790-20793
Index Copernicus value (2015): 58.10 DOI: 10.18535/ijecs/v6i3.70

Reliable and Intelligent Automated Networking Framework for Internet Networking

[#1]A.P.V. Raghavendra,[#2] T.Mohanapriya, [#3] T.Brindha
raghu221084@gmail.com, tmpriya97@gmail.com, strbrindha@gmail.com
Department of Computer Science and Engineering
V.S.B Engineering College Karur, Tamilnadu

***Abstract*— A Self-Healing Network is one, which is used to focus on how to reduce the complexity and cost of the management of dependability policies and mechanisms without human intervention. It also has to monitor the Network Traffic to predict the abnormal traffic patterns. The main objectives of this Self-Healing Network is to spot the problems before they occur, to know immediately when problems arise, to share available data with stakeholders, to detect the security breaches i.e., this network aims at ensuring that the service will continue to work regardless of defects that might occur in the network. One of the problems is chosen to solve as an initial work. When users are accessing any service from the server, the server may unexpectedly close the connection, thus sending an empty response. The tool designed tries to rectify this problem without the knowledge of the user and thus avoids manual fixing of this fault. Nowadays , Internetwork outer surfaces the some of the challenges and tasks based upon the utilization and incremental growth of the users. Prerequisites involved in the network are multipath, multi-home, mobility etc. Here we discussed the techniques which increases the employability of user data transmission through the multipath. Although the several techniques involved, in this paper we target the tunnelling strategy based upon the scalability, performance and time consumption is regarded.**

***Keywords*—** Self healing, Manual fixing, Abnormal traffic, multipath, tunnelling

I. INTRODUCTION

There are two approaches entangled the intelligent automated network framing. The first approach defines Self healing systems are which rectifies a problem occurring in a network and does the necessary adjustments and bring back to the normal condition without the intervention of human. In other words, self healing systems returns back to the healthy state from the unhealthy state without human intervention[3] and the awareness of the users. However the complete mechanism requires human intervention in some way. For example, to make the self healing system successful, human have to perform the designing of template with large training data sets, set parameters and so on. The intervention of human should be lowered in this case also, which is a challenging and a hot area of research. Maintenance of such systems are also so important, due to the dynamic changes in the network.. Another important factor to note is the time taken for recovering must be insignificant. The time taken is expected to be less than that of the time taken by a manual recovering of the problem. Fixing the faulty component and the cause of component is a major challenge which may consume time. There are many issues and challenges in implementing a self healing network. The second approach defines ,multipath is a one of the challenge faced by the network. In which to send a packet from one end to other end multiple paths are described among that, the path which is near to the other end is chosen under the control of ISP(Internet Service Provider).In a single path network it is appropriate one when the more number of resources and several customers included ,this strategy is quite challengeable. In order to improved the network criticality tunnelling and tunnelling under based protocols are utilized. It has the capability to create a virtual links between the source end and destination end[2].By the help of virtual link,the data which is being transferred from one end to remote location user end is secured in a public network even the multiple path connections available. In the way of looking data secure transmission is done in virtual private network under the public network.

This paper focuses a common problem one that is faced in most of the services offered through web, as the initial part of work. Even when the connection exists between the client machine and the remote server, the server sends an empty response message. The possible reasons can be, the server closed the connection from any other remote client; low bandwidth available to transfer the data, so that only the header part is sent without the response message. Normally, this problem is solved by the user by reloading the page again and wait for the response. The work tries to solve this issue by means of a software tool installed at the server. The tool continuously monitors the communication between the server and the client. All the response from the server to the client are sent via the tool. In case of empty response, it tries to solve the issue. The tool designed has to employed with proper security policies.The second problem is security of data beneath the multipath routing.In a virtual private network 2 address implied the end hosts,the first address is a IP address known by all other hosts encircled in the public network.and the second IP address is known by the private network host only.This IP address is called the virtual address.Through this way security is handled.

II. RELATED WORK

A. Self healing and reliable framework

In a network, numerous problems can occur during the communication. Some of them are, prediction of traffic, unauthorized events , ... Most of the problem occur due to security breaches in the network. To the make the network self adaptive to the changing environment, a monitoring infrastructure is constructed which operates at runtime[4]. This monitoring system works on various levels of abstraction. The maintenance of such system may be a tedious process. Another approach is to use a mirroring strategy to identify the issues from external agents[5]. Regeneration is another method followed in self healing systems[2] which involves self assembly of components. It makes the system self configurable to changes. It also involves addition and removal of components. Methods have been formulated to track several parameters like RSS, BER which helps in detecting the kind of defects[6]. There are several issues in network to be analysed and to be solved without human intervention, to make the network self protected. This paper focuses in healing the communication issues between the web server and client.

B.Need of multipath routing

The notification of multipath routing problems are tremendous when the reliable future network has a extremely large resources . Specifically , securable nature of data is influenced .To rectify that some of the multipath routing protocols is deployed on the basis of purposes like reliable data transmission and efficient resource utilization for instance Reliable Information Protocol, Multipath Multispeed Protocol and N-to-1 Multipath Routing Protocol etc[4].Then the Layer 2 tunnelling protocols(L2P) is also played the vital role in securable data transmission such as Cisco's Layer 2 Forwarding Protocol(L2F) and Microsoft Point to Point Tunnelling Protocol(PPTP)[4].Especially ,we focuses on Tunnelling Protocols in order to manage the security of data, efficient data usage and encrypt/decrypt of packet addition with a basic purposes.

III. DESCRIPTION

The monitor tool continuously monitors the activity of the server. It listens the communication between the server and the other clients continuously. When the server sends an empty response, the tool tracks it. The response is not sent to the client, the client is made to wait for a while. The two main reason for this problem is: the server may close the connection because of the response from any remote client; the server may able to send only the header part, and unable to send the body part of the response, which may be due to low bandwidth available to transfer the data. To rectify the first problem, the tool checks for active connection. If the connection is closed, it establishes the connection with the help of the credential observed from the client. This is done without the knowledge of the client, so that the client is unaware of the error occurred.

A.Architecture

In this paper the communication in web is considered. Many services are offered through web. The servers which are responsible for providing the required operations is installed with the designed tool. When a communication is established between the client, the software records all the credentials in a log.

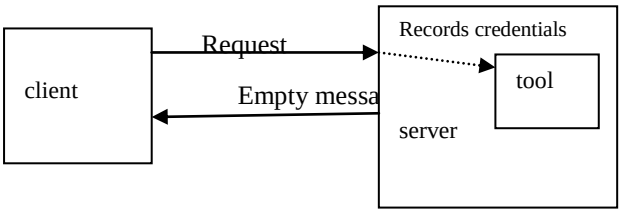

Fig:3.1 unsuccessful communication

The common problem faced by most of the users while accessing a service is that even in case of active connection the server sends an empty message due to several issues. In this case, the user have to manually reload the page or change the browser settings. To overcome this, the proposed tool monitor the communication continuously, and rectifies this problem by itself, so the users are not aware of the problem occurred.

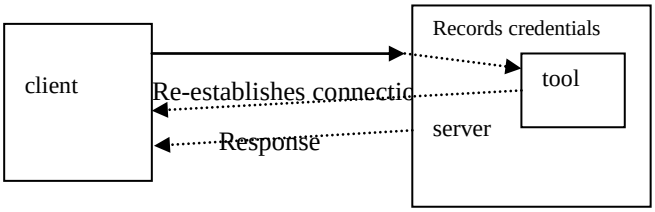

Fig 3.2: Server is about to send empty message

All the response from the server is sent through the tool only. When it is about to send a empty message, the tool re-establishes the connection between them with the recorded credentials. Also tries to prevent closing the connection from the remote client. Thus the tool tries to sustain the connection between the communicators and prevent the users being aware of the issues occurring while in communication.

B.Features

The designed tool is installed in the server. It acts as the server itself while re-establishing the connection between them. The various features of the healing tools are,

- Continuous monitoring : The tool is always active from the server start up
- Tracking the response of the server : All the response of the server are sent through the software tool designed, which helps in tracking
- Withholding the empty response : If any empty response is sent from the server, the tool does not allow to forward this message to the client
- Re-establishing the connection : The tool establishes the connection again with the client without the notice of the client
- Make server ready to provide its service : After establishing the connection, it directs the server to provide the service

These features make the client-server communication occur without any disruption, thus making the server communication reliable one.

C.Design

The implementation of the tool depends in the kind of web server used. It has to be compatible with many kinds of severs. Also, it should require less memory so as to reduce the cost of installation. The credential of the clients is recorded in the tool,

DOI: 10.18535/ijecs/v6i3.70

but it is released when the client has closed the connection with the server. It supports some of the server's functionality which helps in re-establishing the connection between the client. Scripting languages can be used to provide dynamic property.

IV. Multipath provision

The targeted part in this paper is securable data transmission in a public network along with the involvement of multipath .Apart from that , extremely large positiveness is done. Those are multipath bring the load balancing ,Fault tolerance and increment of bandwidth[2]. The load balancing is achieved by multiple paths when data traffic is being disseminated[6]. By using multipath ,conjestion and time consumption is lowered[4].The following figure4.1 show the provision of multipath in a reliable network .In other words, the source end sends a data packet to the destination end where many source ends are participated. The point which is being noticed in this data transmission is data traffic of the entire network is meet at a specific end where the multiple paths are relied.

From this fiqure 3 source ends are participated where each source ends have 2 individual paths to the same destination end. Those paths are denoted as multiple paths from that the suitable path is selected to transmit the data based on some premises such as time consumption,path cost etc.

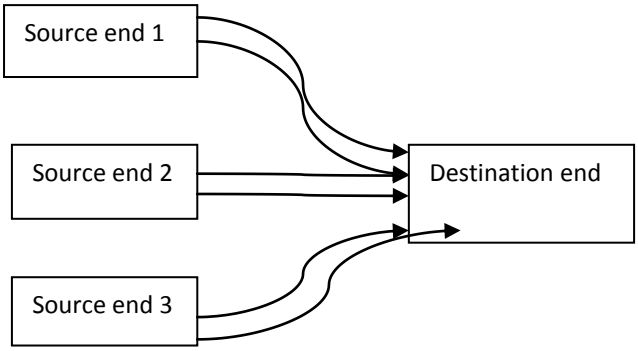

Fig 4.1 Multipath routing

As already detailed, secure data transmission is executed with the help of tunnelling technique such that we are proceeded. The implementation of tunnelling(Port forwarding) move under private network surrounded by th public network where the unique identification is progressed with the IP address ,Virtual link address[4].The fiqure 4.2 shows the implementation of tunnel approach in a wide area network.S1,S2,S3 are the source nodes under a particular network where ISP provides a control to the network nodes to perform data transmission and the destination node is represented as DS. The multiple lines drawn between the ISP and Public network is called a tunnel through which the data packet sent in a secured mode. Where the addresses IP, Virtual address are utilized by the communication nodes.

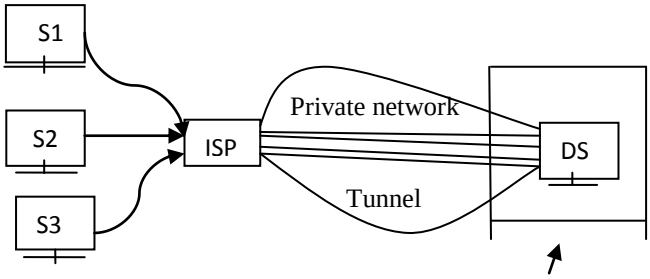

Fig 4.2 Tunnelling technique

That tunnelling approach is progressed under the private network where only we can bring the secure nature to the data packets. By the way ,Tunnelling approach is proceeded in a routine manner.

V. CONCLUSIONS

Software based self healing systems, is sufficient to provide most of the solutions. The designed tool is expected to track the server's response to client. It provides a reliable communication by intelligently tracking and solving the problem. As these systems are typically recovery oriented, they can take their own decision on how to come back to normal state from a broken state .Even though ,the tunneling technique contributes security, scalability and flexible nature to the packets some of the restrictions counted on it which is dial opening act on the network systems[2].Those things to be recovered in future.

VI. FUTURE ENHANCEMENT

There are many issues that occur in a communication between a client and a web server. As the initial part of the work, the empty response problem is tried to be solved. The designed tool has to be compatible with all kinds of servers. Other issues like internet slow down, internet bots are tried to be solved.

REFERENCES

[1] Keun-Woo Lim1, Woo-Sung Jung1, Young-Bae Ko1and YoungHyun Kim2 International Journal of Smart Home Vol. 7, No. 2, March, 2013On the Self-Healing Mechanism in Smart Grid Networks

[2] R. Nagpal, A. Kondacs, C. Chang, Programming methodology for biologically-inspired self-assembling systems, AAAI Symposium, 2003

[3] Debanjan Ghosh , Raj Sharman , H. Raghav Rao , Shambhu Upadhyaya,
2185 Self-healing systems — survey and synthesis, Decision Support Systems 42 (2007) 2164

[4] S.W. Cheng, D. Garlan, B. Schmerl, P. Steenkiste, N. Hu, Software
architecture-based adaptation for grid computing, The 11th IEEE Conference on High Performance Distributed Computing (HPDC'02), Edinburgh, Scotland., 2002.

[5] N. Combs, J. Vagle, Adaptive mirroring of system of systems architectures, Proceedings of the FirstWorkshop on Self-Healing
Systems, 2002.

[6] Chu, Eunmi , Korea, Bang, Inkyu ; Kim, Seong Hwan ; Sung, Dan Keun,Self-organizing and self-healing mechanisms in cooperative small-cell networks, 24th International Symposium on Personal Indoor and Mobile Radio Communications, 1576 – 1581

Authors:

Mr.A.P.V.Raghavendra is persuing Ph.D. from the MANONMANIUM SUNDARANAR UNIVERSITY, Tirunelveli, India from 2013

onwards and Completed M.Tech(CSE) degree from Bharath University, Chennai, India in 2009. He is a Member in ISTE

New Delhi, India, IAENG, Hong Kong. He has the experience in Teaching of 7+Years and in Industry 1 Years. Now He is currently working as an Assistant Professor in Computer Science and Engineering in V.S.B Engineering College, Karur, Tamil Nadu, and India. His research interests include Data Mining, Data Bases, Artificial Intelligence, Software Engineering Networking etc., He had published 2 Annexture – II Scopus indexed, 3 IEEE Conference Journal publications, Collectively 29 international publications. He had participated in several workshops and international conferences and presented papers.

Ms. T.Mohanapriya – Currently Persuing the Bachelor Degree(CSE) in V.S.B Engineering College, Karur under Anna University of India. Her research interests include Networking and Datamining. She is pursuing another degree B.A (HINDI) in Dhakshana Bharat Hindi Prachar Sabha, Delhi. She has participated in several symposiums and workshops and also won the award from the KONGU ENGINEERING COLLEGE,Thirucengode,Erode.

Ms. T.Brindha – Currently Perusing the Bachelor Degree(CSE) in V.S.B Engineering College, Karur under Anna University of India. Her research interests include Networking and Datamining.