Automatic System Packet Generation & Testing of the Network Communication Lines in Network Data Transmission

Sujata Shirwal[1] Manikamma Malipatil[2]
[1]PG Student [2]Assistant Professor
[1,2]Department of Computer Science & Technology
[1,2]Godutai Engineering College for Womens, Kalburagi, Karnataka, India

Abstract— As Networking getting larger and more complex now a days, administrators rely on rudimentary tools and many to debugging problems. Hence we have proposed an automatic systematic approach for the purpose of testing and also debugging networking known as Automatic Test Packet Generating system. ATPG reads every single type router configurations later produces a device independent model. This model is later used for generating minimum set of testing packets to exercise every possible link in the system networking to work with every rule of networking. The Testing packets in the work are transmitted in cyclic manner, detected failure will trigger a separate mechanism for the sake of localizing the fault. It can also detect both the functional and also performance problems. Testing packet in the network goes beyond earlier work for static checking an also localization of faults.

Key words: ATPG (Automatic test packet generation), mac (Media access control), IP (internet Protocol), ISP (internet service protocol)

I. INTRODUCTION

Communication networking is basic idea for every single type of relating to the connected end systems and also their connectivity. It is very often used in the world of connected end systems and their use in different connections. The term communication networking states that the link between many connected end systems and the devices, with vital purpose of sharing data which has been stored in the computer systems, with each other. The network between computing devices which are common now a days due to launching of various hardware components and software components which emphasis in the making the available system activity more convenient to the communication.

General Networking Techniques - The connected end systems communicate on a sniffle or multiple networking , they send out data knowing anyone listening or not. In Connected end systems networking every single type connection to wireless or wired networking which is known as the networking bus. For the different computers distinguish between each other, every single computer has an ID every single type mac id (Media Access Control). This is not only unique for any networking also unique for most of devices that can be linked to system of network . The address is bind with hardware not concerned with ip addresses. As every single type is connected to end systems on the networking receives and send files data which has been sent out from other connected end systems . mac-addresses mainly used for the connected end systems for filtering out the every single type of incoming network data traffic which is addressed for individual computer systems in network.

II. PROBLEM STATEMENT

Network has to be capable of handling the problems like Hardware failures, Software bugs, throughput degradations, reach ability failures etc . The system should allow the user to see and also able to solve the problem associated with it.

III. LITERATURE SURVEY

In [1] here the author proposed detector method is act every single type y based on the video representation which accounts for the both appearance and also for the dynamics, using set of total mixture of the dynamic textured models.

In [2],here author has develop the failure resilient based techniques to the monitoring state link delays. faults within a Service Provider system , Enterprising networking.

In [3],here author present an execution tool, NETEE TOOL, which is capable of checking automatically every single type of generating the tests such that it achieve a high coverage of range in diverse set of the multiple complex also environment of every single type of the y-intensive set programs.

In[4], here author presents the efficient and also structured techniques for the purposed the testing in modified controlling program. Networking tool will applies the model by checking the system explorer to the state of space in the entire computer system. Controller, system switches also the system hosts.

In[5], here Author propose Network diagnosing system ,an algorithm to detect the location of failures in internetworking environment. First, author adapt the Boolean technique for the work in this environment. The Network diagnosing system takes the main advantage of rerouted single paths, routing of the messages collected at every provider's networking and also Looking Glass of servers.

IV. PROPOSED SYSTEM ARCHITECTURE

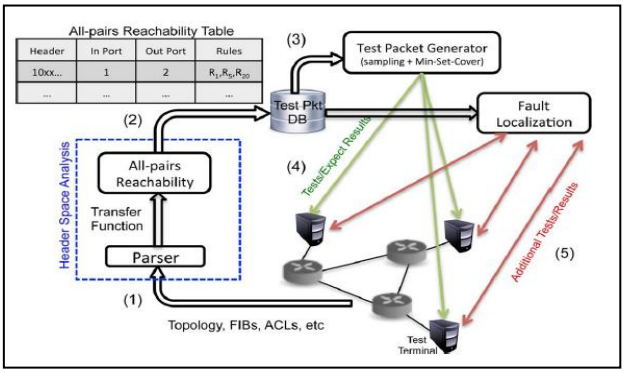

Fig. 3.1: proposed system architecture.

Above figure is diagrammatical representation of the ATPG system. It can be described in the following steps:

It initially collects all forwarding state from network. FIBs, ACLs, and configuration files, and access to topology. It uses Header Space Analysis for calculating contact between all the testing terminals. Result used by test packet selection algorithm for computing the minimal set testing packets in network which test all the rules Testing packets are sent periodically by end terminals In case of the error the fault localization algorithm o detect and trace the error cause.

V. MODULES

1) Generation of the Testing Packets
2) Generating Every single type of test packet
3) ATP Tool
4) Process of Fault Localization

VI. DESCRIPTION OF THE MODULES

A. Generation of the Testing Packets

In this process we assume that set of the testing link terminals in the present networking system can send and also it can receive the testing packets in network. Main goal is to generate set of testing packets in the work to execute the every rule in possible every switching type function, any type of the fault will be observed, at least one testing type of the packet.

Proposed is analogous for the software test suites, such that it will try to test the every possible linked branch in the program. As the broader the goal it can be limited for testing in every link and also every type queue. When system is generating the testing packets in the supported work, and also an Header.

This process can be listed as follows;

Initially user create the node as N1 N2 N3

The testing packet supported but the user wish is passed to the nodes by using one node as an intermediate node. This message is passed through the nodes and reached the destination

B. Generate every single type -Pairs Reachability Table

Testing packet in the network starts it by computing the total complete set of the packet headers that it can be sent from each of the testing terminal for possible every other testing terminal. Each such type header, testing packet in the network has to finds the possible complete set of rules which exercises along the path. For doing this, testing packet in the network has applies the every single type pairs in the reachable algorithm described. On the possible linked every terminal port, every single type header it is applied to the system for transfer function the first type of switch connected for each of the test terminal. Header constraints should be applied here.

C. Testing Packet in the Network Tool

Testing packet in the network produces the minimal number of testing packets in the work such that every type forwarding rule in the networking system it is exercised and also covered by at least possible one type of test packet. When a system or packet error is detected in system, testing packet in the network it uses a fault localization algorithm for determine the system failing rules and also links.

D. Locate the Fault.

Testing packet in the network has periodic in every possible single type y sends a set of testing packets in the wireless work. When a testing packets in the work has failed, the testing packet in the network suggests the fault(s) that has caused the problem. A rule fails if and its observed behaviour has differs from its previous fixed expected behaviour. , testing packet in the network has to keeps track of where the rules failed and using the result function success and also the failure depending on the nature of the processed type rule. An forwarding rules fails if an system based test packet has not been delivered to intended output system port, where as an dropping system rule behaves as it correctly when packets has been dropped. Similarly, a system link failure is a type of the failure of a forwarding rules in the system topology function. Or if an output link has a congested, failure process captured by the system latency of testing packet going to the above a predicted threshold value.

VII. CONCLUSION

By the proposed work of automatic test packet generation system we have achieved the successful goal of receiving the test packets through the help of the intermediate node and also directly with the respected routers. The ATPG tool is capable of capturing the problem in the system to realize it and also it provides the solution. A ticketing scheme has been adopted to achieve the system problem reporting concept to achieve the higher efficiency.

ACKNOWLEDGEMENT

I have taken efforts in this project. However, it would not have been possible with the kind support of My Guide Asst. Prof. Manikamma Malipatil and help of many individuals and organizations. I would like to extend my sincere thanks to all of them.

REFERENCES

[1] P. Barford, N. Duffield, A. Ron, and J. Sommers, "Network performanceanomaly detection and localization," in Proc. IEEE INFOCOM,Apr. , pp. 1377–1385.2004
[2] Y. Bejerano and R. Rastogi, "Robust monitoring of link delays and faults in IP networks," IEEE/ACM Trans. Netw., vol. 14, no. 5, pp. 1092–1103, Oct. 2006.
[3] C. Cadar, D. Dunbar, and D. Engler, "Klee: Unassisted and automatic generation of high-coverage tests for complex systems programs," in Proc. OSDI, Berkeley, CA, USA, 2008,
[4] M. Canini,D.Venzano, P. Peresini,D.Kostic, and J. Rexford, "A NICE way to test OpenFlow applications," in Proc. NSDI, 2012
[5] A. Dhamdhere, R. Teixeira, C. Dovrolis, and C. Diot, "Netdiagnoser:roubleshooting network unreachabilities using end-to-end probes and routing data," in Proc. ACM CoNEXT, 2007

