ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2016

A Comparative Approach on Automated Test Packet Mechanism for Monitoring Faults in Network Failures

L. Pavithra[1], Dr. P. Ponmuthuramalingam[2],

Research Scholar, PG & Research, Dept. of Computer Science, Government Arts College (Autonomous), Coimbatore, India[1]

Associate Professor, PG & Research, Dept. of Computer Science, Government Arts College (Autonomous), Coimbatore, India[2]

ABSTRACT: Networks are becoming very massive and tangled in the real world environment, where the current Internet infrastructure and protocols have been developed. This has lead to a diversification in the way the Internet is used, and therefore changed the requirements of the network. Many traditional techniques and models are used to determine the availability and failure for rates of networks. But Manual performance tuning and diagnosis of such models is hard as the amount of relevant performance data is large. The methodologies mentioned in proceeding section will emphasis, how to detect the network failure more accurately and how to diagnose them effectively in a dynamic way. From the analysis it is evident that this approach will work competently to provide a solution of network failures than the existing models in terms of performance, latency and throughput.

KEYWORDS: Test packet generation, Network troubleshooting, Latency, Fault Monitoring

I. INTRODUCTION

The demand for sophisticated tools for monitoring networks utilization and performance has been growing rapidly by the Internet Service Providers. Tools used in network management tasks ensures service level agreement compliance, fault and congestion detection, performance debugging. The tools are effective and reliable when they are used in small set of networks. When they face Multi-server distributed systems, they are less effective. The tools need to provide high throughput with low latency, which is crucial to achieve with the networks now. Manual performance tuning and diagnosis is not possible with the networks since the data set is too large. It is very hard for the network engineers to detect lacking, fibre breakages, unidentified labels and programmable bugs.

Networks specialist use ping, trace route and tcp dump to find the exact bug rising factor in a system. But this type of monitoring techniques fails when the number of switches in the system increases. These type techniques fail in three reasons [1]: i) The sending state is not dynamic over the switches and firewalls. ii) They require physical logging of the system.iii) Many people are contacting the system at the same time.

Network monitoring systems used now monitor each malfunctioning of the system such as switch system administrator using messaging system, mails and alarm systems. They are done software application packages and tool. Sometimes the analysis of the HTTP codes is the simplest way of monitoring the web pages, such as 404 and 20616 in the case of small network system.

Network monitoring tool uses data for monitoring traffic, video monitoring, stream monitoring and others. [2] Intrusion detection monitors the network threats for the system outside such as overloading of servers, crashes in servers and network connections. The bug fixes in the system can also be as connections which are not established, server time out, message or document not retrieved. These kinds of monitoring will be more reliable when they handle less data source in the system. [3] The conflict between the data occurs when there more servers in different multiple

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2016

areas which will indeed increase the complexity of managing the networks, frequently monitors the system and notifies the drawbacks of this system are lack of live capturing, bugs routing and other latency and throughput problems. The main objective of this work is to analyse and make networks with more throughout.

II. LITERATURE REVIEW

In this section various previous research methodologies that have been conducted in terms of identifying the network failures are discussed briefly.

Yigal et al [4] introduced a two-phased approach for monitoring that enhances complete coverage of the network in the presence of the link failures and minimizes the monitoring overhead on the underlying production networks. This computes location with minimal sets of stations covering all networks even with failures. It also covers the computed ranges of probe messages to send by each station, such that the latency of network link are isolated. They proposed a polynomial-time greedy optimization algorithm which helps to achieve close to the best possible approximations and probe assignment problems.

The previous research does not suit for the liveness of the networks since the technique use base station and many assignment problems which are not very feasible and hard to detect.

Manjula et al [5] introduced a combined user-driven navigation analysis along with the automatic correlation and comparative analysis methods. The method uses number of performance methods such as collecting the performance counters data, visualizing the data, threshold analysis, correlation and comparative analysis of data. The system provides detailed view such as 3D plot, Server view, and Time view. These visualizations of data help in the network people to get more insight about the network issues.

The following research has a drawback is that the system cannot identify the root causes where the new counters are created in the performance counters technique and this does not provide the best feasible debugging results.

Hung et al [6] introduced a technique for locating multiple failures in service providers or enterprise IP networks using active measurement. The approach has 2 phases that reduces both the excess traffic due to probe messages and the measurement infrastructure, costs. The first phase uses the elements from max-plus algebra theory; we show that optimal set of probes can be determined in polynomial time. The second phase, gives the optimal set of probes. It helps to compute the location of the failure points.

The previous research provides a maximum set of the optimal probes for determining the polynomial time, but the generation of probes requires more cost.

Marina et al [7] introduced an approach for anomaly detection namely statistical method, Streaming algorithms and Machine learning. Statistical method includes Wavelet analysis, Covariance matrix analysis and Principal component analysis. Streaming algorithms provide significant changes in traffic patterns such as traffic volume or the number of traffic connections. Due to high link speed and large scale size of the Internet, it is usually not scalable to track per-flow status of traffic. Machine learning approaches attempt to obtain an network failure that adapts to measurements, changing the network conditions. Mapping of data is done using the training sets of data and the failure point is found. The final step of this approach is to create Generalized Likelihood Ratio (GLR) test that can be determined the network failure point.

The above research fails in understanding the data sets which are used for anomaly detection, and these results in false end points of the network diagnosis point.

Marco et al [8] introduced a centralized programming model, where a single controller program manages the network seems to reduce the likelihood of bugs. No Bugs In Controller Execution (NICE) tool applies model checking to explore the system space - the controller, the switches and the hosts. The tool helps to uncover bugs in the open flow program, through a combination of model checking and symbolic execution. The tool is used for automated testing of open flow applications that combine model checking and execution in a novel way of quickly exploring the bugs in networks.

In the previous research, it seems to very challenging since they require large space of switch state, large space of input packets and large space of event ordering.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2016

III. COMPARISON ANALYSIS

In this section, all the research methodologies that are introduced and discussed in the detailed manner and their pros and cons are given as like follows:

Table 1. Comparison Analysis of different research methodologies

S.NO	TOPIC	METHOD	PROS	CONS
1	Robust Monitoring of Link Delays and Faults in IP Networks	Polynomial- Time Greedy Approximation	Enhance complete coverage of the network in presence of the link failures and minimizes the monitoring overhead on the underlying production	The base station and probe assignment problems are hard to detect and they do not suit the liveness of the network
2	Performance Anomaly Detection in Multi-Server Distributed System	Automatic Correlation And Comparative Analysis Technique	It helps to reduce developer's time and efforts in detecting anomalous performance cases and improve developer's ability to perform deeper analysis.	Cant able to analyse root causes in new counters.
3	Active Measurement for Multiple Link Failures Diagnosis in IP Networks	Two Phase Technique	It minimizes the additional traffic due to the probe messages and the measurement infrastructure	Probing costs is high.
4	Anomaly Detection Approaches for Communication Networks	Statistical Method, Streaming Algorithms, Machine learning	It helps in tracking the per-flow status of traffic in networks	Not Feasible to understand what information can best facilitate network anomaly detection.
5	A NICE Way to Test Open Flow Applications	No Bugs In Controller Execution(NICE) tool	The tool helps in testing and automating of Open Flow Applications that combine model checking and execution	They require large space of switch state, large space of input packets and event orderings.

IV. CONCLUSION AND FUTURE WORK

The main contribution in the paper is it generates a minimal batch of packets to debug the liveness of the specified topology and the congruence between the data plane state and configuration specifications. Test packets are sent periodically and detected failure trigger a separate mechanism to localize the fault. The process operates in both

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2016

functional and performance problems. These analysis works discuss the various research works that has been proposed previously by different researches. Those research works are discussed in the detailed manner along with the merits and demerit values. From the performance evaluation it is concluded that AUTOMATED TEST PACKET MECHANISM FOR MONITORING FAULTS IN NETWORK FAILURES is the most efficient approach for testing and debugging the packets. In future scenario, the system should enhance more fault localizations in both functional and performance basis.

REFERENCES

1. R.Radheesha, A.R. Arunachalam, "Fault Diagnosis Using Automatic Test Packet Generation", ISSN 2321-8169, Volume 3, Issue 3, March 2015.
2. Avinash Manne, P.Dharshan, "Detecting Functional and Performance Issues in a Network Using Auto Test Packet Generation", ISSN No:2348-4845, Volume No: 2 , Issue No: 7, July 2015.
3. Anup Kalyanashetti, Divya Hebbar, Pooja Loni "Dynamic Assessment of Router Links By Generation Of Test Packets", ISSN: 0976 – 1353 Volume No: 14 Issue 2, Apr 2015.
4. Y. Bejerano and R. Rastogi, "Robust monitoring of link delays and faults in IP networks", IEEE/ACM Trans. Networks., vol. 14, no. 5, pp.1092–1103, Oct. 2006.
5. P. Barford, N. Duffield, A. Ron, and J. Sommers, "Network performance anomaly detection and localization", in Proc. IEEE INFOCOM, pp. 1377–1385,Apr. 2009.
6..Hung X. Nguyen * and Patrick Thiran, "Active Measurement for Multiple Link Failures Diagnosis in IP Networks", EPFL CH-1015, pp. 185-194, 2004.
7. Marina Thottan, Guanglei Liu, Chuanyi Ji, "Anomaly Detection for Communication Networks", Bell Labs, Alcatel-Lucent, School of Electrical and Computer Engineering, Georgia Institute of Technology, pp. 239-261, 2010.
8. M. Canini, D. Venzano, P. Peresini, D. Kostic, and J. Rexford, "A NICE way to test Open Flow Applications", in Proc. NSDI, pp. 10–10,2012.

BIOGRAPHY

P.Ponmuthuramalingam received his Masters Degree in Computer Science from Alagappa University,Karaikudi in 1988 and the Ph.D. in Computer Science from Bharathiar University, Coimbatore. He is working as Associate Professor and Head in Department of Computer Science, Government Arts College(Autonomous), Coimbatore. His research interest includes Text mining, Semantic Web, Network Security and Parallel Algorithms.

L.Pavithra is an M.Phil Research Scholar in Department of Computer Science, Government Arts College, Coimbatore. She completed M.Sc Computer Science at Government Arts College, Coimbatore. She completed BCA at Kovai Kalaimagal College of Arts and Science, Coimbatore.

.