Research Article Impact Factor: 0.621 ISSN: 2319-507X
Alisha Indurkar, IJPRET, 2014; Volume 2 (8): 416-422 IJPRET

INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

A SURVEY: PERFORMANCE FAILURE DETECTION AND PATH COMPUTATION IN IP NETWORK

ALISHA INDURKAR[1], BALAJI PATIL[2], VINAY KUMAR PATHAK[3]

1. PG Student, Department of Computer, Maharashtra Institute of Technology, Pune, India.
2. Associate Professor, Department of Computer, Maharashtra Institute of Technology, Pune, India.
3. Professor and Dean, Computer Science and Engineering Department, HBTI, Kanpur, India.

Accepted Date: 15/02/2014 ; Published Date: 01/04/2014

Abstract: As the scope of computer network increasing day by day, it is important to maintain the reliability of a network. When all the components are fine but then also the end user is not getting the service, means that there is performance degradation. Such performance failure of a network occurs due to the imbalance of Quality of Service parameters such as delay, jitters, throughput, etc. It is important to detect such failure and find the counter measures. This is a survey paper that discusses the various failure detection techniques along with the technique that finds the optimal path to overcome failure.

Keywords: IP Network, Active Monitoring, Passive Monitoring, QoS Parameters, Multi-Constrained Routing

PAPER-QR CODE

Corresponding Author: MS. ALISHA INDURKAR

Access Online On:

www.ijpret.com

How to Cite This Article:

Alisha Indurkar, IJPRET, 2014; Volume 2 (8): 416-422

INTRODUCTION

In today's world any delay in achieving the information is not tolerated. Everyone wants a rapid and accurate service. Due to this, detection the performance failure in a network is far important. When all the elements of a network are working fine but then also the end users are not getting a proper service. This is due to the performance failure in a network. Performance failure in a network occurs when the network components do not follow Quality of Service parameters. The Quality of Service failure occurs due to the diversion of values from desired Quality of Service parameter values because of congestion, lager delay in packet transmission, insufficient bandwidth, etc. Many techniques in different areas are proposed to detect such type of behaviour which will be discussed further. After detection or monitoring a failure it is necessary to diagnose it and provide corrective measures. When failure is detected in particular which does not follow the Quality of Service constraints, alternate path is made available which fulfills all Quality of Service constraints and reach the destination. The path selection or path computation techniques for choosing the alternative path are analyzed further.

Failure Detection Mechanism

The network failure can be classified into two types – physical failure and performance failure. The physical failure means failure of a network component. Node failures, link failure (single link failure or dual link failure) are physical failure. Performance failure is when all nodes and links are fine but then also the end users are not getting proper service. Performance failure can occur due to insufficient bandwidth, lager transmission delay, more packet drops, etc. These all are the Quality of Service parameters and therefore performance failure can also be called as QoS failure.

The different ways to detect failure can be classified as follows

- Rule-based approach;
- Case-based approach;
- Pattern matching ;
- Finite state machine approach;
- Active and Passive monitoring.

Rule-Based Approach

In rule-based approach an expert system is used which is a database that contains the rules of behaviour of fault to detect the failure in a system. Rule-based approach depends upon the past knowledge of the failure occurred in a system and takes time for detection. Therefore, rule-based system is not suitable for real time applications. As rule-based system depends on previous knowledge, if any new fault comes that don't have any past information will not be detected.

Case-Based Approach

The case-based approach is the extension of rule-based approach. Here along with the previous knowledge of a fault, the event at which the fault occurred is also stored. Event means the time or circumstances at which the fault occurred. To adapt the case-based approach, adaptive learning technique is used to find the functional dependencies. But case-based system also depends on the past knowledge of the fault so it can't detect the entirely new fault.

Pattern Matching

Performance failure can be described as deviation from the normal behaviour. In pattern matching method, a traffic profile is built depending on the symptom-result feature vectors such as link utilization, packet loss, and number of collisions. A template is of mean and standard deviation is formed from the obtained results. The new arrival vector value is compared with the template feature vector. If it matches then it is declared as a fault and produces an alarm as performance failure. This method fails if the traffic profile is not generated accurately. If any new network is given then maximum time will be spend on traffic profiles generation. As today's network is growing fast generating any topology and the data traffic is also increased. This method is not suitable.

Finite State Machine Approach

The finite state machine model generates an alarm sequence for fault detection occurred during and prior to fault events. Using a network fault history data a probabilistic finite state machine model is built. State machines not only detect the fault but also identify and diagnose the problem. The states of the finite state machines are the sequence of alarms that are generated. It is assumed that the alarm contain the information about the device, symptoms and time of occurrence of fault. The best explanations among the number of explanation formed by the cluster of alarms is obtained by a near-optimal set with minimum cardinality and all entities in the set explain all alarms and at least one set is more likely to be in fault. The drawback of this method is that it is not sure whether the assumptions made are true. All faults cannot be captured by a finite state sequence.

Active and Passive Monitoring

Network monitoring can be broadly classified into two types: Active and Passive monitoring. Active monitoring sends traffic into a network to learn its behaviour. The traffic is sent in the form of probes which can be a simple ping or a set of commands or transactions. Passive monitoring does not produce additional traffic. It listens to the flow of traffic through a particular point of network. In more sophisticated implementation, the analysis is by extracting the information of packet header. This method does not require any past knowledge about the network. It emphasis and study the ongoing traffic. Also no assumptions are to be made to detect the fault. Therefore, this method is more appropriate than any other methods. This method can also be used for real time applications.

QoS Path Computation

With the increase in the network traffic, it is very much important to maintain the quality of service. For this the QoS oriented service must be provided in a network which will find all the feasible routes that will satisfy multiple constraints like bandwidth, delay, jitter, etc. along with the effective use of network resources. This type of service is called as QoS routing or constraint-based routing. Many systems are introduced to satisfy this type of service [8]. In ATM PNNI protocol, the source node computes the constraint-based routing to find the suitable paths for request. For QoS routing, it is important to have all information about network resource. This information can be gained by path establishment protocol or existing routing protocol. The protocol such as Open Shortest Path First provides the link state information like delay, bandwidth, etc. The type-of-service field of the protocol contains such information.

There are two types of Multi-Constraint Optimal Path problem - RSP and MCP. If K is the number of constraint then for K=1, the MCOP problem is called as Restricted Shortest Path, whereas for K > 2, the MCOP problem is called as Multi Constrained Path. Both of these problems are NP-Complete and can be solved by pseudo-polynomial-time algorithms. However, these algorithms are computationally very expensive and therefore to deal with this problem, heuristics and approximation algorithms are introduced.

Mainly the previous study for QoS routing was surrounded by only single constraint or QoS in context of bandwidth and delay parameters alone. Many researchers worked on either one or two QoS constraints. But equal importance should be given to all QoS constraints and therefore multi-constrained term was introduced. An effective heuristic algorithm was introduced by Korkmaz and Krunz, for any number of constraints irrespective of their nature and dependencies. But the drawback for this scheme was that, as the heuristic approach was used the performance of algorithm was not always improved. Later Sobrinho introduced the concept of hop-by-hop routing. The forwarding decisions were made independently by each node itself based on the destination address of incoming packet so that path computation takes place locally at the node. But hop-by-hop routing has limitations for QoS support. It does not operate correctly for every type of QoS path.

Mostly, the entire QoS routing algorithm uses unidirectional search to find the path that satisfy all constraints. The search starts from the source node and communicate in a network until a certain condition is satisfied and feasible path is obtained or no feasible path found. In such condition the maximum routing process time is consumed in finding the path between source and destination that satisfies all constraints and the quality of returned path. To reduce the searching time, a bidirectional multi constrained routing algorithm is introduced. The Bidirectional Multi-Constrained Algorithm [1] solves the three major perspectives - find k-shortest paths using bidirectional search, find the halt condition for bidirectional search without hampering the effectiveness of algorithm and gives a novel effective multi constrained routing algorithm.

CONCLUSIONS

In this paper, we have surveyed the different schemes for detection of performance in a network. We have also discussed the different approaches that can be used to find the optimal QoS path from the set of feasible paths. After studying the schemes, we conclude that active and passive monitoring approach is good for failure detection. Just detecting the fault is not enough, but corrective measure must also be taken. Therefore, we suggested to find the QoS path that satisfies all the mentioned constraints and do not hamper the service. Usually link parameters are alone taken into account for QoS, but we suggest that by using both node and link parameters we can find the better results.

ACKNOWLEDGMENT

I would like to thank my guide Prof. B. M. Patil and Co-Guide Prof. S. S. Kinger for the encouragement and instrumental support, which made me, to see the silver lining in every dark cloud. I am also grateful to Prof. Mrs. S. S. Paygude (HOD of Computer Engineering Department, MIT, Pune) for providing me with the required infrastructure facilities. I am pleased to have the valuable guidance from Prof. M. V. Bedekar (M.E. Co ordinator) and Prof. V. S. Jagtap. I would also like to express my sincere appreciation to staff of department of Computer Engineering, Maharashtra Institute of Technology Pune, for their extended help and suggestions at every stage. And at last but not the least this piece of work would have been impossible without the constant support of my fellow batch mates, friends and family.

REFERENCES

1. Baoxian Zhang, Jie Hao, and Hussein T. Mouftah. *Bidirectional Multi-Constrained Routing Algorithms. Computers*, IEEE Transactions, PP(99):1-14, March 2013.

2. Guanfeng Liu, Duncan S. Wong and Yan Wang. *Multiple QoT Constrained Social Trust Path Selection in Complex Social Networks. Trust,* Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference, 624 - 631, June 2012.

3. Gavaskar Vincent and T.Sasipraba. *An Efficient Routing Algorithm for Improving the QoS in Internet*. Emerging Trends in Robotics and Communication Technologies (INTERACT), 2010 International Conference, 381 - 387, December 2010.

4. Shrinivasa Kini, Srinivasan Ramasubramanian, Amund Kvalbein, Audun F. Hansen. *QoS Fault Detection and Localization Mechanisms (FDLM) in Multi-domain Networks Adapted to Export Methods*. Advanced Communication Technology (ICACT), 2012 14th International Conference, 848- 853, February 2012.

5. R. Leela and S. Selvakumar. *Genetic Algorithm approach to Dynamic Multi Constraint Multi Path QoS Routing Algorithm for IP networks (GA-DMCMPRA).* Communication Systems and Networks and Workshops, 2009, COMSNETS 2009, First International, 1 - 6, January 2009.

6. Yu Wang, Lemin Li, Du Xu and Chengdu, P. R. China. *Metrics Transform Based Multi-constrained Optimal Path Selection*. Communications, Circuits and Systems, 2007. ICCCAS 2007. International Conference, 510 - 514, July 2007.

7. Joao Luis Sobrinhoi. *Algebra and Algorithms for QoS Path Computation and Hop-by-Hop Routing in the Internet*. Networking, IEEE/ACM Transactions, 10(4):541 - 550, August 2002.

8. Turgay Korkmaz and Marwan Krunz. *Multi-Constrained Optimal Path Selection*. INFOCOM 2001. Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE, 2:834 - 843, April 2001.

9. Malgorzata Steindera and Adarshpal S. Sethi. *A survey of fault localization techniques in computer networks*. Science of Computer Programming, 53:165-194, 2004.

10. George Katsikogiannis, Sarandis Mitropoulos, and Christos Douligerisi. *Policy-Based QoS Management for SLA Driven Adaptive Routing*. Communications and Networks, Journal, 15(3):301 - 311, June 2013.

11. Shigang Chen, Klara Nahrstedt. *An Overview of Quality-of- Service Routing for the Next Generation High-Speed Networks: Problems and Solutions*. Network, IEEE, 12(6):64 - 79, August 2002.

12. Maitreya Natu and Adarshpal S. Sethi. *Application of Adaptive Probing for Fault Diagnosis in Computer Networks*. Network Operations and Management Symposium, 2008. NOMS 2008. IEEE, 1055-1060, April 2008.

13. Guanjue WANG, Yan QIAO, Xuesong QIU, Luoming MENG. An Improved Network Performance Anomaly Detection and Localization Algorithm. Network Operations and Management Symposium (APNOMS), 2012 14th Asia-Pacific, 1-4, September 2012.