Efficient identification of node failure and recovery through end to end Probing techniques

Chitturi Sai Nikhil¹, Manjula Josephine Bollarapu ¹, Kaja Sai Sree Neeraj², Alaparthi Praveen Kumar³, Manchikalapudi Jaya Sesha Sai Raghuveer⁴

¹, ², ³, ⁴, ⁵Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India.

Corresponding Author: manjulajosephine@gmail.com

Abstract. Identification of Node failure detection and a localization is a very important challenge in a network community to get a quick recovery and avoid useless traffic in network. But it is very difficult to check the failure nodes or locations because of the large number of Screw ups in dense network. As finding the main source for failure of network is always challenging our proposed work will achieve that, it identifies the node failure by using probing measurement of binary state to end to end paths. Apart from identifying the network failure, it also quantifies the total failure nodes and the ip address or vicinity of failure nodes, Identification of node failure is done by monitoring nodes which are deployed in the network. Our Proposed word is divided majorly in two phases one is identifying the node failures by using Probing Packets and other is finding of the failure and its recovery.

Key words: Network probing, Node recovery, Measurement paths, probing mechanisms, Node Recovery, End to end path construction, localization.

1. INTRODUCTION

In order to get reliable and effective network performance, the network operators plays an important role. The main aim of network operators is to provide effective monitoring without disturbing any communication or any of the services. There are many factors which affect the performance of network such as loss of packet, delay in end to end delivery of packets, malfunctioning of nodes, nodes not reachable etc. Network monitors must continuously identify these issues. If these problems are identified in time then network administrator can take appropriate action. The admin can identify location of attacker. Admin can route the packets from one route to another where it is in high demand. Can specify alternate route so that the network performance is not degraded due to heavy packet loss. Tracing the location of malicious node is big challenge, there are many solutions proposed by many authors.
There exists uncertainty in failure node detection and localization, there needed a novel technique, to identify both in network and sub-network area. Network properties highly helpful in identifying sub network area failures. To approach this problem, the solution provided are finding under which conditions node failure occurs, finding whether node failure nodes are in a subset of node[6], which is monitored in particular locations. The routing strategy of probe packets plays crucial role in network monitoring, which is unattended in existing systems. End to end path measurement approach can be implemented with routing probe packets satisfies scope of failure node localizing problem.

In the following sections some of the research related to network monitoring are discussed. In section 3, the details on implementation of proposed methodology is discussed. In Section 4, Results and discussed are given. Finally, Section 5, discussed work Conclusion and further enhancements are discussed.

2. RELATED WORK

Network performance plays a crucial role for industries and business, there has been large amount of study in network failure detection. In Literature, many researched has worked on network failures and path measurements. Some them are discussed in detail in this section. Link delivery delays and link failures are discussed in work [7], The author proposed the greedy approximation algorithm. The Work in [8] about the virtual circuit routing for detecting node failure. The Work in [9] is all about the handling of the various resources in network failure conditions.

3. Methodology

![Work Flow Diagram](image)
The Implementation is done by using the below modules

3.1 Construction of Topology
3.2 Deploying Monitors/Non Monitors
3.3 Finding Neighbors
3.4 Probing & Finding Failure Nodes
3.5 Node Recovery

3.1 Construction of Topology

Initially the network topology is constructed in this Phase with all the nodes, links and edges. The network topology can be undirected and can have sub network as well [14].

3.2 Deploying Monitors/Non Monitors

By using the Binary State Process and unique rules for Measurement and Probing techniques Network will be monitored [15].

3.3 Finding Neighbors

The following figure represents the moderately controlled packet probing strategy, which is sent from monitoring node to normal node.

![Figure: 3 Moderate control packet probing](image)

The following figure represents the controlled packet probing strategy[17], which is sent from monitoring node to next monitoring node. The packed named CPP will be broadcast between one monitor and other monitor as shown below.

![Figure: 4 Control packet probing](image)

The following figure represents the uncontrolled packet probing strategy, which has no restriction on sending probe packet, it may take any route[18]. The route includes the all available neighbour nodes, or may be limited nodes based on a random selection done through this probing strategy. The packets names UPP is broadcast through the network.

![Figure: 5 Un-control packet probing](image)
3.4 Probing & Finding Failure Nodes

Here in this Phase by using binary type states and Probing Mechanisms Node failures will be detected and also there is a recovery mechanism to rectify the failure node.

4. Results and Discussion:

The proposed work is carried out in jdk 1.7 with mysql 5.5 as database. We initially created dynamic topology, in which any range of nodes may be deployed. Nodes, linkas and edges are framed.

Nodes which are deployed in the network and its status can be monitored by monitoring nodes and as mentioned in following figure. For naming monitor nodes are named as M1, M2..etc Non-monitor nodes are named as A, B,C,D…etc. The proposed work considered deployed two monitor nodes M1 and M2 in the network topology. The number of normal nodes deployed in the network are four. Placement of monitor influences the performance of path measurements. If the monitoring nodes are available in between the normal nodes, the monitoring nodes can effective monitor the paths established through Moderate controllable probing packets of uncontrolled packet probing strategies. The following figure shows the monitoring of nodes or neighbour along the paths established.

| Node Name | Status |
|-----------|--------|
| A         | Normal |
| B         | Normal |
| M2        | Normal |
| C         | Faulty |
| D         | Normal |

*Figure 6: Node Status Monitoring*

Three types of Probing message are sent on particular button action. The nodes receive the neighbour and paths are arrived dynamically.

Node can be made as faulty node and the generated path will avoid faulty nodes in routing for message delivery[9]. The message is delivered on network without fail. The faulty node can be retrieved or recovered in the network, in such case, it again joins the routing path on message delivery.

In case of route failures, the proposed system identifies the all available route, to re-route the packets, this ensures the data delivery in network without any loss. The following screen shows the available path generated for sending packets from monitor node to non-monitoring Node 'C', the routing path creating, generated all available path, which has an alternate routes of more than 10 route to deliver. This ensures the packet delivery without any loss in network. The routing paths are generated whenever an event of data delivery on the network or probing packet deliver on the network. The routes are generated among monitor to non-monitor, monitor to monitor and monitor to all available nodes depending on the generated events like data or probe.
5. Conclusion:

Our Proposed work has addressed various challenges in terms of network maintenance as it is the major part of networking and also it addressed various issues in terms of network performance through proper monitoring. The main idea of our work is to identify the failure node and its location through various probing strategies of network. We have achieved this by following various strategies like binary problem to identify the failure node and by using some distinct set of guidelines for calculating the paths and for finding and recovering the failure nodes. And our proposed research work experimentally proved the efficiency of node failure detection through probing strategies.

Future Scope

As the present work involved the detection of node failure as binary case only, in future this is can be extended to multiple class detection, along with identifying specific type of node failures.

REFERENCES

[1] O. J. Pandey, V. Gautam, H. H. Nguyen, M. K. Shukla and R. M. Hegde, "Fault-Resilient Distributed Detection and Estimation Over a SW-WSN Using LCMV Beam forming," in IEEE Transactions on Network and Service Management, vol. 17, no. 3, pp. 1758-1773, Sept. 2020, doi: 10.1109/TNSM.2020.2988994.

[2] M. Dhingra and N. Gupta, "Failure Node Reduction Algorithm to Enhance Fault Tolerance Capability of Cloud Nodes," 2020 12th International Conference on Computational Intelligence and Communication Networks (CICN), 2020, pp. 165-168, doi: 10.1109/CICN49253.2020.9242615.

[3] C. Pachajoa, C. Pacher and W. N. Gansterer, "Node-Failure-Resistant Preconditioned Conjugate Gradient Method without Replacement Nodes," 2019 IEEE/ACM 9th Workshop on Fault Tolerance for HPC at eXtreme Scale (FTXS), 2019, pp. 31-40, doi: 10.1109/FTXS49593.2019.00009.

[4] F. Barbosa, A. de Sousa, A. Agra, K. Walkowiak and R. Goścień, "A RMSA Algorithm Resilient to Multiple Node Failures on Elastic Optical Networks," 2019 11th International Workshop on Resilient Networks Design and Modeling (RNDM), 2019, pp. 1-8, doi: 10.1109/RNDM48015.2019.8949141.

[5] Y. Bejerano and Rajeev Rastogi, "Robust monitoring of link delays and faults in IP networks," IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE
[6] A. A. Minhas, C. Steger, R. Weiss and S. Ehsan, "Node failure detection and path repairing scheme in virtual circuit routing algorithm for wireless ad hoc micro sensor networks," Proceedings of the IEEE Symposium on Emerging Technologies, 2005, Islamabad, Pakistan, 2005, pp. 86-91, doi: 10.1109/ICET.2005.1558860.

[7] I. Vardas, M. Ploumidis and M. Marazakis, "Towards Communication Profile, Topology and Node Failure Aware Process Placement," 2020 IEEE 32nd International Symposium on Computer Architecture and High Performance Computing (SBAC-PAD), Porto, Portugal, 2020, pp. 241-248, doi: 10.1109/SBAC-PAD49847.2020.00041.

[8] Zeng, Hongyi & Kazemian, Peyman & Varghese, George & McKeown, Nick. (2012). Automatic test packet generation. 241-252. 10.1145/2413176.2413205.

[9] H. X. Nguyen and P. Thiran, "The Boolean Solution to the Congested IP Link Location Problem; Theory and Practice," IEEE INFOCOM 2007 - 26th IEEE International Conference on Computer Communications, Anchorage, AK, USA, 2007, pp. 2117-2125, doi: 10.1109/INFOCOM.2007.245.

[10] S. S. Ahuja, S. Ramasubramanian and M. Krunz, "Single-Link Failure Detection in All-Optical Networks Using Monitoring Cycles and Paths," in IEEE/ACM Transactions on Networking, vol. 17, no. 4, pp. 1080-1093, Aug. 2009, doi: 10.1109/TNET.2008.2008000.

[11] Lantz, Bob & Heller, Brandon & McKeown, Nick. (2010). A Network in a Laptop: Rapid Prototyping for Software-Defined Networks. Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks. 19. 10.1145/1868447.1868466.

[12] Mahimkar, Ajay & Ge, Zihui & Wang, Jia & Yates, Jennifer & Zhang, Yin & Emmons, Joanne & Huntley, Brian & Stockert, Mark. (2011). Rapid detection of maintenance induced changes in service performance. 10.1145/2079296.2079309.

[13] B. Schroeder and G. A. Gibson, "A large-scale study of failures in high-performance computing systems," International Conference on Dependable Systems and Networks (DSN'06), Philadelphia, PA, USA, 2006, pp. 249-258, doi: 10.1109/DSN.2006.5.

[14] E. Jeannot, G. Mercier and F. Tessier, "Process Placement in Multicore Clusters: Algorithmic Issues and Practical Techniques," in IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 4, pp. 993-1002, April 2014, doi: 10.1109/TPDS.2013.104.

[15] C. D. Sudheer and A. Srinivasan, "Optimization of the hop-byte metric for effective topology aware mapping," 2012 19th International Conference on High Performance Computing, Pune, India, 2012, pp. 1-9, doi: 10.1109/HiPC.2012.6507513.

[16] W. R. Heinzelman, A. Chandrakasan and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, Maui, HI, USA, 2000, pp. 10 pp, vol.2-, doi: 10.1109/HICSS.2000.926982.

[17] R. L. Carter and M. E. Crovella, "Server selection using dynamic path characterization in wide-area networks." Proceedings of INFOCOM '97, Kobe, Japan, 1997, pp. 1014-1021 vol.3, doi: 10.1109/INFCOM.1997.631117.

[18] Friedman, Timur & Towsley, Donald & Kurose, James. (2004). Scalable End-to-End Multicast Tree Fault Isolation. 1347-1358. 10.1007/978-3-540-27824-5_174.

[19] Y. Breitbart, Chee-Yong Chan, M. Garofalakis, R. Rastogi and A. Silberschatz, "Efficiently monitoring bandwidth and latency in IP networks," Proceedings IEEE INFOCOM 2001. Conference on Computer Communications. Twentieth Annual Joint Conference of the IEEE Computer and Communications Society (Cat. No.01CH37213), Anchorage, AK, USA, 2001, pp. 933-942 vol.2, doi: 10.1109/INFOCOM.2001.916285.

[20] R. Bolliger and T. R. Gross, "Bandwidth monitoring for network-aware applications," Proceedings 10th IEEE International Symposium on High Performance Distributed Computing, San Francisco, CA, USA, 2001, pp. 241-251, doi: 10.1109/HPDC.2001.945193.