ISSN 2229-5518

Health Monitoring of Network Using Probing

Aparna Gaikwad, Balaji Patil, Vinay Kumar Pathak

Abstract—Day by day the nature and the complexity in the network is increasing. The wide spread of Internet brought the world closer as well as challenges too. So monitoring of the networks becomes at most important to face and tackle these challenges of failures, reliability, QoS, etc. Collection of nodes and links between pair of nodes form a complex network. Health monitoring is required for complex and large networks. Network monitoring is one of the prominent phases in the network management. Passive monitoring and active monitoring are two different types of monitoring mechanisms. Passive monitoring gives fine-grained analysis and is capable of computing at-a-point metrics but requires more instrumentation. On the other hand active monitoring provides end-to-end metrics with lesser instrumentation but introduce additional traffic in the network. In our novel approach we have used probing based hybrid monitoring strategy for network health monitoring which effectively outperform existing solutions.

Index Terms— active monitoring, health monitoring, network monitoring, passive monitoring, probing.

1 INTRODUCTION

Day by day the nature and the complexity in the networks are increasing. The wide spread of Internet brought the world closer as well as challenges too. So monitoring of the networks becomes at most important to face and tackle these challenges of failures, reliability, QoS, etc. For monitoring the health of human beings doctors check the relevant anatomical parameters like, blood pressure, sugar level and other relevant health indicators, likewise networks are needed to be monitored for different performance metrics. A network operations team/admin can optimize network uptimes and avoid significant drops in QoS by monitoring and managing prioritized indicators of network health to keep them within optimum range of target states.

Difficult and demanding task on modern network infrastructures is network management. Network management very often requires the human intervention to create management plans, to coordinate network assets, and to face up to fault situations. Because of the increasing cost of network downtime and the complexity of deployed systems, it has become crucial to find a reliable way of managing communication networks and their services. These systems need constant monitoring and probing for the purposes of management, particularly for configuration setting, fault diagnosis, and performance evaluation, but, as the size of networks increases, it becomes more and more difficult to extract the right information from them.

So for getting the right information from the network we require network monitoring which is a prominent function of network management. Network monitoring applications collect data from network management applications. Network monitoring collects useful information from various parts of the network so that the network can be managed and controlled using the collected information. Network monitoring techniques are developed to allow network management applications to check the states of their network devices [3].

There are too many measurable things in the network so what to measure is important. These monitoring metrics are needed to be collected at various layers ranging from hardware layer, operating system to other upper layers. Monitoring techniques compute the performance problems such as: processes using heavy CPU usage, process execution time spent in disk write etc. These metrics are useful for future network expansion and smooth running network.

Quick detection and isolation of unhealthy components in network makes it reliable and robust. Hence passive monitoring and active monitoring techniques are used for monitoring and processing data collected from network components.

Passive monitoring [3] relies on the ongoing traffic to infer the performance of various components. So in absence of traffic it cannot measure such metrics. Hence probes can be used to produce specific traffic and allow passive monitors to observe it. Through passive monitoring, a security admin can gain a thorough understanding of the network's topology, what services are available, which operating systems are in use, and what vulnerabilities may be exposed on the network. It computes the statistics at the thread level, module level and component level. The analysis of these levels can be explained using bayesian networks, neural networks and decision trees.

Probing is nothing but a test transactions, the examples of probes, used for probing [10] are pings, trace-routes, HTTP requests, etc. Previously preplanned probing was used which involves designing a preplanned set of probes that are capable of diagnosing all possible failure scenarios of interest and sending this set of probes periodically in the network. But this generates additional management traffic and increases load on network.

Probes used for this are in the form pings, traceroutes etc.

- *Aparna Gaikwad is currently pursuing masters degree program in Computer engineering in Pune University, India. E-mail:aparnagaikwad18@gmail.com*
- *Balaji Patil is pursuing the Ph. D from Uttarakhand Technical University, Dehradun, India Email- balaji.patil@mitpune.edu.in*
- *Vinay Kumar Pathak, Vice-Chancellor, VMO University, Kota, Rajsthan, India. Email- vinay@vpathak.in*

ISSN 2229-5518

Probes can also be HTTP requests to check the availability and response time of the nodes and server.

Probes can also be ping sent to test connectivity and availability of the nodes.

Active probing adapts the probing strategy to the observed network state. Instead of sending probes for locating all potential problems in the network, it sends a minimal number of probes initially and then adapts the probe set to the observed network state [7]. The probe stations then send probes that provide most information gain. This approach can greatly reduce management traffic and provide more accurate and timely diagnosis. Probing [9] provides flexibility in the design of probe streams with particular properties to match measurement requirements.

This paper is organized as follows. Section 2 gives a brief discussion of related work done. In Section 3, we introduce the concept of health monitoring using probing and present details of health monitoring and identification algorithms for health monitoring. Summary is given in Section 4 and finally Section 5 describes future work.

2 Related Work

During initial stage of monitoring of networks only the passive monitoring is used. But the passive monitors have its own limitations such as collect information at only one point. Work done on the network monitoring also consist of following parts obtaining data from network equipment is based on the IETF standard, SNMP (Simple Network Management Protocol) and NETCONF, Passive monitoring and probing.

There are various tools which collect information from various network components and do processing on it such as traceroute which calculate packet loss and delay but it requires special routers for data collection, MHealth having global reachability but restricted on RTP and SDR applications also require mtrace enhanced routers. MRM is a step forward toward efficient multicast active monitoring; its deployment will be limited because of using a proprietary protocol and special agents. Offline and online tools [5] are used for root cause analysis. But if off-line transaction log analysis does not find the root cause then it will try to find root cause by running more transaction which creates more data storage. Snort is open source network-based intrusion detection system (NIDS) has the ability to perform real-time traf-fic analysis and packet logging on Internet Protocol (IP) networks. Snort performs protocol analysis, content searching, and content matching. The program can also be used to detect probes or attacks, including, but not limited to, operating system fingerprinting attempts, common gateway interface, buffer overflows, server message block probes, and stealth port scans. Passive monitoring measures or monitors the metrics pertaining to certain network element such as link throuput, packet size statistics. It has been used for monitoring web based applications. Analysis in passive monitoring is done with inspecting the packet headers which creates security problems. Also passive monitoring requires more instrumentation but it creates less traffic. Active monitoring [8] is typically used to obtain end-to-end statistics such as latency, loss and route availability. It requires less instrumentation but it creates additional traffic to network. Also the probes used in active monitoring modify the root conditions and perturb the very traffic being monitored.

An extended symptom-fault-action model to incorporate actions into fault reasoning process to tackle the problems is called active integrated fault reasoning (AIFR), which contains three modules: fault reasoning, fidelity evaluation and action selection. Corresponding fault reasoning and action selection algorithms are required for that.

Adaptive monitoring [4] is framework using end-to-end probing based solutions to adapt at-a-point monitoring tools. ILP and greedy algorithms are used for probe selection and monitoring level recommendation and ROC, DFN for probe analysis. But it requires probe station selection and probe set selection. Also it will not work with dynamic changes in the network.

3 Health Monitoring Using Probing

Many researchers have used passive monitoring and active probing [1] in isolation for fault management. In our novel approach wehave combined it to form an integrated probing approach, which is used for distributed health monitoring. Integrated probing sends fewer probes to healthy area of the network and more probes to unhealthy areas which create less traffic as well as it require less instrumentation.

In the architecture of the system main part of the network is server having central control of system. In order to develop a health monitoring system for large network sizes, there is need to develop a distributed approach with central system. The centre node i.e. server is aware of the information of the entire network and make decisions accordingly. In this architecture server will do its own health checking so there are very few chances of server failures.

The architecture shown in fig. 1 consist of three major modules as, Visual module represents the graphical view of output and the user requirements, Monitoring module computes passive and active measurements used for collecting and processing the network traffic, Indication module is used for indicating the criticality of network component. Indication module stores the running process status and other indication of failed network component with its own database. Checking is done in indication module and according to which server will take the action.

ISSN 2229-5518

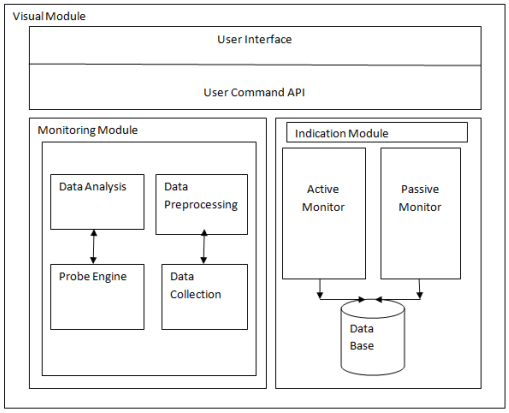


Fig.1 Health monitoring architecture [11]

Indication module is capable of fault detection and correction. In this server sends the probes in the network for monitoring purpose. These probes ping the nodes in the network and starts the passive monitoring at each node. Passive monitoring will check the health parameters of the node continuously. If fault occurred at any node then it is reported to server. After this server will send the additional probes for fault diagnosis and finding out the exact reason of fault is identified. If there are multiple faults occurred at a node then priority algorithm is applied and the fault having high priority is ocalized first.

Server will do server monitoring for checking its own health and sniff the data from the port of nodes so that it will get details of other nodes in the network.

After getting details of network it will store it in the database for further processing. Server will periodically sniff the data i.e. health parameters of the nodes lets say after every 5 minutes and every node will do there passive monitoring after every 1 minute. If the health parameters of node are beyond the threshold, if they are crossing the threshold then the particular node is unhealthy. Then server will get more information from this node immediately by sending the additional probes, this is an adoptive probing. For healthy nodes it will sniff data with less periodicity because of this network will have less traffic load. Server will identify the components or processes responsible for performance degradation. In this way after localizing a fault or unhealthy node of the network with the help of fine probing that can identify bottleneck or estimate cross traffic.

The health parameters are obtained by using WMIC tool. WMIC is a console based tool used for getting criticality of the system and network.

Algorithm for health monitoring can be described as follows:-

Procedure: Health Monitoring System (HMS)

Inputs: Node list <N1,N2.....Nn>

Threshold of health parameters

Output: Faulty Node

Action to be taken on faulty Node

Algorithm:

1. Initialization
2. Server will do self health checkup.
3. It will bind all nodes in the network.
4. Starts passive monitoring at each node.
5. Check threshold of health parameters.
6. For node i=1 to n do
7. If passive monitoring = true (faulty node)

   Find the component that degrades the performance of Ni.

   Take the corresponding action (e.g. suspend or kill process)
8. Else increase time period and goto step 7.

In this way this process continues and it will continuously check the details of network. Probes are used by server for getting details of network. Hence, there is only one probe station [7] for the network. Probe results are further analyzed to infer health of network and for estimating criticality.

By observing the performance degradation or failure, these probes point the processes which are root causes. Nodes having CPU, Memory, Disk, and Network are some critical resources and if the server or nodes are overutilize them, then crash may occurred. Server monitor performances mainly consisting of four categories as: port listener, ping host, analyzer and bandwidth. The major parameters of server or node health consist of CPU utilization and number of running process. With the help of this health of the network can be maintained efficiently.

The algorithm for the passive monitoring is as shown below.

In this we have considered the health parameter as CPU utilization and memory utilization. This algorithm gives output as true if node is faulty or false if node is healthy.

ISSN 2229-5518

Procedure: PassiveMonitoring

Input:

Server address

Port number

List of Processes [$P_1, P_2, \ldots, P_n$]

Output:

True (if node is Faulty)

False (If node is healthy)

Max_proc

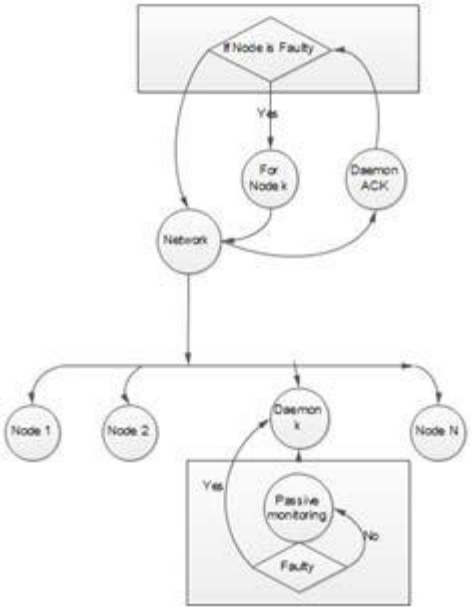
Status \\ Status of Node

ACU \\ Average_CPU_utilization

Algorithm:

1. For each Process i=1 to n do
2. Max_proc=Max(P_i, P_{i+1})
3. ACU=(Total_CPU_utilization)/n
4. If ACU>threshold then
5. Status=Critical
6. return true
7. else
8. Status=Idle
9. return false

The flow diagram of health monitoring is as follows: -



This system will measure and monitor the performance and identify whether it is normal, optimal or overloaded. Server sends probes to clients for their health checkup for e.g. consider server sends 10 probes to 10 clients. In this network of 10 clients if 1 node is unhealthy then server will send the probes continuously to that faulty node only for further analysis. While for healthy nodes server will send less frequent probes. So ultimetly it will reduce the probes for monitoring.

4. Conclusion

With an example of integrated probing, we demonstrated how active probing and passive monitoring can be used to complement each-other to develop effective solutions. We believe that powerful network management solutions can be designed by adopting a hybrid approach that uses both passive monitoring and active probing. Also the system monitoring and recovery of system is helpful to maintain health of the network.

5. Future Work

Health monitoring using probing approach in the network keeps the network healthy and efficient. But working with large, nondeterministic, dynamic, diversified and complex network is still a research challenge to minimize the probing and keeping the network healthy.

References

[1] M. Natu and A. S. Sethi. Probabilistic fault diagnosis using adaptive probing. In DSOM 2007, San Jose, CA, Oct. 2007

[2] M. Natu and A. S. Sethi. Application of adaptive probing for fault diagnosis in computer networks. In NOMS'08, Apr. 2008.

[3] Se-Hee Han, Myung-Sup Kim, Hong-Taek Ju, and James Won-Ki Hong. The Architecture of ng-mon: A passive Network Monitoring System for high speed ip Networks. In DSOM'02, 2002.

[4] Deepak Jeswani, Maitreya Natu and R. K. Ghosh, "Adaptive Monitoring: hybrid approach for Monitoring using Probing, 2012.

[5] Ling Huang, Xuanlong Nguyen, Minos Garofalakis, and Joseph M. Hellerstein. Communication-efficient online detection of network-wide anomalies. In INFOCOM'07, 2007.

[6] Y. Tang, E. S. Al-Shaer, and R. Boutaba. Active integrated fault localization in communication networks. In IM 2005, pages 543–556, May 2005.

[7] M. Natu and A. S. Sethi. Probe station placement for robust monitoring of networks. Journal of Network and Systems Management, 2007.

[8] M. Natu and A. S. Sethi. Using adaptive probing for fault diagnosis. Computer Networks, 2007.

[9] M. Natu and A. S. Sethi. Using adaptive probing for fault diagnosis. In IEEE GLOBECOM 2007, Washington, D.C., Nov. 2007.

[10] M. Natu and A. S. Sethi. Active probing approach for fault localization in computer networks. In End-to-End Monitoring Workshop, E2EMON 2006, Vancouver, Canada, pages 25–33, Apr. 2006.

[11] Mohd Nazri Ismail and Sera Syarmila "Network Management System Framework and Development" in 2009 International Conference on Future Computer and Communication.