VEMANA INSTITUTE OF TECHNOLOGY

Koramangala, Bengaluru-34.

Department of Computer Science and Engineering

Project Phase-I Review 1

ENHANCING NETWORKING MONITORING SYSTEMS BY OVERLAYING PROTOCOLS

By

RAJASHREE – 1VI17CS114

PAVITHRA K – 1VI17CS071

Under the Guidance of

Mr. NOOR BASHA,

Asst. Professor Department of CSE,

Vemana Institute of Technology

BIRD VIEW

- Introduction
- Motivation
- Literature Survey
- Comparative analysis of the survey
- Problem Statement
- Methodology
- System Specification
- Expected outcome
- Applications
- References

INTRODUCTION

- Network monitoring system is a scripted tool that administers a computer network for slow or failing components and that notifies the configured users in case of outages, latencies, upgrades, and other events.
- A computer network is a group of network nodes that use a set of common communication protocols over digital interconnections for the purpose of sharing resources located on or provided by the network nodes.
- A wide range and variety of devices are supported by the system such as Servers, Routers, Switches, Virtual Machines, IoT Devices, Cloud Instances, Data Stores, Wireless Access Points, Endpoint PCs, Printers, Mobiles and so on.
- The proposed system can monitor for following information using various protocols by overlaying them:
  - Performance: Reachability, Availability, Uptime, Throughput, Round-trip-time, Latency
  - Resources: Expansion Plan, Revision Control, Logging, Bandwidth, Customized Alerts
  - Information: Firmware versions, Device Info, Traffic Stats, IP Address, MAC Address
  - Access: SSH Access, Telnet Access

MOTIVATION

- Through various discussions on daily basis, who is a Network Security Engineer in an esteemed MNC that manufactures and maintains network firewalls, uses around 10-11 different web portals to maintain each customer's network that generally consists of 200-400 network nodes.
- The main reason for the large number of portals is due to the lack in support of a variety of devices by a single monitor.
- Moreover, the prices of the monitors range from 2000-3000 USD per 100 network nodes per month which was really not an affordable solution by many customers while their performance wasn't efficient either.
- As a result, there is a dire need of a fully functional network monitor system that can support a wide range of devices and can be economical too.

LITERATURE SURVEY

[1] **Dynamic Network Control with QoS and Resource Priority Monitor Based on Active "eM" for Commercial VoIP** – by Melanie Grah and Dr. Peter Radcliffe 2014

This paper examines methods by which VoIP can be managed using a dynamic method to balance cost and quality. In VoIP systems, quality has a real commercial value as clients will leave a service provider that does not deliver an adequate quality of service. Nearly as important is the network monitoring and prediction function which can tell a carrier of impending problems before they become an annoyance to paying clients.

[2] **Architecture of a Network Performance Monitor for Application Services on Multi-Clouds** – by Young-min Kim, Ki-sung Lee, Jae-cheol Uhm, Si-chang Kim, and Chan-gun Lee 2013

In this paper, essential requirements of network performance monitor for multi-clouds are identified and an architecture is proposed. The necessity of supporting external agents have been addressed in particular and also, there is a discussion on how to integrate with them in a flexible and extensible way. In addition, the issues of timely delivery and off-line analysis of measured results are addressed.

LITERATURE SURVEY

[3] **Measurement-Aware Monitor Placement and Routing: A Joint Optimization Approach for Network-Wide Measurements** – by Guanyao Huang, Chia-Wei Chang, Chen-Nee Chuah, and Bill Lin 2012

This paper presents an MMPR (Measurement-aware Monitor Placement and Routing) framework that jointly optimizes monitor placement and dynamic routing strategy to achieve maximum measurement utility. Several heuristic algorithms have been proposed to approximate the optimal solution and reduce the computation complexity. Through experiments using real traces and topologies, it has been justified that these heuristic solutions can achieve measurement gains that are quite close to the optimal solutions, while reducing the computation times by a factor of 23x and above.

[4] **A Web-based monitor and management system architecture for enterprise virtual private network** – by Ruey-Shun Chen *, Change-Jen Hsu, Chan-Chine Chang, S.W. Yeh 2005

This paper is based on the new network management technologies such as policy-based network management, mobile agent, etc., to design a VPN monitor and management system architecture that contains high level management with low network traffic load. This system architecture integrates both VPN devices and general network devices, such the feature can integrate the monitor and manage the VPN and Intranet at the same time.

LITERATURE SURVEY

[5] **Distributed Interplanetary Delay/Disruption Tolerant Network (DTN) Monitor and Control System :**

This paper exemplifies a case how DTN Monitor and Control system can be adapted into a space network as it is DTN enabled. Also a "DTN Status Diagnose and Treatment Creator" tool is devised to provide a platform for network operator to compose failure treatment methods according to the received DTN BSR (bundle status report), DTN implementation specific log message and the network specifically produced monitor and control data

COMPARATIVE ANALYSIS OF THE SURVEY

- Most common Network Monitoring software available in the existing market are solarwinds, openNMS, WhatsUpGold, Intermapper, OpManager and AppNeta. Almost, all of these software assume that there administrators that will monitor small-to-medium sized business networks and administrator. Further, thy also assume that there are multiple administrators in a network.
- Price of a network monitor for 100 Clients ranges from 2500 USD to 4000 USD for 100 network nodes.
- Most of them don't support Multicast protocols and as a result they are unable to provide device information in real time such as firmware version, os version, update notifications and so on.
- Connection mapping to various network nodes requires manual interaction with the system.
- Almost all the systems use SNMP, ICMP or polling to obtain information about the network topology
- Most of them require the administrator to setup a separate database and configure the same instead of inbuilt nature.
- None of them support IoT or Cloud instances. While some of them do add Virtual Devoice Support, it comes at an extra cost and they use limited community plugins for the same.

PROBLEM STATEMENT

EXISTING SYSTEM

- Networks are the backbone for any enterprise. Any network outage is a colossal loss for the organizations. As a result, they employ a separate team to look after their labs by constantly logging into several system interfaces and manual logging various status information of network nodes.
- Security and monitoring have become a critical concern for every person with internet connectivity.
- Existing Network monitoring systems are designed to support very specific applications such as identifying the device's connectivity or latency or out-of-band analysis and so on.
- Further, they are homogenous in terms of protocol usage. They use generally SNMP or ICMP to monitor a network and report when the client goes down.
- For further analysis, such as gathering information about all network nodes, performance analysis and so on, various tools are available that are expensive and not completely up to today's networking speeds.
- A typical organization that consists of say 100 employees, the network includes at least 3 routers, 5-6 switches, 100-150 PCs, 3-5 servers, a cloud environment consisting of its 3-5 instances and 1-2 data stores, 20-30 VMs for testing their product. Such organizations/homes cannot afford a stack of tools to maintain a stable and high-performance network.

PROPOSED SYSTEM

- Network Monitor is a web application that reports various status changes and updates of various network nodes in an organization
- The system basically comprises of 3 parts
  - Front End: Main functionalities include the following:
    - Logging into the system
    - Adding a device
    - Editing a device
    - Deleting a device
    - Displaying the ‘Devices’ table
  - Database: It comprises of two tables:
    - UserLogin is the administer the secure login activity to network monitor.
    - Device table consists of the device name, locally generated device id, IP Address and System Parameters such as Reachability, Availability, Latency, Mac Address and so on.
  - Back End: A Python script that runs every 10 seconds to obtain information of all network nodes using different protocols and updates the same in the Database

METHODOLOGY

In general, methodology refers to a set of procedures used to conduct a project. The various stages are explained below:

- Project Planning: This is done by allocating tasks that are going to be done within a given time period. This is important to make sure this project can be carried out perfectly and meeting the requirements.
- Research and Analysis: It involves literature survey of related journals, books, research papers and developers' forums to get a better understanding and clear view about the research scope that will be carried out.
- Development of Project: This involves implementing code for various Back-end and Front-end modules of the project. Also, the installation and configuration various software requirements, databases and so on come under this phase.
- System Analysis and Improvement: The developed system is to be thoroughly studied and analyzed to further understand how it works in real environment by deploying it in a simulated network environment.
- Integration and Testing: This system is tested rigorously in this phase with different parameters and configurations to see whether it can meet the required expectations.

SYSTEM SPECIFICATION

Hardware Specifications:

Processor: Intel® Core i5 ™ CPU and above

RAM: 8 GB or higher

Hard Disk: 100 GB or higher

Software Specifications:

Operating System: Windows 10/Ubuntu 20.04 LTS

Architecture: 64-bit OS

Python 3.8 or higher

PIP Packages: RegEx, Flask, Django, Pymysql

Database: MySQL5.7 or higher

JavaScript 1.8.5 or higher

Front End: HTML5, CSS3, Bootstrap4

EXPECTED OUTCOME

- A fully functional network monitoring system that can overlay various monitoring protocols such as ICMP, SNMP, ARP, RARP, LLDP and so on to obtain all information about various network nodes.
- Development of easy installation script setup documentation.
- A lucid, user-friendly User Interface for the application that can display information with right intensity
- Consistent triggering for alerts in any inconsistent conditions that found in a network
- Alerts should be sent to the users configured as per their customizations.

APPLICATIONS

- Networks serve as the backbone for any enterprise. Any network outage during working hours is huge loss for the organizations.
- As a result, they employ a separate team to look after their labs by constantly logging into several system interfaces and checking their statuses.
- It is a tedious task to login to each of these nodes, check if they are reachable and check their health status constantly.
- As the enterprise grows, the numbers increases exponentially.
- Generating network performance reports
- Deploying new technology and software upgrade successfully
- Monitoring the flow of traffic with netflow
- Track user network activity

REFERENCES

[1] **Dynamic Network Control with QoS and Resource Priority Monitor Based on Active "eM" for Commercial VoIP** – by Melanie Grah and Dr. Peter Radcliffe 2014

[2] **Architecture of a Network Performance Monitor for Application Services on Multi-Clouds** – by Young-min Kim, Ki-sung Lee, Jae-cheol Uhm, Si-chang Kim, and Chan-gun Lee 2013

[3] **Measurement-Aware Monitor Placement and Routing: A Joint Optimization Approach for Network-Wide Measurements** – by Guanyao Huang, Chia-Wei Chang, Chen-Nee Chuah, and Bill Lin 2012

[4] **Study on monitor and control of POL transport by road in IOT** – by Yang Chen, Qidong Yong, Dong Xiang 2012

[5] **Distributed Interplanetary Delay/Disruption Tolerant Network (DTN) Monitor and Control System** – by Shin-Ywan Wang 2012

[6] **Overhead Contact System On-line Monitor Technology Based on Wireless Sensor Network** – by Jiangjian Xie and Yi Wang, Tingting Lu 2011

[7] **The Design and implementation of a UPS Monitor and Control System** – by Lidong Fu and Bin Zhang 2011

[8] **Fault-tolerant Schemes for NoC with a Network Monitor** – by Zhang Ying , Wu Ning , Wan Yu Peng , Ge Fen , Zhou Fang 2010

[9] **Using activity sensitivity and network topology information to monitor project time performance** – by Mario Vanhoucke1. 2010

[10] **A transparent virtual machine monitor level packet compression network service** – by Ali Hamidi, Hadi Salimi and Mohsen Sharifi. [2010]

[11] **On evaluating the differences of TCP and ICMP in network measurement** – by Li Wenwei, Zhange Dafang, Yang Jinmin and Xie Gaogang [2007]

THANK YOU