-24-

AN EMPIRICAL NETWORK PERFORMANCE MONITORING SYSTEM APPLICATIONS SOFTWARE ASSESSMENT

Dawodu A. A., Lawal, O.O., Famuyiwa, K.S.A. & Akinyemi, O.S.
Department of ComputerScience, D.S Adegbenro ICT Polytechnic, Itori-Ewekoro, Ogun State
Corresponding Author:opepolawal@gmail.com; 08062160129

ABSTRACT
When it comes to computer networks, speed and efficiency are essential for both the Network Administrator and clients. These factors determine network performance and gauge the effectiveness of the Network Administrator. To ensure optimal network performance, the Network Administrator requires tools that focus on solving performance issues. Network Performance Monitoring Systems (NPMS) is a solution that provides essential tools for maintaining the network, meeting client demands, and enhancing network security. NPMS is a network monitoring system that manages CPU memory usage, hard disk usage, I/O devices, and other network devices.
Keywords: Network utilization, CPU memory usage, Hard disk usage, monitoring systems, and clients.

1. INTRODUCTION
1.1. Background of theStudy
The importance of networking cannot be overstated in the world of computing, telecommunication, and other technology fields. Therefore, it is crucial to keep an eye on the network to make the most of the resources it offers. A network performance monitoring system (NPMS) is a tool used by engineers to diagnose network issues. It is a client/server multi-threaded network diagnostic tool that gathers data about the network's status and availability. By providing network engineers with real-time and historical reports, NPMS enables them to troubleshoot network performance proactively. This tool also allows network administrators to capture, view and analyze network activities, and build network statistics such as network utilization, CPU usage, physical disk, and more.

The Network Performance Monitor is a real-time network monitor that can track network latency, traffic, and other network statistics. It continuously tracks packets crossing a network, thus providing an accurate picture of the network activity at any moment or a historical record of network activity over some time. In addition, the network administrator can use the NPMS to report client names, log-on time, log-out time, etc.

NPMS provides an essential ingredient in making large systems performance-aware and bandwidth adaptive. Performance issues are a significant concern when monitoring a network because when several computers are connected, complex interactions with unforeseen consequences are common. This complexity often leads to poor performance. Identifying bottlenecks that might cause network slowdowns, such as CPU utilization, memory usage, and allocation, is crucial to maintaining a high-performance network.

1.2. Statement of theProblem

As enterprise networks continue to grow in size, scope, and strategic importance, Network Administrators are facing numerous challenges in maintaining the performance and availability of their network. However, as customers deploy new network applications and services, measurements of network performance must recognize different levels of performance based on the different types of network traffic. Given these, the Network Managers often spend too much time trying to identify the source of performance problems and the need for performance troubleshooting tools that can identify performance problems before they seriously impact users and quickly identify the network devices that caused the performance problems once they have occurred. Furthermore, the network managers have the tool they need to identify performance problems, locate performance bottlenecks, diagnose latency, and identify performance trends in the network. Network Performance Monitoring Systems (NPMS) will enable the network manager toperform path and hop performance analysis, thus simplifying the identification of network devices that are contributing to the network performanceproblems.

1.3. Purpose of theStudy

The primary objective of this study is to create a program that can track network activities, including session duration, source IP, network response time, and system performance.

The main goals are as follows:

1. Secure the network against unauthorized access to sensitive data to prevent network congestion.
2. Optimize network resources to avoid overloading issues.
3. Monitor all information and data flowing in and out of the network.
4. Utilize effective monitoring tools to maintain a smooth networking environment.

2. LITERATUREREVIEW

In the Windows NT environment, there is a vast array of performance data available, with many performance counters traceable through standard monitoring tools. However, this abundance of data can lead to overwhelming management problems for analysts if a process is not implemented to quickly identify performance issues and address bottlenecks. Windows NT provides a wealth of data

on system interfaces and application performance, but it is crucial to avoid data overload. Key matrices can provide an overview of system performance for analysts. Despite changes in technology, the basics of analyzing system data have remained the same for over 30 years. If a server is not 100% busy, there may be a problem with the I/O and memory subsystems that require investigation. However, NT servers may run out of memory before any other resource due to changes in the CPU.

The network managed by the Simple Network Management Protocol (SNMP) consists of three essential components:

(a) ManagedDevices:A managed network contains a network node that has an SNMP agent. This node is known as a managed device, which is responsible for collecting and storing management information. This information is then made accessible to Network Management Systems (NMSs) via SNMP. Managed devices, which are also called network elements, can be routers, access servers, switches, bridges, hubs, computer hosts, or printers.

(b) An Agent: The agent is a software module for managing networks that are installed in a device that is being managed. It knows management information and converts it into a format that can be understood by SNMP.

(c) Network Management Systems (NMSs): Applications that monitor and control managed devices are executed by NMSs. These systems provide the necessary processing and memory resources for effective network management. It is essential to have at least one NMS on any managed network.

3. RESEARCH METHODOLOGY ANDFRAMEWORK

This research is focused on gathering non-numerical data through quantitative research methods and experimental validation. The target for assessment is a publicly accessible Network Administrator, and several Network Administrators were interviewed regarding the monitoring of network performance. End users were also asked relevant questions, and Windows NT performance monitoring tools were studied. The system was modeled using Unified Modeling Language (UML) and implemented using Visual Basic. The GFI LAN guard Network Security Scanner (LNSS) is a helpful tool for network administrators to perform a security audit quickly and easily. LNSS functions as a port scanner and creates reports that can be used to fix security flaws on the network. Unlike other scanners, LNSS provides information in a manageable way and includes hyperlinks to security sites for further information on vulnerabilities.

The LNSS has several features and they include:

- LANS is a LAN guard scripting tool that enables script creators to write complex security checks. It features a script editor with syntax highlighting capabilities and a debugger.
- Scheduled scans–You can schedule LNS to scan and send an email listing any differences it finds from the previous scan.
- Hot Fix Checker for Windows Machine–When you scan a machine, the system will now look for any hotfixes installed on it. This process no longer solely relies on checking registry keys, but it will also examine version-specific information on key files.
- Ability to Patch Windows Machines that are missing Hot Fixes – When LNS detects that a machine is without Service Packs, it can now automatically send and install the necessary hot fixes without requiring any user input. The installation can either happen immediately or be scheduled for a later time.

· Configuration Manager – With the LAN guard Network Scanner (LNS), you can now configure and customize your scanning preferences to your liking and save it to an initialization file. This eliminates the need to manually change the settings every time you want to switch between scan types. By saving and quickly reloading your configuration files, you can perform multiple scans in less time.

When conducting a network scan with the LANguard Network Scanner, the entire range entered from the main LNSS window is scanned. The scanner will detect which computers are active and only scan those responsible for it. This is achieved through the use of NetBIOS probes, Internet Control Message Protocol (ICMP) Ping, and SNMP queries.

4. SYSTEM DESCRIPTION AND LANGUAGEUSED

As a network administrator, it's crucial to be able to capture, view, and analyze the activities that occur on a network when users utilize workstations. The Network Performance Monitoring System is a multithreaded diagnostic tool that helps with this task. Network statistics like network utilization percentage, CPU usage, memory usage, physical disk (percent disk time), and physical disk (average queue length) are needed to understand the overall status of the network.

The NPMS system also helps locate traffic bottlenecks within a network. It continuously tracks packets crossing a network, providing an accurate picture of a period to establish a normal performance profile. The Unified Modeling Language (UML) was used to model the NPMS system in the next selection of the project. UML is an exciting tool in the world of system development today.

4.1 Use Case

The use case diagram describes the system's behavior from the user's perspective. In the case of the network performance monitoring system (NPMS), its use case is as follows:

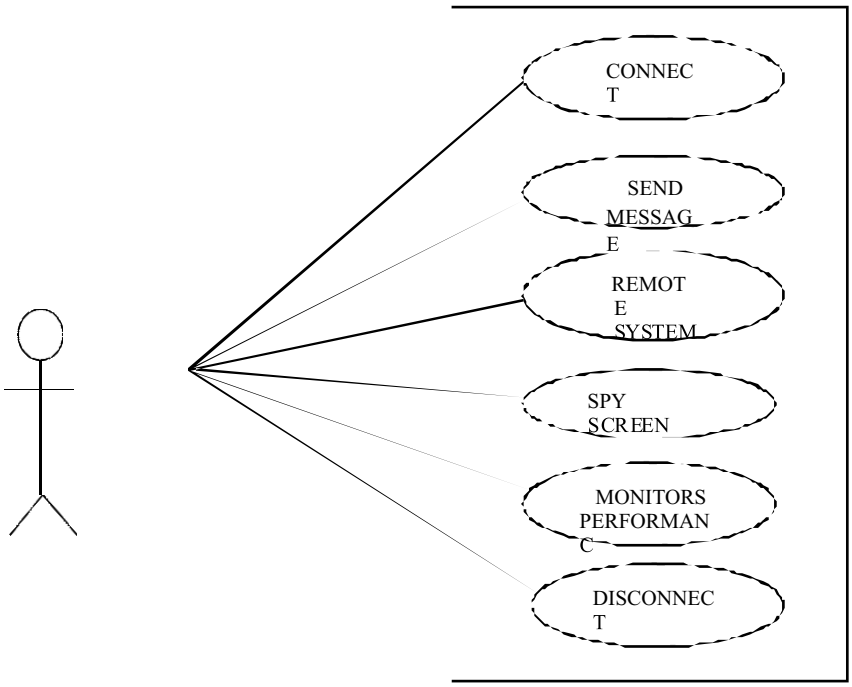


Fig. 1: Use Case Diagram

4.2 The Network Administrator

The only person who interacts with the system (NPMS) is the Network Administrator.

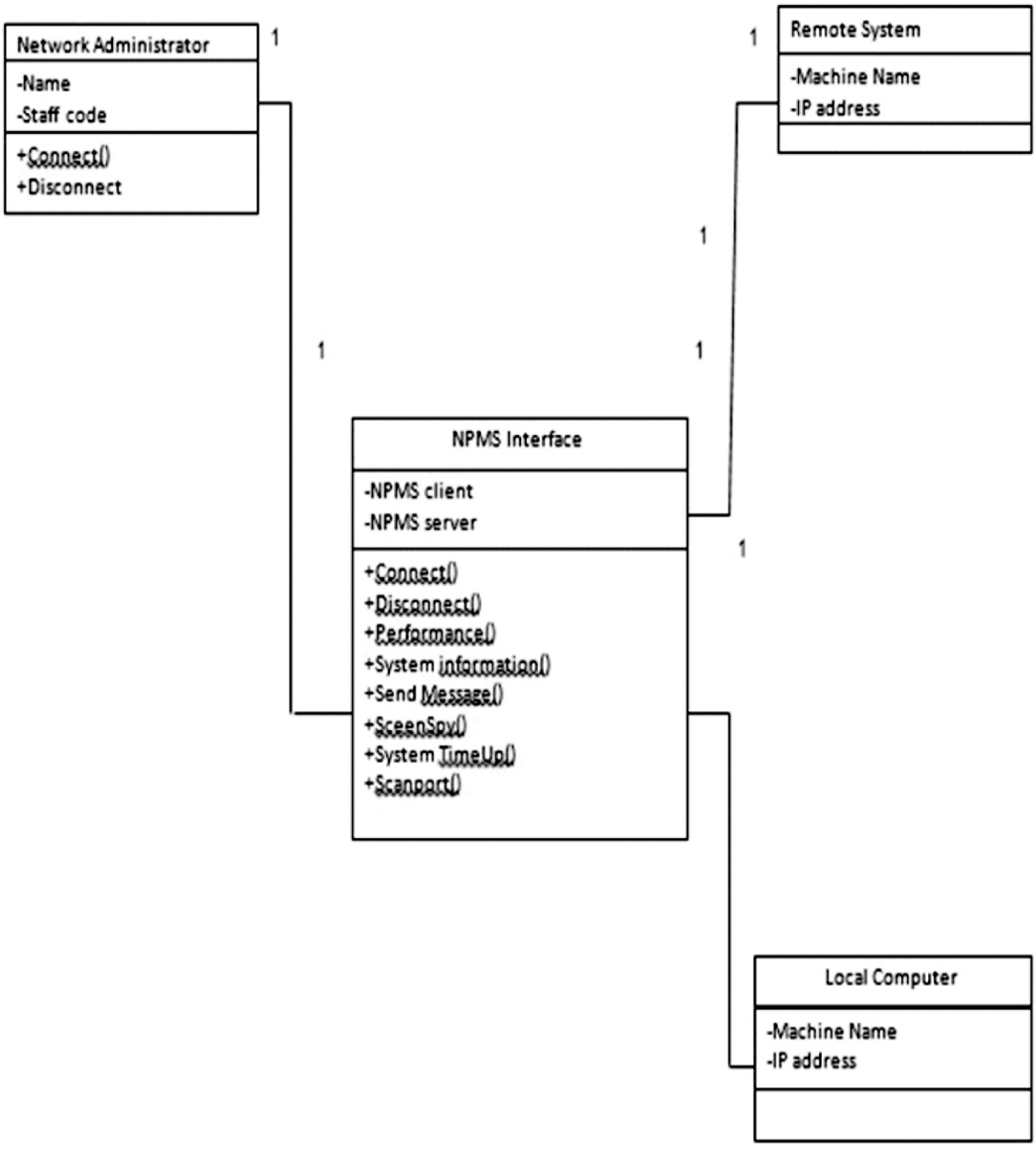


Fig 2: Network Actor Interaction

4.3 Class Diagram

The class diagram is useful for analyzing requirements and serves as a representation for developers to work on. It models each object present in the system.

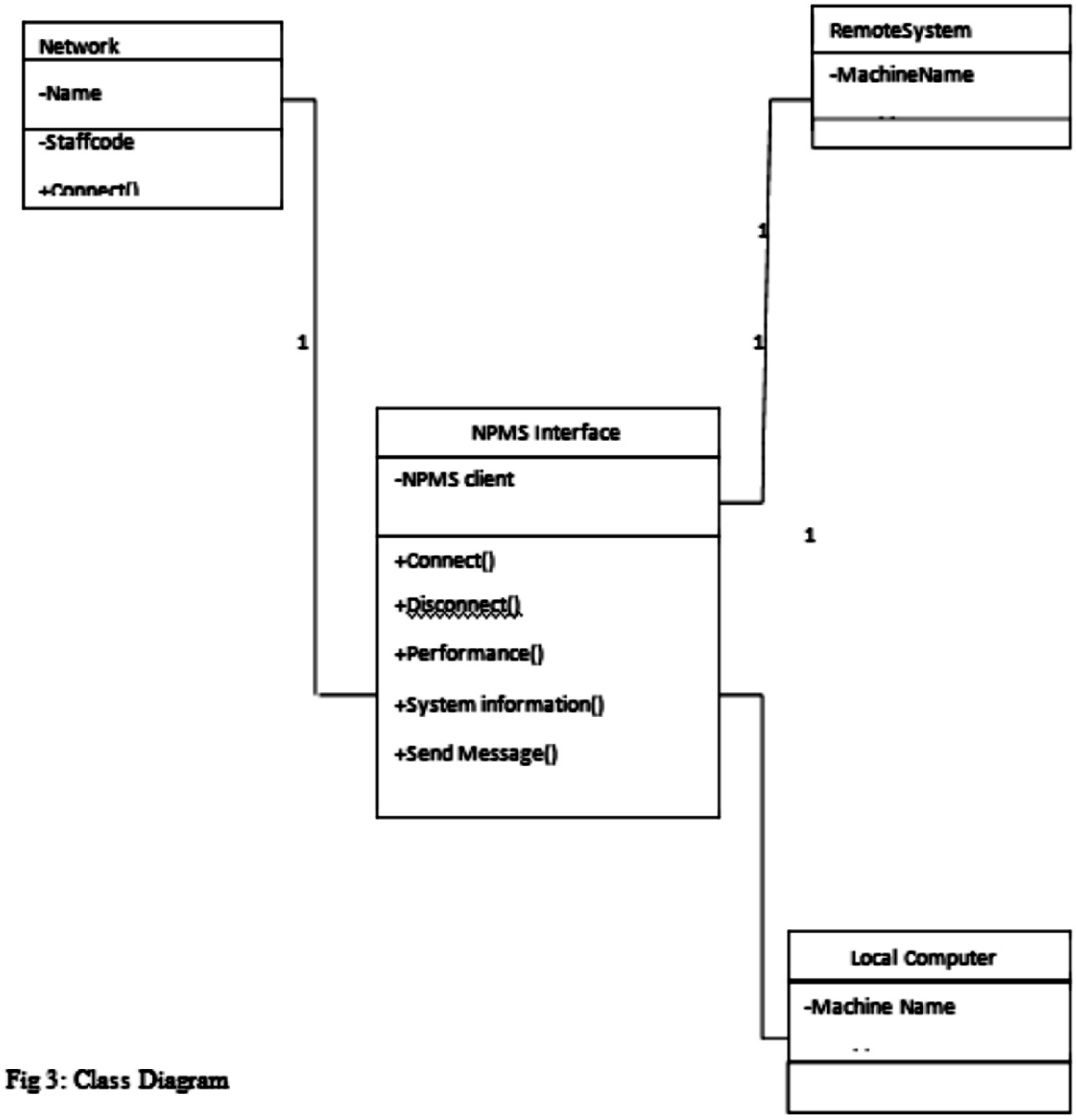


Fig 3: Class Diagram

In the NPMS system, the network administrator is responsible for connecting and disconnecting the machine before and after network monitoring. It's important to note that the monitoring computer (NPMS) can only connect to one remote computer at a time, and the network administrator interacts with just one NPMS.

a. Sequence Diagram

The sequence diagram depicts the chronological behavior of the system's object interaction. NPMS Server is the software installed on the network workstation that offers information regarding a workstation to solve server issues. On the other hand, NPMS Client is the front-end software that requests services from the NPMS Server situated at the back end.

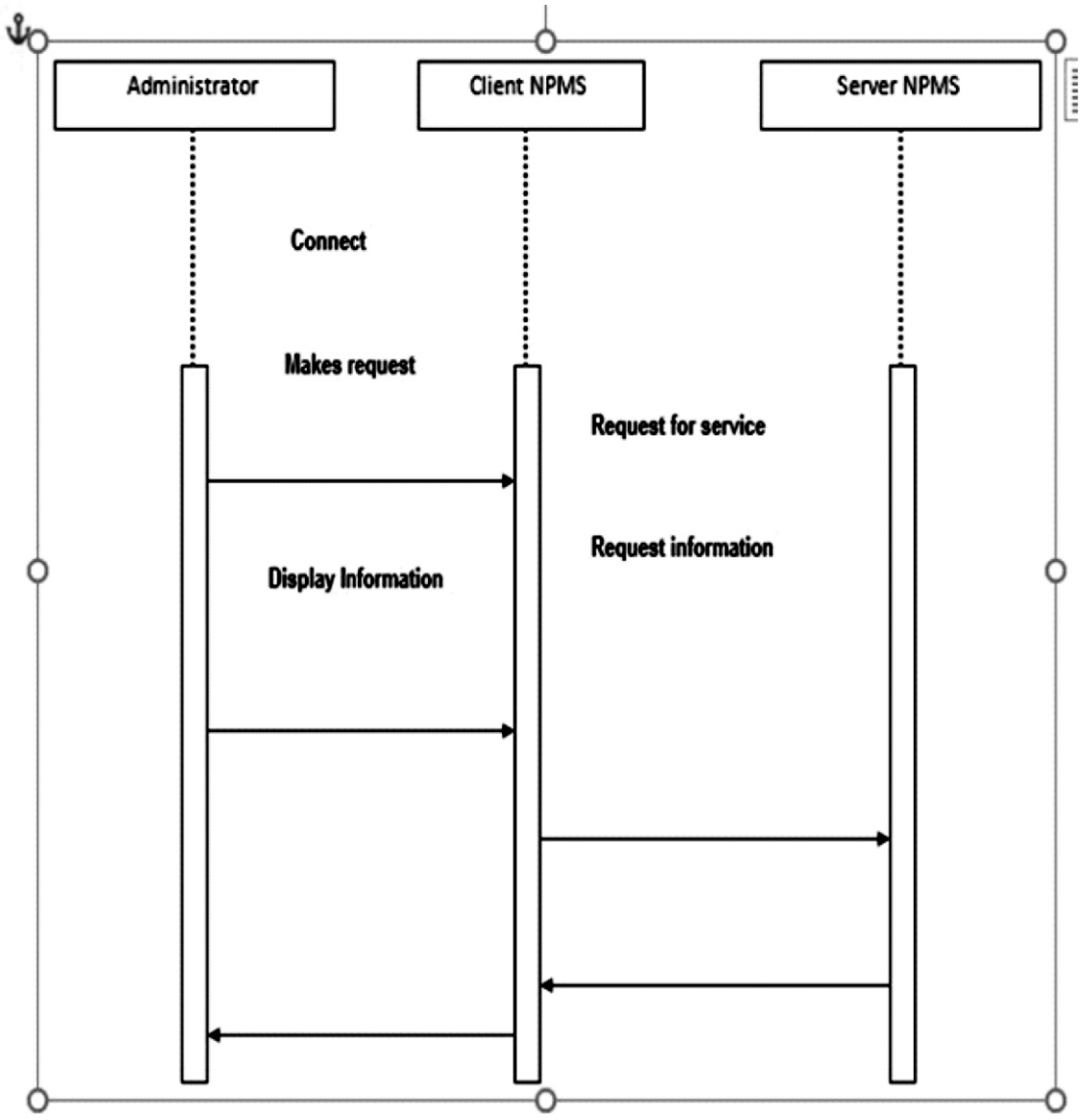


Fig 4: Sequence Diagram

a. ActivityDiagram

An activity diagram is a tool for illustrating activities, decision points, and branches. It depicts the flow of events that occur during an operation and is commonly utilized to model the sequence of events within the objects of a system.

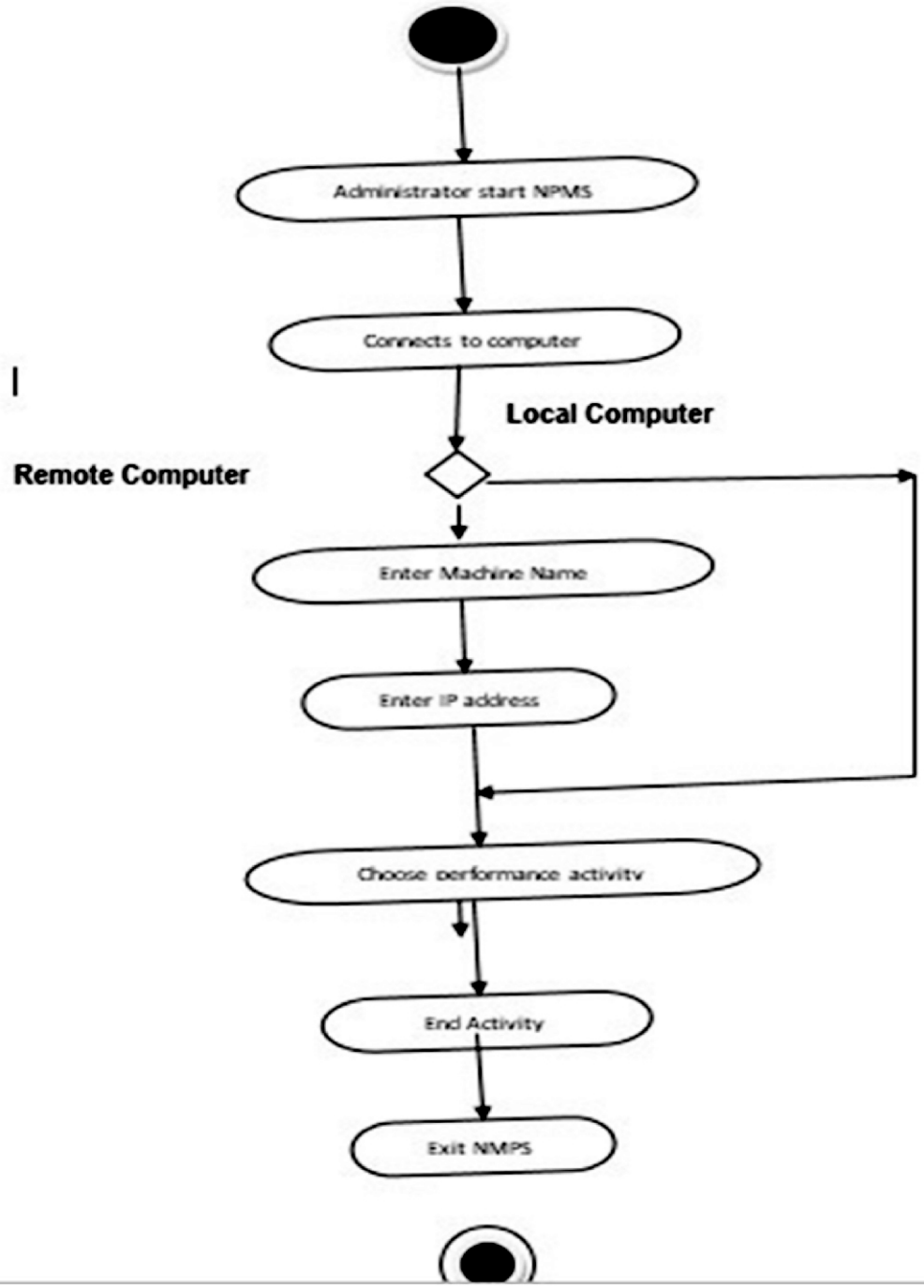


Fig 5: Activity Diagram

4. IMPLEMENTATION

NPM 1.0 is a tool for diagnosing networks, which operates on both client and server sides. It is compatible with Windows QX and other Windows NT platforms. The tool gathers data on the network's status and availability, as well as information on the workstations and local computers it is running on. It uses the latest network research development tools, including socket programming (Winsock in Visual Basic), ActiveX controls, and Windows API functions. The server program should be installed on all remote computers, while the client program should be installed on the monitoring computer.

The two software are designed to identify one another and establish a connection between the computers simultaneously.

1. Server Program: NPMS server
2. Client Program: NMPS client

NPMS server – This software is installed on the network workstation and supplies requested information to the server program. It automatically starts running at Windows startup and sends packets of data to the server program upon request, using integrated socket programming control called Winsock in Visual Basic 6.0.

NPMS client – The front-end software for NPMS requests services from the back-end NPMS server. Developed in a Visual Basic environment, the main interface is called "Network Performance Monitoring System Version 1.0". This dynamic utility includes the following tools:

* Connectivity
* Screen Spy
* Remote Control
* Performance Monitor
* Chatting (Message Sending)
* System Information

5. DISCUSSION

The research findings suggest that the tools used to assess vulnerabilities in Network Performance Monitoring Systems (NPMS) may not strictly adhere to the common vulnerabilities and exposures standard for speed and efficiency. Additionally, there are significant differences in the number of identified vulnerabilities between NPMS and Online Web Application Security. The study shows that proprietary tools like Screen Spy, Performance Monitor, and Nets Parker tend to be more reliable and exhaustive in probing for NPMS vulnerabilities.

It's important to note, however, that subsequent versions of these tools may address the limitations of the older versions. The study also found that some vulnerabilities, such as CSRF, were missed due to the scanners' ineffective functionality. Patil and Gosavi (2015) also discovered that different types of vulnerabilities require different detection methods.

The relevance of these findings is that Network Performance Monitoring Systems Vulnerability Scanners tend to identify more industrial standard results of NMPS application vulnerabilities. However, given the significant number of scanners available, this research is not exhaustive in

NPMS. The case study platform was developed using Internet Control Message Protocol and SNMP queries, and future research on platforms developed with other programming languages, such as XML, PHP, and Java, may be beneficial.

6. CONCLUSION

The Network Performance Monitoring System (NPMS) assists in network utilization, trend analysis, and network capacity planning. This planning involves assessing the current usage of server and network resources and tracking their utilization over time to predict future usage and necessary hardware upgrades. Capacity planning can be performed on a single computer or the entire network. However, further research is required to thoroughly compare open-source and proprietary tools for efficiency, effectiveness, and reliability. Additionally, the platform used for developing the NPMS test should be evaluated to determine any specific capabilities or limitations of open or closed-source tools on NPMS application platforms.

7. CONTRIBUTION TOKNOWLEDGE

NPMS is a crucial tool that aids in the creation of upcoming Network Services. It offers network performance measurement for various network protocols. The capacity to gauge network response time, ascertain device accessibility, scrutinize response time patterns, and provide real-time and historical performance reports are essential needs in modern enterprise networks.

REFERENCES

Andrew S. Tanenbaum, Computer Networks. Third Edition, Published by Prentice HallPTR

Eric Maiwald, Network Security, Published by Osborne/McGraw-Hill Copyright2001

Fred Halsall, Data Communications, Computer Networks, and Open Systems Fourth edition, published by Addison – Wesley LongmanLimited.

James Carless, Communications Engineering http://communications

Janes Chellis, Charles Perkins, Mathew Strebe (1999), MCSE: Networking Essentials Study Guide. Third Edition, Published by Network PressSybex.

Jenny L. Rosenbey, Measuring, and Monitoring Network Performance, SRM Associate,2001 MSDN Library Visual Studio 2008, by MicrosoftPress

Maione, Deennis, MCSE Window 2000 server (Training Guide) MCT (2000), copyright 2000, New Riders Publishing.

Microsoft Press, Windows API functionshttp://www.msn.com/msdn//

Microsoft Press, http://windows.microsoft.com/windows2000/Overview of PerformanceMonitoring.htm

Operating with GI LANguard Network Security Scanner by (MMC) Microsoft Management console, 2000

Peter Hodson, Local Area Network including Internetworking and Interconnection with WANs,2000

Perry Grey, SAMS Teach Yourself Visual Basic in 21Days.