Analyzing Network Security Efficiency in the Financial Industry

Adesina Adewale

A project report submitted in conformity with the requirements
for the degree of Master's of Science in Information Technology

Department of Mathematical and Physical Sciences
Faculty of Graduate Studies
Concordia University of Edmonton

Analyzing Network Security Efficiency in the Financial Industry

Adesina Adewale

Approved:

Dr. Nasim Hajari

Supervisor Date

Committee Member Name, Ph.D.

Committee Member Date

Dr. Alison Yacyshyn

Dean of Graduate Studies Date

Abstract

The financial sector plays an important role in the functioning of the economy. It represents a vast assortment of firms, agencies and institutions with operations ranging from small community banks to massive, international corporations. The ability of this industry to perform at their best heavily depends on their Network infrastructure efficiency and security. Companies usually struggle trying to figure out which Network infrastructure will suite them best at the start, and due to the fact that more people join the network on a regular basis, their Network efficiency has to be optimal and secure. The goal of this project is to analyze common Network architectures used in the financial sector and determine which of them is the best to implement. Each architecture will be simulated using NS-3 (Network simulator 3). Data gotten from these simulations will then be analyzed using Wireshark. and from there the Network efficiency can be determined
Keywords: Financial Industry, Network Infrastructure, Network Analysis, Simulation

Contents

List of Tables

List of Figures

List of Abbreviations

API	Application Programming Interface
DSDV	Destination Sequenced Distance Vector
IAB	Internet Activities Boar
IP	Internet Protocol
ISO	International Standards Organization
IS	information systems
IT	information technology
MNC	multinational company
NS-3	(Network simulator 3)
OLSR	Optimized Link State Routing Protocol
TCP	Transmission Control Protocol
VLANs	Virtual Local Area Networks

1 Introduction

In the age of technology, reliable network is needed for new client acquisition and for retaining current clients. Communication between the business and clients is vital, and it significantly depends on your network infrastructure [3] . Network infrastructure serves as the backbone of your day-to-day operations; everything else in a business relies on that backbone being strong and reliable so they can operate successfully. Majority of business operations rely on the functioning of your network, Especially the Businesses related in the financial sector. An unreliable network can severely affect business operations. A secure network infrastructure minimises downtime and ensures that productivity remains as consistent as possible, no matter what arises.

Network software, because of its complexity, is commonly layered into a hierarchy of protocols. Each protocol exchanges messages with its peers on other machines to implement some abstract communication service [18]. Except at the hardware level, peer-to-peer communication is indirect-the protocol passes messages to some lower level protocol, which in turn delivers the message to its peer. We abstractly represent the protocol layers that make up a communication system with a directed acyclic graph, called a protocol graph. The nodes of the graph correspond to protocols and the edges represent a depends on relation, for example, if protocol A sends messages to its peers using protocol B, then there is an edge from node A to node B [17]. Standardization bodies, such as the ISO and the IAB, typically establish policies about the form and content of the protocol graph for a particular network architecture. For example, Figure 1 illustrates a portion of the protocol graph that represents the TCP/IP network architecture

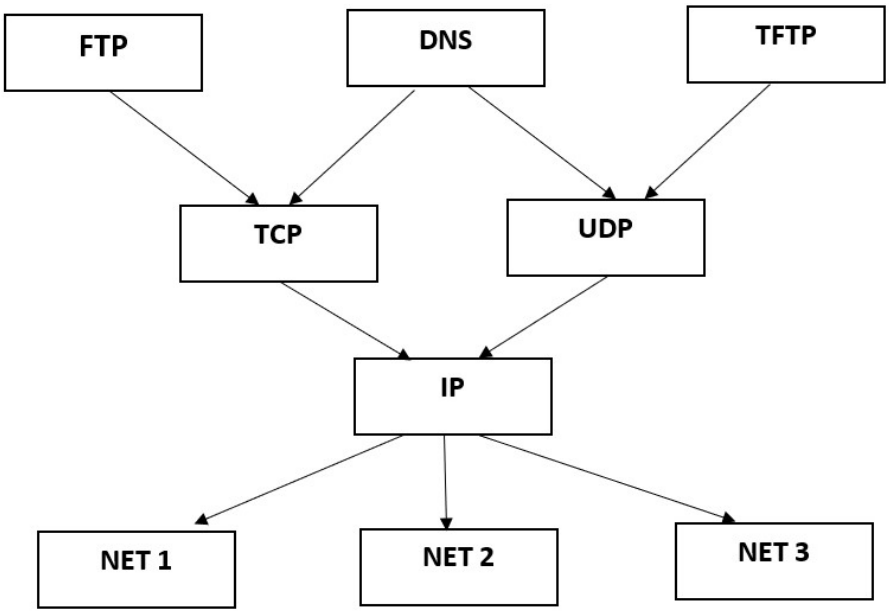

Figure 1: Protocol graph of the TCP/IP network architecture [18]

The Financial sector is an important and delicate sector in the modern world. Financial data represents some of the most sensitive information belonging to a person or an organization. financial institutions are charged with handling it safely while still keeping pace with the world around them. This is why the financial industry is unique in the needs and requirements it has for its network infrastructure. Few businesses must play such a delicate balancing game between security and efficiency as found in this sector [5].

Effective Network infrastructure efficiency can be determined in a number of ways. But according to a study done, it states that the best way is to implement the Network enviroment and perform a series of tests and pass various variables into it so as to determine the efficiency and get a detailed analysis of the network [2]. With the analysis gotten Businesses can now effectively determine the exact amount of devices to purchase, allow sufficient room for scalabilty for future growth of the business and can be confident that the Network performance will be at its very best [4].

The goal of this study is to implement Network infrastructures using simulation Labs. These simulations will give a real world experience of how the Network infrastructures will behave under specific conditions. Different data will be gotten from it such as the Latency, jitter, Packet loss and throughput. With these parameters, the efficiency of a particular network can be determined using a network analysis tool like wireshark. This technique will help to easily pass different variables and possible scenarios into the network and see how it will respond, so as to determine the most optimal Network to use.

Most Companies in this sector use an analysis tool after the Network infrastructure has been completely physically set up to determine their efficiency, but with the proposed approach companies in this sector and virtually view their network without purchasing the equipment. The code for the simulations will be written in C++ in the NS-3 application and will be executed using a Netanim module in the app. further analysis will be done on each network using wireshark network analysis tool.

2 Literature review (and theoretical framework)

Various works have been carried out in the recent years with the goal of finding the best way to calculate network infrastructure efficiency. Many analysis done is based on already establish physical models and mathematical equations.

Qiang Qiang et al. [2] talks about measuring network efficiency in congested networks. The new measure is applied to the Braess paradox network in which the demands are varied over the horizon and explicit formulae are derived for the importance values of the network nodes and links. This research uses Analysis with Mathematical Programming Methods to captures demands, flows, costs, as well as behavior of users of the network and produces network performance results.

A paper written by Anna Nagurney et al. [4] talks about using a N-Q performance/ efficiency tool that captures Network flow and can identify which network components, that is, nodes and links, have the greatest impact in terms of their removal and, hence, are important from both vulnerability as well as security standpoints. It also compares their new N-Q model with already existing model L-M to determine the results gotten corresponds to the previous model [4]. The Authors use a physical Braess Network and a coupled Braess Network to confirm their discoveries, The Network efficiency formula gotten from this model will be implemented in the code used for the simulations in this research.

Substrate Network technique was also a model used by representing the virtual networks using a graph (N,F) in which the physical routers are modelled as the vertices of the graph and the physical links as the edges [6]. They model the substrate network as an undirected graph GS=(NS,ES) = (NF u NX,ES), where NS is the set of substrate nodes, and ES corresponds to the set of bidirectional fiber links and access links. Note that NS consists of NF and NX where NF is the set of facility nodes and NX is the set of optical switches. Facility nodes access the network through access links connecting them to the optical switches NX [6]. With this technique Network implementations were dine using graphs and at the end of the analysis, Network efficiency could be determined

Network infrastructure Efficiency is a tool that businesses have been finding difficult to optimize. Mathematical formulas and implementation through graphs have been some of the ways businesses analyze their network infrastructure before implementation, and after implementation there are various software they can use to improve

their efficiency. But with Computer simulation and analysis, network efficiency can be further analyzed and understood [1].

3 Background

3.1 Network Efficiency

There are different aspects involved when building and optimizing networks such as:

•Network Topology: Network topology refers to the manner in which the links and nodes of a network are arranged to relate to each other. Topologies are categorized as either physical network topology, which is the physical signal transmission medium, or logical network topology, which refers to the manner in which data travels through the network between devices, independent of physical connection of the devices [21]. Network topology are the initial graphical diagrams that helps visualize the communicating devices, which are modeled as nodes, and the connections between the devices, which are modeled as links between the nodes.

•Network Traffic: Network traffic is the amount of data moving across a computer network at any given time. Network traffic, also called data traffic, is broken down into data packets and sent over a network before being reassembled by the receiving device or computer [22]. Network traffic has two directional flows, north-south and east-west. Traffic affects network quality because an unusually high amount of traffic can mean slow download speeds. Traffic is also related to security because an unusually high amount of traffic could be the sign of an attack[3].

•Network Security: Network security is a set of technologies that protects the usability and integrity of a company's infrastructure by preventing the entry or spread within a network of a wide variety of potential threats [8]. A network security architecture is composed of tools that protect the network itself and the applications that run over it. Effective network security strategies employ multiple lines of defense that are scalable and automated. Each defensive layer enforces a set of security policies determined by the administrator. Network security is key to an organization's ability to deliver products and services to customers and employees.

•Network monitoring Tool: These are that tools collect data in some form from active network devices, such as routers, switches, load balancers, servers, firewalls, or dedicated probes, which they analyze to paint a picture of the network's condition. Both collection and analysis are equally important functions of network monitoring tools – network admins need data that is detailed enough for their purposes, and they need comprehensible output that provides them with the knowledge they need [23]. They help bring the status and health of the whole network into one User interface after it has been implemented so that the network admins can see where issues arise, or have chances of arising, so they may take effective measures and restore regular service.

when everything is working seamlessly in a company's network, business runs smoothly and data is transmitted, handled, and used with ease [20]. A seamless network efficiency should have:
• Redundant connections, each with failover solutions at the ready.
• Data security that is provided through separate network paths for public and private usage.
• One interface that is used to manage all communication tools.
• Up-to-date technologies to support SaaS applications.
• Reliable, consistent up time with dependable SLA guarantees from your provider [20].

There are different aspects to promoting network Efficiency.

3.2 Key Metrics

Network Performance also known as quality of the network can be measured using Network key metrics. These metrics are important to any network and are designed to help users evaluate how well their networks are doing and discover any problem areas [7]. With all the information being displayed, though, how do you know what metrics to look at? There a a lot of metrics associated with Networking but we will be looking into the 4 main key metrics.

3.2.1 Latency

In a network, latency refers to the measure of time it takes for data to reach its destination across a network. You usually measure network latency as a round trip delay, in milliseconds, taking into account the time it takes for the data to get to its destination and then back again to its source [8]. Measuring the round trip delay for network latency is important when knowing how to measure network performance because a computer that uses a TCP/IP network sends a limited amount of data to its destination and then waits for an acknowledgement that the data has reached its destination before sending any more. Therefore, this round trip delay has a big impact on network performance [7].

When measuring latency, consistent delays or odd spikes in delay time are signs of a major performance issue that can happen for a variety of reasons. Most delays are actually undetectable from a user's perspective and can therefore go unnoticed but can have a huge impact when using VoIP, or unified communication.

3.2.2 Jitter

network jitter is a network transmission's biggest enemy when using real-time apps such as unified communications, including IP telephony, video conferencing, and virtual desktop infrastructure.These are very common in the Financial Industry. Jitter is a variation in delay. Otherwise known as a disruption that occurs while data packets travel across the network. There are many factors that can cause jitter,

and many of these factors are the same as those that cause delay. One difficult thing about jitter is that it doesn't affect all network traffic in the same way.

Jitter can be caused by network congestion. Network congestion occurs when network devices are unable to send the equivalent amount of traffic they receive, so their packet buffer fills up and they start dropping packets. If there is no disturbance on the network at an endpoint, every packet arrives. However, if the endpoint buffer becomes full, packets arrive later and later. It can also be caused by the type of connection you use. A connection on a shared medium, such as a cable, is more likely to have higher jitter than a dedicated connection. So that's something to keep in mind when choosing a connection medium.

3.2.3 Packet Loss

Packet loss refers to the number of data packets that were successfully sent out from one point in a network, but were dropped during data transmission and never reached their destination. It's important for any IT team to measure packet loss to know how many packets are being dropped across your network to be able to take steps to ensure that data can be transmitted as it should be. Knowing how to measuring packet loss provides a metric for determining good or poor network performance [7].

Packet loss is usually expressed as a percentage of the total number of sent packets. Often, more than 3percent packet loss implies that the network is performing below optimal levels, but even just 1 percent packet loss might be enough to affect VoIP quality [8]. Packet loss is something that is determined over a period of time. If you record 1 percent packet loss over 10 minutes, it can suggest that you have 1percent during the whole 10 minutes, but it can also be that you have 10percent packet loss over 1 min and then 0 percent over the remaining 9 minutes [7].

3.2.4 Throughput

Throughput refers to the amount of data passing through the network from point A to point B in a determined amount of time. The key function of a network is to transmit data from one device to another. Throughput measures the rate of successful data transfer over a period of time. his metric shows you what your network is doing rather than what it's capable of, which is important in determining if it's meeting expectations [8]. Measuring network throughput is usually done in bits per second (bit/s or bps).

Throughput is the ultimate key metric for analyzing Network efficiency. This is because it applies the other 3 key metrics to derive the overall throughput of a Network

4 Technical Framework

4.1 Network Simulation

Network simulation offers an efficient, cost-effective way to assess how the network will behave under different operating conditions. Simulation results can be analyzed to assess network performance, identify potential problems, understand the root cause, and resolve the issues prior to deployment. Since running simulations in the laboratory is much faster and less expensive than performing live tests, it is easier to investigate different alternatives using simulations before deploying a network or making changes to an existing network. Network simulation is the most useful and common methodology used to evaluate different network topologies without real world implementation.

Network simulation can also help network operators assess the resiliency of networks to cyber threats, for example, how vulnerable is the network to cyber attacks and how effective are counter-measures in containing or defending against the threats. This assessment can be done without subjecting the physical network to actual cyber attacks, and hence, without the risk of leakage of the attack vectors into live assets. Thus, network simulation provides a low cost, low-risk, and easy to use means for predicting network behavior and identifying potential problems before deployment.

4.1.1 Simulation Modeling Methodologies

Simulations have been carried out on NS2 to compare and analyze routing algorithms, such as the DSDV, AND OLSR based on various performance metrics. However, performance comparison and analysis between the classical routing protocol types, proactive and reactive, have rarely been done using NS3 in the Linux Ubuntu operating system.

4.2 NS-3 (Network Simulator-3)

Ns-3 is chosen for this project because it has a designed set of libraries that can be combined together and also with other external software libraries. While some simulation platforms provide users with a single, integrated graphical user interface environment in which all tasks are carried out, ns-3 is more modular in this regard. Several external animators and data analysis and visualization tools can be used with ns-3. However, users should expect to work at the command line and with C++ and/or Python software development tools [9].

It is the upgraded version of ns-2. NS-3 provides features not available in ns-2, such as a implementation code execution environment, allowing users to run real implementation code in the simulator, ns-3 provides a lower base level of abstraction compared with ns-2, allowing it to align better with how real systems are put together. Some limitations found in ns-2 (such as supporting multiple types of interfaces on nodes

correctly) have been fixed in ns-3.

some features of the ns-3 are:
• Software core: designed to improve scalability,modularity, coding style, and documentation, the core is written in C++ but with an optional Python scripting interface. Several C++ design patterns such as smart pointers, templates, callbacks, and copy-on-write are leveraged. Object aggregation capabilities enable easier model and packet extensions [10].
• Attention to realism: the Internet nodes are designed to be a more faithful representation of real computers, including the support for key interfaces such as sockets and network devices, multiple interfaces per nodes, use of IP addresses, and other similarities [10].
• Software integration: an architecture to support the incorporation of more open-source networking software such as kernel protocol stacks, routing daemons, and packet trace analyzers, reducing the need to port or rewrite models and tools for simulation [11].
• Support for virtualization: lightweight virtual machines running over a (possibly wireless) simulation network are an attractive combination for current research; ns-3 plans to support a few modes of such operation including a native "process" environment where Posix-compliant applications can be easily ported to run in simulation space with their own private stack, and including support for tying together virtual machines of various types [10].
• Testbed integration: ns-3 will enable the testbedbased researcher to experiment with novel protocol stacks and emit/consume network packets over real device drivers or VLANs. The internal representation of packets is network-byte order to facilitate serialization [11].
• Attribute system: researchers require a means to identify and possibly reassign all values used to configure parameters in the simulator. ns-3 provides an attribute system that integrates the handling and documentation of default and configured values [11].
• Tracing architecture: ns-3 is building a tracing and statistics gathering framework using a callback-based design that decouples trace sources from trace sinks, enabling customization of the tracing or statistics output without rebuilding the simulation core [11].

4.2.1 NS3 Simulation Modeling Methodology

To establish NS3 simulations, several classes such as core-module.h and network-module.h need to be included. These classes plus their detailed descriptions can be found in NS3 API. Moreover, NS3 employs C++ and Python languages, and several simulation steps need to be followed to start any NS3 simulations [**?**]. The NS3 simulation procedures are shown in Figure 2.

4.2.2 NetAnim Module

This a module found in the ns3 program. NetAnim is a stand-alone program which uses the custom trace files generated by the animation interface to graphically display the simulation. The NetAnim GUI provides play, pause, and record buttons. Play and pause start and stop the simulation. The record button starts a series of screenshots of the animator, which are written to the directory in which the trace file was run. Two slider bars also exist. The top slider provides a "seek" functionality, which allows a user to skip to any moment in the simulation. The bottom slider changes the granularity of the time step for the animation. Finally, there is a quit button to stop the simulation and quit the animator [9]. This is the specific module that will be used to visualize the simulations done.

4.3 Wireshark

Wireshark is the world's foremost and widely-used network protocol analyzer. It lets you see what's happening on your network at a microscopic level and is the standard across many commercial and non-profit enterprises, government agencies, and educational institutions [12]. It has some good features in which will be beneficial and works very well with the ns-3 simulator. some of the features are:
•Deep inspection of hundreds of protocols, with more being added all the time.
•Live capture and offline analysis.
•Multi-platform: Runs on Windows, Linux, macOS, and many others.
•Live data can be read from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI, and others.
•Output can be exported to XML (which is used by ns-3), PostScript®, CSV, or plain text [12].

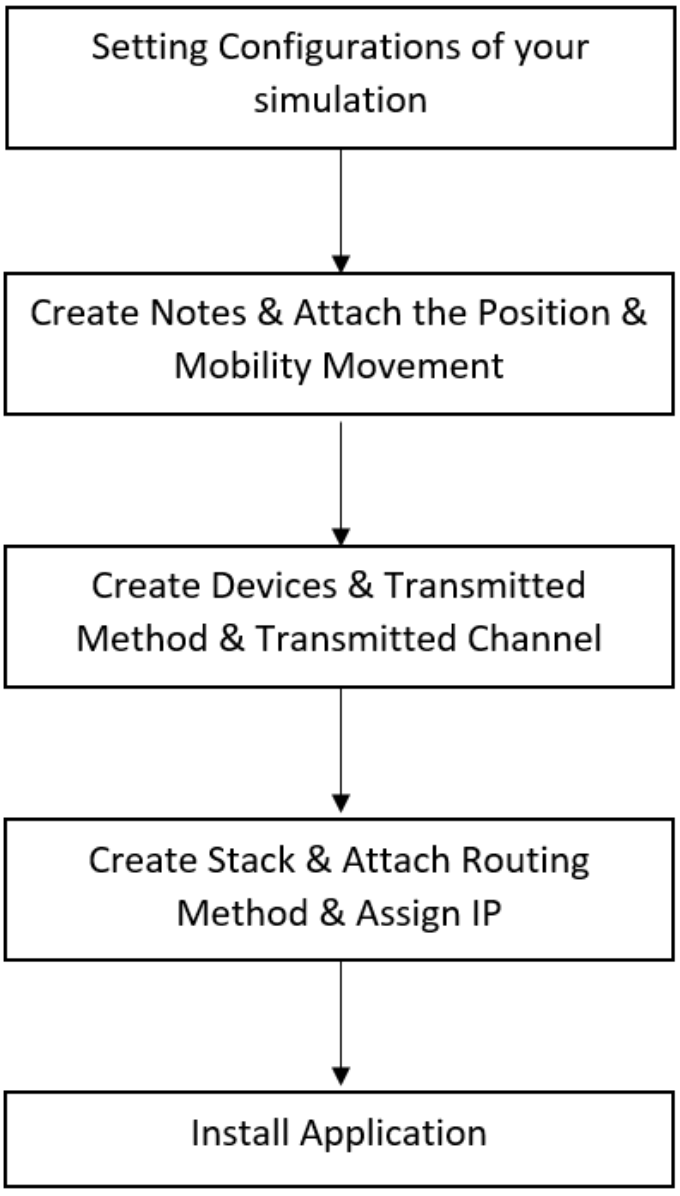

Figure 2: NS3 simulation procedures [24].

Table 1: NS-3 Simulation parameters.

Parameter	**Value**
Operating System	Ubuntu 18.04
Channel Type	Wired & Wireless Channel
Number of Nodes	12-15
Number of Sink Nodes	10, 30, 50
Node Min Movement Speed (m/s)	4
Node Max Movement Speed (m/s)	10
Data Type	UDP
Simulation Total Time (s)	30
MAC Protocol 802.11	802.11
Wi-Fi Transmit Frequency	2.4 GHz
Data Packet Size (bytes)	64, 256, 512
Area of Simulation (m)	500*500
Radio Prop. Model	Two Ray Ground
Routing Protocols	DSDV,OLSR, AODV, DSR
Initial Nodes Power (J)	50
Each Received Consumption Power(J)	0.0174

5 Project Design

5.1 Simulation Parameters

First, all parameter values are presented. Simulation notes are then created and the grid of simulations is defined using the parameters shown in table 1 All functions relative to the nodes will be defined as well. The Internet Layer of the devices will be created, which will declare how the data transmitted between the devices and which channel is using the devices. At the same time, the devices are installed according to the nodes. In the transport layer, the IP address, ports and the routing method are set up. The stack for the Internet to store the IP address, ports, and kind of information are also defined. In the application layer, the source nodes and the sink nodes are assigned for the data transition. Lastly, the simulations are ready to carry out with the schedule time.

5.2 Network Architectures

3 Network diagram have been chosen based on models used in [5] because of their importance to the industry.

5.2.1 Network 1

The first Network to be implemented is based on a Braess network architecture. "Braess paradox that states it is the observation that adding one or more roads to a road network can slow down overall traffic flow through it" [5]. This is an important criteria for a financial business because it is always prone to grow. Figure 3 shows this model as it has many nodes branching from other nodes and other devices can still be added.

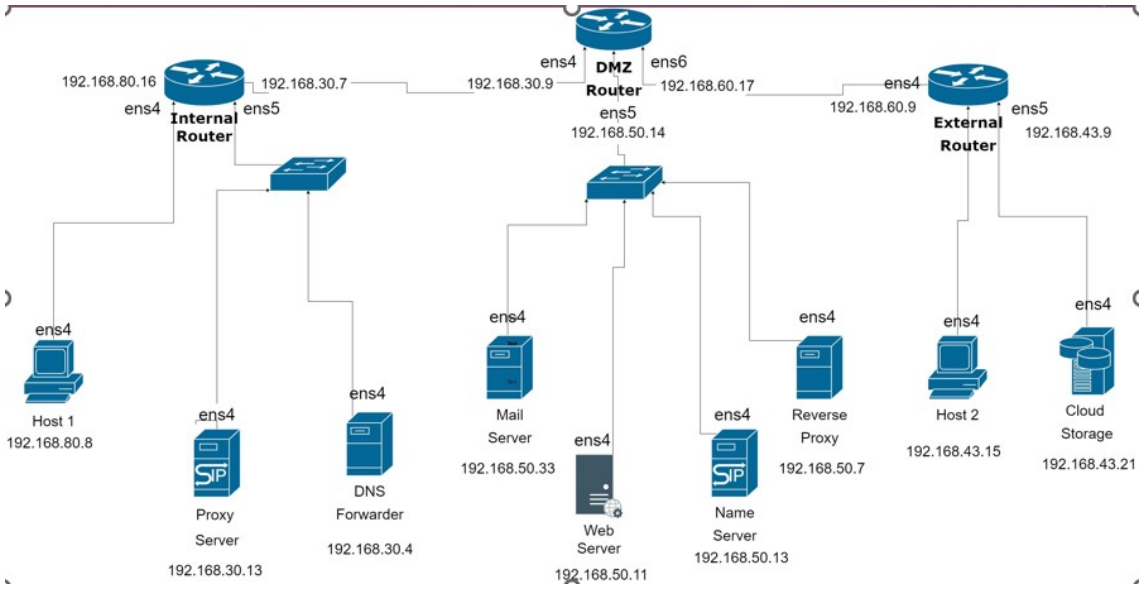

Figure 3: Network 1

5.2.2 Network 2

The second Network is based on Substrate Network architecture. Substrate means considering the architecture as a graph and placing the nodes in specific areas of that graph so as to enable data efficiency in the network [4]. Figure 4 shows this architecture.

5.2.3 Network 3

The third Network is based on the Gradient Network architecture that refers to building complex networks out of existing Networks with as much nodes is needed [5]. This is an extension of substrate network but more complex. Figure 5 shows the network architecture

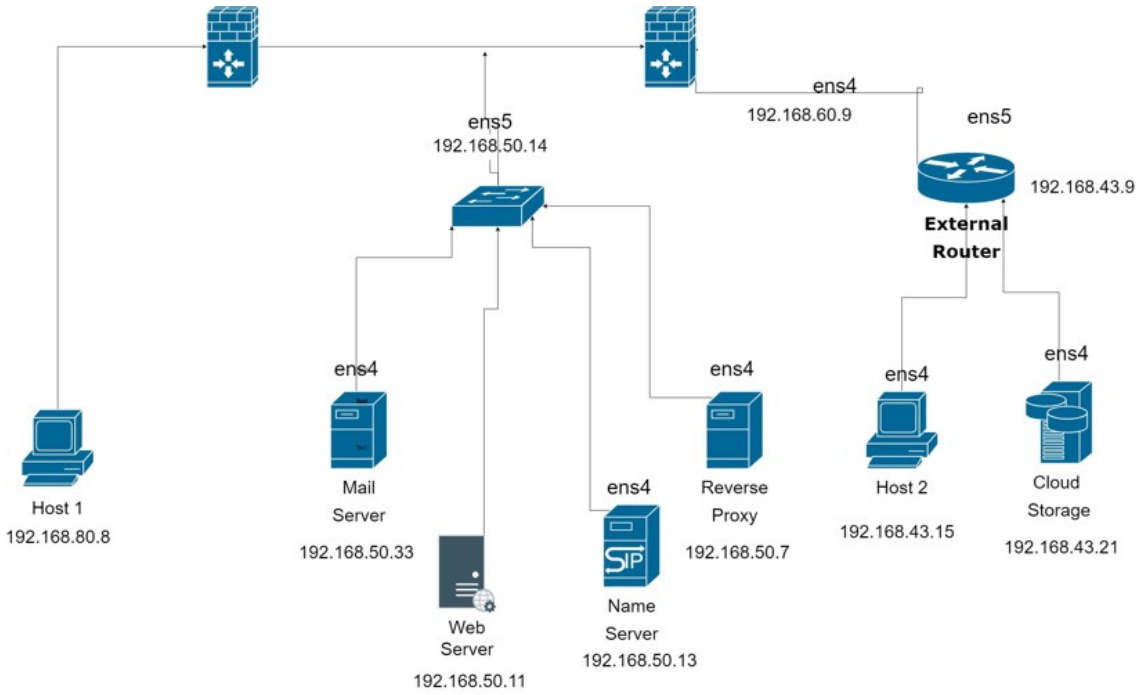

Figure 4: Network 2

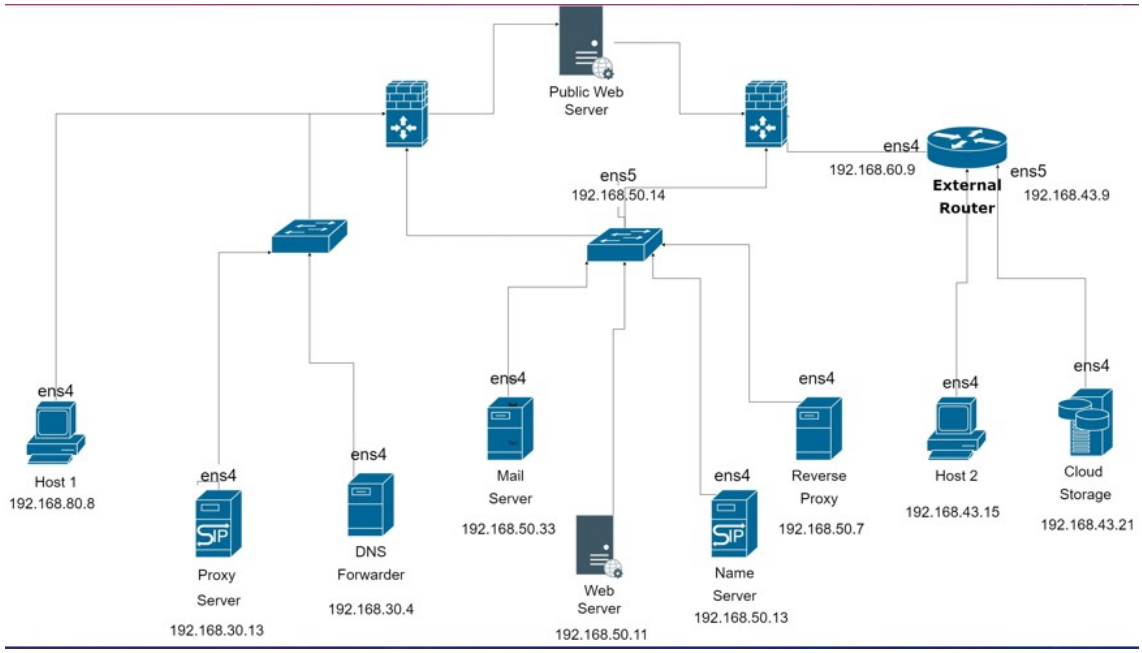

Figure 5: Network 3

5.3 Ns-3 C++ coding

Code for the ns-3 is written in C++ and the formula for throughput established by [2] will be implemented in the code. Different devices like routers and switches will be added using ns-3 modules. A sample of the code is shown in Figure 6. It shows the network diagram and modules attached to the code to be implemented

```
41 // AP0--(1-5 nodes) |   AP1--(1-5 nodes)  |   AP2--(1-5 nodes)
42 //        ---                 ---                 ---
43 //         |                   |                   |
44 //         5m                 5m                  5m
45 //         |                   |                   |
46 //        ---                 ---                 ---
47 //     (-1,0) /----5m----/ (0,0)  /----5m----/  (1,0)
48 // AP3--(1-5 nodes) |AP4(Test)--(1-3 nodes) |   AP5--(1-5 nodes)
49 //        ---                 ---                 ---
50 //         |                   |                   |
51 //         5m                 5m                  5m
52 //         |                   |                   |
53 //        ---                 ---                 ---
54 //    (-1,-1) /----5m----/ (0,-1)  /----5m----/ (1,-1)
55 // AP6--(1-5 nodes) |  AP7--(1-3 nodes)  |  AP8--(1-5 nodes)
56 //================================================================================
57 // Extended Version (flexible model) - MxN grid
58 // M = raws
59 // N = netSize/raws
60 // 1 test AP + netSize other, each 5m away from their neiburhg
61 // AP can take several possitions
62 //================================================================================
63
64 //Include libraries
65 #include "ns3/core-module.h"
66 #include "ns3/network-module.h"
67 #include "ns3/applications-module.h"
68 #include "ns3/wifi-module.h"
69 #include "ns3/mobility-module.h"
70 #include "ns3/internet-module.h"
71 #include "ns3/flow-monitor-module.h"
72 #include "ns3/random-variable-stream.h"
73 #include "ns3/netanim-module.h"
74 #include <iostream>
75 #include <fstream>
76 #include <vector>
77 #include <string>
78 #include <math.h>
```

Figure 6: C++ code showing network diagram and modules

Once the code has been written and implemented all data gotten from the network will be exported into a pcap file as show in Figure 7. Details shown here show the throughput, the source and destination IP, protocol and length of packet sent.

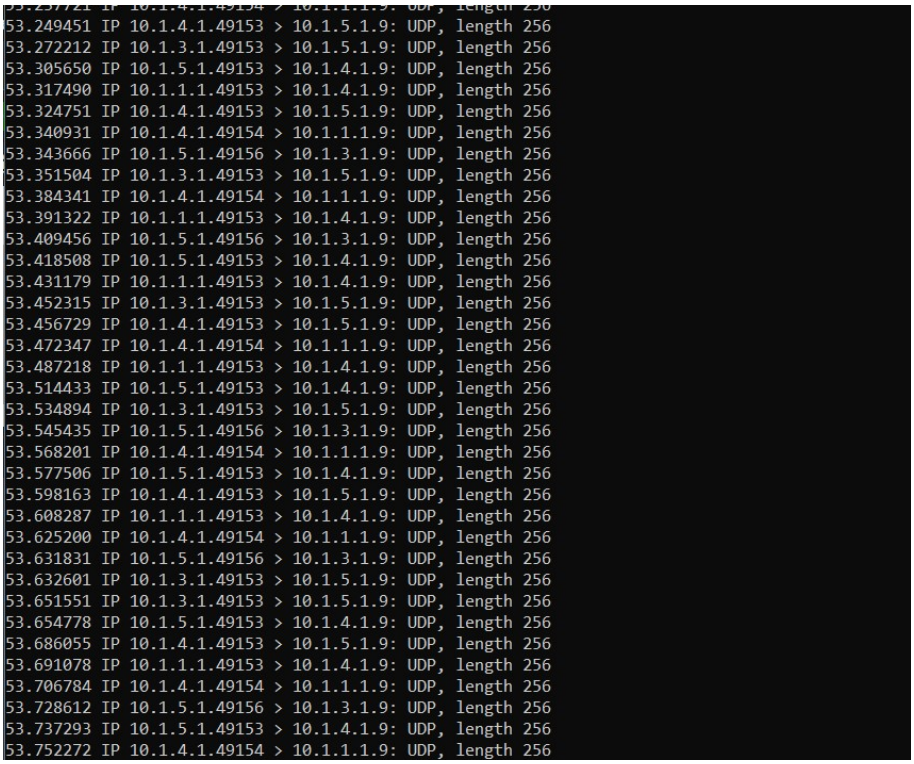

Figure 7: Result of data gotten from Network

5.4 NetAnim Simulation

The Netanim simulation is gotten from an xml file exported after the c++ code has be executed. The simulation shows packets moving through out the network as shown in Figure 8. The simulation shows how the network would behave in a real world circumstance as packets pass through the network.

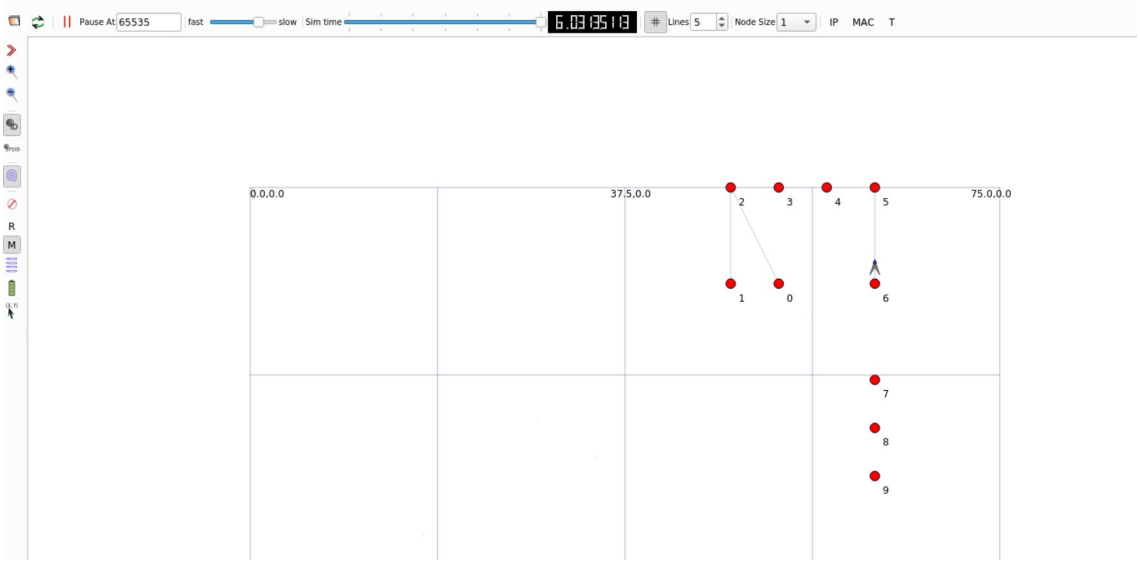

Figure 8: Network Simulation with Netanim

5.5 Wireshark

A wire shark analysis is done on data gotten from the executed code as shown in Figure 7. the analysis is to export a throughput graph using that data. Figure 9 shows wireshark analyzing the data.

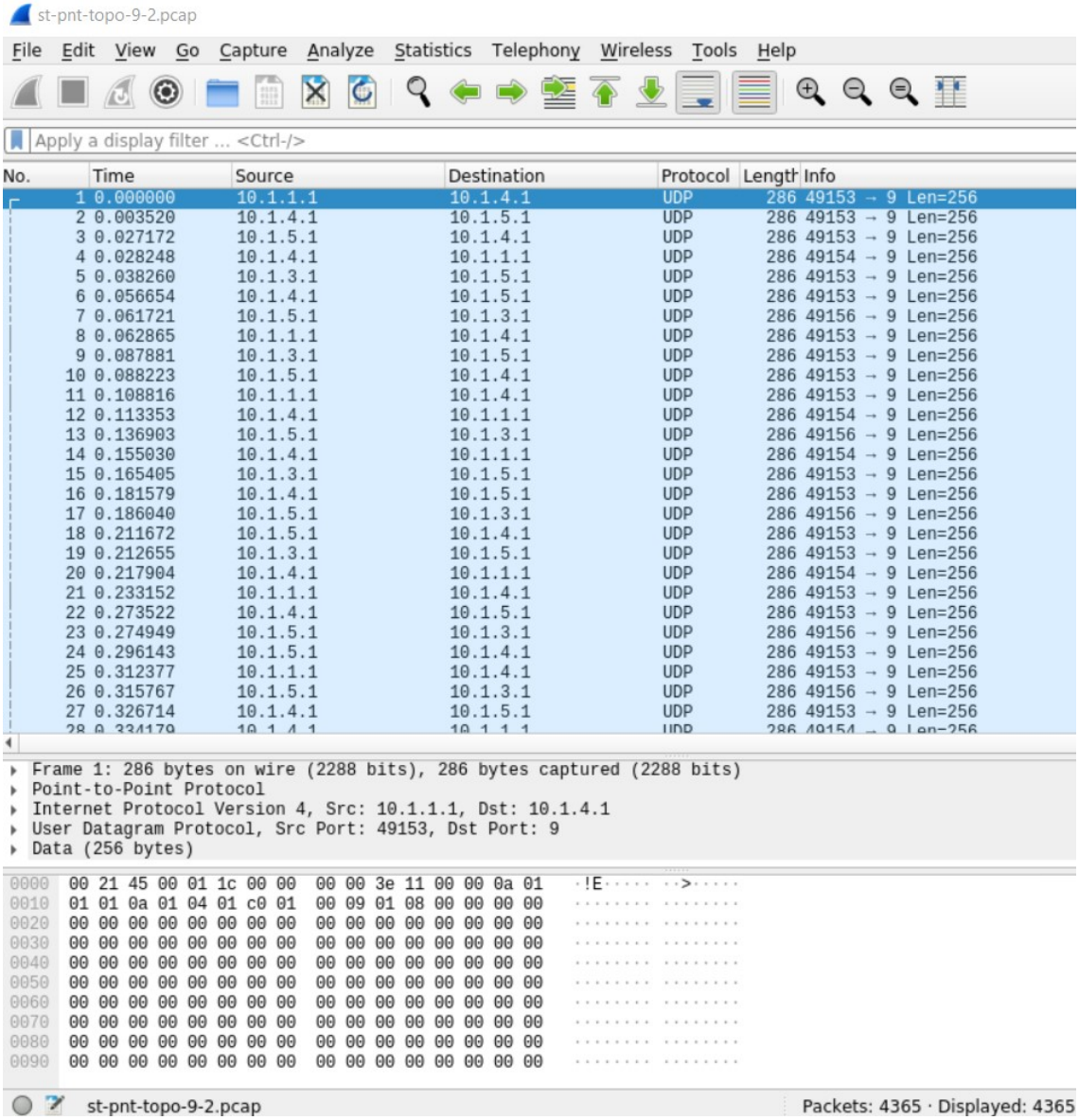

Figure 9: Wireshark data analysis

6 Results

Once Each of the Networks have been analyzed using the wireshark, the graph is plotted using throughput rate against simulation Time. The following graphs can be gotten for each of the previous stated networks.

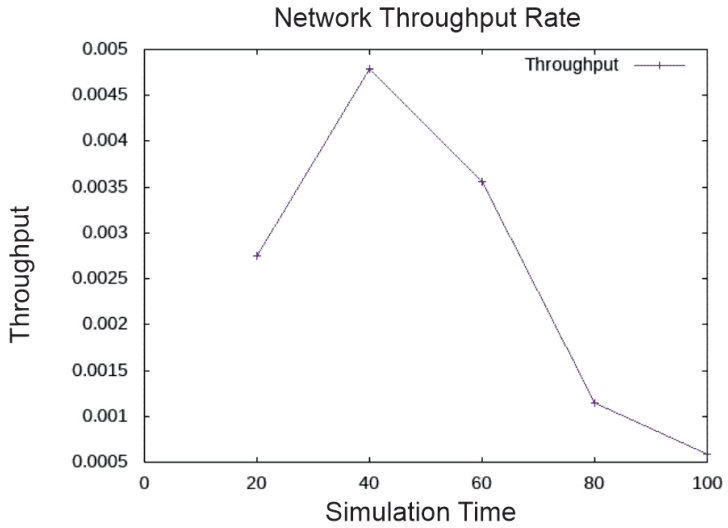

Figure 10: Throughput Graph of Network 1

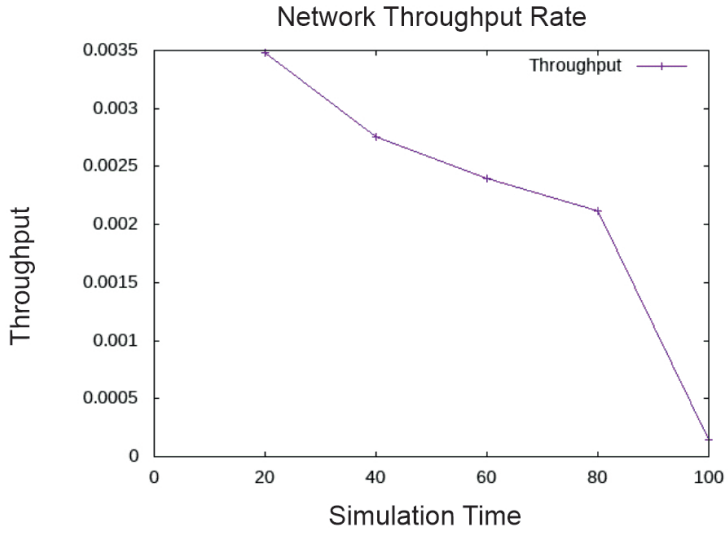

Figure 11: Throughput Graph of Network 2

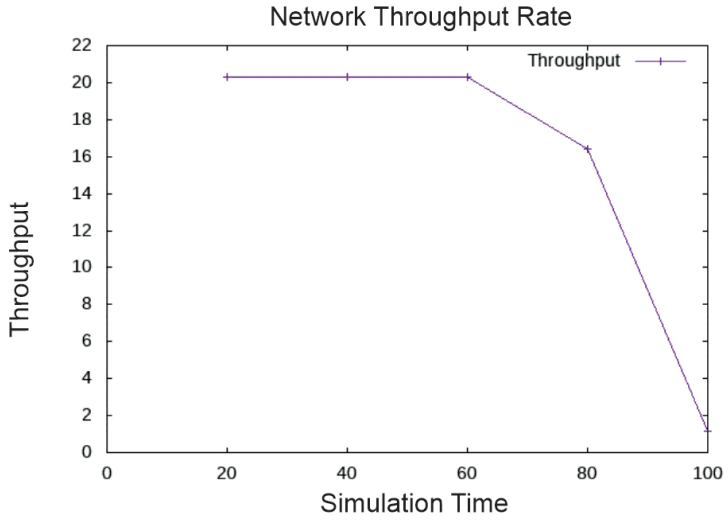

Figure 12: Throughput Graph of Network 3

7 Conclusions

From the results section it can be said that Network 3 has the best throughput rate, due to it being more constant than the other two Networks. With this findings, I recommend that Network 3 be implemented for financial businesses that start out big and the network is prone to grow over time. I would recommend Network 2 for small financial businesses that don't start of too big but is projected to eventually grow.

8 Recommendations

This Process can be used by any startup business to determine the best network architecture for them based on its efficiency. It can also be further developed to see how the networks would behave under certain Networking threats.

9 Acknowledgments

I would like to express my very great appreciation to Dr Nasim Hajari for her valuable and constructive suggestions during the planning and development of this research work.

References

[1] Mohammed, Derek. "Cybersecurity compliance in the financial sector." The Journal of Internet Banking and Commerce 20.1 (1970): 1-11.

[2] Nagurney, Anna, and Qiang Qiang. "A network efficiency measure for congested networks." EPL (Europhysics Letters) 79.3 (2007): 38005.

[3] ndustry news REMARK GROUP „importance of your Network Infrastructure?" 2022 [Online]. Available:(https://www.remark-group.co.uk/industry-news/do-you-know-the-importance-of-your-network-infrastructure)

[4] Nagurney, Anna, and Qiang Qiang. "A network efficiency measure with application to critical infrastructure networks." Journal of Global Optimization 40.1 (2008): 261-275.

[5] Document Solutions, INC „Network Infrastructure for a Financial Institution" 2022. [Online]. Available:(https://blog.dsinm.com/blog/network-infrastructure-for-a-financial-institution) [Accessed 15-July-2022].

[6] Yu, Hongfang, et al. "Cost efficient design of survivable virtual infrastructure to recover from facility node failures." 2011 IEEE international conference on communications (ICC). IEEE, 2011.

[7] Alyssa Lambert „How to Measure Network Performance" Jan 7 2022. [Online]. Available: (https://obkio.com/blog/how-to-measure-network-performance-metrics/) [Accessed 15-July-2022].

[8] Daniel Hein „5 Key Metrics to Analyze When Evaluating Network Performance" Jan 29, 2019, Available:(https://solutionsreview.com/network-monitoring/5-key-metrics-to-analyze-when-evaluating-network-performance/) [Accessed 16-July-2021].

[9] nsam „Introduction to ns3" 2018 . [Online]. Available: (https://www.nsnam.org/docs/tutorial/html/introduction.com) [Accessed 16-July-2022].

[10] M. Lacage and T. R. Henderson. Yet another networksimulator. In WNS2 '06: Proceeding from the 2006 workshop on ns-2: the IP network simulator, page 12, New York, NY, USA, 2006. ACM.

[11] Henderson, Thomas R., et al. "Network simulations with the ns-3 simulator." SIGCOMM demonstration 14.14 (2008): 527.

[12] SharkFest „About Wireshark" 2022. [Online]. Available: (https://www.wireshark.org/) [Accessed 16-July-2022].

[13] Al-Fedaghi, Sabah, and Mousa Alsulaimi. "Reconceptualization of IT Services in Banking Industry Architecture Network." 2018 7th International Conference on Industrial Technology and Management (ICITM). IEEE, 2018.

[14] Minoiu, Camelia, and Javier A. Reyes. "A network analysis of global banking: 1978–2010." Journal of Financial Stability 9.2 (2013): 168-184.

[15] Baskerville, Richard, et al. "Extensible architectures: the strategic value of service oriented architecture in banking." (2005).

[16] Ula, Munirul, Zuraini Ismail, and Zailani Mohamed Sidek. "A Framework for the governance of information security in banking system." Journal of Information Assurance and Cyber Security 2011 (2011): 1-12.

[17] Hofmann, Markus, and Leland R. Beaumont. Content networking: architecture, protocols, and practice. Elsevier, 2005.

[18] O'Malley, Sean W., and Larry L. Peterson. "A dynamic network architecture." ACM Transactions on Computer Systems (TOCS) 10.2 (1992): 110-143.

[19] Wolf, Tilman, et al. "Choice as a principle in network architecture." Proceedings of the ACM SIGCOMM 2012 conference on Applications, technologies, architectures, and protocols for computer communication. 2012.

[20] Fantacci, Romano, et al. "A network architecture solution for efficient IOT WSN backhauling: challenges and opportunities." IEEE Wireless Communications 21.4 (2014): 113-119.

[21] heavyAI „Network Topology" 2022. [Online]. Available: (https://www.heavy.ai/technical-glossary/network-topology) [Accessed 16-July-2022].

[22] Boss, Michael, et al. "Network topology of the interbank market." Quantitative finance 4.6 (2004): 677-684.

[23] Petr Pecha „What are network monitoring tools", 2021. [Online]. Available: https://www.flowmon.com/. [Accessed 15-July-2021].

[24] Bai, Yuxia, Yefa Mai, and Nan Wang. "Performance comparison and evaluation of the routing protocols for MANETs using NS3." (2017).