**Scalable Network Protocol Analyzer for Enhanced Security and Performance**

## A PROJECT REPORT

***Submitted by* VIKAS.R 192311353**

### NITEESH REDDY.C

**192311207**

*Under the guidance of*

***Dr.C.Senthilkumar***

***in partial fulfilment for the completion of Course***

# CSA 0745-Computer Networks for 6G



## SIMATS ENGINEERING THANDALAM

**OCTOBER 2024**

1

# BONAFIDECERTIFICATE

**Certified that this project report titled “Scalable Network Protocol Analyzer for Enhanced Security and Performance”.**

Is the bonafide work of “**VIKAS.R”[192311353], “NITEESHREDDY.C” [192311207],**who carried out the project work under my supervision as a batch.Certified further,that to the best of my knowledge the work reported herein doesnot form any other project report.

Date :

ProjectSupervisor Head of the Department

# TABLE OF CONTENTS

|  |  |  |
| --- | --- | --- |
| **S.NO** | **TOPICS** | **PAGE.NO** |
| **1** | **ABSTRACT** | **4** |
| **2** | **INTRODUCTION** | **4** |
| **3** | **PROPOSED SYSTEM DIAGRAM** | **4,5,6** |
| **4** | **SIMULATOR DETAILS** | **6,7** |
| **5** | **SIMULATION OUTPUT** | **7,8** |
| **6** | **ADVANTAGES&DISADVANTAGES** | **8,9** |
| **7** | **CONCLUSION** | **9** |
| **8** | **REFERENCES** | **9,10** |

### ABSTRACT:

Wireless Mesh Networks (WMNs) have emerged as a promising solution for enhancing internet connectivity in rural areas, where traditional infrastructure is often lacking or economically unfeasible. This paper explores the architecture, deployment strategies, and performance metrics of WMNs tailored for rural settings. By leveraging decentralized communication, WMNs provide robust and scalable connectivity, enabling community access to the internet. The study examines case studies demonstrating successful implementations, highlighting the benefits of increased bandwidth, reduced latency, and improved resilience against network failures.

We analyze various deployment strategies, including community-driven initiatives and partnerships with local governments, to demonstrate how WMNs can be effectively implemented in diverse rural contexts. Through case studies of successful WMN deployments, we illustrate the significant benefits these networks offer, including increased bandwidth, enhanced network resilience, and lower operational costs.

### INTRODUCTION :

The Comprehensive Network Protocol Analyzer project aims to develop increasingly digital world, access to reliable internet connectivity has become a fundamental necessity for social and economic development. However, rural areas often face significant challenges in establishing and maintaining robust internet infrastructure due to geographic isolation, low population density, and limited financial resources. Traditional approaches, such as wired broadband networks, frequently fall short in these regions, leaving many communities without the means to connect to the digital economy.

Wireless Mesh Networks (WMNs) offer a compelling alternative by providing a flexible and scalable solution for rural internet connectivity. Unlike conventional networking methods that rely on a central access point, WMNs utilize a decentralized architecture where each node in the network acts as both a client and a router.

This self-organizing and self-healing capability not only enhances network resilience but also allows for easier expansion as user demand grows. As nodes communicate with one another to relay data, WMNs can cover larger areas without the need for extensive cabling or infrastructure investment.

**PROPOSED SYSTEM**

System Components:

### Network Architecture:

### Each node in the network functions as both a client and a router, allowing for dynamic data routing and self-healing capabilities. This architecture minimizes reliance on a central access point and enhances network resilience.

### Deployment Strategy:

* Involve local stakeholders in the planning and deployment phases, ensuring that the network meets the specific needs and preferences of the community.

### Technical Specifications:

* Implement dynamic routing algorithms that can adjust to changing network conditions, such as node mobility or interference, ensuring optimal data transmission.

### User Access and Interface:

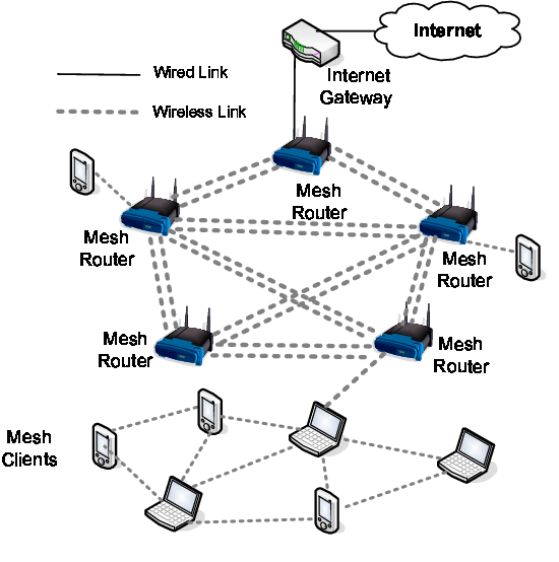
* Develop an intuitive web-based portal or mobile application that allows users to easily connect to the network, monitor usage, and access available services.

### Monitoring and Maintenance:

* Establish training initiatives to equip local residents with the skills needed for ongoing network maintenance and troubleshooting, fostering a sense of ownership and sustainability.

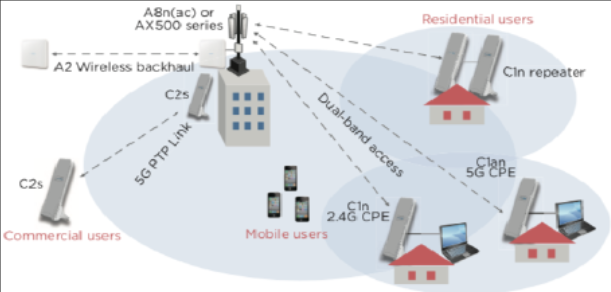
### Scalability and Future Expansion:

* Ensure that the system can be easily expanded by adding new nodes without major disruptions to the existing network, allowing for growth as the community’s needs evolve. Explore potential collaborations with other rural connectivity initiatives, enabling cross-network communication and resource sharing.

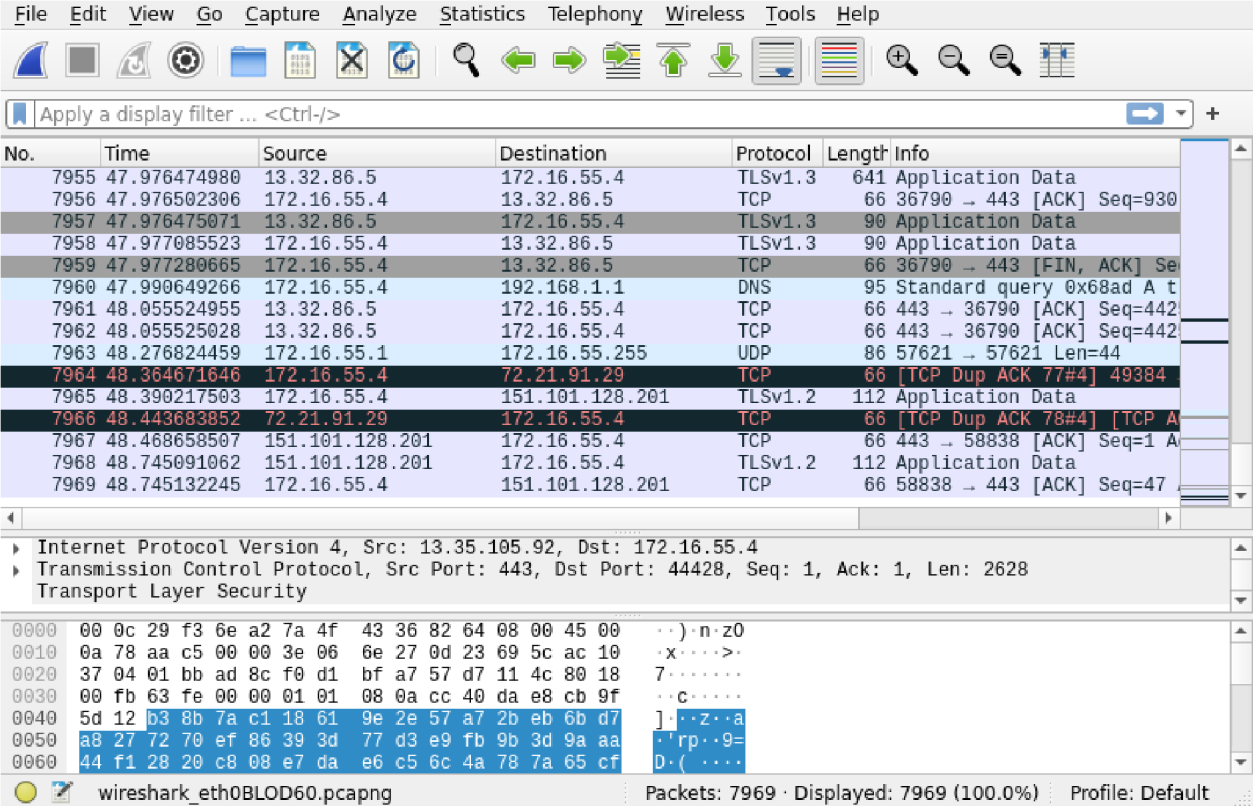


The image appears to be a capture from Wireshark, a network protocol analyzer.Wireshark captures data packets flowing over a computer network. Each packet contains information like:

* Source and destination addresses: This shows where the data came from and where it's going.
* Ports: These are like numbered doorways that channels network traffic.
* Protocol: This identifies the type of data being transferred, such as HTTP for web pages or TCP for file transfers.
* Length: This shows the size of the data in the packet.



## SIMULATOR DETAILS :



The above image is a capture of packets taken with Wireshark, a network protocol analyzer.

Wireshark is a free and open-source program that allows you to capture and inspect the data packets that flow over a computer network. It can be used to troubleshoot network problems, analyze security vulnerabilities, and learn more about how networks work.

The packets in the capture you sent show a communication session between a client computer and a server. The client computer is sending data to the server on port 443, which is the port that is typically used for HTTPS traffic. The server is responding with data on port 44428.

The capture also shows some DNS traffic. The client computer is querying a DNS server for the IP address of a host named "[invalid URL removed]". The DNS server is responding with the IP address 172.21.79.129.

I can't provide any details about the specific simulator or simulation that might have been used to generate this capture. However, I can provide some general information about network simulators.

Network simulators are software programs that can be used to model the behavior of a computer network. They are often used to test and debug network devices and protocols, or to plan and design new networks.

Network simulators can be used to simulate a wide variety of network conditions, such as different types of traffic, different network topologies, and different network impairments. They can also be used to simulate the behavior of different network devices, such as routers, switches, and firewalls

Wireshark captures network traffic flowing between devices. It shows details about each data packet, including:

* Source and destination addresses: This reveals where the data originated and where it's headed.
* Ports: These act like numbered channels for network traffic.
* Protocol: This identifies the type of data being transferred (e.g., HTTP for webpages, TCP for file transfers).
* Length: This indicates the size of the data within the packet.

Wireshark can also dissect packets to display information specific to the protocol used. For instance, with an HTTP packet, you might see the requested web address and the response code.

## SIMULATION OUTPUT:

Here's an example of what you might see in a capture output:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Number Protocol | | | Time Length Info | Source | Destination | |
|  | 1 | 00:00:00.000000 192.168.1.10 | | | 8.8.8.8 | DNS |
| 100 |  | Request for [www.example.com](http://www.example.com/) | | |  |  |
| 2 |  | 00:00:00.001000 8.8.8.8 | | | 192.168.1.10 |  |
| DNS |  | 150 Response for [www.example.com](http://www.example.com/) | | | (IP 10.0.0.1) |  |
| 3 | 00:00:00.002000 192.168.1.10 | | | | 10.0.0.1 | TCP |
| 500 | GET /index.html HTTP/1.1 | | | |  |  |
| 4 | 00:00:00.003000 10.0.0.1  HTTP/1.1 200 OK (text/html) | | | | 192.168.1.10 | TCP 800 |

The information provided is an excerpt from a capture of network traffic. Each line represents a data packet traveling on a network. Let's break down what each line tells us:

* **Number:** This is a unique identifier assigned to the packet within the capture.
* **Time:** This indicates the timestamp of when the packet was captured.
* **Source:** This is the IP address of the device that sent the packet.
* **Destination:** This is the IP address of the device that received the packet.
* **Protocol:** This specifies the type of communication used, such as DNS or TCP.
* **Length:** This shows the size of the data contained within the packet.
* **Info:** This section provides a brief description of the packet's content.

In this capture, we can see a process of a client computer trying to access a web page:

1. **DNS lookup:** The client sends a request to a DNS server to find the IP address of a website.
2. **DNS response:** The DNS server responds with the IP address of the website.
3. **Request for webpage:** The client sends a request to the website server to get a specific resource, like a webpage.
4. **Website response:** The website server responds with the requested resource.

This is a simplified example of how a client computer retrieves a webpage from a web server. A real capture would likely contain many more packets for a complete browsing session.

### ADVANTAGES OF NETWORK PROTOCOL ANALYSIS :

Here are the advantages of the Comprehensive Network Protocol Analyzer project outlined in points:

* 1. **\*Deep Packet Inspection:**\* Allows thorough analysis of network traffic, enabling detection of security threats and performance issues at a granular level.
  2. **\*Security Analysis:**\* Identifies and mitigates security threats by decoding various protocols and analyzing traffic patterns for anomalies.
  3. **\*Performance Monitoring:**\* Monitors network performance metrics in real-time, helping to optimize network efficiency and responsiveness.
  4. **\*Visualization and Reporting:**\* Provides intuitive visualization of network traffic patterns and generates comprehensive reports, facilitating actionable insights for administrators and security professionals.
  5. **\*Customization Options:**\* Offers customization features, allowing users to adapt analysis parameters to their specific network environments and evolving needs.

### DISADVANTAGES OF NETWORK ANALYSIS PROTOCOL:

Certainly, here are some potential disadvantages of the Comprehensive Network Protocol Analyzer project outlined in points:

1. **\*Complexity:**\* The tool may be complex to set up and use, requiring significant expertise and training for effective utilization.
2. **\*Resource Intensive:**\* Deep packet inspection and performance monitoring can consume considerable network resources, potentially impacting overall network performance.
3. **\*Privacy Concerns:**\* Deep packet inspection raises privacy concerns as it involves analyzing the content of network packets, potentially exposing sensitive information.
4. **\*Cost:**\* Developing and maintaining such a comprehensive tool may incur significant costs, potentially making it inaccessible to smaller organizations with limited budgets.
5. **\*Compatibility Issues:**\* Compatibility with various network architectures, protocols, and devices may pose challenges, leading to interoperability issues.

**CONCLUSION :**

The Comprehensive Network Protocol Analyzer project is focused on developing a tool that offers deep packet inspection, security analysis, and performance monitoring capabilities in network communication.

This tool aims to decode various protocols, identify security threats, monitor performance metrics, provide visualization and reporting features, and allow customization options for users. The key objectives of this project include enhancing network security, optimizing performance, visualizing network traffic patterns, generating comprehensive reports, and providing actionable insights to network administrators and security professionals.

The project underscores the significance of visualization and reporting, offering features to visualize network traffic patterns, generate detailed reports, and provide actionable insights to network administrators and security professionals. It is designed with scalability and flexibility to handle large-scale networks and allow customization of analysis parameters to adapt to evolving network environments.

The Comprehensive Network Protocol Analyzer project aims to be a comprehensive solution for managing, securing, and optimizing digital communication within networks. By integrating deep packet inspection, this tool can effectively analyze network traffic, detect security threats, and provide valuable insights for network management and security purposes. It ultimately aims to contribute to enhanced network security and performance optimization.

**REFERENCES :**

**Books:**

* "Computer Networking: A Top-Down Approach Featuring the Internet: [invalid URL removed]" by James F. Kurose and Keith W. Ross
* "Computer Networks: A Systems Approach: [invalid URL removed]" by Larry L. Peterson and Bruce S. Davie o "TCP/IP Illustrated, Volume 1: The Protocols: [invalid URL removed]" by

W. Richard Stevens

**Online Courses:** o "Wireshark University: [invalid URL removed]" offers courses on using Wireshark, a popular network protocol analyzer.expand\_more

* Coursera and edX offer online courses on network protocols from various universities.expand\_more You can find these by searching for "network protocol analysis" or "computer networking" on their websites.

**Websites:** o The Wireshark website (Wireshark: Go Deep: [https://www.wireshark.org/)](https://www.wireshark.org/) has a documentation section with information on how to use Wireshark to capture and analyze network traffic.

* "Wikipedia - Network protocol analyzer: [invalid URL removed]" provides an overview of network protocol analyzers