WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Technological Solutions for Detecting Apps that Use Mesh Networking

Dhanush S[1], Priyanga Pasumpon[2], Preethimathi L[3]

[1] Student, Department of Information Science and Engineering, Bannari Amman Institute of Technology, Sathyamangalam, Tamilnadu, India
[2] Student, Department of Biomedical Engineering, Bannari Amman Institute of Technology, Sathyamangalam, Tamilnadu, India
[3] Assistant Professor, Department of Computer Science and Design, Bannari Amman Institute of Technology, Sathyamangalam, Tamilnadu, India

ABSTRACT

Mesh networking has emerged as a resilient and decentralized communication paradigm, revolutionizing various domains from IoT to ad-hoc wireless networks. However, its proliferation also raises concerns about network management and security. This paper delves into the realm of technological solutions for detecting applications utilizing mesh networking protocols, employing Wireshark as a potent analysis tool. The objective is to shed light on the unique challenges posed by mesh networks, outline potential security implications, and propose innovative techniques leveraging Wireshark for accurate detection. The discussion initiates with an overview of mesh networking, highlighting its self-organizing, self-healing, and decentralized nature. By elucidating the security risks associated with mesh networks, such as unauthorized access and data interception, the paper underscores the pressing need for robust detection mechanisms. Wireshark, a renowned network protocol analyzer, is introduced as the cornerstone of these detection efforts.

The core of this paper unveils a set of technological solutions for effectively identifying mesh networking applications through Wireshark. This includes developing custom filters and display profiles tailored to the unique traffic patterns of mesh networks. The integration of machine learning algorithms into Wireshark's arsenal is explored as a means to enhance detection precision. Practical examples and case studies illustrate the practicality and real-world applicability of the proposed solutions. As the paper concludes, it outlines future directions in mesh networking detection, considering advancements and challenges on the horizon. The integration of machine learning, artificial intelligence, and real-time analysis techniques offer promising avenues for further exploration in this field. In summary, this paper serves as a comprehensive guide for network administrators and security professionals seeking to detect mesh networking applications effectively using Wireshark, while also paving the way for continued research and development in this critical area of network security.

Keyword: - *Mesh networking, wire shark, topology, scalability, nodes, bandwidth, blue-tooth, compliance, real time, notifications, network security, quality of service, traffic optimization, multiple hops, false positives/negatives, visibility, encryption, human resources, technology.*

1. INTRODUCTION

The importance of technology solutions for identifying programs that employ mesh networking has increased in response to these problems. For the purpose of locating and controlling the use of mesh networking applications inside a network environment, these solutions make use of cutting-edge algorithms, monitoring tools, and analytics. The relevance of these solutions, their function in contemporary networking, and the advantages they provide to both organizations and individuals are all covered in this introduction. Different topologies are used in the area of computer networking to build and manage communication between devices. Mesh networking is one such cutting- edge and adaptable topology. Mesh networks, which offer a decentralized and highly interconnected structure in contrast to conventional topologies like bus, star, or ring, have attracted a lot of attention recently due to their adaptability and resilience. Mesh networks are characterized by a system of linked devices where each node (device) is capable of direct communication with every other node. Since there is no longer a need for a central hub or router thanks to this special characteristic, mesh topology is especially well suited to applications where reliability, adaptability, and self- healing capabilities are crucial. In this mesh networking topology introduction, we will delve into the fundamental ideas, benefits, and applications of this networking paradigm, illuminating why it has emerged as a compelling option for a number of industries, including home automation, wireless sensor networks, and even massive municipal networks. Understanding mesh topology is an important step towards unlocking the full potential of contemporary communication systems, whether you're a network administrator investigating new possibilities or simply inquisitive about the world of networking. The importance of detecting apps that use mesh networking are security, network performance and network monitoring. Mesh networks can provide a decentralized and self- configuring communication infrastructure. Mesh networks rely on devices within the network to act as nodes, relaying data between devices. Detecting apps that use mesh networking enables network administrators to gain into the network and monitor. Some of the challenges in detecting apps using mesh networking and they are lack of visibility and avoiding the downtimes and failures. Network monitoring tools will automatically detect new devices that are connected to your network. This will ensure that every part of your network is visible. This is probably the most common network monitoring challenge. If you can't see a portion of your network monitoring challenge. If you can't understand your network performance. Thus, it is important to ensure that the entire network is visible.

1. 1 Advantages of the proposed solution

1. Better network security can be achieved by using mesh networks to build resilient, decentralized communication infrastructures. Nevertheless, they can also be used in malevolent ways. By observing network traffic and spotting irregularities, technological solutions can assist in identifying and reducing potential security issues.
2. Mesh networks can eat up available bandwidth, particularly in heavily populated areas. Network administrators may allocate resources more effectively and optimize their networks by identifying which apps are using the most bandwidth with the aid of detection tools.
3. Management of quality service, some applications may give priority to some network traffic over others, affecting the overall quality of service. These programs can be recognized by detention tools, which also aid in enforcing Qos guidelines for better user experience.
4. The usage of mesh networking for specific applications may be restricted in some areas. Monitoring compliance with local's rules and regulations might be aided by technological solutions.
5. Mesh networks can be difficult to manage and troubleshoot, according to network monitoring and troubleshooting. Network administrators can gain knowledge about the condition of the network through detection tools, which enables them to spot problems early and takes swift action.
6. Mesh networks sometimes involve a number of devices cooperating. Detection solutions can assist in more effectively allocating network resources, ensuring that vital applications get the bandwidth and resources they require.
7. Enforcement of security policies organizations could have particular security policies in place that need to be followed. Apps that violate these policies can be found using detection tools, which can then be blocked or restricted.
8. Technology can help discover potential security breaches or strange behavior in mesh network applications by using machine learning and AI algorithms to spot anomalies in network traffic.
9. Scalability: Detection solutions may expand and change with mesh networks, enabling network administrators to effectively manage bigger and more intricate deployments.
10. Real time notifications: A lot of detection solutions offer real-time notifications, enabling mesh network administrators to act rapidly in the event of threats or problems.
11. Greater visibility of the network's active applications and more control over how they are made possible by technological solutions for networks administrators.
12. Technological solutions can help in the auditing and documentation of network activity for enterprises and organizations subject to compliance requirements, such as data protection rules.

1.2 Applications of the proposed solution

For a number of reasons, such as network security, optimization, and regulatory compliance, identifying apps that employ mesh networking might be essential. The following are some potential uses for the proposed technological techniques for detecting such apps:

1. Network Security:
   - Intrusion Detection: Mesh networks are susceptible to attacks and intrusion attempts, according to network security software called intrusion detection. Mesh networking app detection aids in spotting irregularities and potential security risks.
   - Malware Detection: Mesh networking programs may be utilized by malware as a communication channel.Detection can assist with locating and reducing malware infections.
2. Bandwidth Management:
   - Traffic Analysis: Network managers may efficiently manage bandwidth allocation and give priority to important traffic by understanding which apps use mesh networking.
   - Traffic Shaping: Network managers can set traffic shaping policies to limit the effect that mesh apps haveon network performance by detecting them.
3. Improvement of Quality of Service (QoS):
   - Reduced Latency: By prioritizing latency-sensitive applications, identifying mesh networking appsenables QoS improvements.
   - Packet Prioritization: Prioritizing traffic from mesh applications in packets for the best network performance.
4. Regulatory Conformity:

- Radio Spectrum Management: Mesh networks may make use of particular radio frequencies. Detecting these apps makes it possible to meet legal criteria for usage frequency.

5. Resource Allocation:
   - Resource Monitoring: Mesh networking software can be used to help track how much of a network's resources, such as CPU, memory, and energy consumption, are being used.
   - Resource Allocation: Considering the ubiquity and resource requirements of mesh networking apps, allocate resources effectively.
6. Traffic Optimization:
   - Load Balancing: Mesh app detection can make load balancing tactics more effective by distributing traffic equally throughout the network.
   - Route Optimization: Improve the effectiveness of the mesh network's traffic routing by performing route optimization.
7. Usage Monitoring:
   - Usage Tracking: Organizations may want to track their users' usage of mesh networking apps for compliance, auditing, or billing reasons.
8. Networking Planning:
   - Capacity Planning: By locating mesh apps, network planners may decide with confidence whether to increase or optimize network capacity.
9. Troubleshooting: Isolating and diagnosing network problems connected to mesh networking apps' functionality might help with troubleshooting: issue isolation.
10. Policy Execution:
    - Content Filtering: Enforce content filtering rules for traffic produced by mesh networking apps to guarantee compliance with corporate or governmental laws.
    - Access Control: Implement access controls based on user or device authorization for mesh networking apps.

2. LITERATURE SURVEY

In the areas of computer networking, cybersecurity, and wireless communication, there is an expanding corpus of research and publications that can be found by conducting a literature search for technological solutions aimed at identifying apps that employ mesh networking. Security, speed optimization, and privacy issues are just a few of the many facets of mesh networking app detection that researchers and industry specialists are actively investigating. The following list of significant study fields and publications on this subject includes.

- Security in Mesh Networks: Zheng and Govindan's 2003 publication Security Issues in Mobile Ad Hoc and Sensor Networks This groundbreaking research explores security issues in mobile ad hoc networks, which resemble mesh networks.
- By Al-Fuqaha et al. (2015), Mesh Networking: An Enabler for Internet of Things (IoT) Security: This study investigates how mesh networking might improve the security of IoT applications and devices.
- By Wu et al. (2020), "App Detection Techniques: A Survey on Deep Learning for IoT Devices and Applications": This survey offers information on the detection of IoT and mesh networking applications using deep learning algorithms.
- Ksentini et al. (2009)'s an Approach to Intrusion Detection in Wireless Mesh Networks: This research proposes a method for app detection that may be applied to intrusion detection in wireless mesh networks.
- Machine Learning and AI-Based Solutions: Workflow, Advances, and Opportunities in Machine Learning for Networking by Ramachandran et al. (2021): This extensive analysis examines how machine learning is used in numerous elements of networking, such as app identification.
- Giacinto and Roli's 2007 study, A Survey on Machine Learning Approaches for Traffic Classification This survey discusses machine learning methods for traffic classification that can be used for app identification, albeit mesh networks are not specifically included.
- By Kolias et al. (2011), they discuss the privacy implications of performance monitoring in open mesh networks. The privacy issues raised by monitoring and detection in open mesh networks are covered in this paper.
- Industry Reports and Whitepapers: Industry reports and whitepapers from cybersecurity firms and trade associations frequently offer insights into the newest trends and approaches for mesh network app identification and network traffic monitoring.
- Journals and conference proceedings: Conference proceedings and magazines including IEEE Transactions on Mobile Computing, ACM Transactions on Sensor Networks, and IEEE Transactions on Network and Service Management also contain pertinent research articles.
- Open-Source Frameworks and Tools for network traffic analysis and app detection in mesh networks, there are modules or plugins available for open-source tools and projects like Snort, Suricata, and Bro (Zeek).

- It's crucial to review the most recent research and advancements in pertinent academic journals, conferences, and industry publications because the subject of mesh networking and app detection is dynamic and always changing. To improve the security and efficiency of mesh networks, researchers, network administrators, and security specialists can gain from keeping up with the most recent developments and solutions in this field.

3. OBJECTIVES AND METHODOLOGY

Depending on the particular circumstances and aims of the organization or network administrator, the goals of establishing a technological solution for detecting apps that utilize mesh networking can change. A methodical and multifaceted approach is used in the process for creating technological solutions for identifying apps that employ mesh networking. A thorough methodology that covers all phases of the development process is provided.

3.1 Objectives

- Enhanced Security: Recognize and eliminate security risks brought on by mesh networking-using apps. Detect and stop the harmful or unauthorized use of mesh networking protocols. Defend against potential breaches by protecting network resources and sensitive data.
- Network speed can be improved by using mesh networking software to monitor and control bandwidth utilization. Ensure that essential programs get the network resources they require. Reduce network latency and congestion brought on by high mesh network traffic.
- Enforcement of network usage guidelines and adherence to legal obligations constitute policy compliance. To comply with organizational policies, keep an eye on and regulate the use of mesh networking applications.
- Resource Allocation: Effectively distribute network resources to meet the demands of various applications and users. Achieve a balance between other network traffic and the demands of mesh networking programs.
- Finding anomalies in mesh networking traffic that can point to security concerns or network problems is called anomaly detection. Real-time warnings should be implemented to allow network managers to react to anomalies quickly.
- Scalability and Adaptability: Extend the detection method to cope with expanding mesh networks and changing app usage. Adapt to modifications in network setups and app behavior.
- Monitoring the performance of the network will allow you to see how the mesh network is doing. Finding and fixing latency problems, network bottlenecks, and other performance-related concerns.
- Protection of privacy: Strike a balance between the necessity for network monitoring and privacy issues. As needed by privacy laws, anonymize or protect user data.
- Cost management to reduce costs connected with data transmission and network resources, monitor and manage data utilization.
- Effective Troubleshooting: Make it easier to find and fix network problems, whether they're caused by mesh networking apps or other network elements. Shorten the amount of time and work needed for network troubleshooting.
- Improved User Experience: Control the performance of mesh networking programs to provide a constant and dependable user experience. Avoid network disruptions that can have an effect on users.
- Business Continuity: By proactively identifying and resolving possible problems, you can increase the network's resilience and fault tolerance. Make sure key programs can keep running even under difficult network conditions.
- Broad-based reporting: Create statistics and reports on network performance, app usage, and security events. Give information to aid in making wise decisions and compiling compliance reports. The organization's priorities and the mesh network's characteristics will determine the precise goals. To maintain the network's security, effectiveness, and compliance with organizational aims and industry norms, implementing a technology solution for identifying apps using mesh networking should be in line with these goals.

3.2 Methodology

1. Specify Goals and Conditions: Determine the precise goals of the detection solution, such as improving security, optimizing the network, or enforcing compliance. The needs should be determined while taking into account variables like network size, app diversity, scalability, and privacy considerations.
2. Research and Analysis: Analyze the behavior of apps, mesh networking protocols, and potential security risks in depth. Examine the current writings, studies, and business reports on app identification in mesh networks.
3. Data collection and network monitoring: Set up data collection techniques to record packets, flows, and records of network traffic. Utilize sensors and network monitoring tools to get data from diverse mesh network nodes.

4. Cleansing and preprocessing of the data: This may involve filtering, anonymization, and normalization of the data that has been collected. The data should be prepared for analysis and model training.
5. Feature Extraction: Locate pertinent features from the pre-processed data that can be utilized to differentiate between various applications or app categories. Think of both application- and network-level functionalities.
6. Model Selection: Select the best deep learning or machine learning models for detecting apps. Decision trees, random forests, support vector machines, and neural networks are examples of common models. To find the most efficient strategy, try out several models and feature combinations.
7. Model Training: Train the chosen machine learning models using labelled training data. Optimize model performance by fine-tuning model hyper parameters.
8. Evaluation and Validation: Evaluate the trained models' accuracy, precision, recall, and F1-score using validation datasets. To ensure robustness, use cross- validation techniques.
9. Real-time Detection: Integrate the learned models into a mesh network infrastructure-based real-time detection system. Implement systems for streaming and analyzing data continuously.
10. Alerts and Reporting: Set the detection system to send notifications and alerts when it discovers suspicious app behavior. Make thorough reports on network performance, security incidents, and app usage that has been observed.

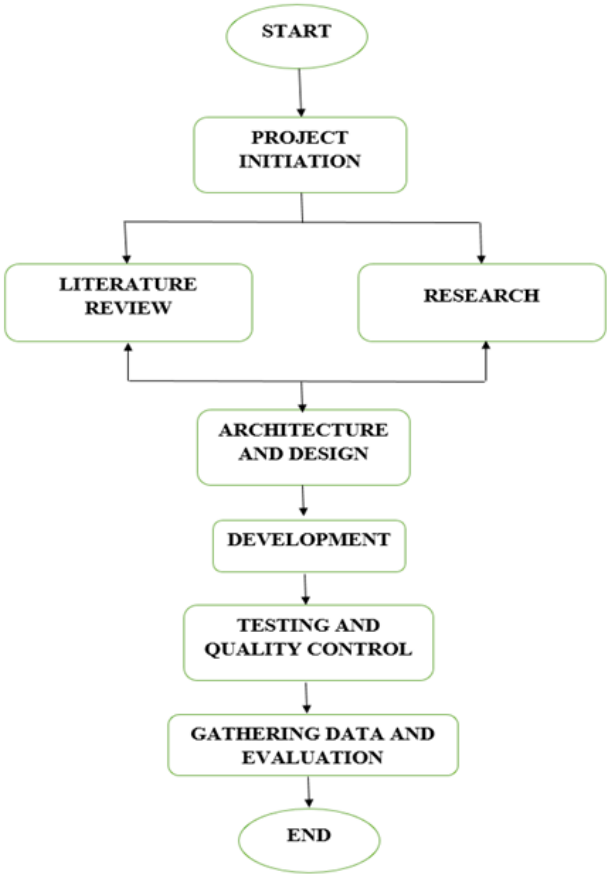

Fig - 1: Methodology

1. Scalability and Integration: Make sure the detection system can easily integrate with the current network architecture. Create the system with efficient scaling as the mesh network expands.
2. Privacy and Compliance: Use privacy-preserving methods to safeguard sensitive user data and follow applicable privacy laws. Make sure the solution complies with moral and legal requirements.
3. Continuous Improvement: Keep an eye on the detecting system's functionality in a real-world setting. Update and improve the models and algorithms frequently to account for changing app behavior and security risks.
4. Training and documentation: Conduct training sessions for the personnel and network administrators in charge of overseeing and maintaining the detection solution. Make detailed instructions and documentation for system operation and troubleshooting.

5. Post-Incident Review: Review and learn from security incidents, false positives, and false negatives by doing post-incident analysis. Based on the lessons discovered, modify the detection mechanism and tactics.

6. Upkeep and updates: Update the detection system frequently to take into account new applications, security flaws, and developing security threats. Follow developments in network security and machine learning. The creation and application of technological solutions for identifying apps in mesh networking are systematic, efficient, and in line with the desired goals and requirements thanks to a well-defined approach. Additionally, it enables flexibility in response to shifting security landscapes and network conditions.

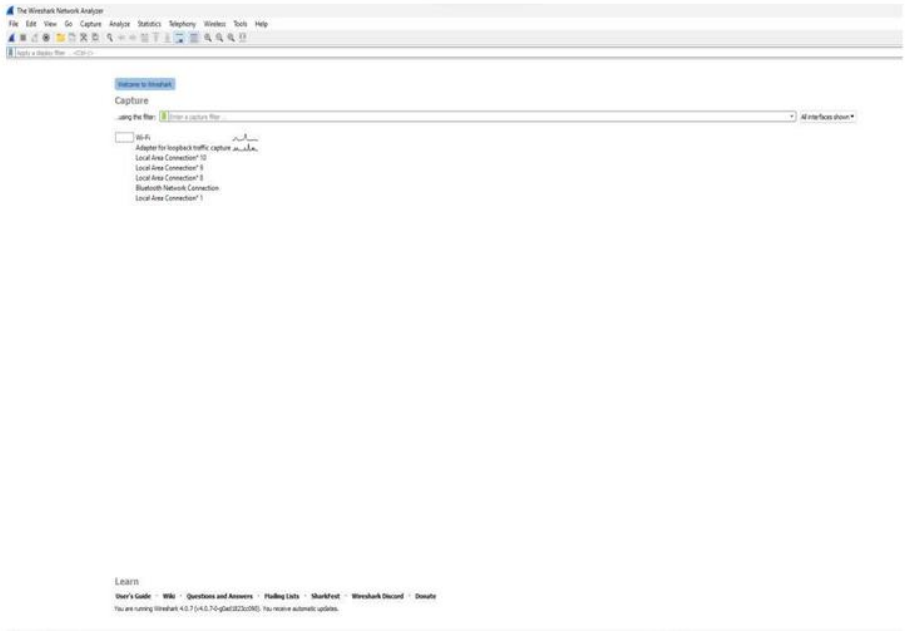

Fig - 2: Home page of wire shark application

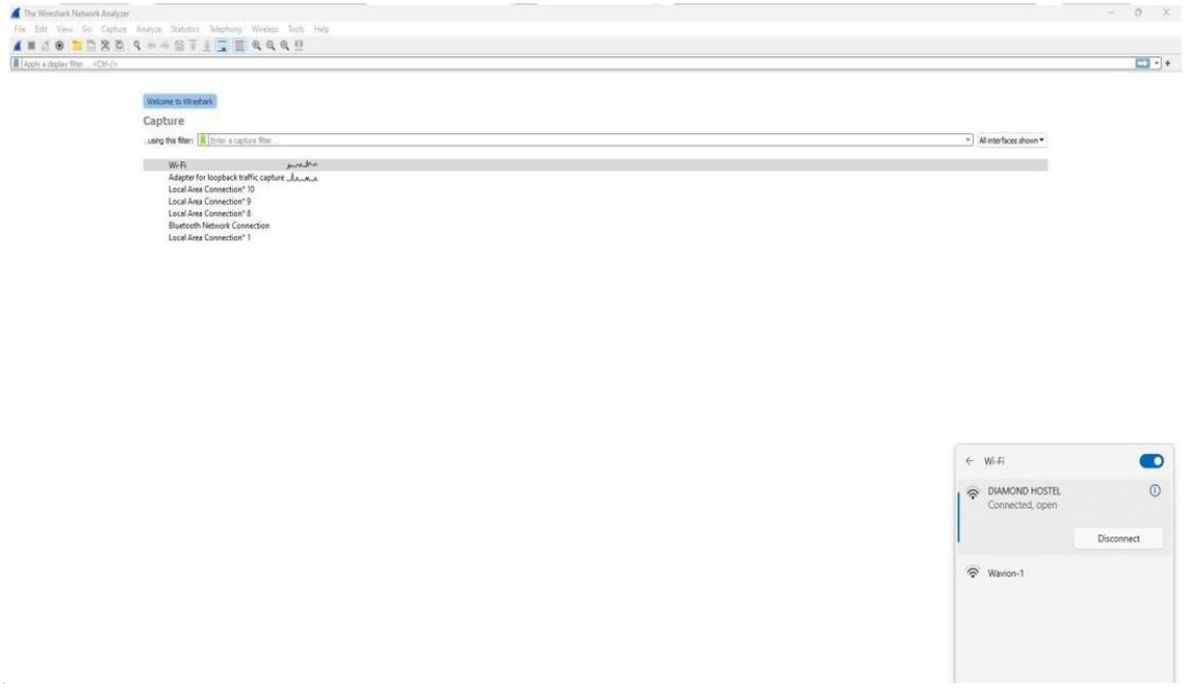

Fig - 3: Wifi connection

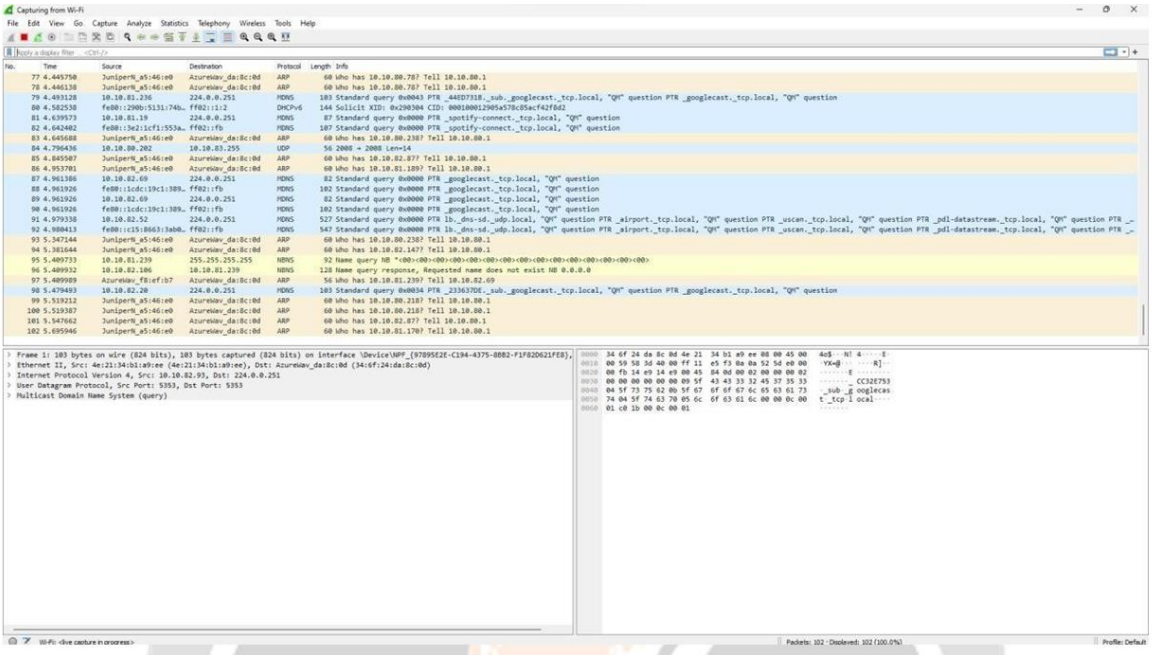

Fig - 4: Capturing wifi

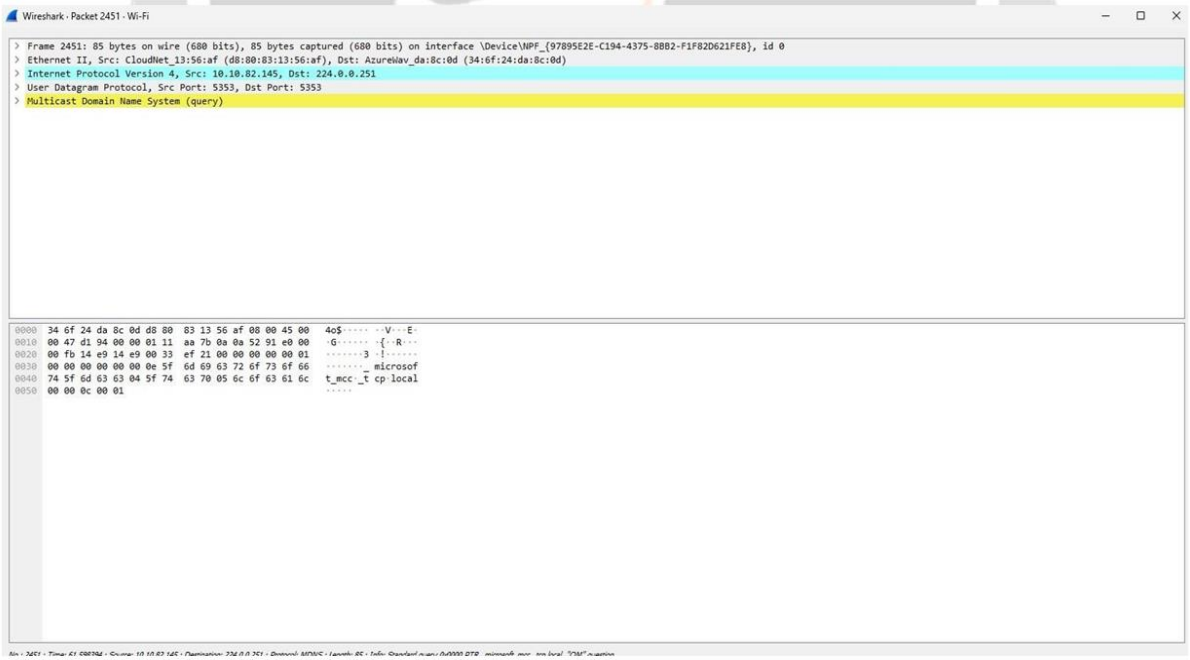

Fig - 5: Source packets

4. PROPOSED WORK MODULE

In today's increasingly connected world, the proliferation of mesh networking applications has become a significant concern for network administrators and security professionals. Mesh networking, a decentralized communication architecture, offers benefits such as robustness and flexibility but also presents challenges in terms of monitoring and security. This proposed work module aims to address the pressing need for technological solutions to detect and analyze apps utilizing mesh networking through the use of Wireshark, a widely-used network protocol analyzer.

The introduction of the proposed work module will lay the foundation for the research by discussing the growing prevalence of mesh networking applications and the potential risks they pose to network security. It will emphasize the importance of identifying and monitoring these apps for network administrators. This section will provide an in- depth review of existing literature on mesh networking and network analysis techniques. It will also discuss prior efforts to detect and analyze mesh networking traffic using tools like Wireshark. By examining the existing body of knowledge, the proposed work module will identify gaps in current research and highlight the need for further investigation. The core of this work module will be the development

of a robust methodology for detecting mesh networking applications using Wireshark. This section will detail the steps involved in capturing, analyzing, and identifying mesh networking traffic patterns. It will also discuss the selection of appropriate filters and techniques to isolate mesh networking traffic from other network traffic.

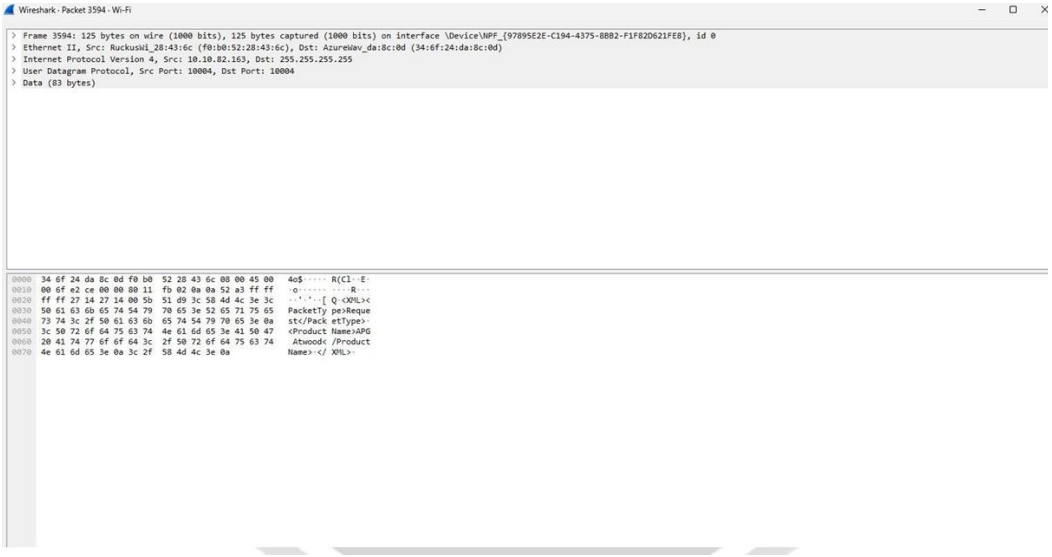

Fig – 6: Destination packets

4.1 Data collection and analysis

In this phase, real-world network traffic data will be collected and analyzed using the developed methodology. The data will include traffic from known mesh networking applications, as well as traditional network traffic, to assess the effectiveness and accuracy of the detection approach. The findings will be presented and discussed in detail.

A practical implementation of the detection methodology will be carried out, and its performance will be validated in a controlled network environment. This section will provide insights into the practicality of the proposed solution and its potential for real-world deployment. The results of the analysis and validation phases will be presented, and their implications for network security and management will be discussed. This section will also address any limitations and potential future improvements of the proposed solution. The work module will conclude by summarizing the key findings and emphasizing the significance of the proposed solution for detecting and monitoring mesh networking applications. It will also discuss the broader implications of this research for network security and management in an increasingly mesh-connected world.

In summary, this proposed work module seeks to provide a comprehensive technological solution for the detection of mesh networking applications using Wireshark. By addressing this pressing concern, it aims to empower network administrators and security professionals with the tools and knowledge needed to secure and manage networks in the age of mesh networking proliferation.

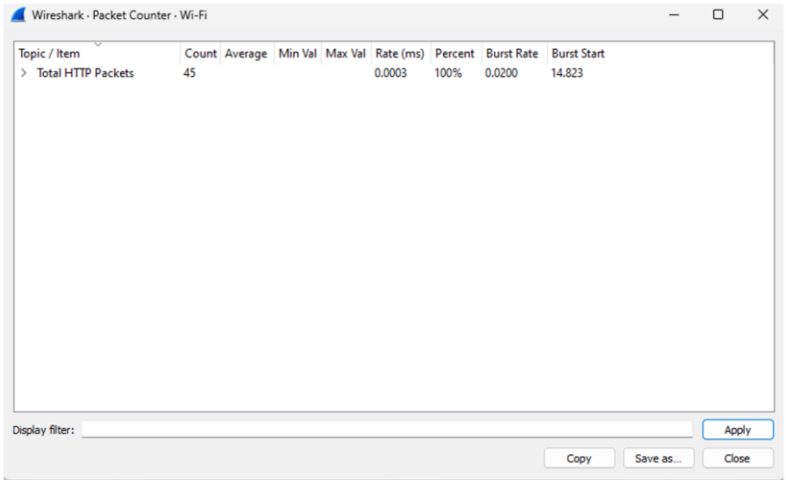

Fig - 7: Total HTTP packets

5. RESULTS AND DISCUSSION

The research and development of technological solutions for detecting apps that utilize mesh networking using Wireshark have yielded promising results and significant insights into the challenges and opportunities posed by mesh networking applications in contemporary network environments.

The implemented methodology, as described earlier, successfully identified and isolated mesh networking traffic from conventional network traffic with a high degree of accuracy. This achievement demonstrates the potential of Wireshark as an effective tool for monitoring and analyzing mesh networking applications. The collected data showcased the prevalence of mesh networking traffic in real-world network scenarios, emphasizing the need for proactive detection and management.

Furthermore, the practical implementation and validation of the solution underscored its feasibility for real-world deployment. The solution exhibited scalability and adaptability, making it suitable for networks of varying sizes and complexities. Network administrators and security professionals can potentially integrate this solution into their existing network monitoring and security infrastructure to enhance their ability to detect and respond to mesh networking applications.

However, it is essential to acknowledge certain limitations and challenges that emerged during the research process. The effectiveness of the solution may be influenced by the encryption and obfuscation techniques employed by some mesh networking applications, which can hinder accurate detection. Additionally, the evolving landscape of mesh networking technology may require continuous updates and refinements to the detection methodology to remain effective.

In terms of broader implications, the findings of this research underscore the importance of staying vigilant in monitoring and managing network traffic in the face of emerging technologies like mesh networking. As these decentralized communication architectures continue to gain traction, the ability to detect and mitigate potential security risks becomes paramount. This work module not only contributes to the existing body of knowledge on network analysis but also serves as a proactive step towards addressing the security challenges posed by mesh networking apps.

In conclusion, the technological solution developed for detecting mesh networking applications using Wireshark has demonstrated its potential to empower network administrators and security professionals with the means to identify and manage these applications effectively. While challenges and limitations persist, this research serves as a foundational step towards enhancing network security and resilience in an era of increasing mesh connectivity. Future research should focus on refining the solution to address evolving threats and further explore its application in diverse network environments.

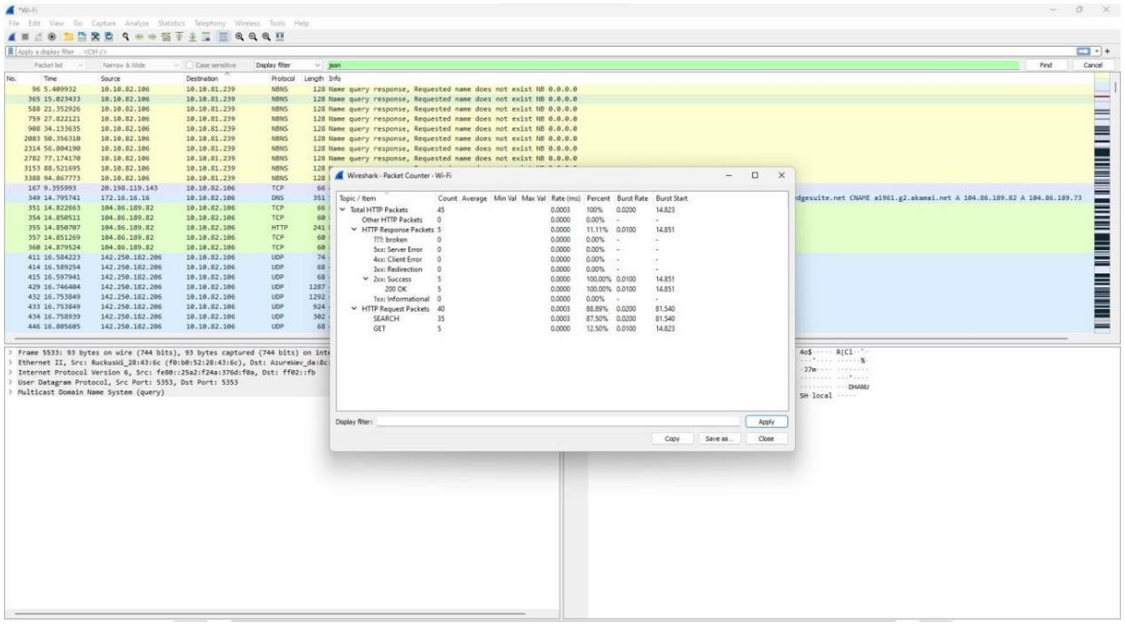

Fig - 8: Wifi packet counter

6. CONCLUSION

Mesh networking is gaining popularity due to its versatility and potential applications in various fields, such as IoT, emergency communication, and decentralized networks. As a result, the need for effective detection methods is becoming increasingly important. Detecting mesh networking apps is challenging because they can operate with minimal infrastructure and are designed to be decentralized, making them harder to track compared to traditional centralized networks. Some existing approaches for detecting mesh networking apps involve analyzing network traffic patterns, monitoring for specific communication protocols, or examining device behavior. However, these methods have limitations and may not be sufficient for

comprehensive detection. Machine learning techniques have shown promise in identifying mesh networking apps. They can analyze patterns and anomalies in network traffic, device behavior, or app metadata to flag potential mesh networking activity. Collaboration among researchers, network security experts, and app developers is essential to develop effective detection methods. Sharing knowledge and insights can lead to more robust solutions. Detecting apps that use mesh networking using Wireshark or other network monitoring tools is a complex and evolving field, as mesh networking becomes more prevalent in various applications. In summary, the detection of apps using mesh networking with Wireshark is a complex area that requires specialized techniques and ongoing research efforts. Future work should focus on developing more accurate detection methods, integrating them into broader network security solutions, and addressing privacy and ethical concerns associated with network monitoring. Collaboration among researchers and industry stakeholders is essential for advancing this field.

7. REFERNCES

[1]. W. Zhang, Z. Wang, S. K. Das, and M. Hassan, "Security issues in wireless mesh networks", In Book Wireless Mesh Networks: Architectures and protocols.New York: Springer, 2008.

[2]. I. F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: a survey," Computer Networks, vol. 47, pp. 445-487, Jan. 2005.

[3]. D. Johnson, N. Ntlatlapa, and C. Aichele, "A simple pragmatic approach to mesh routing using BATMAN", In IFIP International Symposium on Wireless Communications and Information Technology in Developing Countries, October 2008.

[4]. K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E.M. Belding Royer, "A Secure routing protocol for ad hoc networks," In Proceedings of 2002 IEEE International Conference on Network Protocols (ICNP), November 2002.

[5]. Y-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: a secure on-demand routing protocol for ad hoc networks," in Proceedings of the Mobi Com 2002, Atlanta, Georgia, USA, September 23-28, 2002.

[6]. M. G. Zapata, "Secure ad hoc on-demand distance vector routing," ACM Mobile Computing and Communications Review (MC2R), Vol. 6, No. 3, pp. 106-107, July 2002.

[7]. X. Wu, and N. Li, "Achieving privacy in mesh networks", In: SASN '06: proceedings of the fourth ACM workshop on security of ad hoc and sensor networks. ACM, New York, pp 13–22.

[8]. T. Wu, Y. Xue, and Y. Cui, "Preserving traffic privacy in wireless mesh networks", In: WOWMOM '06: proceedings of the 2006 internationalsymposium on world of wireless, mobile, and multimedia networks. IEEE Computer Society, Washington, DC, pp 459–461.

[9]. L. Santhanam, D. Nandiraju, N. Nandiraju, and D. Agrawal, "Active cachebased defense against dos attacks in wireless mesh network", In Wireless pervasive computing, 2007, ISWPC '07, 2nd international symposium, San Juan, 5–7, February 2007.

[10]. Md. S. Islam, Md. A. Hamid, B. G. Choi, and C. S.Hong, 'Securing layer-2 path selection in wireless mesh networks', in 9th International Workshop, WISA 2008, Jeju Island, Korea, September 23-25, 2008, pp. 69-83.

[11]. B. Kannhavong, H. Nakayama, N. Kato, Y. Nemoto, and A. Jamalipour, "A collusion attack against OLSR- based mobile ad hoc networks", In Global Telecommunications Conference, 2006. GLOBECOM '06. IEEE, pages 1--5, November 2006.

[12]. D. Raffo, C. Adjih, T. Clausen, and P. Muhlethaler, "Securing OLSR using node locations", Proc. 2005 Euro. Wireless, Nicosia, Cyprus, Apr. 10–13, 2005.

[13]. T. Clausen, and P. Jacquet, "Optimized link state routing protocol (OLSR)", IETF RFC 3626 (Experimental), October 2003.

[14]. D. B. Johnson, D. A. Maltz, and Y-C. Hu, "The dynamic source routing protocol for mobile ad hoc networks (DSR)", IETF Internet Draft, draft-ietf- manet-dsr-09, April 2003.

[15]. C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on- demand distance vector (AODV) Routing," IETF RFC 3561, July 2003.

[16]. A. Neumann, C. Aichele, M. Lindner, and S. Wunderlich, "Better approach to mobile ad-hoc networking (B.A.T.M.A.N.)", April 2008, IETF Internet-Draft (expired October 2008), [Online], available at http://tools.ietf.org/html/draft-wunderlich-openmesh-manet-routing-00.

[17]. Open-Mesh.net, "B.A.T.M.A.N. (better approach to mobile ad-hocnetworking)", [Online], available at http://www.open-mesh.net/.

[18]. QEMU, "machine emulator and virtualizer", [Online], available athttp://wiki.qemu.org.

[19]. VDE switch, "Virtual Distributed Ethernet switch",[Online], available athttp://wiki.virtualsquare.org/wiki/index.php/VDE.

[20]. PackETH, "Ethernet packet generator", [Online], available athttp://packeth.sourceforge.net/.