Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 10, October - 2025

Framework for Detection and Prevention of Intrusion in Computer Networks

Albert Armah , Samuel Asare
St. Monica's College of Education, Mampong-Ashanti, Ghana

Abstract - Man-in-the-middle (MITM) attacks represent a significant threat to the confidentiality and integrity of data communications within computer networks. Such attacks occur when an attacker intercepts and potentially alters the data being exchanged between two communicating parties, thereby compromising sensitive information and transactions. Many cryptographic systems lacking robust authentication measures are susceptible to MITM attacks, underscoring the pressing need for effective security solutions.This study presents the EL_ALBI framework, an innovative approach that combines the strengths of Intrusion Prevention System (IPS) rules with DHCP Snooping protocols to detect and prevent MITM attacks in computer networks. The IPS rule component continuously analyzes network traffic, employing predefined rules and signatures to identify and block malicious activities and patterns associated with MITM attacks. At the same time, the DHCP Snooping protocol maintains a binding table of valid IP address, MAC address, and port mappings, ensuring that only authorized devices can obtain IP addresses from legitimate DHCP servers, thereby preventing unauthorized network access. The proposed framework was implemented and evaluated through simulations using Packet Tracer 8.1 network simulation software. The simulation environment consisted of network devices such as switches and routers, with designated devices acting as attackers and servers to replicate real-world MITM attack scenarios. The framework's performance was assessed based on key metrics, including packet loss, network availability, and the mitigation of denial-of-service (DoS) attacks. The results demonstrated the effectiveness of the EL_ALBI framework in reducing packet loss, maintaining network availability, and mitigating DoS attacks related to MITM incidents, surpassing the efficacy of traditional security measures. These findings highlight the potential of the proposed framework to enhance network security and protect sensitive information from unauthorized access and modification.

Keywords: Man-in-the-middle (MITM) attacks, Network Security, Intrusion Prevention System (IPS), DHCP Snooping, Packet loss mitigation, DoS attack prevention

1. INTRODUCTION

In today’s interconnected world, where nearly every facet of our lives depends on the internet or cellular networks, the threat of cyberattacks remains ever-present. Online services and connected devices store and transmit sensitive user information, making them attractive targets for hackers. Among the most prevalent and effective types of attack are man-in-the-middle (MITM) attacks, which enable attackers to intercept and manipulate data communications between two parties who mistakenly believe they are communicating directly with each other (Nirwan & Dhaliwal, 2023).

In a MITM attack, the attacker secretly relays and potentially alters messages, allowing them to eavesdrop on or decrypt the intended communication. This makes these attacks particularly difficult to detect. With the rapid expansion of e-commerce and the increasing exchange of sensitive information over computer networks, the risk of data theft or modification has escalated significantly. The repercussions of such attacks can be severe, resulting in financial losses, data breaches, and compromised personal information (Prasad & Chandra, 2022).

The growing sophistication of cyber threats underscores the need for robust security measures to protect computer networks and secure sensitive data. Traditional security mechanisms, such as firewalls and antivirus software, may prove inadequate in detecting and preventing man-in-the-middle (MITM) attacks, which often take advantage of vulnerabilities within network protocols and encryption techniques. As a result, there is an urgent demand for advanced intrusion detection and prevention systems capable of effectively identifying and mitigating these threats (Dave et al., 2023; Tetteh, 2024).

Current algorithms and techniques for intrusion detection and prevention have inherent limitations that may not fully address the challenges posed by MITM attacks (Thankappan et al., 2022). For instance, while strong WEP/WAP encryption on access points

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 10, October - 2025

and secure router login credentials can offer protection, they often fall short against more advanced attacks that exploit weaknesses in network protocols or encryption algorithms (Thankappan et al., 2024).

This study seeks to develop a secure framework known as the EL_ALBI framework, specifically aimed at detecting and preventing intrusions, particularly MITM attacks, within computer networks. The framework integrates two protocols: DHCP Snooping and IPS Rule, creating a multi-layered defence strategy against these attacks. By harnessing the strengths of these protocols, the framework aspires to enhance network security, safeguard data confidentiality and integrity, and reduce the risks associated with MITM attacks.

The objectives of this research include examining the effectiveness of existing intrusion detection and prevention methods, identifying their limitations, and proposing a secure framework designed to address vulnerabilities while providing comprehensive protection against MITM attacks on computer networks.

2. RELATED WORKS

Michael West (2009) defined a network intrusion as the unauthorized access to a computer within an organization or assigned domain. Intrusions can be classified as passive, where the attacker gains entry without detection, or active, where they make changes to the network resources. These intrusions can originate both from outside the network or from within, such as from an employee, customer, or business partner. The consequences of network intrusions can be severe, leading to data breaches, system downtime, and substantial financial losses.

According to Mallik et al. (2019), man-in-the-middle (MITM) attacks involve the installation of malware that can access, read, and modify confidential information without the users' knowledge. Many cryptographic systems that lack proper authentication security are vulnerable to these attacks. In a MITM attack, the attacker positions themselves between two communicating parties, intercepting and potentially altering the data being exchanged. This undermines the confidentiality, integrity, and authenticity of the communication, posing a significant threat to sensitive information and transactions.

Salifu (2012) highlighted the vulnerabilities associated with the Address Resolution Protocol (ARP), which lacks authentication and can be exploited by malicious parties to redirect network traffic, leading to data disclosure, alteration, and denial-of-service attacks. ARP spoofing is a common technique used in MITM attacks, where the attacker sends falsified ARP messages to redirect traffic through their system, enabling them to intercept and manipulate data.

Existing algorithms for intrusion detection and prevention include strong WEP/WAP encryption on access points and strong router login credentials (Sowah et al., 2019). While these measures can provide a certain level of protection, they may not be sufficient to address the evolving threats posed by MITM attacks. Strong encryption alone cannot prevent MITM attacks if the attacker can successfully insert themselves between the communicating parties and intercept the encrypted traffic.

Intrusion Detection Systems (IDSs) and Intrusion Prevention Systems (IPSs) are widely used to detect and mitigate network attacks, including MITM attacks. IDSs monitor network traffic and alert administrators when suspicious activities are detected, while IPSs take proactive measures to prevent or block detected threats (Scarfone & Mell, 2007). However, traditional IDSs and IPSs may struggle to keep up with the constantly evolving techniques used in MITM attacks, necessitating more advanced and adaptive security solutions.

To address the limitations of existing methods, researchers have proposed various techniques and frameworks for detecting and preventing MITM attacks. These include machine learning-based approaches (Doshi et al., 2018), blockchain-based solutions (Li et al., 2018), and hybrid systems that combine multiple detection and prevention mechanisms (Almusaylim & Zaman, 2018). However, many of these solutions are still in the research and development phase and may have limitations or challenges in terms of computational overhead, scalability, or real-world deployment.

The main theory underpinning this research is the development of a comprehensive framework, called the EL_ALBI framework, to detect and prevent man-in-the-middle (MITM) attacks on computer networks. The framework combines two protocols: the Intrusion Prevention System (IPS) Rule and DHCP Snooping, to create a multi-layered defense against MITM attacks.

The IPS Rule component of the framework is based on the theory of intrusion prevention systems, which are designed to actively monitor network traffic and take appropriate actions to prevent or mitigate detected threats. The IPS Rule leverages predefined

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 10, October - 2025

rules and signatures that define malicious network activities and patterns associated with MITM attacks, such as ARP spoofing, DNS spoofing, SSL hijacking, and SSL stripping (Al-Hamami & Al-Saadoon, 2013; Gupta et al., 2023; Pandey, 2013).

The DHCP Snooping component of the framework is grounded in the theory of network access control and authentication. DHCP Snooping acts as a firewall between untrusted hosts and trusted DHCP servers, building and maintaining a binding table of valid IP addresses/MAC address/port mappings (Buamona et al., 2023). This ensures that only authorized devices can obtain IP addresses from legitimate DHCP servers, preventing unauthorized access to the network and mitigating the risk of rogue devices or attackers attempting to launch MITM attacks from within the network (Tamsir Ariyadi, 2022).

The main theory suggests that the combination of these two protocols, the IPS Rule and DHCP Snooping, will create a robust and effective defense against MITM attacks on computer networks. By addressing different aspects of MITM attacks, such as unauthorized network access, malicious traffic patterns, and active prevention measures, the EL_ALBI framework aims to provide a comprehensive security solution that maintains data confidentiality, integrity, and authenticity in network communications.

To validate the effectiveness of the proposed EL_ALBI framework, an empirical study was conducted through simulations and testing using the Packet Tracer 8.1 network simulation software. The empirical study involved implementing the framework on network devices like switches and routers, enabling the simulation of various network scenarios and attack vectors.

The simulation environment allowed researchers to test the framework under different conditions, including scenarios where devices on the network acted as attackers and servers, mimicking real-world MITM attack situations. The performance of the framework was evaluated based on several key metrics, including packet loss, network availability, and the mitigation of denial of service (DoS) attacks.

The empirical study involved comparing the performance of network setups with and without the EL_ALBI framework implemented. In scenarios without the framework, traditional security measures such as encryption on access points and strong router login credentials were employed. This allowed researchers to assess the limitations of these traditional measures in preventing MITM attacks and compare them with the performance of the proposed framework.

The empirical data collected from the simulations provided valuable insights into the effectiveness of the EL_ALBI framework. The results demonstrated that the framework significantly reduced packet loss, maintained network availability, and effectively mitigated DoS attacks associated with MITM attacks, outperforming traditional security measures.

The empirical study also allowed researchers to identify potential limitations or areas for improvement in the framework's implementation. By analyzing the simulation data and observing the framework's performance under various attack scenarios, researchers could refine the algorithm, optimize the implementation, and address any identified vulnerabilities or challenges.

The empirical study played a crucial role in validating the theory and demonstrating the practical effectiveness of the EL_ALBI framework in detecting and preventing MITM attacks on computer networks. The simulation results provided tangible evidence of the framework's capabilities and highlighted its potential for real-world deployment in enhancing network security and safeguarding sensitive information.

3. METHODOLOGY

The proposed methodology involves the developing and implementating of the EL_ALBI framework, a novel approach that combines two protocols: IPS Rule and DHCP Snooping, to detect and prevent man-in-the-middle (MITM) attacks on computer networks. The framework aims to address the vulnerabilities associated with MITM attacks, which can compromise data confidentiality, integrity, and authenticity, posing a significant threat to sensitive information and transactions.

3.1 DHCP Snooping

DHCP Snooping is a security feature that acts as a firewall between untrusted hosts and trusted DHCP servers. It is implemented on network switches to mitigate rogue DHCP server attacks and ensure that only authorized devices can obtain IP addresses from legitimate DHCP servers (Tok & Demirci, 2021). The DHCP Snooping protocol builds and maintains a database of valid IP address/MAC address/port mappings, called the DHCP Snooping binding table.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 10, October - 2025

When a host attempts to request an IP address from the DHCP server, the switch checks the DHCP Snooping binding table to determine if the request is coming from an untrusted port. If the request originates from an untrusted port, the switch forwards the request to the DHCP server. However, if the request comes from a trusted port or a port that is not configured as an untrusted port, the switch drops the request, preventing unauthorized access and potential MITM attacks.

3.2 IPS Rule

The Intrusion Prevention System (IPS) Rule is a set of predefined rules or signatures that define malicious network activities and specify the actions to be taken when such activities are detected. The IPS continuously analyzes network traffic and inspects data packets for patterns that match the defined rules (Song et al., 2020). When a match is found, the IPS takes appropriate actions based on the rule configuration, such as blocking or logging suspicious traffic.

In the EL_ALBI framework, the IPS Rule is configured on the router to analyze network traffic and detect MITM attack patterns. The IPS Rule can be customized to include specific signatures or rules that identify known MITM attack techniques, such as ARP spoofing, DNS spoofing, SSL hijacking, and SSL stripping. By continuously monitoring network traffic and comparing it against these predefined rules, the IPS can effectively detect potential MITM attacks in real time.

3.3 Description of the Proposed Framework

The EL_ALBI framework combines the DHCP Snooping and IPS Rule protocols to create a multi-layered defence against MITM attacks. DHCP Snooping is enabled on the network switch to build a binding table of valid IP-MAC address mappings, ensuring that only authorized devices can obtain IP addresses from legitimate DHCP servers. This layer of security helps to prevent rogue DHCP servers and unauthorized devices from gaining access to the network.

Concurrently, the IPS Rule is configured on the router to analyze network traffic and detect MITM attack patterns. The IPS continuously inspects data packets for signatures or patterns that match known MITM attack techniques. If an attack is detected, the IPS Rule takes appropriate actions, such as blocking the malicious traffic or logging the event for further analysis and investigation. The synergy between DHCP Snooping and IPS Rule provides a comprehensive security solution that addresses different aspects of MITM attacks. While DHCP Snooping itigates unauthorized access to the network, the IPS Rule ensures that any malicious traffic or MITM attack attempts are promptly detected and addressed, maintaining the confidentiality, integrity, and authenticity of network communications.

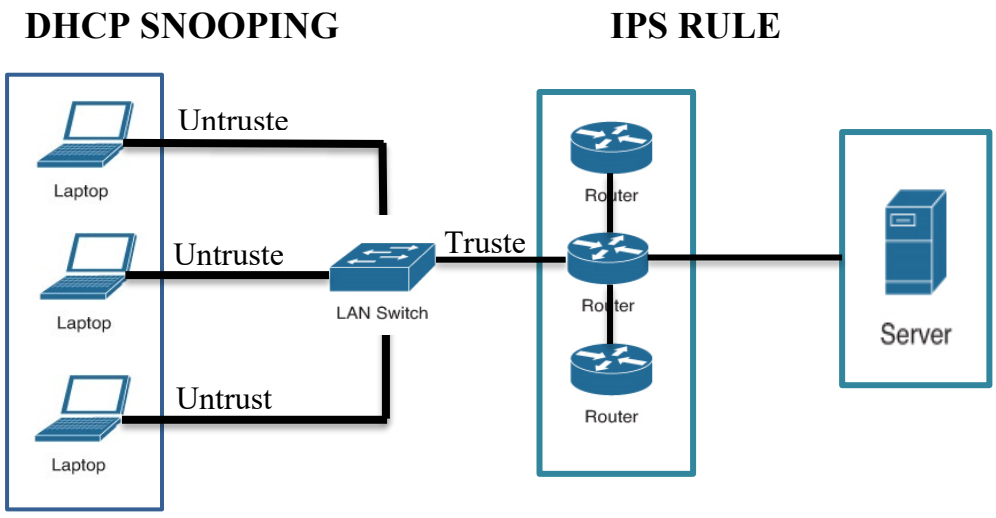


Figure 1: Block Diagram of Proposed Framework (EL_ALBI framework)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 10, October - 2025

3.4 Pseudocode of Proposed EL_ALBI Framework

Step 1: Start the switch

Step 2: Enable DHCP Snooping globally on switch

Step 3: Create VLAN you want to protect

Step 4: Configure trusted interface for DHCP Server connected

Step 5: Enable DHCP Server Detection

Step 6: Configure function for discarding DHCP reply packets

Step 5: Check connections on switch

Step 6: Not valid? Go to Step 3

Step 7: Start the router

Step 8: Enable IPS security on Router

Step 9: Verify network connectivity for successful connection

Step 10: Create an IPS configuration in memory/flash

Step 11: Configure IPS signature storage location

Step 12: Create IPS rule

Step 13: Configure system logging to display attack notification

Step 14: Set system clock to enable timestamp

Step 15: Configure system timestamp services for logging messages

Step 16: Configure IPS to use signature categories

Step 17: Apply the IPS rule to router interface

Step 18: Configure event action to alert and drop incoming packets

Step 19: Verify that IPS is working properly

Step 20: Not valid? Go to Step 12

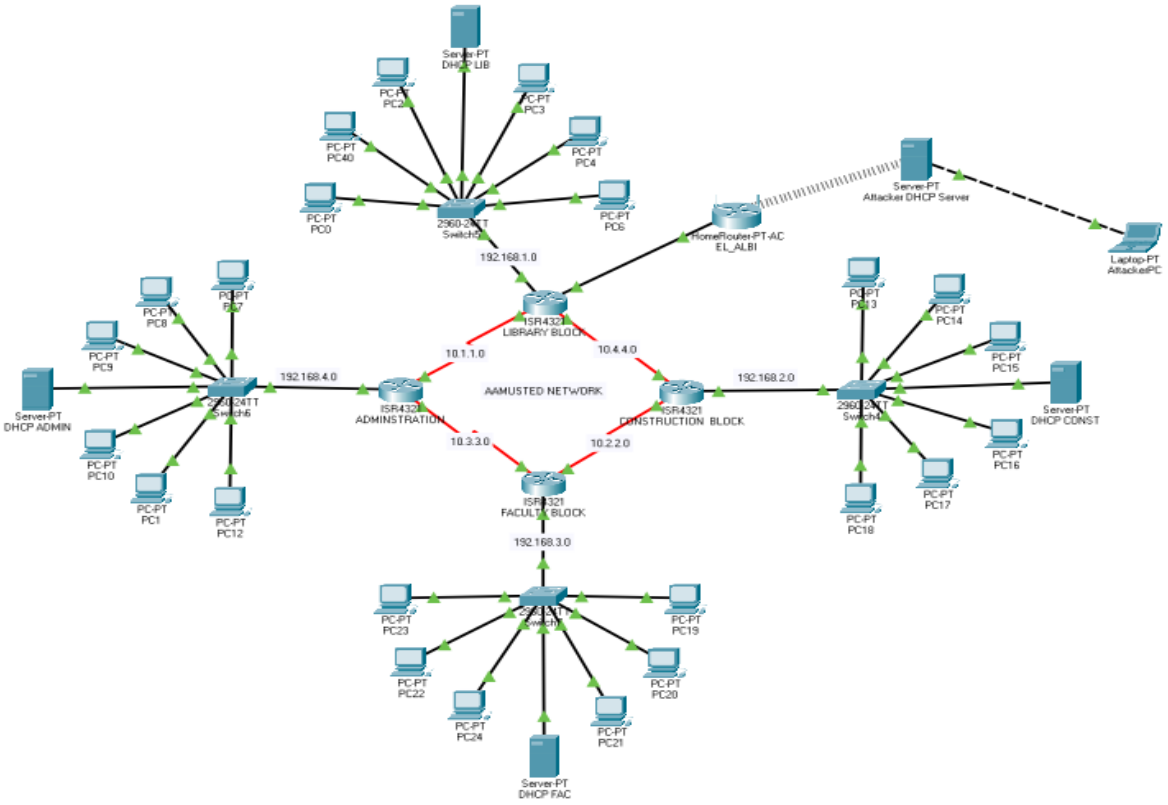
Step 21: End.

3. 5 Simulation and Testing

To evaluate the effectiveness of the proposed EL_ALBI framework, a simulation environment was set up using Packet Tracer 8.1, a widely used network simulation software. The algorithm of the framework was implemented on network devices like switches and routers, enabling the simulation of various network scenarios and attack vectors.

The framework was tested using devices on the network as attackers and servers, simulating real-world MITM attack scenarios. The performance of the framework was evaluated based on several parameters, including packet loss, denial of service (DoS) attacks, and network availability. These parameters were measured and compared across different network setups, both with and without the EL_ALBI framework, to assess its efficacy in detecting and preventing MITM attacks

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 10, October - 2025



.

Figure 2: Logical layout of Proposed Framework

The simulation and testing phase allowed for the comprehensive evaluation of the proposed framework, enabling the researchers to identify potential limitations, optimize the algorithm, and refine the implementation for real-world deployment.

4. RESULTS

The results of the study demonstrate the effectiveness of the proposed EL_ALBI framework in detecting and preventing man-in-the-middle (MITM) attacks on computer networks. The framework's performance was evaluated based on several key metrics, including packet loss, network availability, and mitigation of denial of service (DoS) attacks.

4.1 Packet Loss

One of the significant challenges faced in computer networks is packet loss, which can occur due to various factors, including network congestion, faulty hardware, or malicious attacks. MITM attacks can contribute to packet loss by intercepting and manipulating network traffic, leading to data corruption or dropped packets.

The findings of this study reveal that the EL_ALBI framework significantly reduced packet loss compared to network setups without the framework implemented. In scenarios where only encryption on access points and strong router login credentials were employed, packet loss was observed, indicating the limitations of these traditional security measures in preventing MITM attacks.

However, with the implementation of the EL_ALBI framework, packet loss was minimized. The combination of DHCP Snooping and IPS Rule protocols effectively mitigated the impact of MITM attacks on network traffic, ensuring more reliable and secure data transmission. By preventing unauthorized access to the network and actively detecting and blocking malicious traffic patterns, the framework maintained the integrity of network communications, reducing the likelihood of packet loss.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 10, October - 2025

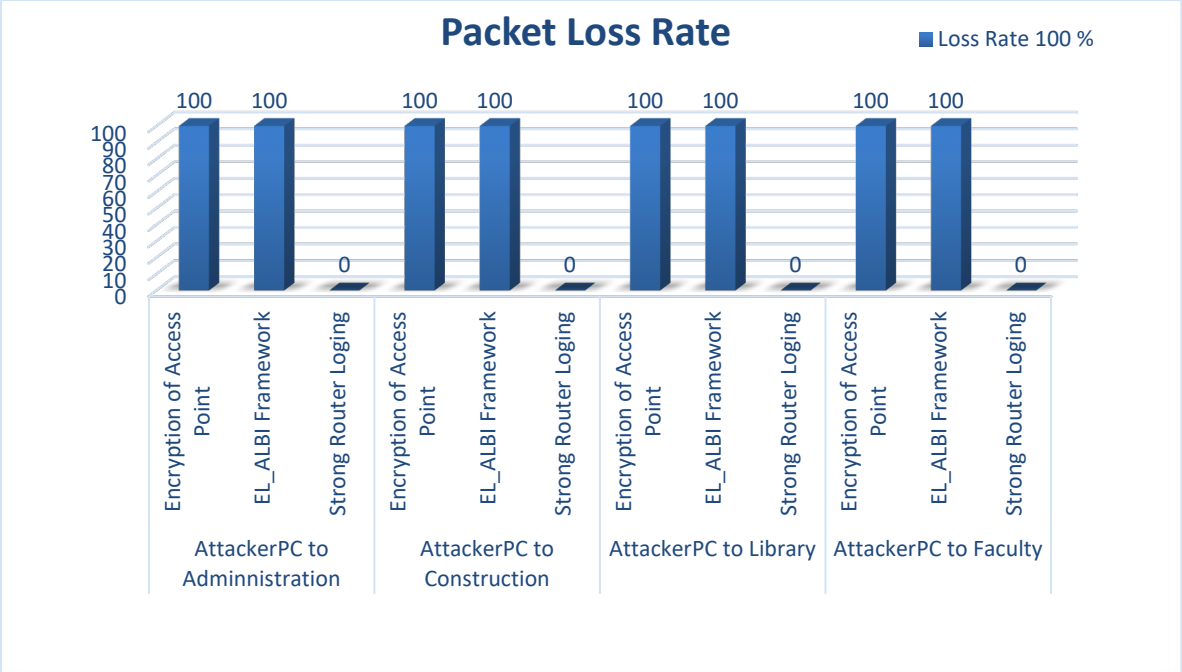


Figure 3: Packet Loss Rate

Comparing number of packets lost in the setups with Encryption of Access Point, Strong Router Login and network configured with EL_ALBI Framework, it was realized that more packets were lost when the attacker sent ICMP data in the setup that involved Encryption of Access Point and with EL_ALBI Framework than the setup with Strong Router Login Credentials

4.2 Network Availability

Network availability is a critical aspect of computer networks, as it determines the accessibility and reliability of network resources for legitimate users. MITM attacks can significantly impact network availability by disrupting connections, intercepting and manipulating data, or launching denial of service attacks.

The study findings reveal that the network availability was higher in the network setup with the EL_ALBI framework compared to setups without the framework implemented. By effectively detecting and preventing MITM attacks, the framework maintained uninterrupted communication between legitimate parties, ensuring that authorized users had continuous access to network resources.

The DHCP Snooping component of the framework played a crucial role in maintaining network availability by preventing unauthorized devices from gaining access to the network. This mitigated the risk of rogue devices or attackers attempting to disrupt network operations or launch DoS attacks.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 10, October - 2025

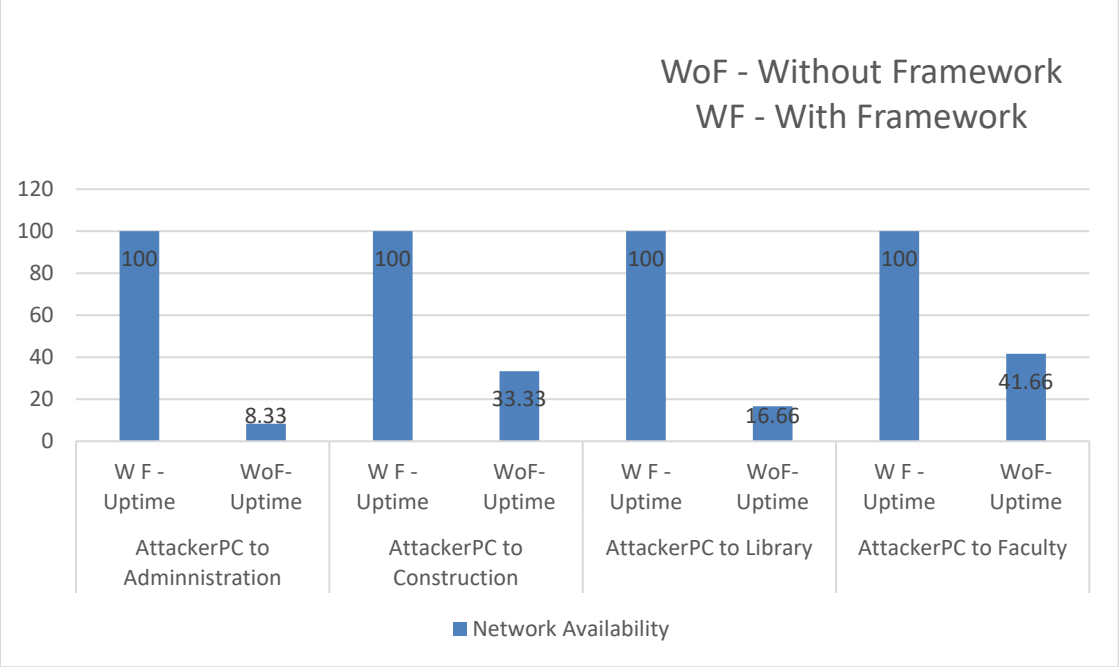


Figure 4: Network Availability Setup with EL_ALBI Framework

4.3 Denial of Service (DoS) Mitigation

Denial of service (DoS) is a common threat to computer networks, aimed at overwhelming network resources and rendering them unavailable to legitimate users. MITM attacks often involve DoS techniques to disrupt network operations and gain control over network traffic.

The findings of this study demonstrate that the EL_ALBI framework effectively mitigated DoS attacks associated with MITM attacks. Network setups without the framework implemented were susceptible to DoS attacks, as traditional security measures like encryption and strong login credentials may not be sufficient to detect and prevent these attacks.

However, with the EL_ALBI framework in place, DoS attacks were successfully prevented. The IPS Rule component played a crucial role in detecting and blocking malicious traffic patterns associated with DoS attacks. By continuously monitoring network traffic and comparing it against predefined rules and signatures, the IPS could promptly identify and mitigate DoS attempts, ensuring the availability and responsiveness of network resources.

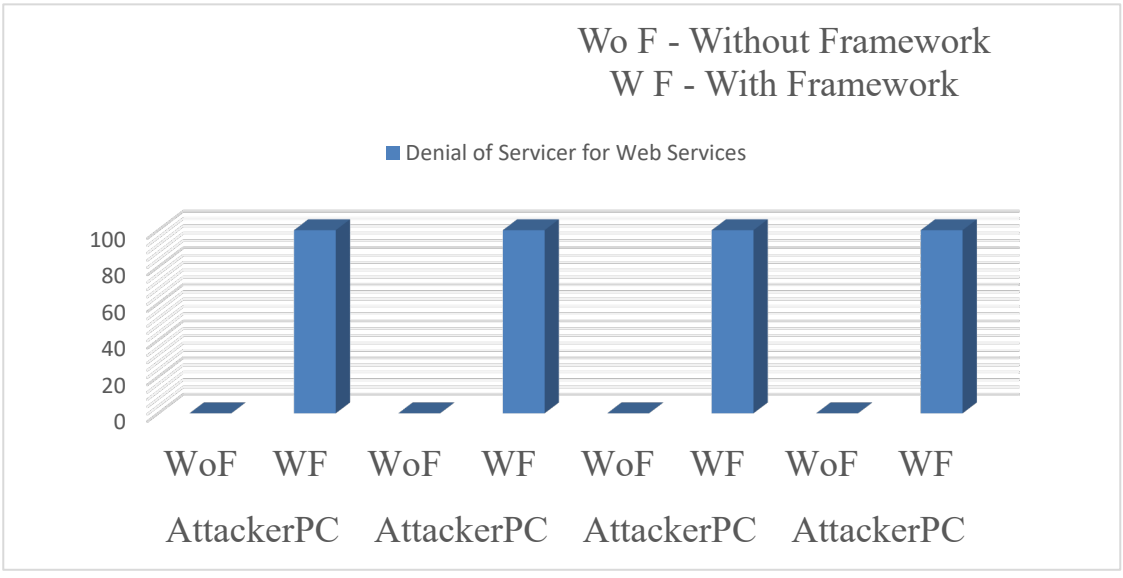


Figure 5: Denial of Service (DoS) in the Network Setup

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 10, October - 2025

Overall, the findings of this study highlight the effectiveness of the EL_ALBI framework in addressing the critical challenges posed by MITM attacks, including packet loss, network availability, and DoS mitigation. By combining the strengths of DHCP Snooping and IPS Rule protocols, the framework provides a comprehensive and robust security solution for computer networks, enhancing data confidentiality, integrity, and authenticity.

5. CONCLUSION

In the ever-evolving landscape of cybersecurity threats, man-in-the-middle (MITM) attacks pose a significant risk to computer networks, compromising the confidentiality, integrity, and authenticity of data communications. This study addressed the critical challenge of MITM attacks by proposing the EL_ALBI framework, a novel and robust solution that combines the strengths of two protocols: The Intrusion Prevention System (IPS) Rule and DHCP Snooping.

The EL_ALBI framework was meticulously designed to detect and prevent MITM attacks, ensuring the security and reliability of network communications. The IPS Rule component continuously analyzed network traffic, leveraging predefined rules and signatures to identify malicious activities and patterns associated with MITM attacks. Upon detecting a potential attack, the IPS Rule took immediate action, blocking the malicious traffic or logging the event for further investigation.

Complementing the IPS Rule, the DHCP Snooping protocol acted as a firewall between untrusted hosts and trusted DHCP servers. It maintained a binding table of valid IP address/MAC address/port mappings, ensuring that only authorized devices could obtain IP addresses from legitimate DHCP servers. This layer of security prevented unauthorized access to the network, mitigating the risk of rogue devices or attackers attempting to launch MITM attacks from within the network.

To evaluate the efficacy of the proposed framework, a comprehensive simulation and testing phase was conducted using the Packet Tracer 8.1 network simulation software. The EL_ALBI framework was implemented on network devices such as switches and routers, enabling the simulation of various network scenarios and attack vectors. Devices on the network were utilized as attackers and servers, mimicking real-world MITM attack scenarios.

The simulation results demonstrated the remarkable effectiveness of the EL_ALBI framework in addressing the challenges posed by MITM attacks. Notably, the framework significantly reduced packet loss, a common consequence of malicious network activities, by maintaining the integrity of network communications and preventing data corruption or dropped packets.

Furthermore, the framework excelled in maintaining network availability, a critical aspect of computer networks. By effectively detecting and preventing MITM attacks, the EL_ALBI framework ensured uninterrupted communication between legitimate parties, granting authorized users continuous access to network resources without disruption.

Notably, the framework's ability to mitigate denial of service (DoS) attacks associated with MITM attacks was particularly impressive. While network setups without the framework were susceptible to DoS attacks, the EL_ALBI framework successfully prevented such attacks, ensuring the availability and responsiveness of network resources.

By implementing the EL_ALBI framework, organizations and individuals can enhance the security of their computer networks, safeguarding sensitive information from unauthorized access and modification. The framework's multi-layered security approach provides a comprehensive and robust solution against MITM attacks, addressing the vulnerabilities and limitations of traditional security measures.

As cybersecurity threats continue to evolve, further research and development efforts can be directed toward enhancing the EL_ALBI framework's capabilities and addressing emerging challenges. This ongoing commitment to innovation will ensure the continued protection of computer networks, maintaining the confidentiality, integrity, and authenticity of data communications in an increasingly interconnected world.

REFERENCES

[1] Al-Hamami, A. H., & Al-Saadoon, G. M. W. (2013). Development of a network-based: Intrusion Prevention System using a Data Mining approach. 2013 Science and Information Conference.

[2] Almusaylim, Z. A., & Zaman, N. (2018). A review on smart home present state and challenges: linked to context-awareness internet of things (IoT). Wireless Networks, 24(2), 4299-4314

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 10, October - 2025

[3] Buamona, N. Q., Hamid, M., & Gunawan, E. (2023). Analisis Dan Implmentasi Keamanan Jaringan Menggunakan Metode DHCP Snooping dan Swirch Port Security. Jurnal Teknik Informatika (J-Tifa), 6(1), 23-31.
[4] Dave, D., Sawhney, G., Aggarwal, P., Silswal, N., & Khut, D. (2023). The new frontier of cybersecurity: emerging threats and innovations. 2023 29th International Conference on Telecommunications (ICT),
[5] Doshi, R., Apthorpe, N., & Feamster, N. (2018). Machine learning DDoS detection for consumer internet of things devices. In IEEE Security and Privacy Workshops (SPW) (pp. 29-35).
[6] Gupta, N., Jindal, V., & Bedi, P. (2023). A Survey on Intrusion Detection and Prevention Systems. SN Computer Science, 4(5), 439.
[7] Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2018). A survey on the security of blockchain systems. Future Generation Computer Systems, 87, 841-853.
[8] Mallik, A., Ahsan, A., Shahadat, M. M., & Tsou, J. C. (2019). Man-in-the-middle-attack: Understanding in simple words. International Journal of Data and Network Science, 3(2), 77-92.
[9] Nirwan, S., & Dhaliwal, B. K. (2023). A Comprehensive Study Cyber Attacks and Countermeasures. 2023 International Conference on Inventive Computation Technologies (ICICT),
[10] Pandey, P. (2013). Prevention of ARP spoofing: A probe packet based technique. 2013 3rd IEEE international advance computing conference (IACC),
[11] Prasad, A., & Chandra, S. (2022). Defending arp spoofing-based mitm attack using machine learning and device profiling. 2022 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS),
[12] Salifu, W. (2012). Authentication protocols for computer and network security. International Journal of Computer Applications, 45(9), 17-24.
[13] Scarfone, K., & Mell, P. (2007). Guide to intrusion detection and prevention systems (IDPS) (NIST Special Publication 800-94). National Institute of Standards and Technology.
[14] Song, W., Beshley, M., Przystupa, K., Beshley, H., Kochan, O., Pryslupskyi, A., Pieniak, D., & Su, J. (2020). A software deep packet inspection system for network traffic analysis and anomaly detection. Sensors, 20(6), 1637.
[15] Sowah, R. A., Ofori-Amanfo, K. B., Mills, G. A., & Koumadi, K. M. (2019). Detection and prevention of man-in-the-middle spoofing attacks in MANETs using predictive techniques in artificial neural networks. Journal of Computer Networks and Communications, 2019, 1-14.
[16] Tamsir Ariyadi, T. (2022). Desain keamanan DHCP snooping untuk mengurangi serangan Local Area Network (LAN). DESAIN KEAMANAN DHCP SNOOPING UNTUK MENGURANGI SERANGAN LOCAL AREA NETWORK (LAN).
[17] Tetteh, S. G. (2024). A Systematic Performance Review of Security Methods for the Cyberworld. Asian Journal of Research in Computer Science, 17(5), 10-18.
[18] Thankappan, M., Rifà-Pous, H., & Garrigues, C. (2022). Multi-Channel Man-in-the-Middle attacks against protected Wi-Fi networks: A state of the art review. Expert Systems with Applications, 210, 118401.
[19] Thankappan, M., Rifà-Pous, H., & Garrigues, C. (2024). A signature-based wireless intrusion detection system framework for multi-channel man-in-the-middle attacks against protected Wi-Fi networks. IEEE Access.
[20] Tok, M. S., & Demirci, M. (2021). Security analysis of SDN controller-based DHCP services and attack mitigation with DHCPguard. Computers & security, 109, 102394.
[21] West, M. (2009). Network security: A practitioner's guide to intrusion detection and prevention. CRC Press.