

Design of mobile IPv6 IDS for Mitigating DoS Attacks on the correspondent node, Home Agent, and Mobile Node

Supriyanto Praptodiyono, Rido Zulfahmi, Henki Bayu Seta, Novi Trisman Hadi, Moh. Jauhari, Rian Fahrizal, and Teguh Firmansyah

Abstract—This study investigates the implementation of an Intrusion Detection System (IDS) in a Mobile IPv6 network to mitigate Denial of Service (DoS) attacks targeting the Correspondent Node (CN), Home Agent (HA), and Mobile Node (MN). The IDS was designed to detect abnormal network traffic by identifying the time and IP address of the attacker, providing real-time alerts. To enhance security, the IDS was integrated with a firewall capable of blocking detected DoS attacks. Performance evaluation was conducted under multiple scenarios, including normal operation, under attack, and under attack with the IDS-firewall system active. Testing on the CN demonstrated a reduction in throughput loss to 20.30% and 11.65%, with CPU usage decreasing by 59.48% and an average attacker block time of 0.9 seconds. On the HA, throughput loss was reduced to 16.05% and 18.87%, CPU usage decreased by 50.52%, and the block time was 1.2 seconds. Testing on the MN showed a reduction in throughput degradation to 45.98% and 56.09%, with CPU usage decreasing by 17.86%. The results indicate that an IDS integrated with a firewall effectively mitigates DoS attacks in Mobile IPv6 networks, improving both network performance and system resilience. This approach demonstrates a practical solution for maintaining reliable communication and protecting critical network nodes against DoS threats.

Keywords—CN; DDoS; IDS; HA; MN

I. INTRODUCTION

INTERNET developments have profoundly influenced human lifestyles, particularly the increasing demand to remain connected to the internet anytime and anywhere. As of November 2018, mobile devices—excluding tablets—accounted for 48.2% of global internet traffic, with the proportion in Asia exceeding 61% [1]–[5]. According to the Global System for Mobile Communications Association (GSMA) Intelligence, the number of mobile device users worldwide has reached 5.035 billion, with one billion users added in just four years. Consequently, nearly 5 billion of the world's 7.5 billion people now rely on mobile devices—including smartphones, tablets, and feature phones—resulting

in high user density and continuous connectivity demand worldwide [6]–[9].

Many internet users access online services while on the move, and vehicles are increasingly equipped to connect automatically to the internet for diverse applications. One technology that supports seamless connectivity in IPv6 networks is the Mobile IPv6 (MIPv6) protocol [10]–[12]. MIPv6 allows mobile nodes (MNs) to maintain uninterrupted communication when moving across different network domains, a process known as handover [13]–[15]. This capability is essential due to the dynamic nature of mobile users, ensuring that applications and services remain accessible during mobility. However, the growing use of MIPv6 networks also attracts potential threats, such as Denial-of-Service (DoS) attacks. These attacks aim to overwhelm network resources by sending excessive traffic, preventing legitimate users from accessing the network [16]–[18]. A notable example occurred in July 2018 when Ubisoft servers suffered repeated DDoS attacks, causing performance degradation across several games, including Far Cry 5, Rainbow Six: Siege, and Ghost Recon: Wildlands. Previous studies have highlighted the vulnerability of MIPv6 networks to DoS attacks. It was demonstrated that MIPv6 performance significantly decreases under such attacks. To counteract these threats, network-based Intrusion Detection Systems (IDS) have been proposed [19], [20].

Research by [21] confirmed that IDS can detect DoS attacks using predefined rules, monitoring network traffic and generating alerts when anomalies are detected [23]–[25]. However, conventional IDS approaches are largely reactive: they detect threats but do not directly prevent them, leaving network performance vulnerable until administrative action is taken [22]. Building on these insights, the present research proposes an enhanced approach in which the IDS is integrated with a firewall. This system not only detects DoS attacks in Mobile IPv6 networks but also actively controls packet flow based on IDS alerts, mitigating attacks in real-time. The proposed solution is tested on all critical MIPv6 nodes—Correspondent Node (CN), Home Agent (HA), and Mobile Node (MN)—demonstrating its ability to reduce throughput degradation, lower CPU utilization, and decrease response time during DoS attacks, thereby maintaining network performance and reliability under attack conditions.

This research is proposed design of Mobile IPv6 IDS for

The first four authors are with Universitas Pembangunan Nasional Veteran Jakarta (UPNVJ), Indonesia (e-mails: supriyanto.fik@upnvj.ac.id, rido.zulfahmi@upnvj.ac.id, henkiseta@upnvj.ac.id, novitrismanhadi@upnvj.ac.id).

Universitas Sultan Ageng Tirtayasa (UNTIRTA), Indonesia (e-mails: moh.jauhari73@gmail.com, rian.fahrizal@untirta.ac.id, teguhfirmansyah@untirta.ac.id).



mitigating DoS attacks on the correspondent node, home agent, and mobile node. The novelty of this research lies in the integration of an Intrusion Detection System (IDS) with a firewall for Mobile IPv6 networks, enabling real-time mitigation of Denial-of-Service (DoS) attacks. Unlike traditional IDS implementations that only detect attacks and send alerts to administrators, the proposed system automatically controls malicious packet flow, preventing network degradation as attacks occur. The main contributions of this study are:

- 1) Implementation of IDS and firewall protection on all critical MIPv6 nodes—Correspondent Node (CN), Home Agent (HA), and Mobile Node (MN)—ensuring that both stationary and mobile elements of the network are safeguarded.
- 2) Experimental results demonstrate a significant reduction in throughput degradation during DoS attacks, showing the system’s ability to maintain communication performance.
- 3) The system reduces excessive CPU utilization on network nodes during attacks, ensuring efficient operation under high-load scenarios.
- 4) The IDS-firewall integration allows fast detection and blocking of attacker IPs, minimizing the delay between attack detection and mitigation.
- 5) By combining detection and prevention, the system transitions IDS from a reactive tool to a proactive network defense mechanism in Mobile IPv6 environments.

Overall, this research demonstrates a practical and effective method for improving network resilience against DoS attacks in Mobile IPv6, providing measurable improvements in throughput, CPU performance, and mitigation response time.

II. METHOD

A. Proposed system for investigation

The system was developed by preparing a Linux kernel with Mobile IPv6 support, installing the required software, and configuring IPv6 addresses and applications on each node to enable Mobile IPv6 communication. Hardware devices and an Intrusion Detection System (IDS) were installed and configuration a server. All configuration and integration between the firewall and the IDS were performed on Ubuntu 16.04. The evaluation consisted of launching attacks against the Mobile IPv6 setup by sending large volumes of request packets to the nodes that play key roles in MIPv6: the Mobile Node (MN), Home Agent (HA), and Correspondent Node (CN). During the attacks, the IDS monitored incoming and outgoing traffic on the server and generated alerts for the administrator. The firewall then enforced mitigation actions based on the IDS rules to control the malicious traffic.

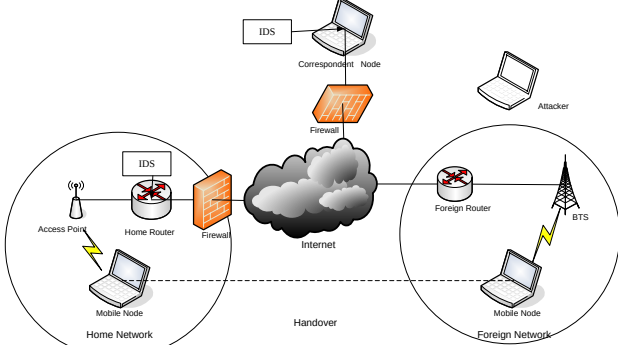


Fig. 1. System Implementation

Fig. 1 illustrates the complete system, which integrates a firewall and an Intrusion Detection System (IDS) within the network. In this topology, the firewall and IDS are installed only on the Home Router and the Correspondent Node. The IDS implementation in MIPv6 was evaluated on a laboratory-scale local network comprising the main MIPv6 entities: the Mobile Node (MN), Home Agent (HA), Foreign Agent (FA), and Correspondent Node (CN). The system was tested by launching DoS attacks and measuring network performance. Three scenarios were considered: (i) normal operation, (ii) under DoS attack, and (iii) under DoS attack with an active IDS integrated with a firewall. Attacks were directed at the MN, HA, and CN, with the MN operating in both HA and FA networks. The evaluation metrics included CPU utilization on the target node, throughput, and IDS response time in performing blocking actions.

B. Correspondent Node (CN) Attack Scenario

In the first scenario, the network is configured with a MIPv6 system and the attack target is the Correspondent Node (CN), which has an IDS installed.

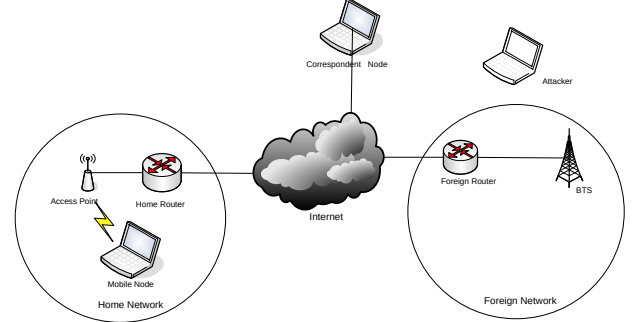


Fig. 2. MIPv6 under normal conditions with the Mobile Node (MN) in the Home Agent (HA).

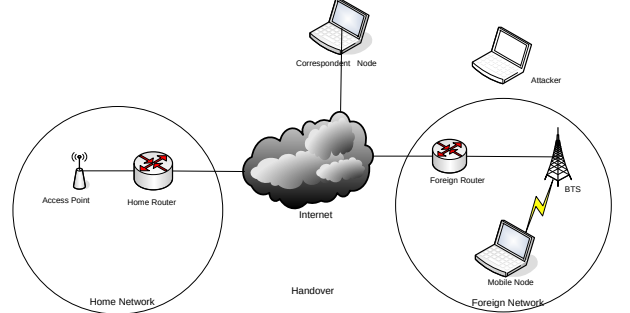


Fig. 3. MIPv6 under normal conditions with the Mobile Node (MN) in the Foreign Agent (FA).

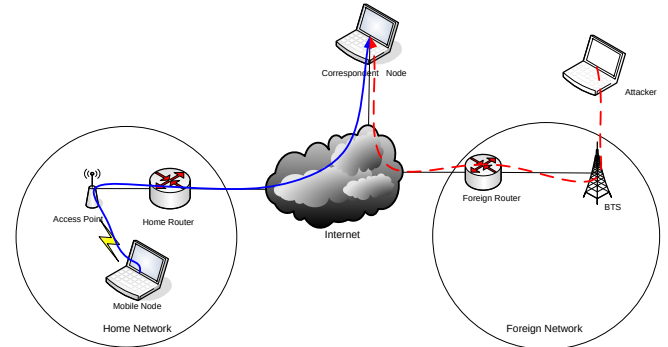


Fig. 4. MIPv6 CN attack condition with the Mobile Node (MN) in the Home Agent (HA).

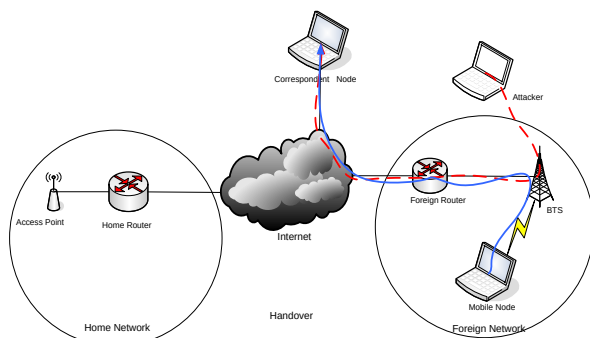


Fig. 5. MIPv6 CN attack condition with the Mobile Node (MN) in the Foreign Agent (FA).

Each condition was tested in two states. In the first state, when the MN was in the HA, the MN performed data transfer to the CN using the iperf3 tool, and data were collected on CPU utilization, throughput, and IDS response time. In the second state, when the MN was in the FA, the MN again performed data transfer to the CN using iperf3, with the same parameters measured. Data collection was repeated 10 times for each state.

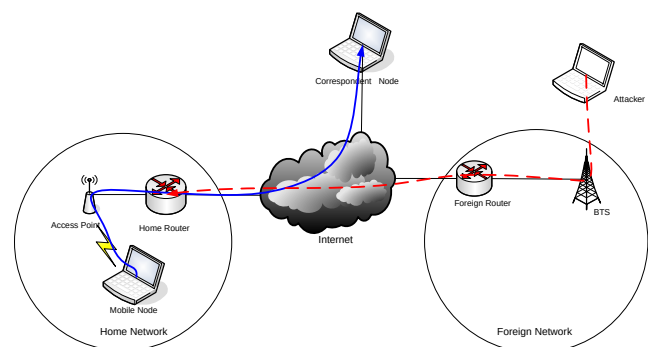


Fig. 8. MIPv6 HA attack condition with the Mobile Node (MN) in the Home Agent (HA).

This scenario was tested under two conditions: (i) a DoS attack with an IDS not integrated with a firewall, and (ii) a DoS attack with an IDS integrated with a firewall.

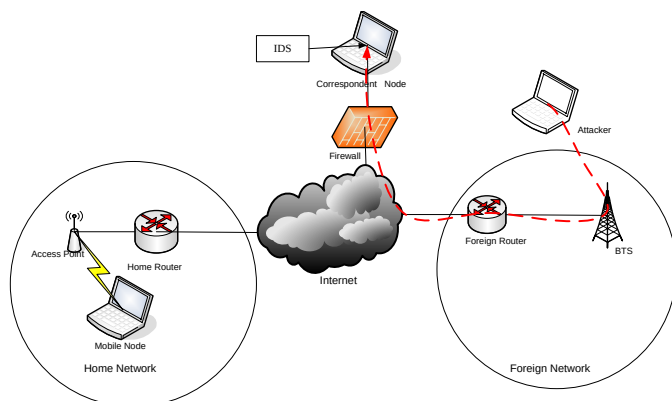


Fig. 6. MIPv6 CN attack condition with integrated IDS–firewall and the Mobile Node (MN) in the Home Agent (HA).

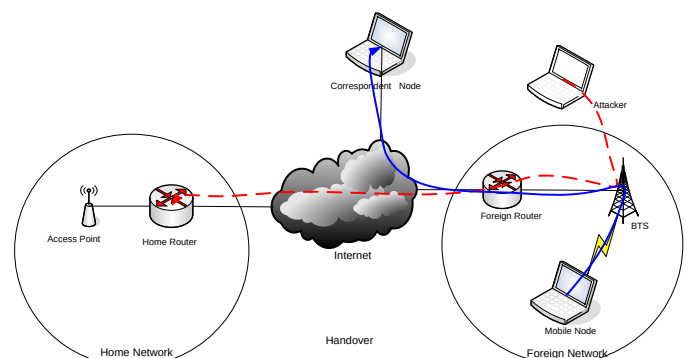


Fig. 9. MIPv6 HA attack condition with the Mobile Node (MN) in the Foreign Agent (FA).

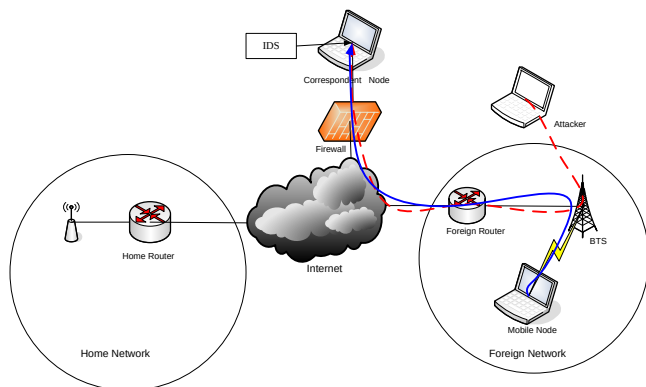


Fig. 7. MIPv6 CN attack condition with integrated IDS–firewall and the Mobile Node (MN) in the Foreign Agent (FA).

C. Home Agent (HA) Attack Scenario

In the second scenario, the network is configured with a MIPv6 system, and the attack target is the Home Agent (HA), which has an IDS installed.

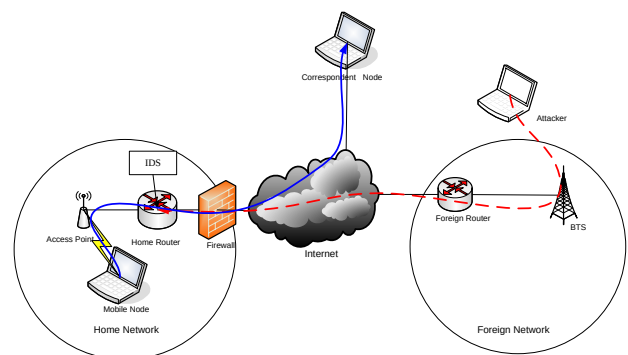


Fig. 10. MIPv6 HA attack condition with integrated IDS–firewall and the Mobile Node (MN) in the Home Agent (HA).

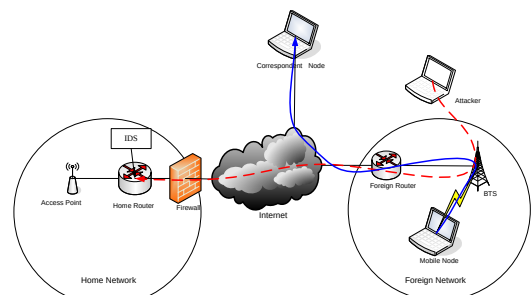


Fig. 11. MIPv6 HA attack condition with integrated IDS–firewall and the Mobile Node (MN) in the Foreign Agent (FA).

Each condition was tested in two states. In the first state, when the MN was in the HA, the MN performed data transfer to the CN using the iperf3 tool. Data were collected on CPU utilization, IDS response time at the HA, and throughput. In the second state, when the MN was in the FA, the MN performed data transfer using iperf3 and executed a ping to the CN. Data were collected on CPU utilization, throughput, and IDS response time. Each measurement was repeated 10 times in both states.

D. Mobile Node (MN) Attack Scenario

In the third scenario, the network is configured with a MIPv6 system, and the attack target is the Mobile Node (MN), with the IDS installed in the Home Agent (HA).

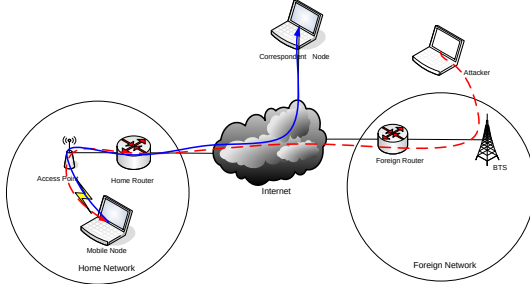


Fig. 12. MIPv6 MN attack condition with the Mobile Node (MN) in the Home Agent (HA).

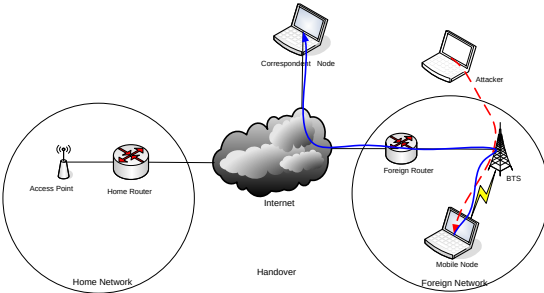


Fig. 13. MIPv6 MN attack condition with the Mobile Node (MN) in the Foreign Agent (FA).

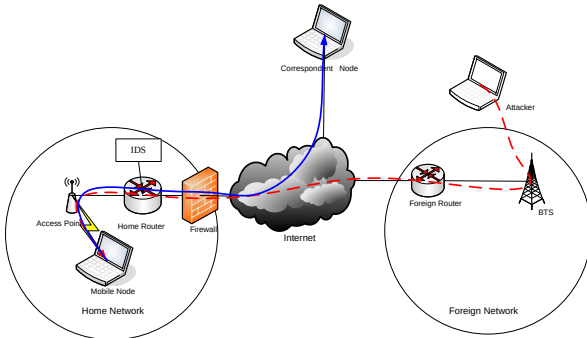


Fig. 14. MIPv6 MN attack condition with integrated IDS-firewall and the Mobile Node (MN) in the Home Agent (HA).

This scenario was tested under two conditions: (i) a DoS attack with an IDS not integrated with a firewall, and (ii) a DoS attack with an IDS integrated with a firewall. Each condition was tested in two states. In the first state, when the MN was in the HA, the MN performed data transfer to the CN using the iperf3 tool and executed a ping. Data were collected on CPU

utilization, throughput, and IDS response time. In the second state, when the MN was in the FA, the MN again performed data transfer using iperf3 and executed a ping to the CN, with the same parameters measured.

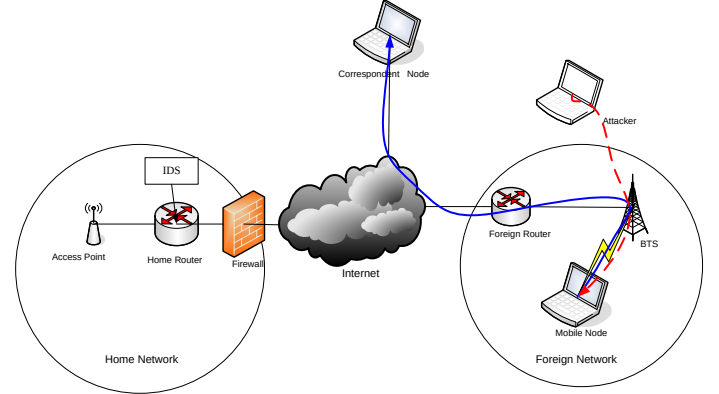


Fig. 15. MIPv6 MN attack condition with integrated IDS-firewall and the Mobile Node (MN) in the Foreign Agent (FA).

III. RESULTS AND DISCUSSION

This section explains the system testing process, conducted based on the design described in the previous chapter. The testing involved performing a DoS attack on the MIPv6 network to evaluate its performance before and after integrating the firewall with the IDS during the attack.

A. IDS Implementation on the MIPv6 Network

The IDS was implemented on a MIPv6 network using Snort software version 2.9.9.0, configured according to the scenarios described in the previous chapter and operated in network intrusion detection system (NIDS) mode. The IDS monitored incoming and outgoing packets and compared them against its alert database. When abnormal traffic was detected that matched an entry in the database, the IDS generated a log entry and stored it as an alert file. Fig. 16 presents an example of the detected alerts.

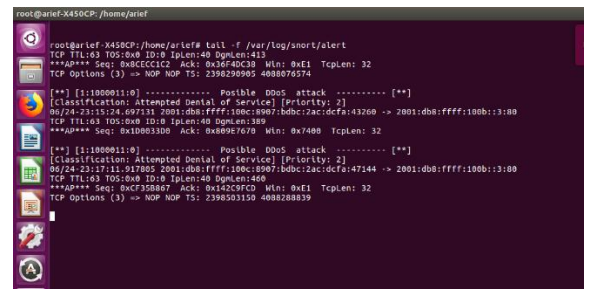


Fig. 16. IDS Detection Alert on DoS Attack

Fig. 16 illustrates an IDS alert generated during a DoS attack. The alert provides details such as the timestamp of the detected attack and the source IP address of the attacker. The IDS alert database is subsequently processed by the firewall, which uses this information to block the attacker's IP address.

In this system, the firewall utilizes the iptables feature to enforce blocking rules. The configuration enabling the firewall to read IDS alert files is implemented through a Linux bash script named protect.sh. A flowchart of the firewall process for parsing and applying rules from the alert file is presented in Fig. 17.

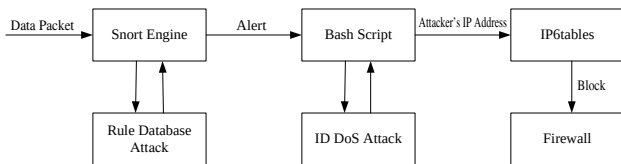


Fig. 17. Block Diagram of IP Blocking Process by Firewall

Based on the flowchart in Fig. 17, the process begins when an incoming data packet arrives. The IDS inspects the packet and compares it against the attack signature database. If the packet matches an entry in the IDS alert database, the traffic is classified as an attack and logged into the alert file. This alert file is continuously updated with new attack reports and subsequently analyzed by a bash script. The script compares the alert ID with predefined rules in its configuration. If a match is found, the script extracts the attacker's source IP address and inserts it into iptables. The firewall then processes the updated iptables rule set, effectively blocking the malicious IP address. The outcome of this process, showing the attacker's IP successfully blocked by the firewall, is illustrated in Fig. 18.

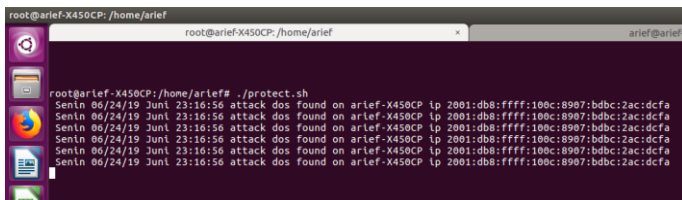


Fig. 18. Display of the Attacker's IP Address After Being Blocked

The attack was performed using a DoS script developed with the Scapy library in Python 3. To execute the attack, the script requires the target's IP address and an open port. In this scenario, the attacks were directed at port 80, located at the application layer. Port 80 was chosen because it is widely used for web server communication, enabling connections between clients and websites. Fig. 19 shows the attacker's PC, which successfully launched the DoS attack before being detected and blocked by the IDS–firewall integration.

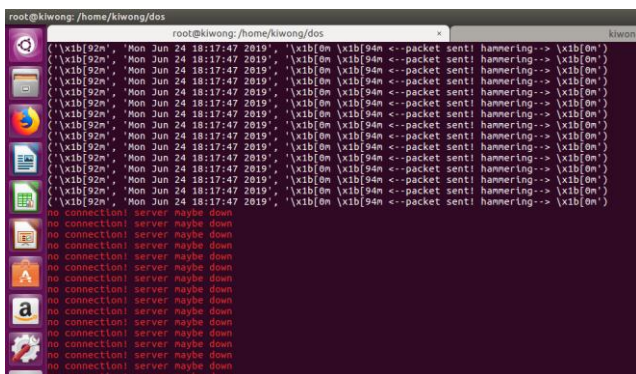


Fig. 19. DoS Attack Display Before and After Blocking

Fig. 19 presents the view from the attacker's PC during the DoS attack process. When the IDS–firewall system successfully blocks the attack, the target no longer responds to the incoming packets. Consequently, the attacker's display changes to indicate “no connection”, highlighted in red. Conversely, if the

target has not yet blocked the attack, the attacker's PC continues to send packets without interruption, and the display remains unchanged.

B. System Testing Analysis

The IDS implementation on the MIPv6 network was evaluated through a series of DoS attacks targeting all primary MIPv6 nodes, namely the Correspondent Node (CN), Home Agent (HA), and Mobile Node (MN). The attacker was positioned at the access point within the Foreign Agent (FA) network. During the testing process, performance data were collected, including CPU utilization, RAM usage, throughput, and IDS response time.

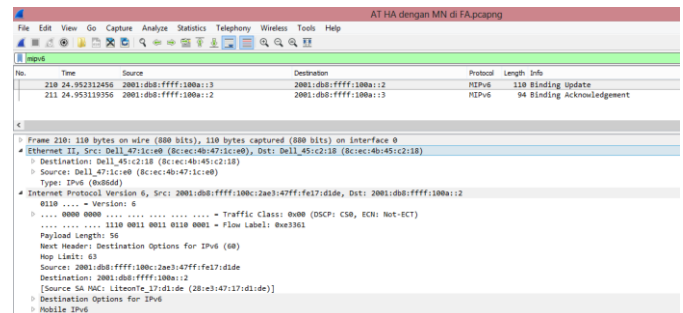


Fig. 20. Capture Results of Mobile IPv6

Fig. 20 illustrates the packet capture when the MIPv6 system is operational. The protocol field clearly indicates Mobile IPv6, with both source and destination addresses displayed in IPv6 format. The test data obtained are analyzed by comparing three conditions: (i) normal operation with the IDS not integrated with the firewall, (ii) under DoS attack with the IDS not integrated with the firewall, and (iii) under DoS attack with the IDS integrated with the firewall.

C. Testing on the Correspondent Node (CN)

The Correspondent Node (CN) is one of the key entities in the MIPv6 system, functioning as a server. In this test scenario, two experimental conditions were evaluated: (i) the Mobile Node (MN) located in the Home Agent (HA) network and (ii) the MN located in the Foreign Agent (FA) network.

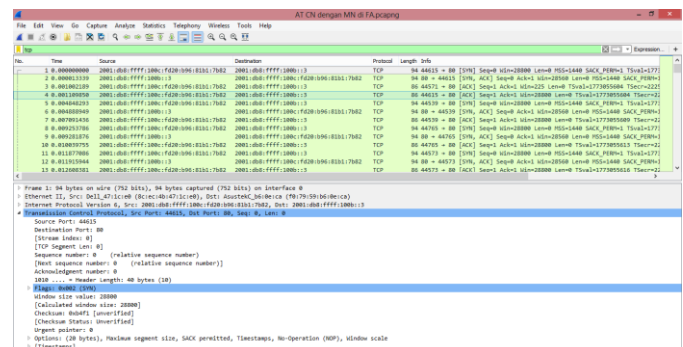


Fig. 21. Attack on CN

The Correspondent Node (CN) was subjected to a DoS attack originating from an attacker (AT) connected to the FA, as illustrated in Figs. 4–7. The DoS attack used was a SYN flood attack, where packets were transmitted in large numbers according to the maximum capacity of the attacker's PC. A Wireshark capture of the attack traffic between the attacker

and the CN is shown in Fig. 21. Based on Fig. 21, the attack protocol is identified as TCP. The attacker's IP address is 2001:db8:ffff:100c:fd20:b96:81b1:7b82, while the CN's IP address is 2001:db8:ffff:100b::3. The data transfer process between the attacker and the CN follows the standard TCP three-way handshake: SYN (synchronization) initiates the connection request from the client, SYN-ACK (synchronization acknowledgment) confirms the request from the server, and ACK (acknowledgment) finalizes the connection. This process establishes communication between client and server under normal conditions. However, in this experiment, SYN packets were sent in massive quantities, overwhelming the server. As a result, the CN continuously replied with SYN-ACK packets, consuming system resources and leaving legitimate clients unable to establish connections. The packet exchange between the attacker and the CN during the attack is shown in Fig. 22.

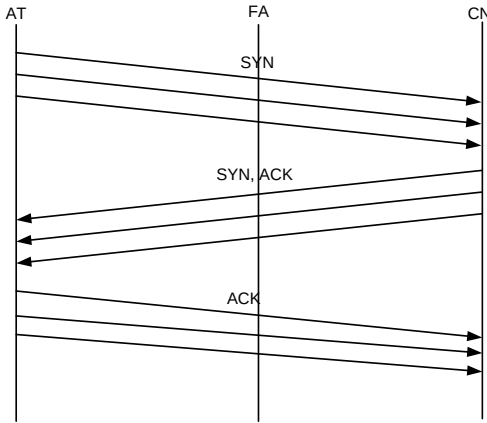


Fig. 22. Passing Message Attacker With CN

CN testing was conducted under two conditions, with the MN located in the HA and in the FA. The measured parameters included throughput, CPU utilization, RAM usage, and response time. Measurements were taken under three traffic conditions: (i) normal traffic, (ii) during a DoS attack, and (iii) during a DoS attack with active blocking.

1) CN Throughput Analysis

Throughput is one of the key parameters measured in this network test. The average throughput results for the CN test with the MN connected to the HA are presented in Fig. 23. Throughput is the effective data transfer rate measured in bits per second (bps), or the total number of packets received at the destination during a specific time interval. It can also be expressed in bytes per second, packets per second, or bits per second. It shows that the average throughput in normal traffic, when the MN sends TCP packets to the CN via the HA, is 69.573 Mbit/sec, before a DoS attack occurs and with no other clients communicating with the CN. In the second condition, the average throughput decreases from 69.573 Mbit/sec to 46.945 Mbit/sec.

This decrease occurs because the CN is under a DoS attack, where a portion of the throughput is consumed by the attacker sending SYN requests and occupying the CN with SYN-ACK replies. The throughput increases to 61.067 Mbit/sec after the DoS attack is blocked by the IDS–firewall system.

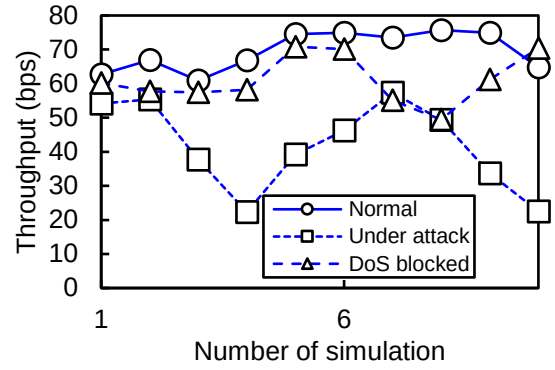


Fig. 23. CN Test Throughput with MN Connected to HA

Although the DoS attack is mitigated, the throughput does not fully return to the normal value because the attacker continues sending SYN packets to the CN. The blocking process only prevents the CN from responding to the attacker's requests, leaving the attack packets in the traffic flow. The integration of the IDS system with the firewall improves Mobile IPv6 traffic performance at the CN when the MN is in the HA. During the DoS attack, throughput decreased by 32.524%, while after the DoS was blocked, the decrease was reduced to only 12.226%.

The next test involved launching a DoS attack on the CN while the MN, located in the FA, was communicating with the CN. Fig. 24, where the MN sends TCP packets using the iPerf3 tool to the CN within the MIPv6 network with the MN connected to the FA.

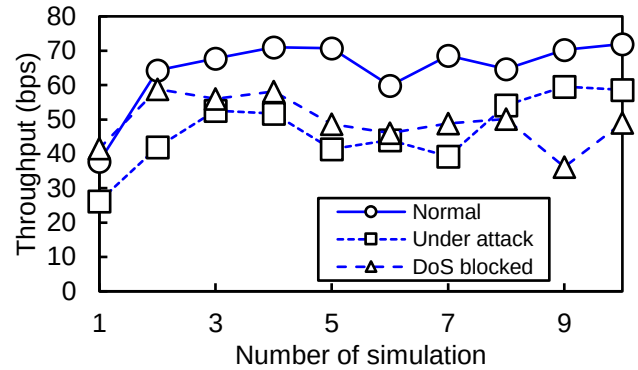


Fig. 24. CN Test Throughput with MN Connected to FA

The test results in Fig. 24 were obtained when the MN was located in the FA and transmitted TCP packets to the CN in the MIPv6 network using the iPerf3 tool. Throughput measurements were performed ten times, and the average values were taken. The results were then compared under three traffic conditions: (i) normal operation, (ii) under DoS attack, and (iii) after the DoS attack was blocked with the IDS–firewall integration while the MN was connected to the FA. It shows that the average throughput under normal traffic, when the MN sent TCP packets to the CN via the FA, was 64.697 Mbit/sec, with no DoS attack and no competing clients communicating with the CN. During the DoS attack, throughput decreased significantly to 41.821 Mbit/sec. This reduction occurred because the CN was overwhelmed by SYN packets from the attacker, forcing it to respond with SYN-ACK packets and leaving fewer resources for legitimate connections.

After the DoS attack was blocked by the IDS–firewall system, throughput increased to 49.354 Mbit/sec. Although performance improved, the throughput did not fully return to normal levels because the attacker continued to send SYN packets. The firewall prevented the CN from replying to the malicious requests but could not eliminate the packets entirely from the traffic flow. These results demonstrate that integrating an IDS with a firewall can significantly improve MIPv6 traffic performance at the CN when the MN is in the FA, though residual attack traffic still prevents full restoration of normal throughput. Throughput decreased by 35.36% during the DoS attack, and after the DoS attack was blocked, the decrease was reduced to 23.71%. The MIPv6 system testing was conducted using five PCs and two access points. These access points served as Wi-Fi connections between the MN and HA, as well as between the MN and FA. Consequently, the MN was connected to both HA and FA via wireless technology, leading to fluctuating and unstable throughput during testing. The throughput values under normal traffic conditions differ. This variation is influenced by the distance between the MN and the wireless access points during measurement and data collection. The attack results also reveal that increased attack traffic directly reduces the available throughput for legitimate MN–CN communication. Furthermore, comparison of result shows that when the MN is located in the FA, its throughput is consistently lower than when it is in the HA. This is due to the MN sharing the same access point during FA testing, which reduces the available throughput compared to the HA scenario.

2) CPU Utilization Analysis on CN

CPU utilization is one of the performance parameters measured in this network testing. CPU utilization refers to the total CPU usage during the experiment, observed using several monitoring tools and based on the request–reply process between the MN and the CN. The average CPU utilization results for the CN test are presented in Fig. 25. The measurements were obtained when the MN transmitted TCP packets to the CN on the MIPv6 network using the iPerf3 tool. Data collection was performed 10 times to ensure accuracy and consistency. This experiment was conducted to evaluate the variation in CPU usage on the CN under three conditions: normal traffic without attack, during a DoS attack, and after the DoS attack was mitigated by the integrated firewall on the CN.

It shows that under normal conditions, when the CN only receives TCP packets from the MN, the CPU utilization is 9.96%. This test was conducted by transmitting TCP packets from the MN to the CN using the iPerf3 tool. It indicates a significant increase in CPU usage, rising from 9.96% to 16.02%. This increase is caused by the large number of requests generated by the attacker during the DoS attack, forcing the CN to send a high volume of reply packets (SYN-ACK). The continuous reply process to the attacker results in additional workload on the CN, thereby increasing CPU utilization.

Meanwhile, the fourth column shows that CPU usage decreases from 16.02% to 10.09% once the DoS attack is successfully mitigated by the CN's firewall. In this case, the CN no longer responds to the attacker's requests, which reduces unnecessary processing overhead. The remaining 10.09% CPU utilization is primarily attributed to legitimate MN traffic combined with the firewall's handling of the attacker's request

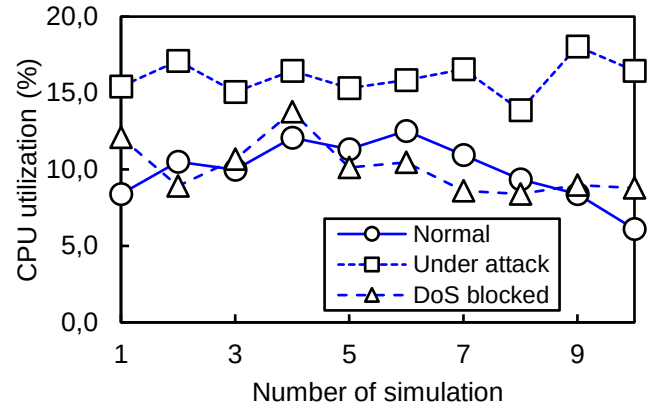


Fig. 25. CPU Utilization Analysis on CN

packets. In summary, an IDS system integrated with a firewall is proven to reduce CPU usage on the CN during and after a DoS attack. During the DoS attack, CPU utilization increased by 60.79%, indicating a significant overhead caused by the CN replying to the attacker's requests. After the DoS attack was successfully blocked, CPU usage increased by only 1.31% compared to normal conditions. This demonstrates that the firewall and IDS combination effectively prevents the CN from responding to malicious traffic, thereby minimizing unnecessary CPU load and stabilizing system performance.

3) CN Response Time Analysis

Response time is one of the parameters measured in CN testing. In this case, response time refers to the amount of time required by the IDS system and the firewall at the CN to block an attacker conducting a DoS attack. When the IDS detects a DoS attack, it generates an alert in the form of a log entry. This log is then processed by the CN's firewall, which blocks the attacker's IP address to prevent further malicious requests.

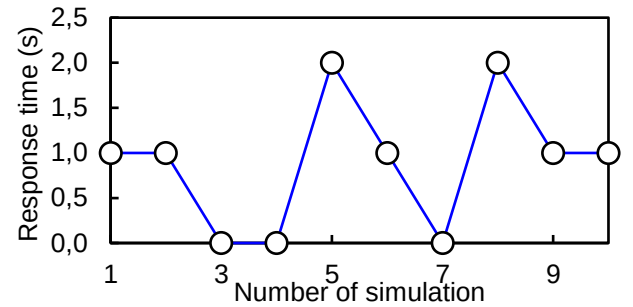


Fig. 26. Response Time of CN in Blocking Attacker's IP Address

Fig. 26 shows that the average time required for the CN to block an attacker is 0.9 seconds. This blocking time is calculated from the moment the attack begins until the attacker is successfully blocked by the firewall. The variation in blocking time on the CN is strongly influenced by the IDS detection speed in analyzing incoming traffic. Since the IDS must inspect each packet header and behavior pattern, the number of incoming data packets directly impacts the response. When packet traffic is high and involves multiple clients, the IDS requires additional processing time to identify anomalies, resulting in a longer blocking delay.

D. Testing on Home Agent (HA)

The Home Agent (HA) is a crucial node in the Mobile IPv6 (MIPv6) system, serving as the central hub of communication. When a Mobile Node (MN) performs a handover, it must first notify the HA to ensure that the MN's IP address remains unchanged and communication continuity is maintained. The testing scenario on the HA is carried out in a manner similar to the Correspondent Node (CN) testing, with parameters such as throughput, CPU utilization, RAM usage, and response time being measured.

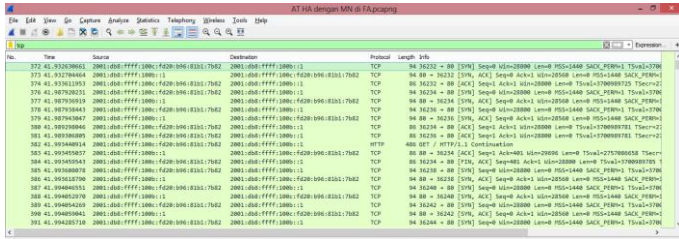


Fig. 27. Attack on HA

Fig. 27 shows a captured screenshot of the attack scenario. In this case, the IP address 2001:db8:ffff:100a::2 represents the HA that becomes the target of the attacker. The attacker launches a DoS attack by sending a large number of TCP SYN packets toward the HA. As a result, the HA is forced to process the requests and generate SYN-ACK replies, which overloads its resources. Subsequently, the IDS system detects the abnormal traffic and generates an alert log. This alert is forwarded to the firewall on the HA, which then blocks the attacker's IP address. This mechanism prevents further processing of malicious requests, allowing legitimate MN-HA communication to recover.

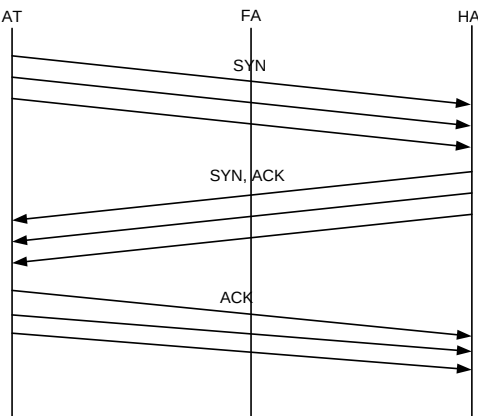


Fig. 28. Passing Message Attacker with HA

It shows the passing message results obtained from the Wireshark capture. The message flow illustrates the interaction between the attacker and the HA during the DoS attack. The attack mechanism on the HA is essentially the same as that carried out on the CN. In this scenario, the attacker connects to the Foreign Agent (FA) and sends a large number of TCP SYN packets toward the HA. The attacker's IP address remains unchanged throughout the attack. As a result, the HA continuously receives SYN requests and responds with SYN-ACK messages, which leads to an overload of resources. This excessive exchange of packets prevents legitimate clients (i.e., MN) from establishing proper communication with the HA.

1) HA Throughput Analysis

Throughput testing was measured by the MN sending TCP packets to the CN via the HA and FA. The HA was then subjected to a DoS attack by an attacker through the FA, and the impact of the HA attack on the throughput obtained from communication between the MN and CN was observed. Fig. 29 shows the results of this test. It was obtained when the MN was in the HA, sending TCP packets using the iPerf3 tool to the CN in the MIPv6 network. Data collection was carried out 10 times, and the average value was taken. This test was conducted to determine the difference in MIPv6 network performance by comparing packet delivery during normal traffic, under a DoS attack on the HA, and after the DoS was blocked by the HA.

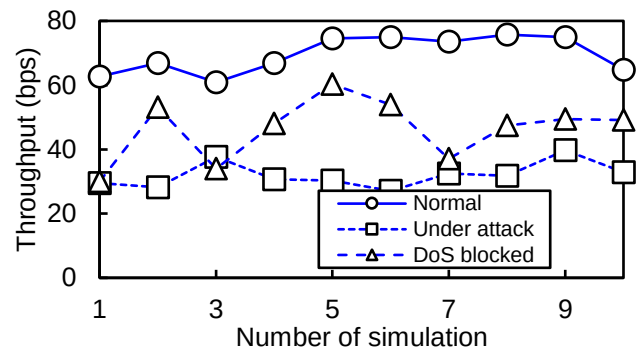


Fig. 29. HA Test Throughput With HA Connected MN

Fig. 29 shows the change in throughput values from the HA testing process, indicating the impact on communication between the MN and CN. In MIPv6, the HA is a node that must always be traversed by the MN when communicating with the CN. Therefore, when the HA is attacked by an attacker originating from the FA, the communication path from the MN to the CN becomes congested with DoS packets sent by the attacker (based on the topology used). It shows that the average throughput in normal traffic, when the MN sends TCP packets to the CN via the HA, is 69.573 Mbit/sec before the DoS attack and when no other clients are communicating with the CN. The third column shows that the average throughput decreased from 69.573 Mbit/sec to 35.287 Mbit/sec. At this stage, the HA was attacked with a DoS attack by the attacker, so part of the throughput/communication path from the MN to the CN was filled with DoS packets. The attacker sends SYN request packets and keeps the HA busy replying with SYN-ACK packets. At this stage, the DoS attack carried out by the attacker was successfully blocked by the HA, so the throughput increased from 35.287 Mbit/sec to 46.4524 Mbit/sec. However, even though the DoS attack was blocked, traffic could not return to normal. This is because the attacker continued to send SYN packets to the HA. The blocking process performed by the HA only denies communication with the attacker, meaning the HA does not reply to the request packets but still allows them to enter the traffic.

The next test is the attacker performs a DoS attack on the HA by taking data from the MN in the FA while communicating with the CN. The test results were obtained under conditions when the MN is in the FA, then the MN sends a TCP packet using the iPerf3 tool to the CN in the MIPv6 network.

Throughput data is taken 10 times and the average value is taken. Then the *throughput data* obtained is compared with 3 traffics, namely normal, DoS attack on the HA and after DoS is blocked by the HA with the MN connected to the FA. The average *throughput results* of the HA test with MN in the FA can be seen in Fig. 30 which shows changes in the average *throughput value* from the HA test process. This indicates an influence obtained on communication between the MN and the CN. HA in MIPv6, HA is a node that is always passed by the MN in communicating with the CN. So when HA is attacked by an attacker originating from FA, the path taken by MN to CN is filled with DoS packets sent by the attacker (based on the topology used).

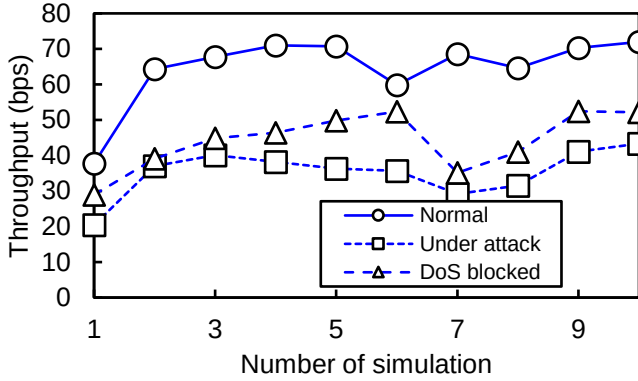


Fig. 30. HA Test Throughput With FA Connected MN

Fig. 30 shows that the average throughput in normal traffic, when the MN sends TCP packets to the CN via the HA, is 64.697 Mbit/sec before a DoS attack and when no other clients are communicating with the CN. It shows a decrease in average throughput from 64.697 Mbit/sec to 32.307 Mbit/sec. At this stage, the HA was attacked using a DoS attack by the attacker, causing part of the throughput/communication path from the MN to the CN to be filled with DoS packets. The attacker sends SYN request packets and keeps the HA busy replying with SYN-ACK packets. In this case, the DoS attack carried out by the attacker was successfully blocked by the HA, so the throughput increased from 32.307 Mbit/sec to 44.242 Mbit/sec. However, even after blocking the DoS attack, traffic cannot return to normal. This is because the attacker continues sending SYN packets to the HA. The HA's blocking process only denies communication with the attacker, preventing the HA from responding to the attacker's request packets while still allowing these packets to enter the traffic. It shows that the use of an IDS system integrated with a firewall can improve Mobile IPv6 traffic in the HA with the MN in the FA. During a DoS attack, throughput decreased by 50.481%, and after the DoS attack was blocked, throughput increased again, with a reduction of only 31.61% compared to normal traffic.

2) CPU Utilization Analysis on HA

CPU utilization is one of the parameters measured in this network testing. It represents the total CPU usage during the test, including the processing of packets from the MN to the CN. The test results in Fig. 31 were obtained when the MN sent TCP packets using the iPerf3 tool to the CN in the MIPv6 network. Data collection was carried out 10 times, and the average values

were recorded. This test was conducted to determine the difference in CPU usage on the HA by comparing three conditions: normal operation without an attack, during a DoS attack, and after the DoS attack was blocked by the firewall on the HA. The CPU measurement results in Fig. 31 show that under normal conditions, when the HA is used only as a connection medium between the MN and CN during MIPv6 handover, CPU usage on the HA was 6.04%. The test was conducted by activating the UMIP system for MIPv6. After UMIP was activated, the MN sent TCP packets to the CN using the iPerf3 tool, and CPU usage on the HA was then measured.

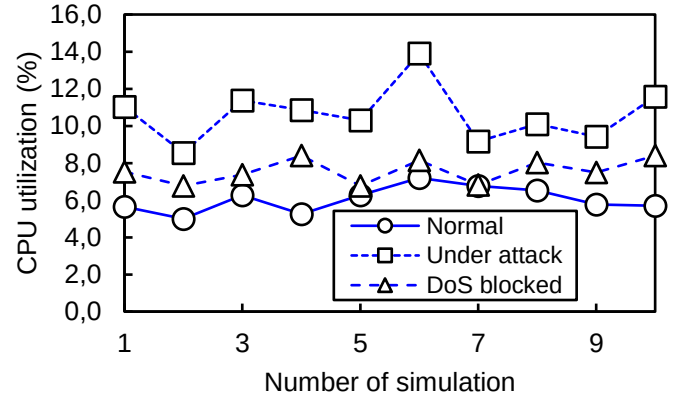


Fig. 31. HA Testing CPU Utilization

It shows an increase in CPU usage, from 6.04% to 10.63%. This increase is due to the large number of requests sent by the attacker during the DoS attack on the HA, which forces the HA to respond to the attacker repeatedly. The HA's reply process to the attacker increases CPU load and overall utilization. Furthermore, the fourth column of Fig. 31 shows a decrease in HA CPU usage from 10.63% to 7.58%. In this case, the DoS attack was successfully blocked by the HA using the firewall, so the HA no longer responds to the attacker's requests. The remaining CPU usage of 7.58% results from the operation of the UMIP system for MIPv6 and the continued presence of attacker requests in the traffic. It shows that using an IDS system integrated with a firewall can reduce CPU usage on the HA before and after a DoS attack is blocked. During a DoS attack, CPU usage increases by 75.88%, while after the DoS attack is blocked, CPU usage increases by only 25.36%.

3) HA Response Time Analysis

Response time measurements were also performed on the HA. In this test, response time is defined as the amount of time required by the IDS system and firewall in the HA to block an attacker conducting a DoS attack. When the IDS detects a DoS attack, it generates an alert in the form of a log, which is then used by the HA firewall to block the attacker's IP address. Fig. 32 shows that the average time required for the HA to block an attacker is 1.2 s. This time is measured from the start of the attack until the attacker is blocked. Variations in HA blocking time are influenced by the speed of the IDS in processing incoming attacks. The IDS response time is affected by the number of incoming data packets—the more packets received, the longer the IDS response time. Consequently, the time required to block the attacker increases.

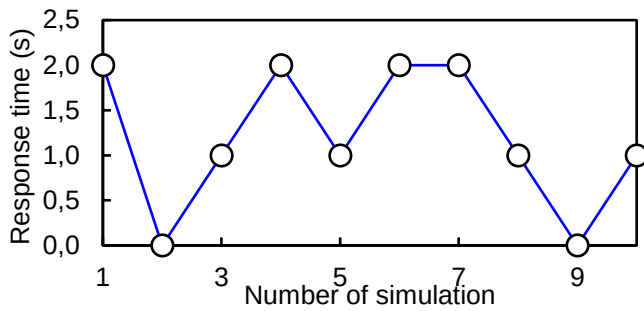


Fig. 32. Response time HA Block attacker IP

E. Testing On Mobile Node (MN)

The MN is a crucial node in MIPv6 for the handover process, which occurs when the MN moves from the HA router to the FA router. MN testing was conducted to determine the performance impact on the MIPv6 network. The tests performed on the MN are the same as those conducted on the CN and HA. An IDS system integrated with a firewall is installed on the HA because all traffic from the MN passes through the HA to communicate with the CN. Testing was carried out by launching a DoS attack on the MN node.

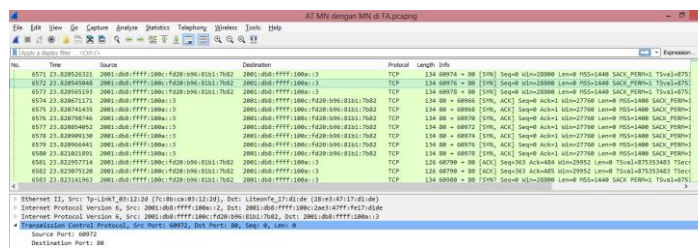


Fig. 33. Attack on MN

Fig. 33 shows a Wireshark capture when the MN is targeted by a DoS attack. The attacker continuously sends TCP SYN packets to the MN in large quantities, according to the capacity of the PC used. The MN's IP address is 2001:db8::ffff:100a::3, and the attacked port is port 80. The packet flow observed when the attacker targets the MN while positioned in the FA is as follows.

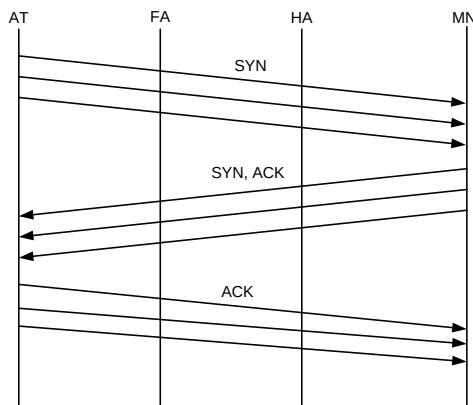


Fig. 34. Passing Message Attacker With MN

Fig. 34 illustrates an attack on the MN, similar to attacks on the CN and HA. The attacker connects through the FA and sends

a large number of SYN packets. The attacker's IP address remains unchanged and bypasses the HA to reach the MN. The MN responds with SYN-ACK messages, which keeps the target busy and consumes its resources.

1) MN Throughput Analysis

Throughput testing was conducted by having the MN send TCP packets to the CN via the HA and FA. The MN was then targeted by a DoS attack originating from the FA, and the impact of this attack on MN throughput was observed.

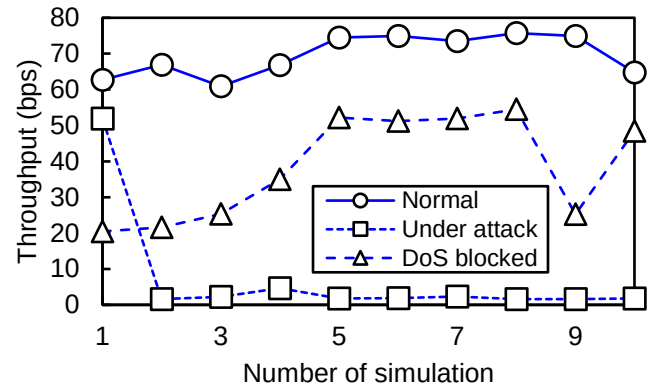


Fig. 35. MN Test Throughput With HA Connected MN

Based on Fig. 35 the DoS attack on the MN has a significant impact on the MIPv6 network. It shows that the average throughput under normal traffic, when the MN sends TCP packets to the CN via the HA, is 69.573 Mbit/sec before the attack. In the third column, the average throughput drops dramatically from 69.573 Mbit/sec to 6.65011 Mbit/sec. This decrease occurs because the MN is attacked with DoS, filling the communication path from the MN to the CN with SYN request packets, causing the MN to be busy replying with SYN-ACK packets. Simultaneously, the MN tries to send TCP packets to the CN, but many packets cannot be sent due to the MN being occupied with replies to the attacker, resulting in the drastic throughput reduction. The DoS attack has been successfully blocked by the HA, raising the throughput from 6.65011 Mbit/sec to 38.6375 Mbit/sec. Although the DoS attack was blocked, traffic did not return to normal because the attacker continued sending SYN packets to the MN in large numbers. The HA's blocking process only denies communication with the attacker, so the MN does not respond to the attacker's requests, but the request packets remain in the MN's traffic. It shows that using an IDS system integrated with a firewall can improve Mobile IPv6 traffic for the MN when it is connected in HA. During a DoS attack, throughput decreased by 90.441%, and after the attack was blocked, throughput increased again, with a decrease of only 44.465%.

The next test involved a DoS attack on the MN while it was in FA, communicating with the CN. Data was collected 10 times. It was obtained when the MN, connected to FA, sent TCP packets using the iPerf3 tool to the CN in the MIPv6 network. This test was conducted to evaluate the impact on MIPv6 network performance by comparing packet delivery under normal traffic, during a DoS attack on the MN, and after the DoS attack was blocked by the HA.

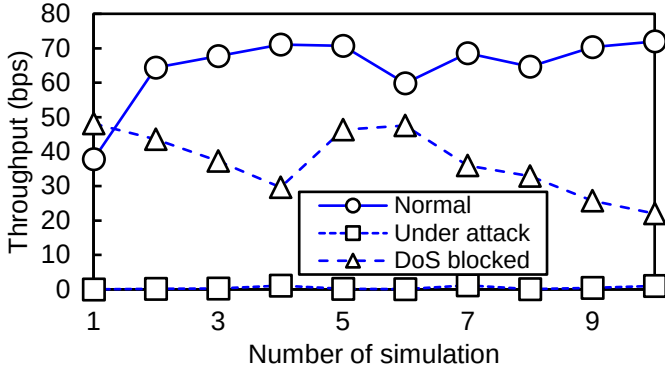


Fig. 36. MN Test Throughput With FA Connected MN

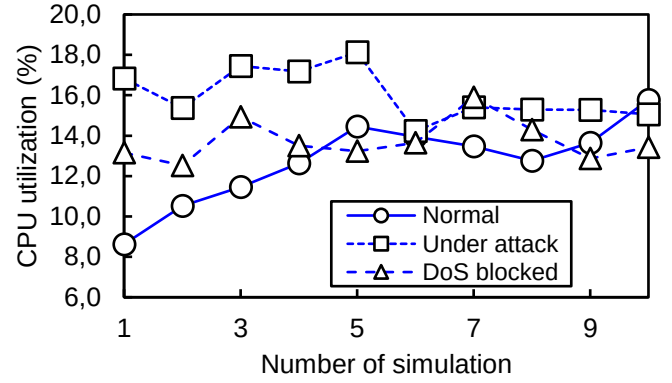


Fig. 37. CPU Utilization MN Testing

The throughput changes observed from the MN testing process indicate that the attack on the MN has a significant impact on the MIPv6 network. The MN communicates with the CN via the same path as the attacker, namely through the FA. Therefore, the MN is directly targeted by the attacker. The average throughput under normal traffic, when the MN sends TCP packets to the CN via HA, is 64.697 Mbit/sec before the DoS attack. During the attack, the average throughput drops drastically, from 64.697 Mbit/sec to 0.451 Mbit/sec. The MN has been attacked using a DoS attack, so that the communication path from the MN to the CN is flooded with SYN packets from the attacker. The attacker continuously sends a large number of SYN request packets, keeping the MN busy replying with SYN-ACK packets along the same communication path. As a result, the MN's communication path is heavily controlled by the attacker. At the same time, the MN attempts to send TCP packets to the CN, but because it is too busy responding to the attacker, many packets fail to reach the CN. This explains the drastic decrease in throughput during the attack.

After the attack, the DoS attack has been successfully blocked by the HA. In a MIPv6 network, even when the MN is connected to the FA, communication with the CN must first pass through the HA. Therefore, attacks targeting the MN are filtered by the HA. Consequently, MN throughput increases from 0.451 Mbit/sec to 36.7399 Mbit/sec. Even though the DoS attack is blocked, traffic does not fully return to normal. This is because the attacker continues to send SYN packets to the MN in large numbers. The HA blocking process only denies communication with the attacker, so the MN does not reply to the attacker's requests but still allows the packets to enter the MN traffic. The use of an IDS system integrated with a firewall significantly improves Mobile IPv6 traffic for the MN when connected via FA. During a DoS attack, throughput decreased by 99.30%, and after the attack was blocked, throughput recovered, showing a decrease of only 43.21% compared to normal traffic.

2) CPU Utilization Analysis on MN

The data were obtained when the MN sent TCP packets using the iperf3 tool to the CN on the MIPv6 network. Data collection was performed 10 times for each sending process. This test was conducted to determine the differences in CPU usage on the MN under three conditions: normal operation without attacks, during a DoS attack, and after the DoS attack was blocked by the firewall on the HA.

Fig. 37 shows that under normal conditions, when the MN is only used as a connection medium between the MN and CN during MIPv6 handover, CPU usage on the MN is 12.73%. Testing was performed by activating the umip system for MIPv6. After umip was activated, the MN sent TCP packets to the CN using the iperf3 tool, and CPU usage on the MN was measured. It shows an increase in CPU usage, from 12.73% to 16.02%. This increase is due to the large number of requests sent by the attacker during the DoS attack on the MN, causing the MN to respond to the attacker in large numbers. The MN's reply process increases CPU load and overall CPU usage. Furthermore, the fourth column shows a decrease in MN CPU usage from 16.02% to 13.75%. In this case, the DoS attack carried out by the attacker was blocked by the HA using the HA firewall. Since all incoming and outgoing traffic to the MN in MIPv6 passes through the HA, blocking at the HA reduces the load on the MN. The remaining 13.75% CPU usage results from activating the umip system, sending packets to the CN, and handling legitimate requests from the attacker. Using an IDS system integrated with a firewall can reduce CPU usage on the network both before and after a DoS attack is blocked. CPU usage during a DoS attack increases by 25.87%, while CPU usage after the DoS attack is blocked increases by only 8.01%.

The firewall integrated with the IDS is not installed on the MN but on the HA. In the MIPv6 system, the MN always communicates with the CN through the HA, whether the MN is in the HA or in the FA. All traffic entering and leaving the MN is visible to the HA, including DoS attacks directed at the MN. Therefore, the HA interrupts the attacker's DoS traffic on the MN when the IDS system is active. The response time measured in this test remains the same, as the IDS installed on the HA effectively protects both the HA and MN from DoS attacks.

IV. CONCLUSION

This research demonstrated that the implementation of an Intrusion Detection System (IDS) integrated with a firewall is an effective approach to mitigating Denial of Service (DoS) attacks in Mobile IPv6 networks. The system was tested across three critical nodes—Correspondent Node (CN), Home Agent (HA), and Mobile Node (MN)—under both Home Agent (HA) and Foreign Agent (FA) scenarios. The experimental results show that the IDS is capable of detecting DoS attacks by identifying the attacker's IP address and timestamp. More importantly, when integrated with a firewall, the IDS not only detects but also blocks the malicious traffic in real time, thereby preventing further network degradation. At the CN, throughput

degradation was reduced from 32.524% to 12.226% when the MN was in HA, and from 35.36% to 23.36% when in FA. CPU utilization overhead decreased drastically, from 60.79% to 1.31%, with an average block time of 0.9 seconds. At the HA, throughput decline was reduced from 49.25% to 33.23% (HA scenario) and from 50.48% to 31.61% (FA scenario), with CPU usage overhead reduced from 75.88% to 25.36% and a block time of 1.2 seconds. Finally, at the MN, throughput degradation decreased from 90.44% to 44.465% (HA scenario) and from 99.30% to 43.21% (FA scenario), while CPU utilization increased by only 8.01% compared to 25.87% under attack. Overall, these results confirm that integrating IDS with a firewall can significantly enhance MIPv6 resilience against DoS attacks by minimizing throughput loss, reducing CPU overhead, and enabling rapid blocking responses. This approach ensures better Quality of Service (QoS) and Quality of Experience (QoE) for mobile users, making it a promising solution for securing future IPv6-based mobile networks.

V. ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to the Universitas Pembangunan Nasional Veteran Jakarta for providing financial support for this study during the fiscal year 2025.

VI. REFERENCES

- [1] H. Guo, R. Huang, and Z. Xu, "The design of intelligent highway transportation system in smart city based on the internet of things," *Sci. Rep.*, vol. 14, no. 1, p. 28122, 2024.
- [2] H. Kandil and H. Benaboud, "About scalability and end-to-end security in internet of things: an overview," in *Proceedings of the 7th International Conference on Networking, Intelligent Systems and Security*, 2024, pp. 1–7.
- [3] A. Folorunso, "Assessment of internet safety, cybersecurity awareness and risks in technology environment among college students," *Cybersecurity Aware. Risks Technol. Environ. among Coll. Students (July 01, 2024)*, 2024.
- [4] A. Sanggel et al., "5G Opportunities for Future Technology," *Interdiscip. J. Adv. Res. Innov.*, vol. 2, no. 1, pp. 22–26, 2024.
- [5] I. You, X. Chen, V. Sharma, and G. Choudhary, "Introduction to the special issue on advanced security for future mobile internet: a key challenge for the digital transformation," *C. Model. Eng. Sci.*, vol. 141, no. 3, pp. 1907–1909, 2024.
- [6] D. Broeders and A. Sukumar, "Core concerns: The need for a governance framework to protect global Internet infrastructure," *Policy & Internet*, vol. 16, no. 2, pp. 411–427, 2024.
- [7] Y. Zhang et al., "Transfer learning framework integrating attention mechanism and domain adaptation for Low Earth Orbit satellite network traffic prediction," *Eng. Appl. Artif. Intell.*, vol. 161, p. 111992, 2025.
- [8] B. K. Pandey et al., "An industry-focused traffic system utilising internet of things," in *Emerging Engineering Technologies and Industrial Applications*, IGI Global Scientific Publishing, 2024, pp. 200–213.
- [9] J. Ehmer, Y. Savaria, B. Granado, J.-P. David, and J. Denoulet, "Network attack classification with a shallow neural network for internet and internet of things (iot) traffic," *Electronics*, vol. 13, no. 16, p. 3318, 2024.
- [10] S. Sharma et al., "The role of 6G technologies in advancing smart city applications: Opportunities and challenges," *Sustainability*, vol. 16, no. 16, p. 7039, 2024.
- [11] H. L. Tong et al., "The use of mobile technologies to promote physical activity and reduce sedentary behaviors in the Middle East and North Africa region: systematic review and meta-analysis," *J. Med. Internet Res.*, vol. 26, no. 1, p. e53651, 2024.
- [12] A. S. A. Nisha, N. V. Rao, G. Venkatesh, S. Murugan, and B. Meenakshi, "Efficient Congestion Management Through IoT-Driven Road User Charging Systems with Reinforcement Learning," in *2024 Second International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI)*, 2024, pp. 431–436.
- [13] S. Islam, A. Z. Abdulsalam, B. A. Kumar, M. K. Hasan, R. Kolandaisamy, and N. Safie, "Mobile networks toward 5G/6G: Network architecture, opportunities and challenges in smart city," *IEEE Open J. Commun. Soc.*, vol. 6, pp. 3082–3093, 2024.
- [14] P. Mahenthiran and D. Muruganadam, "Handoff performance analysis of PMIPv6-based distributed mobility management protocol-urban scenario," *Concurr. Comput. Pract. Exp.*, vol. 36, no. 11, p. e8010, 2024.
- [15] M. Aman et al., "Cost analysis of IPv6 distributed mobility management protocols in comparison with TFMIPv6," *PLoS One*, vol. 19, no. 8, p. e0306132, 2024.
- [16] P. Krishnan, K. Jain, A.-S. D. Alluhaidan, and P. Prabu, "Highly secured authentication and fast handover scheme for mobility management in 5G vehicular networks," *Comput. Electr. Eng.*, vol. 116, p. 109152, 2024.
- [17] U. D. Maiwada, G. S. S. Abdalla, N. S. S. Singh, and A. A. Salameh, "Efficient energy utilization in LTE networks with intelligent handover mechanisms," *J. Radiat. Res. Appl. Sci.*, vol. 18, no. 3, p. 101599, 2025.
- [18] R. M. Abdullah, I. Al-Surmi, G. R. S. Qaid, and A. A. Alwan, "Energy-Efficient Handover Algorithm for Sustainable Mobile Networks: Balancing Connectivity and Power Consumption," *J. Sens. Actuator Networks*, vol. 13, no. 5, p. 51, 2024.
- [19] M. Amaadid, A. El Ksimi, and B. Ettaki, "IPv6 Security Challenges: A comprehensive study of current issues and real case simulation," *Int. J. Commun. Networks Inf. Secur.*, vol. 17, no. 2, pp. 18–33, 2025.
- [20] A. Zilberman, A. Dvir, and A. Stulman, "IPv6 Routing Protocol for Low-Power and Lossy Networks Security Vulnerabilities and Mitigation Techniques: A Survey," *ACM Comput. Surv.*, vol. 57, no. 11, pp. 1–77, 2025.
- [21] Pragya, B. Kumar, and G. Kumar, "Optimized duplicate address detection for the prevention of denial-of-service attacks in IPv6 network," *IETE J. Res.*, vol. 70, no. 9, pp. 7231–7256, 2024.
- [22] A. Gankotiya, V. Kumar, and K. S. Vaisla, "Building IPv6 addressing scheme using hybrid duplicate address detection to prevent denial of service attack," *Comput. Electr. Eng.*, vol. 117, p. 109229, 2024.
- [23] M. Šimon, L. Huraj, and D. Hrinkino, "Home Assistant platform under DDoS attacks for IPv4 and IPv6 networks," in *2024 IEEE 17th International Scientific Conference on Informatics (Informatics)*, 2024, pp. 402–407.
- [24] Y. Wang, X. Wang, Q. Ni, W. Yu, and M. Huang, "BCDM: An Early-Stage DDoS Incident Monitoring Mechanism Based on Binary-CNN in IPv6 Network," *IEEE Trans. Netw. Serv. Manag.*, 2024.
- [25] Pragya and B. Kumar, "Hamming Distance Based Duplicate Address Detection in IPv6 Network," *Int. J. Commun. Syst.*, vol. 38, no. 10, p. e70135, 2025.