

# Analysis of the Impact of Implementing Wireless Security Protocol (WPA2-PSK and WPA3-SAE) on Handover Performance on 5Ghz Network

**Sofian Dwi Hadiwinata\***

Magister Informatika, Universitas  
Amikom Yogyakarta, Yogyakarta,  
55283, Indonesia

[sofian@students.amikom.ac.id](mailto:sofian@students.amikom.ac.id)

*\*Corresponding author*

**Alva Hendi Muhammad**


Magister Informatika, Universitas  
Amikom Yogyakarta, Yogyakarta,  
55283, Indonesia

[alva@amikom.ac.id](mailto:alva@amikom.ac.id)

**Ilham Setya Budi**

Teknik Informatika, Universitas  
Muhammadiyah Kalimantan Timur,  
Samarinda, 75124, Indonesia

[isb753@umkt.ac.id](mailto:isb753@umkt.ac.id)

 Submitted: 2025-05-20; Accepted: 2025-05-31; Published: 2025-06-05

**Abstract**—This study aims to analyze the impact of implementing wireless security protocols WPA2-PSK and WPA3-SAE on handover performance in 5 GHz networks. Efficient handover is crucial to maintaining seamless connectivity and quality of service in WiFi networks, especially on the 5 GHz frequency band widely used for high bandwidth applications. The research method involves testing and measuring handover performance parameters such as handover latency, connection handover success rate, and signal stability for both security protocols. The analysis results indicate that although WPA3-SAE offers significant security improvements compared to WPA2-PSK, there are differences in handover performance that need to be considered. WPA3-SAE tends to cause slightly higher handover latency due to its more complex authentication process but still provides good connection stability. Conversely, WPA2-PSK show lower handover latency but with a lower level of security. These findings provide important insights for network administrators in selecting a security protocol that balances security needs and handover performance to optimize user experience on 5 GHz networks.

**Keywords**—WPA2-PSK, WPA3-SAE, Handover, Latency, Packet Loss, RSSI.

## I. INTRODUCTION

The advancement of wireless networking technology has led to the emergence of the latest standard, IEEE 802.11ax, which is designed to enhance connectivity quality. This standard offers advantages such as data transfer speeds of up to 9.6 Gbps, improved spectrum efficiency, and support for both 2.4 GHz and 5 GHz frequency bands, which help reduce interference and enhance overall network performance. (Saputro & Raharjo, 2022) The rapid development of wireless technology has led to the emergence of 802.11ax Wi-Fi standard as the latest generation. By offering significant improvements in speed, capacity, and spectrum efficiency, 802.11ax is expected to be able to meet the increasing connectivity

needs in the digital era. The use of 5 GHz frequency in this standard also provides advantages in reducing interference and improving performance (Mandal & Tewari, 2022). However, behind all its advantages, there are still several challenges that need to be overcome. One of the main challenges is the handover mechanism, which is the process of switching between access points when users move locations (Kumar & Om, 2020). An uneven handover process can cause connection disruptions and decreased service quality. Building on this, the context begins with channel scanning and AP selection aspects that influence switching performance and introduces a WiFi-based handover optimization scheme (Bandyopadhyay et al., 2023). 802.11ax channel aggregation offers greater flexibility in the use of secondary channels; however, it poses challenges in terms of coexistence with users operating on a single channel. (Khairy et al., 2019) Latency is a network performance metric that measures the time it takes for data to travel from the source to the destination and back again. This parameter reflects the delay in data transmission, which can be influenced by factors such as physical distance, network capacity, traffic load, and device configuration. (Wahyudin Hasyim, 2024) In addition, latency or delays in data delivery are also a concern, especially for time-sensitive applications such as real-time video streaming and online gaming. Losing data packets or packet loss can also be an obstacle, because it can cause decreased service quality and interfere with the user experience. RSSI (Received Signal Strength Indicator) is a unit used in wireless communication systems to measure the strength of the signal received by a device. (Rifki et al., 2022) Unstable signal strength or RSSI can also affect network performance and cause connection drops.

On a modern campus, a reliable and fast internet network is essential to support academic and administrative activities. Handover in a wireless network is the process in which a client device switches from one access point to another with a stronger signal or better connection quality. The goal is to ensure smooth and uninterrupted user experience in the wireless connection (Adnan et al., 2023). A reliable and high-speed internet

network is essential to support both academic and administrative activities. Access points are strategically placed to provide Wi-Fi coverage for the entire campus community. Network security is a top priority, with WPA2 and WPA3 protocols implemented to protect data from threats that could compromise security. To maintain a stable connection while moving between locations, handover technology is utilized, allowing devices to remain connected across access points without interruption.(Siahaan & Suartana, 2022) Despite the progress achieved in prior studies, most have addressed the key components of WLAN planning such as access point (AP) placement, channel allocation, and load balancing in a fragmented manner, neglecting the intrinsic interdependence among these elements. There exists a strong correlation between AP placement and density, user connection quality, interference levels, and the overall network throughput.(Lima et al., 2023) To manage network distribution, campuses typically use devices such as routers and switches, which help manage data traffic and ensure a stable connection. Access Points are placed in strategic locations to provide wireless (Wi-Fi) access to students, faculty, and staff. Network security is a top priority, with WPA2 and WPA3 protocols used to protect data and prevent unauthorized access (Kwon & Choi, 2021). In addition, to ensure a smooth and uninterrupted connection when users move from one area to another on campus, network handover technology is implemented, allowing devices to switch from one access point to another without losing connection.

Computer network security has become a critical aspect as the number of devices connected to the internet continues to grow. This increase also raises the potential for attacks that could compromise data security. The WPA2 and WPA3 protocols are relevant for analysis, as they are designed to protect data transmitted over Wi-Fi networks (Halbouni et al., 2023). Wi-Fi network security has become a crucial issue as the number of devices connected to the internet through wireless access points increases. The WPA2 and WPA3 security standards have become common standards used to protect data transmitted over Wi-Fi network (Kwon & Choi, 2021). Although WPA2 has been a standard for quite some time, several weaknesses in this protocol have been discovered, allowing attacks that can compromise the security of user data. The emergence of WPA3 as the latest standard is expected to overcome the weaknesses in WPA2. However, the migration process to WPA3 is still ongoing and not all devices support this standard. A rapid and reliable approach is presented for selecting channel width and assigning channels in 802.11 WLANs utilizing channel bonding. The proposed method selects a uniform channel width for all Access Points (APs) within the WLAN, with the goal of preventing starvation in any individual AP across the network.(Chadda et al., 2021) This study aims to compare the level of security between the WPA2 and WPA3 protocols on 802.11ax Wi-Fi networks. In addition, this study will also analyze the impact of using WPA3 on network performance, especially in terms of latency and packet loss. Thus, this study is expected to provide a

clearer picture of the advantages and disadvantages of each protocol as well as recommendations in choosing the right security protocol for various types of network environments.

Wireless network roaming is the process by which mobile devices, such as smartphones or laptops, can move from one network to another without losing connectivity (Calle et al., 2023). This is a very important feature in the increasingly connected or mobile world of networks, where users often move between locations, whether within a building, campus, city, or even between countries (Gherman & Marcu, 2022). However, although roaming provides many benefits, there are a number of issues and challenges that need to be addressed to ensure a seamless and uninterrupted user experience. IP packets are encapsulated in a data-link layer (Layer 2) protocol, such as Ethernet or Wi-Fi. An IP packet contains the source and destination IP addresses, along with additional information describing the protocol it contains. TCP and UDP are the most commonly used protocols that run on top of the IP protocol.(Toulson et al., 2025)

SDN-based WLAN networks have better performance in managing user mobility and reducing Handover delay compared to traditional WLAN networks, even though there are multiple switches between APs. This shows that even if the number of switches between APs increases, the performance of SDN-based networks will be better than traditional networks in terms of data rate and Handover delay.(Emran, 2020) Although there are international standards for roaming, such as 3GPP for cellular networks and IEEE 802.11 for Wi-Fi, implementations in the field often vary (Ito & Izuka, 2023). Channel width, according to the IEEE (Institute of Electrical and Electronics Engineers), is a term that refers to the bandwidth or frequency spectrum allocated for wireless communication use. Differences in network configuration, security protocols and network management can cause compatibility issues and degrade the quality of service when devices attempt to move between networks. The quality of service while roaming can vary greatly. Users often experience reduced data rates, increased latency, or even disconnections when moving from one network to another. This can be caused by a variety of factors, including limited network capacity, signal interference, or different network priority settings (Shao et al., 2023).

Roaming also brings significant security challenges. Every time a device moves to a new network, there are potential security risks that need to be managed, such as man-in-the-middle attacks, data theft, or exploitation of network vulnerabilities (Kumar & Om, 2020). Service providers must ensure that all access points and other network infrastructure are well protected to prevent these threats. One of them is the authentication process of Wireless protocols such as Open Security WPA, WPA2 and WPA3, the higher the use of authentication protocols the higher the resulting throughput decrease. (Saputro et al., 2021).

Therefore, this study aims to analyze the performance of 802.11ax Wi-Fi networks at 5 GHz frequency with a focus on handover mechanisms, latency, packet loss, and

the effect of RSSI on these parameters. The results of this study are expected to provide recommendations to improve the quality of Wi-Fi network services in densely populated environments. So that the Roaming Process or Handover of user transfer between Access Points and the Wireless security protocol process that occurs at the Access Point needs to be researched to see which is more effective in its implementation, especially in the topology design of Wireless networks that are widely implemented in buildings or rooms in schools, campuses, industries and offices.

## II. METHODS

Experimental is a method used in this experimental scenario to obtain data which will then be analyzed into a result and conclusion. The stages of this research are divided into 3 stages as in Figure 1.

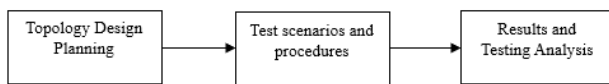


Figure. 1. Research Stages

### A. Topology Design Planning

In Topology Design Planning, the scenario used is basic network topology as shown in Figure 2.

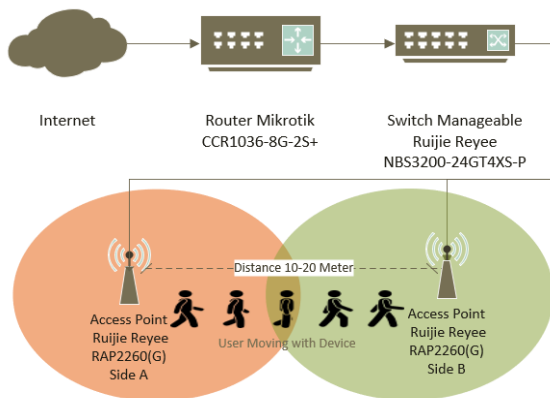


Figure. 2. Testing Topology

In the topology design using IP Address 4 which configuration will be done on the Mikrotik Router with 2 DHCP Servers and different VLANs: IP 192.168.10.1/24 VLAN 10 Side A and IP 192.168.20.1/24 VLAN 20 Side B, both IP Addresses are distributed to the Manageable Switch in the form of a VLAN which is forwarded to the Access Point. The User here as the object of the User's experimental scenario uses a Device in the form of a laptop or Smart Phone Support 5Ghz VHT80 and will simulate the Access Point transfer, then the roaming data will be recorded in the Mikrotik log and Wire Shark Application, which in this case simulates the transfer of different IP seqmen such as moving between buildings. Furthermore, several stages of testing have been determined. The parameters used for testing as stated in the following Table 1.

Table 1. Testing Parameters

Category	Parameter	Description	Unit	Measurement Method
QoS (Quality of Service)	Handover Time	The time required by the device to switch between Access Points	ms	Measurement with network analysis software
QoS (Quality of Service)	Latency	The delay experienced by data during transmission	ms	Ping test or network monitoring tools
QoS (Quality of Service)	Packet Loss	Percentage of data packets lost during transmission	%	Analysis with Wireshark or similar tools
RSSI	Received Signal Strength Indicator	Signal strength received by the device	dBm	Measurement using Wi-Fi analyzer or mobile devices

### B. Testing Scenario Stages

At this stage, the aim is to describe the basic pattern simulation in the network topology configuration where the Wireless protocol security mode uses WPA2 and WPA3 and the same SSID simulation, for example SSID: AMIKOM-5Ghz, with of course the researcher carrying out special configurations such as selecting a Channel width of 40 and 80 Mhz in the channel. Band Ribbon 5 Ghz Frequency and Optimization with and without RSSI Limiter. Here is the scenario Table 2.

Table 2. Testing Scenario without RSSI Limiter

Stage	Scenario	Test Parameters		
		Wireless Security	Channel Band	Channel Width
1	Wireless Security WPA2-PSK Same Channel Band	WPA2-PSK	AP1 = 38, AP2 = 38	AP1 = 40 MHz, AP2 = 40 MHz
2	Wireless Security WPA3-AES Same Channel Band	WPA3-AES	AP1 = 38, AP2 = 38	AP1 = 40 MHz, AP2 = 40 MHz
3	Wireless Security WPA2-PSK Same Channel Band	WPA2-PSK	AP1 = 42, AP2 = 42	AP1 = 80 MHz, AP2 = 80 MHz
4	Wireless Security WPA3-AES Same Channel Band	WPA3-AES	AP1 = 42, AP2 = 42	AP1 = 80 MHz, AP2 = 80 MHz
5	Wireless Security WPA2-PSK Different Channel Band	WPA2-PSK	AP1 = 38, AP2 = 46	AP1 = 40 MHz, AP2 = 40 MHz

6	Wireless Security WPA3-AES Different Channel Band	WPA3-AES	AP1 = 38, AP2 = 46	AP1 = 40 MHz, AP2 = 40 MHz	
7	Wireless Security WPA2-PSK Different Channel Band	WPA2-PSK	AP1 = 42, AP2 = 58	AP1 = 80 MHz, AP2 = 80 MHz	
8	Wireless Security WPA3-AES Different Channel Band	WPA3-AES	AP1 = 42, AP2 = 58	AP1 = 80 MHz, AP2 = 80 MHz	

6	Wireless Security WPA3-AES Different Channel Band	WPA3-AES	AP1 = 38, AP2 = 46	AP1 = 40 MHz, AP2 = 40 MHz	-67 dBm
7	Wireless Security WPA2-PSK Different Channel Band	WPA2-PSK	AP1 = 42, AP2 = 58	AP1 = 80 MHz, AP2 = 80 MHz	-67 dBm
8	Wireless Security WPA3-AES Different Channel Band	WPA3-AES	AP1 = 42, AP2 = 58	AP1 = 80 MHz, AP2 = 80 MHz	-67 dBm

Table 3 describes the eight stages of testing carried out in the two main scenarios that have been explained previously. The first scenario involves the use of the same and different Channel Bands without using RSSI Limiter, while the second scenario involves the use of the same and different Channel Bands with the implementation of RSSI Limiter. Both scenarios are tested with a combination of WPA2 and WPA3 wireless security protocols. The hardware used in each stage of testing is shown in Table 4.

Table 3. Testing Scenario with RSSI Limiter -67 dBm

Stage	Scenario	Test Parameters			
		Wireless Security	Channel Band	Channel Width	RSSI Limit
1	Wireless Security WPA2-PSK Same Channel Band	WPA2-PSK	AP1 = 38, AP2 = 38	AP1 = 40 MHz, AP2 = 40 MHz	-67 dBm
2	Wireless Security WPA3-AES Same Channel Band	WPA3-AES	AP1 = 38, AP2 = 38	AP1 = 40 MHz, AP2 = 40 MHz	-67 dBm
3	Wireless Security WPA2-PSK Same Channel Band	WPA2-PSK	AP1 = 42, AP2 = 42	AP1 = 80 MHz, AP2 = 80 MHz	-67 dBm
4	Wireless Security WPA3-AES Same Channel Band	WPA3-AES	AP1 = 42, AP2 = 42	AP1 = 80 MHz, AP2 = 80 MHz	-67 dBm
5	Wireless Security WPA2-PSK Different Channel Band	WPA2-PSK	AP1 = 38, AP2 = 46	AP1 = 40 MHz, AP2 = 40 MHz	-67 dBm

Table 4. Testing Hardware

Hardware	Function	Specification
Mikrotik CCR2116-12G-4S+	BGP Router as Internet Source	CPU ARM64 16 Core 2000 MHz, RouterOS version 7, RAM 16 GB, BGP full route peer to ISP
Mikrotik CCR1036-8G-2S+	Router as DHCP Server, DHCP Client, VLAN	CPU Tilegx 36 Core 1200 MHz, RouterOS version 7, RAM 16 GB
Ruijie Reyee NBS3200-24GT4XS-P	Manageable Switch as Distribution Switch to Access Points	24 x 10/100/1000Base-T PoE+ ports, 4 SFP+ uplinks, Max PoE Budget 370W, Switching Capacity 128 Gbps, VLAN 4094
Belden UTP CAT6	LAN Cable as Connection between Router, Switch, and Access Point	UTP CAT 6
Ruijie Reyee RAP2260(G)	Wireless Access Point as Simulation for Connecting Two Buildings	Dual-stream dual-band radio, Wi-Fi 6 protocol (IEEE 802.11ax), Operating Bands 5 GHz: 5.150–5.350 GHz, 5.725–5.850 GHz (country-specific)

This test also involves various software used to capture data, configure devices, and analyze network performance. Each software has a specific function that supports this test. The software used in the test is shown in Table 5.

Table 5. Testing Software

Software	Function	Specification
Mikrotik RouterOS 7	Capturing handover process logs between wireless networks from the router side	Routing, VLAN, DHCP Server
Cloud Ruijie Reyee	Configuration of Switch and Access Point	Cloud Access cloud-as.ruijienetworks.com
Wifi Analyzer	Capturing Access Point logs (Desktop version)	Desktop-Based Application
WifiMan / Wifi MOHO / Ruijie Reyee	Capturing Access Point logs (Mobile version)	Android-Based Application

### C. Method of collecting data

The data collection stages are taken from various sources as follows:

#### 1. Literature Study Method

Researchers conducted a data search on the internet to obtain information related to IEEE 802.11ax, Channel Band, Channel width and Wireless security protocols. The results were the development of Wireless networks and the influence of Wireless security protocols in the Handover process between network Access Points.

#### 2. Observation Method

Researchers conducted an observational study by conducting several stages of experiments based on previously determined network topology design scenarios. The experimental steps include the system and device configuration stages to the testing stage and drawing conclusions using predetermined parameters.

### D. Research Flow

There are stages in conducting the research process of the impact or influence of the use of Wireless security protocols on the Handover process between Access Points on the 802.11ax 5Ghz Wireless network. Here are the stages:

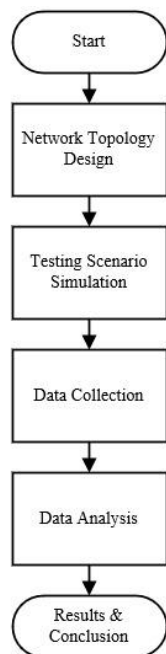


Figure. 3. Research Flow

Figure 3 is a conceptual framework diagram of the research to be conducted. Here is the explanation:

#### 1. Step 1: Designing Topology Design

Topology design is carried out to support this research to obtain the desired results.

#### 2. Step 2: Test Scenario Simulation

At this stage, at least 2 test scenarios were carried out with 8 stages of the experiment, according to the explanation in the previous research method in Table 2 and 3.

#### 3. Step 3: Data Retrieval

The data collection steps resulting from the previous test scenario simulation in step two. After the research

topology is designed, the researcher conducts simulations and tests to test the validity and reliability of the selected design. This process ensures that the approach taken can produce consistent and reliable data to answer the previously formulated research questions.

#### 4. Step 4: Data Analysis

The collected data is then analyzed using appropriate methods, which are appropriate to the nature of the data collected and the research design used. Statistical analysis or qualitative analysis is used to interpret the data and find patterns or relationships that are relevant to the research question.

#### 5. Step 5: Results & Conclusions

The results of the data analysis are presented in a clear and systematic form, using tables, graphs, and supporting narratives. The researcher evaluates these findings in the context of the initial research questions and concludes the implications and significance of the findings. The conclusions drawn must provide clear answers to the previously formulated research questions.

### III. RESULTS and Discussion

This section discusses the results of Wi-Fi network performance testing based on three main parameters: average latency, time consumed, and packet loss rate. The testing was conducted under two conditions: (1) without using an RSSI limiter, and (2) with an RSSI limiter applied at -67 dBm as the handover threshold. Each parameter was analyzed based on eight test scenarios conducted under different conditions.

Table 6. Result data collection Scenario without RSSI Limiter

Sta ge	Time Consu med (ms)	Packet loss during roaming	Packet loss rate (%)	Packe t loss count	Avera ge RSSI (dBm)	Averag e Latenc y (ms)
1	9	0	0	0	-56	17
2	22	0	0	0	-52	17
3	39	0	1,7	1	-64	18
4	39	0	0	0	-51	17
5	26	0	1,7	1	-65	42
6	125	0	2	1	-55	21
7	38	0	0	0	-66	70
8	79	0	2	1	-64	65

In the scenario without an RSSI limiter in Table 6, roaming proceeded smoothly. The average hand-off time stayed below 80 ms, with a single outlier of 125 ms at Stage 6. Across the eight test stages, no packets were lost except for four stages (3, 5, 6, 8) where only one packet was lost each—yielding a very small packet-loss rate ( $\leq 2\%$ ).

Average signal strength (RSSI) ranged from -51 dBm to -66 dBm, which is considered “fair-to-good” for WLAN. Latency remained stable (17–21 ms) aside from two spikes at Stage 5 (42 ms) and Stage 7 (70 ms), still acceptable for non-real-time applications.



Overall, without a limiter the system maintained connection continuity with near-zero packet loss and low latency; performance variability was driven more by natural signal fluctuations than by any software-control mechanism.

Applying a  $-67$  dBm RSSI threshold (Table 7) had a marked impact. Roaming time increased—peaking at 247 ms in Stage 6—because the device was “forced” to switch when the signal dipped below the threshold. This led to a substantial rise in lost packets: 18 in total, with a loss rate of 45.6 % in Stage 6.

Average signal strength tended to be weaker ( $-49$  dBm to  $-79$  dBm) because hand-offs occurred when RSSI neared the limit. Consequently, latency jumped sharply: up to 549 ms (Stage 6) and frequently above 100 ms, undermining delay-sensitive applications (VoIP, real-time video).

In short, a tight RSSI limiter increased roaming frequency, lengthened handovers, and boosted both packet loss and latency—the opposite of the intended QoS improvement.

Table 7. Result data collection Scenario with RSSI Limiter  $-67$  dBm

Stage	Time Consumed (ms)	Packet loss during roaming	Packet loss rate (%)	Packet loss count	Average RSSI (dBm)	Average Latency (ms)
1	15	1	6,1	3	-68	109
2	122	3	25,50	9	-73	491
3	21	0	5,60	0	-64	65
4	64	3	12,5	0	-56	70
5	38	0	2	0	-49	56
6	247	7	45,6	36	-79	549
7	45	0	0	0	-64	109
8	82	4	1,8	1	-59	76

Figure 4 illustrates the time consumed during data transmission in each test scenario. The results align with those seen in latency. Under the RSSI limiter condition, particularly in Scenario 2 and Scenario 6, processing times increased significantly, exceeding 130 ms and 250 ms, respectively. This indicates that handover or reconnection processes require a non-trivial amount of time.

In contrast, the no RSSI limiter setup shows significantly lower and more consistent processing times, typically ranging from 40 to 120 ms. These values indicate that the system efficiently maintains the connection while the signal remains tolerable, avoiding frequent and unnecessary transitions. This highlights greater efficiency and connection stability.

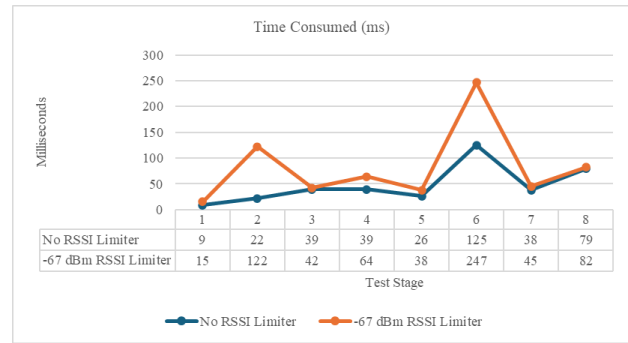


Figure. 4. Comparison of Time Consumed (ms)

As shown in Figure 5, the average latency measurements indicate that the use of an RSSI limiter significantly increases latency. In the condition with the  $-67$  dBm RSSI limiter, there are extreme latency spikes, especially in Scenario 2 and Scenario 6, reaching almost 500 ms and 600 ms, respectively. These values are considerably high and can cause serious disruptions in real-time services such as VoIP, video streaming, and IoT device communication.

This latency increase is attributed to suboptimal access point handovers triggered prematurely by the RSSI limiter. The limiter forces the device to seek a new access point once the signal falls below the  $-67$  dBm threshold, even if the current signal is still acceptable. This initiates rehandovers and re-association processes that require additional time, leading to increased latency.

Conversely, under the no RSSI limiter configuration, latency values are more stable, ranging between 60 to 90 ms across all scenarios. This shows that the device remains connected to an access point longer before switching, allowing for smoother and more stable communication. This configuration is better suited for environments with moderate to high mobility, where connection stability is prioritized over signal strength alone.

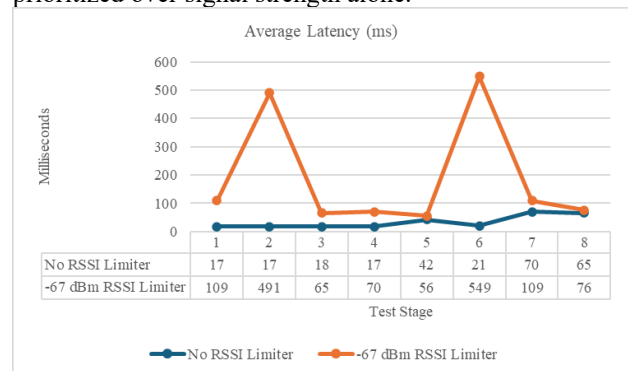


Figure. 5. Comparison of Average Latency (ms)

Figure 6 presents the packet loss rate across the eight test scenarios. Network reliability appears to degrade significantly under the RSSI limiter configuration. Again, Scenario 2 and Scenario 6 are the most problematic, with packet loss rates reaching around 30% and nearly 50%, respectively. This means nearly half of the transmitted data was lost in certain conditions—an unacceptable rate for most network applications.

This high packet loss is likely due to mistimed handovers, where the device begins data transmission before completing the AP transition, or due to connection interruptions during the switch. The high loss rate also suggests that new AP selections may not lead to better overall connections, as they are based solely on signal strength and not on other factors such as traffic load or channel quality.

In contrast, results from the no RSSI limiter configuration show very low and stable packet loss rates, generally under 5%. This indicates greater reliability and connection stability. In many applications, a packet loss rate below 5% is still acceptable and recoverable by communication protocols through retransmission mechanisms.

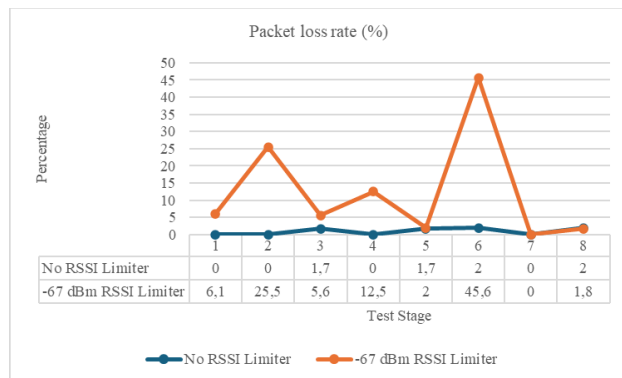


Figure. 6. Comparison of Packet Loss Rate (%)

Figure 7 compares the average Received Signal Strength Indicator (RSSI) measured at eight test points under two conditions: without an RSSI limiter and with a  $-67$  dBm RSSI limiter. In the baseline scenario (blue line), RSSI values cluster within  $-52$  dBm to  $-66$  dBm, reflecting a stable link budget that should sustain moderate Wi-Fi throughput. Activating the limiter (orange line) shifts the mean signal level closer to the target  $-67$  dBm, yet it simultaneously amplifies variance. At several locations (points 1, 2, 6), the limiter over-attenuates the signal to as low as  $-79$  dBm, risking higher packet-retry rates and possible disconnections. Conversely, at point 5 the limiter undershoots, allowing RSSI to surge to  $-49$  dBm—high enough to create a near-far problem that could drown out weaker clients on the same channel. These  $\pm 24$  dB swings indicate that the limiter's control loop lacks sufficient hysteresis or stepwise correction limits, causing it to react too aggressively to instantaneous channel conditions. Thus, while the limiter succeeds in reducing average transmit power, its inconsistent adjustments degrade overall link quality and user experience. Refining the algorithm with moving-average filtering, bounded correction steps, and performance-based feedback is essential before the technique can be recommended for production-grade WLAN deployments.

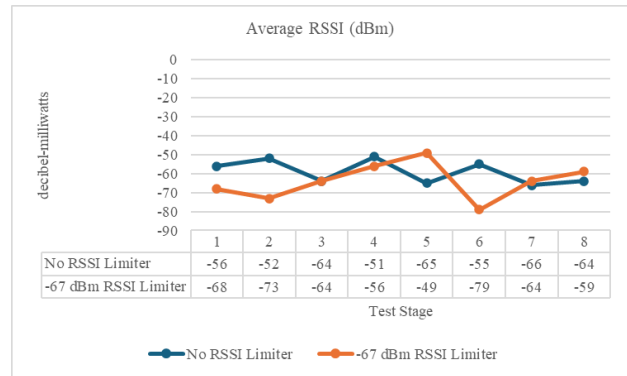


Figure. 7. Comparison of Average RSSI (dBm)

#### IV. CONCLUSION

Based on the analysis and testing conducted on the implementation of wireless security protocols WPA2-PSK and WPA3-SAE on a 5GHz Wi-Fi network, it can be concluded that the security protocol has a significant impact on handover performance, particularly in networks that require high mobility and low latency, such as those operating in the 5GHz band.

The WPA3-SAE protocol, although offering higher security through the Simultaneous Authentication of Equals (SAE) mechanism, shows an increase in handover time compared to WPA2-PSK. This is due to the more complex authentication process in WPA3. However, the difference remains within an acceptable range for most user applications.

Meanwhile, WPA2-PSK, with its simpler authentication process, demonstrates faster handover times, but with a lower level of security, especially against brute force and key reinstallation attacks (KRACK).

Therefore, the choice of security protocol should consider the trade-off between security and performance. For scenarios where security is the main priority (such as in enterprise or government environments), WPA3-SAE is more recommended. However, for applications that prioritize performance and faster handover (such as in fast-moving devices or IoT), WPA2-PSK may still be considered, with the addition of supplementary security measures.

#### REFERENCES

- Adnan, M., Ali, J., Ayadi, M., Elmannai, H., Almuqren, L., & Amin, R. (2023). Leveraging Software-Defined Networking for a QoS-Aware Mobility Architecture for Named Data Networking. *Electronics* (Switzerland), 12(8). <https://doi.org/10.3390/electronics12081914>
- Bandyopadhyay, D., De, S., Hom Roy, S., Biswas, D., Bhose, M., & Karmakar, R. (2023). Network Throughput Improvement in Wi-Fi 6 over Wi-Fi 5: A Comparative Performance Analysis. *ICCECE 2023 - International Conference on Computer, Electrical and Communication Engineering*. <https://doi.org/10.1109/ICCECE51049.2023.10085684>

- Calle, L., Castel, J., & Amaya, M. (2023). Implementation of a ROS Node for Roaming between APs for an Autonomous Mobile Robot. 2023 IEEE Latin American Electron Devices Conference, LAEDC 2023. <https://doi.org/10.1109/LAEDC58183.2023.10209140>
- Chadda, A., Stojanova, M., Begin, T., Busson, A., & Guérin Lassous, I. (2021). Assigning channels in WLANs with channel bonding: A fair and robust strategy. *Computer Networks*, 196. <https://doi.org/10.1016/j.comnet.2021.108200>
- Emran, M. (2020). Performance Analysis of Traditional and SDN Based Handovers in Wireless LAN Networks. Institute of Electrical and Electronics Engineers. <https://doi.org/10.1109/IEMTRONICS51293.2020.9216435>
- Gherman, A. G., & Marcu, M. (2022). Instrumentation and Analyzis of Handover in Wi-Fi Networks. 2022 15th International Symposium on Electronics and Telecommunications, ISETC 2022 - Conference Proceedings. <https://doi.org/10.1109/ISETC56213.2022.10010306>
- Halbouni, A., Ong, L.-Y., & Leow, M.-C. (2023). Wireless Security Protocols WPA3: A Systematic Literature Review. *IEEE Access*, 11, 112438–112450. <https://doi.org/10.1109/ACCESS.2023.3322931>
- Ito, K., & Izuka, N. (2023). Proposal of Client-Server Based Vertical Handover Scheme Using Virtual Routers for Edge Computing in Local 5G Networks and WLANs. 2023 IEEE 13th Annual Computing and Communication Workshop and Conference, CCWC 2023, 999–1004. <https://doi.org/10.1109/CCWC57344.2023.10099150>
- Khairy, S., Han, M., Cai, L. X., Cheng, Y., & Han, Z. (2019). A renewal theory based analytical model for multi-channel random access in IEEE 802.11ac/ax. *IEEE Transactions on Mobile Computing*, 18(5), 1000–1013. <https://doi.org/10.1109/TMC.2018.2857799>
- Kumar, A., & Om, H. (2020). Design of a USIM and ECC based handover authentication scheme for 5G-WLAN heterogeneous networks. *Digital Communications and Networks*, 6(3), 341–353. <https://doi.org/10.1016/j.dcan.2019.07.003>
- Kwon, S., & Choi, H.-K. (2021). Evolution of Wi-Fi Protected Access: Security Challenges. *IEEE Consumer Electronics Magazine*, 10(1), 74–81. <https://doi.org/10.1109/MCE.2020.3010778>
- Lima, M. P., Takahashi, R. H. C., Vieira, M. A. M., & Carrano, E. G. (2023). Multiobjective planning of indoor Wireless Local Area Networks using subpermutation-based hybrid algorithms. *Knowledge-Based Systems*, 263. <https://doi.org/10.1016/j.knosys.2023.110293>
- Mandal, B. K., & Tewari, B. P. (2022). Interference Aware Handoff Through Dynamic Channel Switching in High Speed 802.11ac WLAN. 2021 19th OITS International Conference on Information Technology (OCIT). 358–363. <https://doi.org/10.1109/ocit53463.2021.00077>
- Rifki, M. I., Ikhsan, M., Nasution, R. H., & Handira, D. (2022). Analysis of WLAN Network Handover Performance using RSSI and Threshold on Mobile Devices. *INFOKUM*.
- Saputro, V. A., & Raharjo, S. (2022). Pengaruh Penggunaan Beacon Interval Dalam Meningkatkan Throughput Jaringan Wireless IEEE 802.11ax. *Jurnal Sistem Komputer dan Kecerdasan Buatan*, IV(1). <https://doi.org/10.47970/siskom-kb.v6i1.324>
- Saputro, V. A., Raharjo, S., & Pramono, E. (2021). Pengaruh Wireless Security Protocol Pada Throughput Jaringan Wireless 802.11ax. *Paradigma - Jurnal Komputer Dan Informatika*, 23(2). <https://doi.org/10.31294/p.v23i2.10947>
- Shao, S., Zheng, J., Zhong, C., Lu, P., Guo, S., & Bu, X. (2023). IEEE 802.11ax Meet Edge Computing: AP Seamless Handover for Multi-Service Communications in Industrial WLAN. *IEEE Transactions on Network and Service Management*, 20(3), 3396–3412. <https://doi.org/10.1109/TNSM.2023.3239404>
- Siahaan, C., & Suartana, I. M. (2022). Simulasi Handover pada Jaringan Nirkabel Berbasis Software Defined Network. *Journal of Informatics and Computer Science*, 04. <https://doi.org/10.26740/jinacs.v4n03.p256-263>
- Toulson, R., Wilmschurst, T., & Spink, T. (2025). Further Aspects of the IoT. In *Fast and Effective Embedded Systems Design* (pp. 395–420). Elsevier. <https://doi.org/10.1016/B978-0-323-95197-5.00013-9>
- Wahyudin Hasyim, A. L. B. S. R. (2024). Analisis Jaringan Internet menggunakan Parameter Quality of Service (QoS) Di Universitas Muhammadiyah Gorontalo. *Jurnal Informatika Teknologi dan Sains (JINTEKS)*, 6(2), 306-313 <https://doi.org/10.51401/jinteks.v6i2.4156>