TEKNIKA: JURNAL SAINS DAN TEKNOLOGI

Journal homepage: http://jurnal.untirta.ac.id/index.php/ju-tek/

Analysis security system performance MIPv6 in signaling process using AES and Twofish algorithms

Supriyanto Praptodiyono [a,1], ***Fadil Muhammad*** [a], ***Dhandy Wiriyadinata*** [a]

[a]*Department of Electrical Engineering, Faculty of Engineering, Universitas Sultan Ageng Tirtayasa, Jl. Jenderal Sudirman KM 3, Kotabumi, Purwakarta, Cilegon City, Banten 42435, Indonesia.*
[1]*E-mail: supriyanto@untirta.ac.id*

ARTICLE INFO

Article history:
Submitted 9 October 2021
Reviewed 1 November 2021
Received 5 November 2021
Accepted 16 November 2021
Available online on 20 November 2021

Keywords:
Mobile IPv6, IPsec, AES, Twofish.

Kata kunci:
Mobile IPv6, IPsec, AES, twofish.

ABSTRACT

Mobile technology has become a necessity for modern society in the digital era. The ease of various information processes is a driving force for the growth of mobile users. To support continuous connectivity, Mobile IPv6 (MIPv6) is a solution and successor to the current Mobile IPv4 technology. Mobility in accessing a wide range of services is carried out via the Internet, but activities on the Internet make us vulnerable to various malicious acts. Issues such as information security as well as high overheads are a concern for mobile communications. An encryption mechanism is required throughout the signaling phase to construct security associations to enhance MIPv6 security performance. IPsec offers security services at the network layer. There are three encryption algorithms in IPsec, namely DES, 3DES, and AES. The DES algorithm is no longer recommended due to security factors, while AES is still not optimal in wireless networks. This study aims to analyze the performance of the MIPv6 security system and service quality with the AES and Twofish algorithms. Twofish algorithm is a candidate that has the potential for better performance. The experiment concluded that the performance of the Twofish algorithm is superior based on the security of cryptanalysis attacks with a cracking time that is twice as long as AES. In terms of service quality, Throughput Twofish has an increase of 20.05% with a small delay compared to AES, while packet loss is 0.023% for Twofish and 0.077% for AES.

ABSTRAK

Teknologi seluler menjadi kebutuhan masyarakat modern di era digital, kemudahan berbagai proses pengelolaan informasi menjadi pendorong pertumbuhan pengguna seluler. Untuk mendukung konektivitas berlanjut, Mobile IPv6 (MIPv6) menjadi solusi sekaligus penerus teknologi Mobile IPv4 saat ini. Mobilitas akses layanan yang luas dilakukan melalui Internet, namun aktivitas di jaringan Internet membuat kita rentan terhadap berbagai tindakan jahat. Masalah seperti keamanan informasi serta *overhead* yang tinggi menjadi perhatian komunikasi seluler. Untuk meningkatkan performa keamanan MIPv6, diperlukan metode enkripsi saat proses pensinyalan yang akan membangun asosiasi keamanan. IPsec menawarkan layanan keamanan di lapisan jaringan. Terdapat 3 algoritma enkripsi dalam IPsec, yaitu DES, 3DES, dan AES. Algoritma DES sudah tidak direkomendasikan karena faktor keamanan, sementara AES masih belum optimal dalam jaringan nirkabel. Penelitian ini bertujuan untuk menganalisis performa sistem keamanan dan kualitas layanan MIPv6 dengan algoritma AES dan Twofish. Algoritma Twofish merupakan kandidat yang memiliki potensi performa yang lebih baik. Eksperimen berhasil menyimpulkan bahwa performa algoritma Twofish unggul berdasarkan keamanan serangan kriptoanalisis dengan waktu *cracking* dua kali lebih lama dibandingkan AES. Dari segi kualitas layanan, *Throughput* Twofish memiliki kenaikan 20,05% dengan *delay* yang kecil dibanding AES sementara *packet loss* masing-masing 0,023% pada Twofish dan 0,077% pada AES.

Available online at http://dx.doi.org/10.36055/tjst.v17i2.13069

1. Introduction

Mobile technology is developing rapidly along with the changes in the digital era. The Association of Indonesian Internet Service Providers (APJII) survey results noted that in the second quarter of the 2019/2020 period, the number of internet users in Indonesia was 196.71 million out of a total population of 266.91 million or around 73.7% [1]. Many internet users use various internet services while on activity or traveling. The services become important to support user mobility in the network under any conditions. The technology on IPv6 networks that supports mobility of data access is the Mobile IPv6 protocol (MIPv6) [2]. During mobility, users transfer from one network to another, supported by a handover, thus maintaining the user's connection [3]. This handover concept is known as vertical handover (VHO) [4].

Mobility on the Internet makes our activities vulnerable to various malicious acts. The things such as confidentiality, integrity, and availability of shared information are open issues [5]. Mobile IPv6 is vulnerable to information attacks during the signaling process, so information must be protected with a security protocol. The protection can be done with IPsec, a security protocol at the network layer [6]. IPsec provides several encryption algorithms as the current encryption method, DES, 3DES, and AES. DES algorithm is no longer recommended due to security factors, so DES and 3DES themselves will no longer be used after 2023 [7]. Meanwhile, analysis of the AES algorithm has been carried out [8], the performance of AES is still not optimal in wireless networks, and in terms of security, the password strength analysis has been carried out by cryptanalysts revealing that with the trend of increasing computational capabilities, eight out of ten rounds of AES have been successfully dismantled. In the near time, the remaining two rounds can be broken [9].

The choice of encryption algorithm becomes important during the MIPv6 signaling process, which will build security associations. In cryptography, symmetric keys are most appropriate when large amounts of data are held [10]. Based on research conducted by [11], a comparative analysis was carried out between several encryption algorithms. It was concluded that the Twofish algorithm has advantages over AES and Blowfish in evaluating encryption, decryption, and throughput time metrics. Twofish has a lot of potentials [12] . Besides, the security performance of Twofish is considered good in securing information [13]. Related research that implements IPsec on Mobile IPv6 networks has also been carried out by [14] and [15]. Based on [14], AES has a very good performance than DES and 3DES. Meanwhile, the research results [15] carried out by implementing the Elliptic Curve algorithm increased performance by reducing the delay during signaling by 67%.

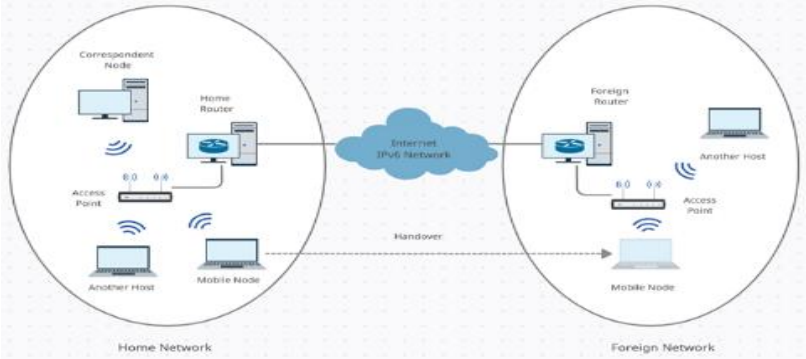
The research mentioned does not explain the performance of the algorithm in the security system of the MIPv6 network. In contrast, related research has only implemented DES, 3DES, and AES, which are encryption standards on IPsec, and also the Elliptic Curve algorithm, which is an asymmetric key algorithm, so that is less effective in securing data if used in traffic that requires sending a large amount of data. Therefore, this research was conducted by implementing the AES and Twofish algorithms on IPsec to improve the MIPv6 network and compare the performance of the two in terms of encryption performance, security performance, and the quality of network services provided.

2. Research Methodology

2.1. Experimental Design

In order to implement the algorithm using IPsec on the research, an experimental topology was built on the Mobile IPv6 network, as shown in Figure 1. The topology consists of two different network blocks based on subnetting representing the home network and foreign network. IPsec is implemented on mobile nodes, home agents, and foreign agents to protect signaling information and packet traffic after handover.

.



Gambar 1. Network topology.

Before running the experiments, there needs to prepare the kernel so that the network can support the Mobile IPv6 feature. In addition, some supporting software such as Linux Mobile IPv6 Daemon, RADVD (Router Advertisement Daemon), IPsec-tools, Racoon, Iperf3, and Wireshark also need to be configured for this function to work. Table 1 lists the IPv6 addresses of all nodes involved in the test.

Table 1. Distribution of node addresses in the network**.**

Node	Interface	Connection	IPv6 Address
Home agent	enp2s0	Cloud	2001:db8:ffff:100b::1/64
	enp5s0	Access point	2001:db8:ffff:100a::2/64
Foreign agent	enp2s0	Cloud	2001:db8:ffff:100b::2/64
	enp5s0	Access point	2001:db8:ffff:100c::2/64
Correspondent node	wlp4s0	Access point	2001:db8:ffff:100a::100/64

The experiments are carried out in three scenarios: algorithm performance analysis, cryptanalysis testing, and QoS analysis. Each experiment was conducted to determine several parameters of the overall algorithm performance between AES and Twofish in terms of computational capabilities, security, and service quality. The following are three experiment scenarios in the research carried out:

1. The experimental scenario of the algorithm's performance is carried out by taking several parameters in the form of encryption and decryption computation time, CPU and memory usage, and the results of the encrypted file size.
2. The experimental cryptanalysis scenario is carried out by performing a brute force attack, and the algorithm is compared to determine the algorithm's strength in securing information. The attack scheme is carried out by two methods for each key size of 128, 192, and 256-bit, using a key without adding a hash and a key with an added hash. Parameters are taken in the form of cracking time and information results.
3. The QoS experimental scenario is carried out by measuring the quality of the services provided based on the implementation of the algorithm in IPsec. The parameters taken are delay, jitter, throughput, packet loss, and CPU utilization.

2.2. Software Design

Implementing the AES and Twofish algorithms in the experimental scenario of algorithm performance is done by creating a simple program for the encryption and decryption of several files. Figure 2 shows a simple tool designed to encrypt and decrypt files that contain information. Python-based application using the cryptography library -- crypto dome, for the interface is made with the PySide2 GUI framework. The output of encrypted files will be added with the .encrypted extension, while the decrypted files will be added with the .decrypted extension. Supported file extension formats include documents, PDFs, images, audio, and videos.

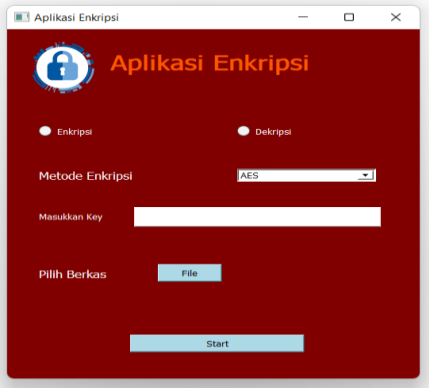


Figure 2. Encryption tools.

3. Results and Analysis

3.1. Analysis of Algorithm Performance Experiment

Experiments were carried out to find out how the performance of the two algorithms in managing information. Parameters measured are processing time, output file size, and memory usage to execute encryption and decryption processes on some file extensions and sizes. Data is taken ten times for each type of file extension based on variations in file size in general. Based on Figures 3(a) and 3(b), the execution time for the encryption and decryption processes in AES and Twofish has a significant comparison. In each type of extension, the ability of the file encryption process is faster in the AES algorithm than the Twofish algorithm. The biggest difference is obtained when the execution of video files where the processing time is very much different for the same file size and type. AES and Twofish are based on substitution-permutation networks (SPNs) and Feistel networks, respectively. This network is implemented in loops where AES has 10, 12, or 14 loops depending on the key size while Twofish applies 16 loops.

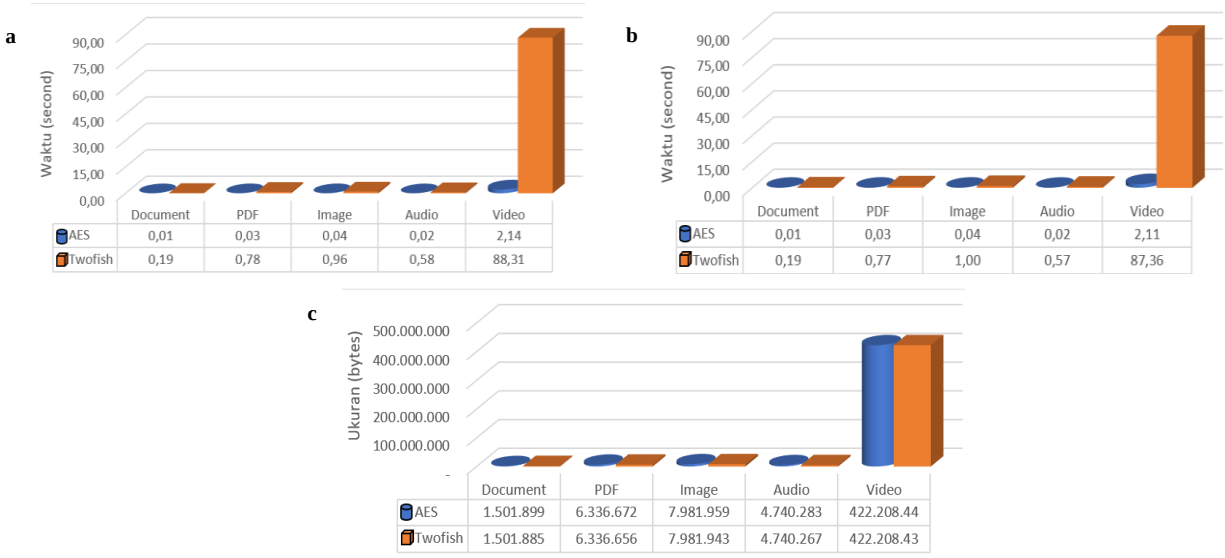


Figure 3. (a) Average encryption performance; (b) Average decryption performance; (c) Average encrypted file size.

The analysis is then continued on the size of the encrypted packet. The analysis was carried out by comparing the two algorithms' sizes of the encrypted and decrypted files. Figure 3(c) shows a graph of the encrypted file size data. The Twofish algorithm has a slightly smaller encrypted file size compared to AES in all tests. The result is analyzed based on the encrypted information generated in both algorithms, where there are additional random bits in AES compared to Twofish. The size of the data bytes is a concern because, of course, sending files can be more efficient by minimizing the size of the data. In addition, by minimizing the size, of course, the storage resources needed are more efficient. In terms of information itself, the resulting information payload follows the original information.

The next experiment was conducted to analyze the use of resources during the encryption and decryption processes. Table 2 shows the experimental results on the CPU for both encryption and decryption processes. The Twofish algorithm uses fewer CPU resources than the AES algorithm. As for memory (RAM), AES uses less than Twofish. The performance relationship between the CPU and RAM itself in the encryption process occurs when reading data. The CPU requires RAM to place programs and data during execution. So that when reading a file occurs, memory stores bytes of data which is then accessed by the CPU to be executed based on instructions.

Table 2. Resources used for computing**.**

Format	CPU Usage		Memory Usage	
	Encryption	Decryption	Encryption	Decryption
	AES	Twofish	AES	Twofish
Document	1,70%	1,49%	8 Mb	18 Mb
PDF	3,50%	3,09%	49 Mb	104 Mb
Image	3,10%	1,30%	48 Mb	154 Mb
Audio	0,79%	0,39%	39 Mb	62 Mb
Video	3,30%	2,80%	3075 Mb	1080 Mb

The encryption process time depends on the environment, and each computer has a different computing speed or instruction processing according to the processor used. The Twofish inefficiency in this test refers to developing AES-NI (Intel Advanced Encryption Standard New Instructions) technology, where most of the processors made recently have been equipped with the AES instruction set to improve algorithm performance. So that AES computing time becomes more effective. However, apart from this, based on the test results' overall encryption and decryption processing performance, AES is superior in computing time and memory usage, while Twofish has a smaller encrypted data bit size and lower CPU usage.

3.2. Experiment Cryptanalysis based of Brute-Force Attacks

Factors that affect vulnerability at the time of an attack are basically due to weak or commonly used credentials. To increase the security of the encryption method, a more complicated credential key, a combination, or the padding method is required. Another alternative is to add a hash function to the credential key to make it more computationally complex. Hash is used in passwords to disguise passwords to anticipate data leaks.

- *Non-Hashed Key*

  The first test method is carried out on the file using a key input with a key variation of 128-bit, 192-bit, and a 256-bit key, which is directly applied to the encryption process. The key entered is not added to the hash function, and then a brute force attack analysis is performed. Based on Table 3. for keys without a hash, the time required to unpack the Twofish file is 81.8% longer than AES at 128-Bit size, while for other key sizes, the computation time for Twofish is close to twice the computation time for AES. Twofish's complexity is indeed superior so that the security performance on Twofish is stronger than AES, although both do have good security against this type of attack because the time it takes to crack both encryptions is impossible to do with the computing capabilities of today's devices. However, Twofish's security is better than AES's if the attacker already knows several key bit gaps as an encryption key.
- *Hashed Key*

  The second test method is carried out on the file using a key input with a key variation of 128-bit, 192-bit, and a 256-bit key, which is added to the hash function sha-256 first before entering the encryption process. The encrypted file is then tested against brute force attacks. Based on Table 3, for hashed keys, the two algorithms increase computation time, which means there is an increase in the security of the encryption key itself. The 128 and 192-bit keys, respectively, have the same computational time as the 256-bit keys because of the additional padding value of the hash function sha-256 to the key used. Comparison of the computation time required to solve the Twofish algorithm is 102.08% longer than AES for all key sizes. Information that is cracked using the original 128-bit key without adding a hash function has a random bit result and does not show the original information. Meanwhile, when utilizing a key that has been added to a hash, the information in the file is restored to its original state.

Table 3. Cryptanalysis computing time**.**

Key	Non-Hashed Key		Hashed Key	
	AES	Twofish	AES	Twofish
128-Bit	1.1 x 10^25 years	2 x 10^25 years	4.8 x 10^63 years	9.7 x 10^63 years
192-Bit	2.3 x 10^44 years	4.1 x 10^44 years	4.8 x 10^63 years	9.7 x 10^63 years
256-Bit	4.8 x 10^63 years	9.7 x 10^63 years	4.8 x 10^63 years	9.7 x 10^63 years

3.3. MIPv6 Network Implementation

MIPv6 implementation is done by testing the communication between nodes. After each node has been configured and connected to the network, observations are made by sending a PING packet. Figure 4 illustrates the message during the handover process, in which the mobile node transitions from the home network to the foreign network. The mobile node sends a binding update to notify the home agent of the mobile node's new IPv6 address. Following receipt of the new address by the home agent, a binding acknowledgment message is sent. When the binding process is complete, communication between the correspondent node and the mobile node can be done by utilizing the mobile node address on the home network.

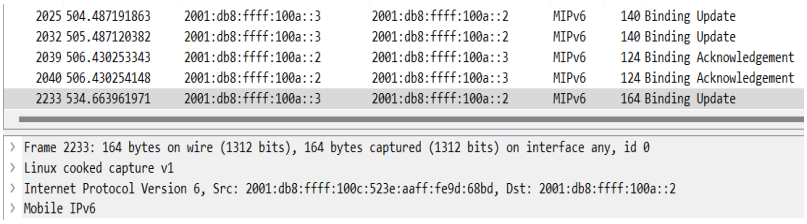
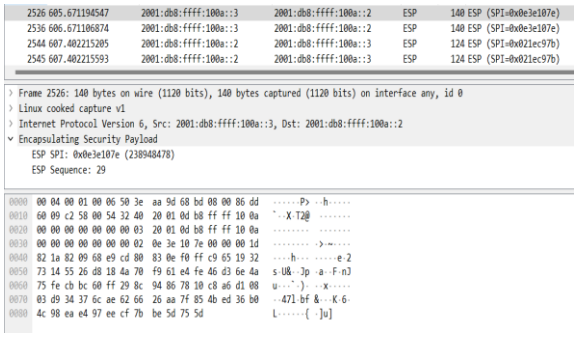


Figure 4. MIPv6 signaling information.

Packet information that the IPsec protocol has secured has some different fields. The IPsec protocol mode implemented is the ESP protocol. The ESP protocol wraps the packet by encrypting the original IP packet information containing the IP header, protocol, and data in the communication, and then an authentication feature is added that wraps the encrypted packet. Figure 5(a) shows the signaling information encapsulated by the IPsec protocol, the protocol recorded in the traffic is identified as ESP in the packet header. Packet information is wrapped in ESP headers so that information sent during establishing security associations cannot be known. Figure 5(b) shows the signaling information that has been decrypted based on the established security association.

a



b

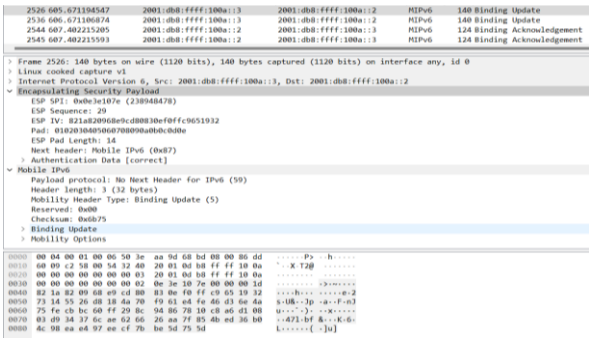


Figure 5. (a) Encapsulated MIPv6 Package; (b) Decrypted ESP Package.

3.4. QoS Experiment using IPsec on MIPv6

Security protocols are not only used to increase information security but also the quality of the services provided. During the communication process, the feasibility factor of a network is the number of packets sent accordingly, and the time delay is small. The factors that become parameters that support the feasibility of a network are the value of Delay, Jitter, Throughput, and Packet Loss Value.

Tabel 4. Delay and Jitter Measurement Results**.**

Parameter	Delay		Jitter	
	AES	Twofish	AES	Twofish
Max	0.19937 ms	0.17478 ms	0.25018 ms	0.34760 ms
Min	0.17252 ms	0.15399 ms	0.19301 ms	0.30225 ms
Average	0.17779 ms	0.16560 ms	0.20545 ms	0.32156 ms
Standard Deviation	0.00670 ms	0.00627 ms	0.01432 ms	0.01371 ms

Analysis of the measurement results found that the performance of the Twofish algorithm is better than the AES algorithm based on the smaller delay value in Table 4. Delay affects performance because every bit of data sent must, of course, match the packet flow rate. If there is a delay, it can cause packet stacking and make service is interrupted. This delay value is categorized as "very good," with index four based on the TIPHON standard because both algorithms have an average delay value of < 150 ms.

Meanwhile, for jitter, the jitter value of Twofish is higher than that of AES, but if analyzed from the standard deviation value between the two values based on Table 4, the delay variation of the Twofish algorithm is smaller than that of AES. The standard deviation itself is the level of variation of the data from some data. The use of standard deviation values is very suitable for finding out how close individual data is to the average sample value. The greater the deviation value, it indicates that the data for each test is far from the average. This jitter measurement can mean that Twofish traffic is quite more stable than AES because a smaller data distribution is obtained on Twofish. However, in terms of performance, both are still in a good standard of jitter value. The standardization of this jitter value is categorized as "Good" with index three based on the TIPHON standard because the average jitter value of the two algorithms is in the range of 0 - 75 ms.

Tabel 5. Network Throughput Measurement Results**.**

Parameter	Throughput in Bytes		Throughput in Bit	
	AES	Twofish	AES	Twofish
Max	5686557	6983073	45492457	55864584
Min	4898278	6238966	39186223	49911731
Average	5509707	6614820	44077657	52918564

Throughput experiments were carried out with a packet delivery scheme of 100MB using Iperf3 between the mobile node and the correspondent node. Mobile nodes transmit data with AES and Twofish encrypted tunnels. Table 5 contains throughput statistical data. Throughput is related to the bandwidth in a network, and bandwidth is the maximum capacity of the transmission medium to transmit a certain amount of data at one time. Meanwhile, throughput itself is a parameter that shows the actual ability of the transmission medium to deliver data.

Based on the measurement results, data obtained that the average throughput value generated using the AES algorithm is 44077657 Bit data. Meanwhile, the Twofish algorithm has an average throughput value of 52918564 Bit, which means it is bigger than AES. The resulting throughput can also be influenced by the size of the data being sent. The factor is because the packet is fragmented. That is, it breaks the packet into several parts according to the MTU capacity value. The more fragmentation that is done to the datagram, the smaller the throughput will be. Throughput decreases because many packets are transmitted, which causes long delays. However, this has the advantage of not causing total data loss in the event of a packet loss.

The packet loss parameter indicates the total number of packets lost during transmission. This packet loss can be caused by packet collision or congestion in the network. In general, network devices have buffers to hold received data temporarily. If congestion occurs for a long time, the buffer will be full and cannot accommodate the new data to be received, resulting in the loss of the next packet. The following is Table 6, which contains data from packet loss measurements.

Tabel 6. Packet Loss Measurement Results**.**

Parameter	Lost Segment as Packets		Lost Segment in Bytes		Percentage	
	AES	Twofish	AES	Twofish	AES	Twofish
Max	138	38	196830	54568	0.117%	0.04%
Min	49	13	70364	18668	0.044%	0.012%
Average	88	23	125596	32310	0.077%	0.023%

The results in Table 6 are obtained from observations of the packet loss value in the Wireshark tool, which is carried out by analyzing *tcp.analysis.lost_segment*. As with the previous discussion, packet loss can occur due to the influence of packet transmission; in this case, bit transmission errors can cause packet retransmission which will disrupt network efficiency. In addition, a packet queue that causes the buffer capacity to be full makes some packets that come later are lost. The comparison of the value of packet loss can be concluded that the reliability of the Twofish algorithm is better than the AES algorithm, judging by the packet loss parameters. The packet loss value on Twofish has an average of 0.023%, while the average value of AES is 0.077%. The standardization of the packet loss value is categorized as "very good" with index four according to the TIPHON standard because the values for both algorithms are in the range of 0 ms.

Tabel 7. CPU Utilization Measurement Results**.**

Parameter	Sender		Receiver	
	AES	Twofish	AES	Twofish
Max	2,80%	4,10%	3,00%	1,80%
Min	2,10%	3,20%	0,40%	0,10%
Average	2,55%	3,65%	1,60%	0,97%

Algorithm performance in CPU usage is measured when client-server communication occurs and then analyzed for the results of both algorithms. CPU data is fetched for both nodes on the sending side and also the receiving side. The following graph of the measurement results is presented in Table 7. Based on the measurement data analysis, it is known that the CPU processing usage on the client-side of the Twofish algorithm is higher than the AES algorithm. The complexity of the Twofish algorithm influences this increase during the process of building security associations referring to the Twofish algorithm computation. However, the Twofish algorithm uses lower CPU consumption on the server-side than the AES algorithm.

4. Conclusion

The AES and Twofish algorithms are implemented directly to secure packets on the IPsec protocol to increase the confidentiality of information. Implementing IPsec on an IPv6 cellular network is quite effectively used to improve security performance during the vertical handover signaling process. The registration information between the communicating nodes is successfully encapsulated so that the original information loaded cannot be known to others. The results of performance testing between AES and Twofish algorithms show that the computational ability of the encryption and decryption process, AES is superior in computational time than Twofish. However, Twofish computing is more complicated than AES. Twofish's performance is quite superior in several test scenarios that have been carried out. The encrypted file size in Twofish is slightly smaller than AES. Then, the results of the security system performance also show that the Twofish algorithm is more secure with a twofold increase than AES based on the computational cracking time for

all key sizes. In addition, Twofish performs very well in wireless network implementations where every network service quality test parameter is superior to AES performance. Twofish provides better security with a more reliable quality of service than AES for mobile networks with the same overhead. Based on the overall scenario testing, the Twofish is potentially used as an encryption algorithm for IPsec and further implemented to secure our mobile communications.

REFERENCES

[1] Asosiasi Penyedia Jasa Internet Indonesia. *Laporan Survei Internet APJII 2019 – 2020*. Accessed on September 3, 2021. Available at https://apjii.or.id/survei.

[2] Perkins, C. E., & Johnson, D. B. (1996). Mobility support in IPv6. *Proceedings of the 2nd annual international conference on Mobile computing and networking*, pp. 27-37.

[3] Nurcahyani, W. T., Yulianto, F. A., & Herutomo, A. (2015). Analisis performansi Fhmipv6 (fast handover for hierarchical Mobile Ipv6) pada jaringan wave (wireless access in vehicular environment) 802.11 p. *eProceedings of Engineering*, vol. 2, no. 2, pp. 6550-6557.

[4] Praptodiyono, S., Firmansyah, T., Alaydrus, M., Santoso, M. I., Osman, A., & Abdullah, R. (2020). Mobile IPv6 vertical handover specifications, threats, and mitigation methods: A survey. *Security and Communication Networks*, vol. 2020, pp. 1-18.

[5] Abikoye, O. C., Garba, Q. A., & Akande, N. O. (2017). Implementation of textual information encryption using 128, 192 and 256 bits advanced encryption standard algorithm. *Annals. Computer Science Series*, vol. 15, no. 2, pp. 153-159.

[6] Frankel, S., & Krishnan, S. (2011). Ip security (ipsec) and internet key exchange (ike) document roadmap. Request for Comments, no. 6071.

[7] Barker, E., & Roginsky, A. (2018). Transitioning the use of cryptographic algorithms and key lengths (No. NIST special publication (SP) 800-131A Rev. 2 (Draft)). Maryland: National Institute of Standards and Technology.

[8] Oluwakemi, C. A., Haruna, A. D., Abubakar, A., Akande, N. O., & Asani, E. O. (2019). Modified advanced encryption standard algorithm for information security. *Symmetry*, vol. 11, no. 12, pp. 1-16.

[9] Zodpe, H., & Sapkal, A. (2020). An efficient AES implementation using FPGA with enhanced security features. *Journal of King Saud University-Engineering Sciences*, vol. 32, no. 2, pp. 115-122.

[10] Mahendra, L. I. B., Santoso, Y. K., & Shidik, G. F. (2017, October). Enhanced AES using MAC address for cloud services. *2017 International Seminar on Application for Technology of Information and Communication (iSemantic)*, pp. 66-71.

[11] Ghosh, A. (2020). Comparison of encryption algorithms: AES, Blowfish and Twofish for security of wireless networks. *International Research Journal of Engineering Technology*, vol. 7, pp. 4656-4658.

[12] Harahsheh, H., & Qatawneh, M. (2018). Performance evaluation of Twofish algorithm on IMAN1 supercomputer. *International Journal of Computer Applications*, vol. 179, no. 50, pp. 1-7.

[13] Divya, V., & Gobinath, R. (2019). Two fish cryptography for data security in network communication. *Int. J. Recent Technol. Eng.*, vol. 8, no. 2 Special Issue 4, pp. 986–989.

[14] Praptodiyono, S., & Barita, D. (2020). Peningkatan kinerja sistem keamanan pada proses pensinyalan dalam vertical handover MIPv6". *Setrum: Sistem Kendali-Tenaga-elektronika-telekomunikasi-komputer*, vol. 9, no. 1, pp. 1-7.

[15] Praptodiyono, S., Santoso, M. I., Firmansyah, T., Abdurrazaq, A., Hasbullah, I. H., & Osman, A. (2019). Enhancing IPsec performance in mobile IPv6 using elliptic curve cryptography. *2019 6th International Conference on Electrical Engineering, Computer Science and Informatics* (*EECSI*), pp. 186-191.