Journal of Engineering Science and Technology
Vol. 16, No. 3 (2021) 2312 - 2325

IMPROVING THE SECURITY OF MOBILE IPV6 SIGNALLING USING KECCAK / SHA-3

SUPRIYANTO PRAPTODIYONO[1,*], TEGUH FIRMANSYAH[1], RAJA KUMAR MURUGESAN[2], MUDRIK ALAYDRUS[3], RANDY APRILIA[1], YU-BENG LEAU[4]

[1]Department of Electrical Engineering, Universitas Sultan Ageng Tirtayasa, Jl. Jenderal Sudirman Km. 3 Cilegon, Banten 42435 Indonesia
[2]School of Computer Science and Engineering, Taylor's University, Taylor's Lakeside Campus, No 1, Jalan Taylors, 47500 Subang Jaya, Selangor, Malaysia
[3]Department of Electrical Engineering, Universitas Mercu Buana, Jl. Raya Meruya Sel., Kec. Kembangan, Jakarta 11650 Indonesia
[4]Faculty of Computing and Informatics, Universiti Malaysia Sabah, Jalan UMS, 88400 Kota Kinabalu, Sabah, Malaysia
[*]Corresponding Author: supriyanto@untirta.ac.id

Abstract

Most people nowadays use their mobile devices to stay connected to the internet all over the place and all the time. In order to provide their customers with excellent service, all Internet Service Provider (ISP) worked together to make a handover process from one ISP to another. The signalling process is an integral part of the handover that makes it easier for devices to register their new address. If no security is used, attackers could initiate an adverse action during the signalling time. The Mobile IPv6 standard mandates the use of Internet Protocol Security (IPsec) to secure the handover process, particularly during the signalling step. The conventional IPsec uses Keyed-Hash Message Authentication Code-Secure Hash Algorithm-1 (HMAC-SHA-1) to authenticate signalling messages. However, the SHA-1 has been detected and broken by collision attacks and length-extension attacks. Hence, the signalling process on the Mobile IPv6 is vulnerable. The aim of this paper is to find a hash algorithm that is resistant to both attacks. Subsequently, it can be implemented on IPsec to secure the Mobile IPv6 signalling process. The experimental result showed that the SHA-3 algorithm could fulfil the requirements. It can enhance security performance and, at the same time, does not lengthen the authentication time significantly.

Keywords: Authentication, Mobile IPv6 Internet protocol security (IPsec), Security, SHA-3.

1. Introduction

In this digital era, every human activity involves internet technology. This condition contributed to a lack of internet addresses, prompting the Internet Engineering Task Force (IETF) to develop Internet Protocol Version 6 (IPv6) [1]. Internet users tend to retain their business communications and continue to participate in entertaining activities, such as watching online videos or playing online games, even though they move from one location to another. This fact was supported by the data showing that the use of mobile devices has grown exponentially [2]. The number of active mobile broadband subscriptions per 100 inhabitants continues to rise 18.4 percent year-on-year. To provide internet users with the best services, IPv6 offers mobility support, namely Mobile IPv6 [3], and has some enhancements over the current Mobile IP [4]. The two factors that must be considered when using internet services are performance and security. Users want a consistent internet connection with fast data rate and persistent security against harmful activities. Unfortunately, the performance usually does not fit with protection needs. High security requires additional features that can cause the network overhead and degrade its performance. For example, IPv6 has several advantages, including simplifying header format and removing options fields from main header, which speed up the data transmission [1]; however, it requires a high-security system. The standard for IPv6 mandates the use of IPsec to secure IPv6 data transmission, but the researchers had reported several obstacles to use IPsec [5, 6].

The Mobile IPv6 standard, RFC 6275 [3], also prescribes the use of IPsec to operate with keyed hashing for message authentication, using SHA-1 [7]. RFC 2104 stated that HMAC depends on which hash function is being used. Unfortunately, SHA-1, which is a hash function algorithm based on Merkle-Damgard, has been proved vulnerable to collision attacks [8] and length-extension attacks [9, 10]. Using SHA-1 is no longer secure in Mobile IPv6. A number of researchers proposed replacing the SHA-1 with the Keccak algorithm-based SHA-3. Ramya and SairamVamsi [11] have submitted securing MANET using SHA-3 Keccack Algorithm. It did not implement the proposal, however, but was using NS2 to simulate it in a non-IPv6 environment. The simulation approved that the SHA-3 algorithm can eliminate blackhole, flooding, and wormhole attacks. Chandrana and Manuel [7] proposed the modification of SHA-3 on the Field Programmable Gate Array (FPGA) device. The author compared the conventional step by step algorithm with a mux algorithm involved. The modified one may correct errors but, at the same time, introduce overhead.

The objective of this research is to find out which SHA-1 successor can be implemented on IPsec to secure the Mobile IPv6 signalling. We carried out an extensive experiment involving SHA-3 hash algorithm. An evaluation was done to find which algorithm on the current Mobile IPv6 implementation can increase security performance without increasing the burden. The performance includes the individual resistance to collision attacks and length-extension attacks as well as the impacts on the handover process for Mobile IPv6 implementation.

The rest of this paper is organized as follows: an overview of mobile IPv6 security, including the signalling process in section 2. Section 3 describes the topology and scenario used in the experiments, and section 4 discusses the experimental results to find a justification for the hash algorithm candidates. Section 5 concludes this paper by offering several future research directions.

2. Overview of Mobile IPv6 Security

People need to move from one place to another to carry out their daily activities. In their movements, they seek to remain connected to the internet in order to maintain their communication with friends and family. This service is provided by Mobile IP technology. However, there are several drawbacks, including limited IPv4 address space and triangle routing problem, as depicted in Fig. 1. Its routing mechanism pushes all messages from the mobile node (MN) to the corresponding node (CN), or vice versa through the home agent (HA) that adds to network latency. The problem is the result of an inefficient routing mechanism. All packets sent by the MN must go to their home agents and then tunnel to the corresponding node, using encapsulation within IP [12]. Mobile IPv6 has been developed to address these issues. Mobile IPv6 is an integral part of IPv6 and offers a large IP address space. The problem of address space can therefore be resolved. The implementation of optimization can address the problem of triangle routing.

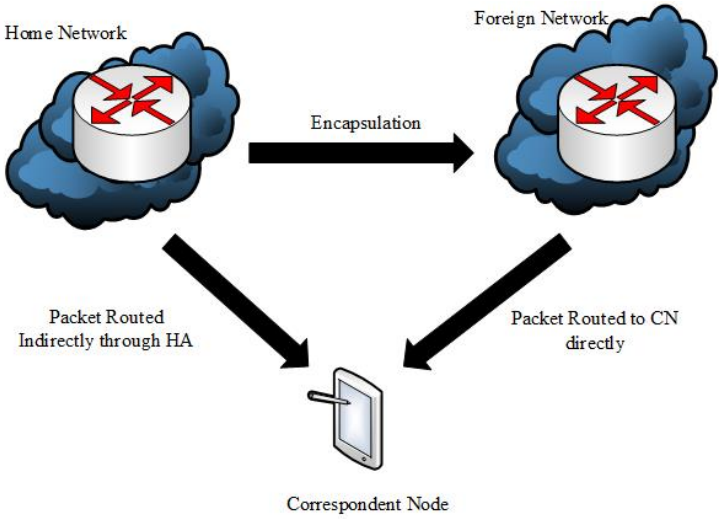

Fig. 1. Triangle routing on mobile IP.

The route optimization mechanism is shown in Fig. 2. The mechanism will break the direction of travel by making a direct route from the MN to the CN. As in Fig. 2, the first packet of the CN is sent to the HA. It is then tunnelled to the MN while in a foreign network (FN). Once receiving the packet, the MN knows the address of the CN. It sends a binding update (BU) message to the address to inform its care-of address (CoA). Upon receiving the BU message, the CN may respond by sending a binding acknowledgment (BA) message. A direct route has been established between the MN and the CN. Furthermore, the communication path can be used to relay the following IPv6 packets.

Using the route optimization mechanism, the MN can communicate directly with its corresponding node after obtaining a new CoA. Generating a new CoA can employ stateless autoconfiguration, using SLAAC [13], a secure address generation, CGA [14, 15], or a stateful address, using DHCPv6 [16]. However, the

MN must first register the new CoA to its HA before sending messages to the CN. The registration method is called the signalling process, as depicted in Fig. 3.

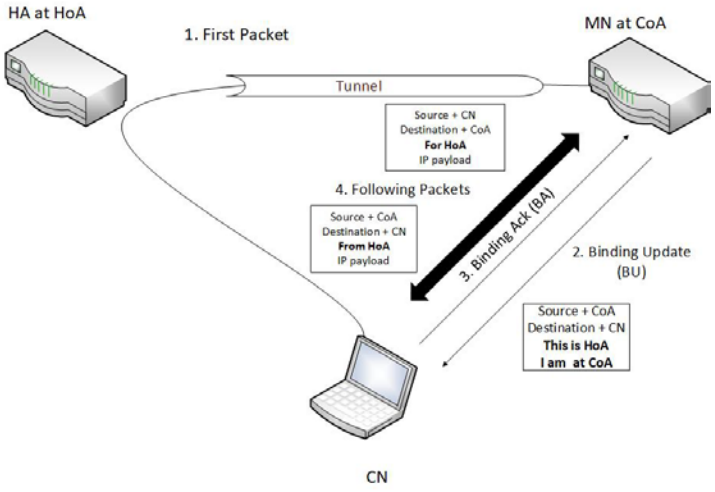

Fig. 2. Route optimization mechanism.

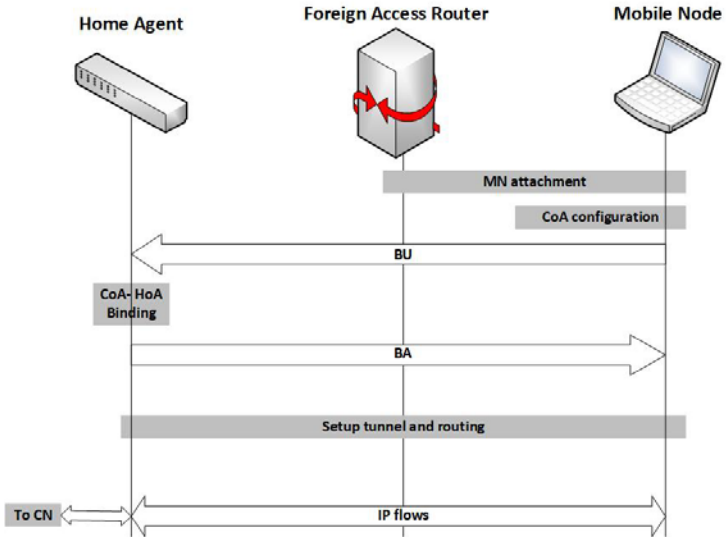

Fig. 3. Signalling messages passing on mobile IPv6.

The signalling process in Fig. 3 consists of the following steps.

- The MN leaves its HA and attaches to a foreign network. It configures a CoA based on the new access router information, using the Neighbor Discovery Protocol [17]. The configuration can use either SLAAC or DHCPv6. The new CoA is then checked and differs from duplication, using standard DAD [18].
- The MN sends a BU message containing the CoA and home address (HoA) binding on the HA, informing the latter of its new location. The HA processes the received BU message and then stores the binding in its Binding Cache Entry.

- The HA replies by sending a BA message to the CoA of the MN. It also configures a tunnel between the HA and the MN, using its address as the endpoint.
- The MN configures a tunnel in the reverse direction after receiving the BA message. Bidirectional transmission is established once the tunnel is built.
- Upon completion of the registration, the MN begins to transmit the BU message to a CN, using its registered CoA. Finally, the CN responds to the received message by sending a BA message. Now they can communicate with each other.

Signalling in Mobile IPv6 is a necessary process that allows the MN to register its generated CoA to its HA. If the signalling process is not done, the CoA of the MN will be unregistered and any contact with the CN will be hindered. The signalling process may be compromised by a malicious node, making the signalling process fail or intercept the process to make a wrong registration. For example, a BU message sent by the MN can be captured by an attacker, who can then interrupt the transmission or modify the message. The HA can get the wrong message, which causes the CoA configuration to malfunction. IPsec is a security standard in Mobile IPv6 to secure the signalling process [19]. The IPsec suite is a set of security protocols that use the Encrypted Security Payload (ESP) and or Authentication Header (AH) mode to protect the signalling process. Thus, the MN and the HA can authenticate each other. The BU and BA messages are protected against attempt by attacker to manipulate the signalling process.

Securing the signalling process is essential and protecting the BU and BA messages should not be neglected. RFC 3776 has standardized IPsec use to secure Mobile IPv6 signalling between MN and HA. Both MN and HA should use the ESP in transport mode to protect binding updates, binding acknowledgments, and prefix discovery. The authentication algorithm is used to provide connectionless integrity, data origin authentication, and anti-replay protection. However, due to the increase of such attack vectors, up-to-date cryptographic, and authentication algorithms of IPsec should be considered overtime to keep IPsec interoperable [19]. Furthermore, standard on ESP and AH have always evaluated and obsoleted over time since RFC 2404 on 1998, RFC 4305, RFC 4835, RFC 7321, and the latest is RFC 8221 on 2017.

The latest standard, RFC 8221 [19], has required a conservative algorithm to minimize the risk of compromise, appropriate for a wide range of CPU architectures, including tiny and low-power devices implemented in Mobile IPv6 and Internet of Things (IoT). The RFC has defined the encryption and authentication algorithms as listed in Table 1.

Table 1. Encryption and authentication algorithm of IPsec.

Algortihm	Type	Implementation status
ENCR_AES_GCM_16	Encryption	MUST
ENCR_AES_CCM_8	Encryption	SHOULD
ENCR_AES_CTR	Encryption	MAY(*)
ENCR_3DES	Encryption	SHOULD NOT
AUTH_HMAC_SHA1_96	Authentication	MUST-
AUTH_AES_128_GMAC	Authentication	MAY
AUTH_NONE	Authentication	MUST/MUST NOT

It can be seen in Table 1, the latest standard still recommends using AUTH_HMAC_SHA1_96 for authentication, but the implementation status is MUST-. The level indicates that the standard expects some point of the algorithm will no longer be a MUST in the future. The HMAC-SHA1 has been broken by collision attacks and length-extension attacks, as reported by some researchers such as in [20-22]. Furthermore, it is important to find an authentication mechanism that is resistant to attack vectors that can further protect the signalling process in mobile IPv6.

To secure the signalling process, we proposed to use an authentication mechanism called Keccak Message Authentication Code (KMAC) [23, 24]. The KMAC algorithm is using SHA-3 as an authentication algorithm [9]. SHA-3 has been developed by Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. In 2015, NIST picked SHA-3 as the winner of its hash function competition.

3. Experimental Topology

Figure 4 shows the topology used in this experimental research of the Mobile IPv6 operation, including the signalling process. The topology has been set up in a limited network that uses Raspberry Pi 3B+ as the Mobile Node. The processor is Broadcom BCM2837B0 Quad-Core A53 (ARMv8) 64-bit @ 1.4GHz, and the connectivity uses 1 x 10/100 Mbps Ethernet, 2.4GHz 802.11n 150 Mbps Wireless. The distance between the home agent (HA) and foreign router (FR) was determined without overlapping of the signal. The MN may lose the connection to the HA when moving to the FR. Further, the MN would conduct the handover form HA connection to FR connection. The experiments focus on the network level since the IPsec is a network layer security. Thus, the lower layer security was not evaluated. All nodes are configured with UMIP Linux Mobile IPv6 [25, 26]. The routers are configured to activate their router advertisements using Router Advertisement Daemon (RADVD), and the hosts are configured using mip6d.conf.

The operating distance between HA and FR was set at 30 meters to disconnect the MN while moving. It will discover a new network by receiving a Router Advertisement message from FR. The first pre-requisite is that the MN is connected to the HA, and the MN address is the HoA. It communicates with the CN which is part of the same network. In the second condition, the MN moves to the foreign link in another network. During the movement, the MN will lose its connection (disconnect with the CN) and try to discover a new network. Once the FR coverage is hit, it receives a RA message. It then generates a CoA and updates its status by sending BU messages to the HA and the CN. This signalling process will be terminated once the MN receives the BA message.

The two parameters measured in this experiment are the latency (handover time) and the security performance of HMAC candidates. According to [27], latency consists of a detection period, address configuration interval, and registration time. It begins when the MN disconnects from its home and goes before it receives the BA message from the HA. The latency was calculated for 10 experiments. It was influenced by generating BU and BA messages that included the hash operation. Security performance is measured by conducting collision attacks and length-extension attacks to the hash functions candidates, SHA-3, which can be contrasted to SHA-1. The SHA collider [28] and lhextend [9] were used to measure the performance of the hash function algorithm.

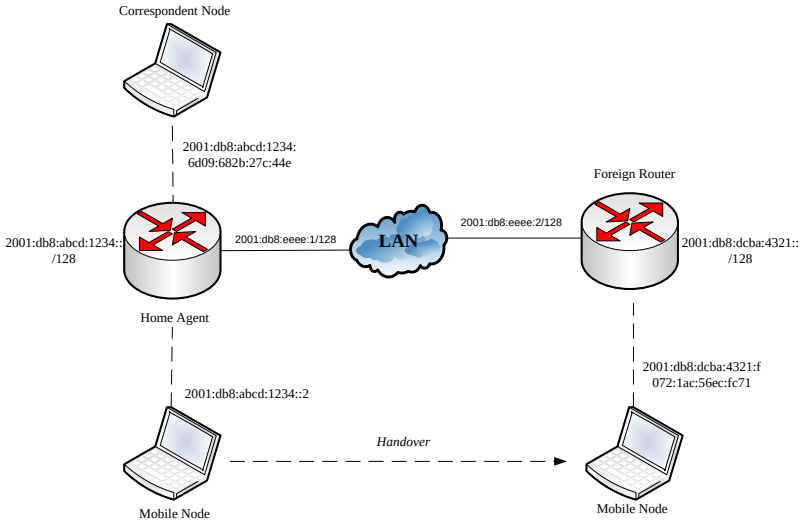

Fig. 4. Experimental topology for mobile IPv6 operation.

4. Results and Discussion

4.1. SHA-3 implementation on mobile IPv6

The experiments have been used to enforce IPsec on securing the Mobile IPv6 signalling process, in particular to protect BU and BA messages. The experiments focused on the using of ESP to protect the IPv6 packet containing BU or BA messages. The ESP encrypts the entire original IPv6 packet and authenticates all the containing fields. The experiments compared the existing authentication algorithm (SHA-1) and the possible successor (SHA-3) to authenticate the signalling messages. The authentication results are ICV (integrity check value) which is then put in the last field of the protected IPv6 packets. The experimental results will be proof that the use of SHA-3 to secure a Mobile IPv6 signalling message is feasible. The following subsection discusses the security performance of SHA-3 and the impact on SHA-3 implementation on handover time.

Standards on mobile IPv6 mandated using ESP to secure the signalling messages (Binding Updates and Binding Acknowledgements) both in the mobile nodes and the home agents. The ESP involves the encryption and authentication algorithm, as listed in Table 1. However, caution should be taken when selecting suitable encryption and/or authentication algorithms for ESP. Experiments have been conducted using the experimental topology shown in Fig. 4 to ensure that SHA-3 is the best ESP candidate for securing mobile IPv6. The signalling message transmission was performed 100 times. Figure 5 shows the implementation of SHA-3 in the signalling process.

The IPsec was configured in both MN and HA using the following configuration command:

IPsecPolicySet {

HomeAgentAddress 2001:db8:abcd:1234::1;

HomeAddress 2001:db8:abcd:1234::2/64;

IPsecPolicy Mh UseESP 10;
IPsecPolicy TunnelPayload UseESP 11;
}

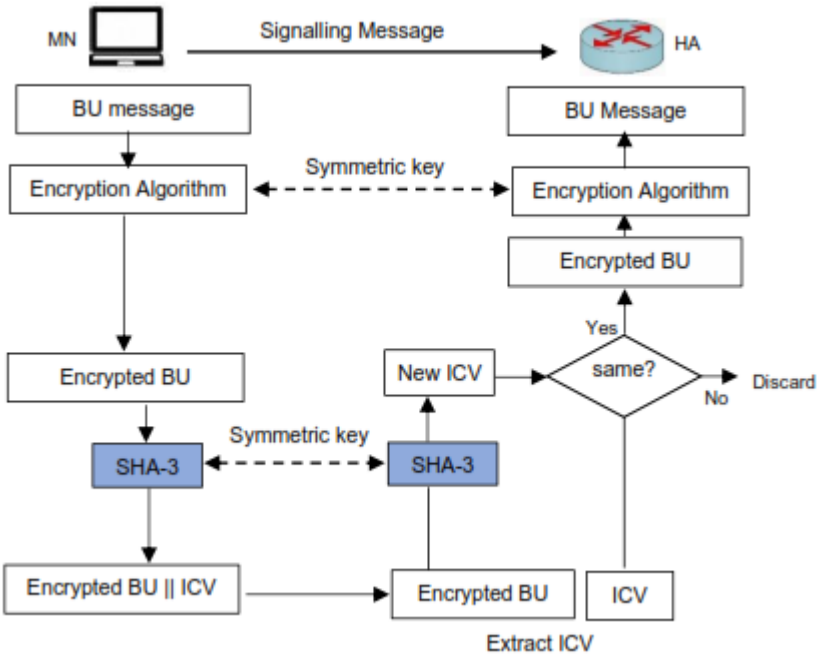

Fig. 5. Implementation of SHA-3.

ESP requires two cryptographic mechanisms (encryption and authentication), with the first encryption being done. The encrypted BU packet is then hashed using SHA-3 to produce an Integrity Check Value (ICV). The ICV is concatenated to the encrypted BU to be transferred from MN to HA. Upon receiving the protected message, the HA will extract the ICV and hash the encrypted BU resulting in a new ICV. It compares the two ICVs to know the authentication of the BU message. The experiments confirmed that the SHA-3 implementation in securing Mobile IPv6 is well underway. However, we need to analyse the security performance and its impact on the Mobile IPv6 handover.

4.2. Security performance

- **Collision attack resistance**

To test the security performance, two attacks were conducted on both hash algorithms. A file named *file1.jpg* was changed to *file1-modifikasi.jpg* by modifying the content of *file1.jpg*. By using an SHA-1-collider, the hash code can be generated as shown in Table 2. The experiment was repeated 10 times. The output for both files remained the same during the examination. This finding proves that SHA-1 is no longer resistant to collision attack and that it is not a reliable authentication mechanism for Mobile IPv6 signalling.

Table 2. Hash results for SHA-1.

Input data	Hash SHA-1	SHA-3
Original File	5289402981518e96ffa5fd37ba020ed3bfeb9358	8044fa3906884749a638a43cd40d1cab6aad923d07c2b48e7a17e3bc942dea3f
Modified File	5289402981518e96ffa5fd37ba020ed3bfeb9358	30f64bb47a62122ac16f13af468cf14c60c3d318ec599ebc30779dafd8fa7e21

Applying the same scenario, the original file has been hashed with SHA-3. The results of hashing the original file (*file1.jpg*) are shown in Table 2 (first row). Part of the content in the same file is modified (*file1-modifikasi.jpg*) and results in a different hash code, as shown in Table 2 (second row). The SHA-3 was attacked 10 times, none of which was succeed. The experimental results revealed that SHA-3 is resistant to collision attacks.

- **Length extension attack resistance**

The second test was performed by executing length extension attacks on the two hash algorithms. This attack was generated with lhextend software. A length extension attack can be conducted in three steps.

Step 1.

Define the data and a key to encrypt the data (ex. skripsi+randy), and generate a digest using SHA-1. Figure 6 shows the digest when 'skripsirandy' was hashed using SHA-1.

```
>>> import hlextend
>>> sha1 = hlextend.new('sha1')
>>> sha1.hash('skripsirandy')
>>> print ("SHA-1: " + sha1.hexdigest())
SHA-1: d3b9a898a3492ee83e2b11587a06124ad7a14a6a
```

Fig. 6. First digest for key and data.

Step 2.

Give a padding to the data (ex. aprilia) and generate a digest from the 'padding+data+length of key+first digest'. Figure 7 shows the second digest using SHA-1.

```
>>> import hlextend
>>> sha = hlextend.new('sha1')
>>> sha.extend('aprilia', 'randy', 7, 'd3b9a898a3492ee83e2b11587a06124ad7a14a6a')
>>> print ("SHA-1: " + sha.hexdigest())
SHA-1: 6ba03cd6379c088ed32ec98404f783bf7b2d0db4
```

Fig. 7. Second digest for padding, data and first digest.

Step 3.

Generate a digest using SHA-1 for the combination of the key, data and padding. The third operation results in the last digest, as shown in Fig. 8, which is the same as the second digest.

```
>>> import hlextend
>>> sha1 = hlextend.new('sha1')
>>> sha1.hash('skripsirandyaprilia')
>>> print ("SHA-1: " + sha1.hexdigest())
SHA-1: 6ba03cd6379c088ed32ec98404f783bf7b2d0db4
```

Fig. 8. Third digest for key, data and padding.

The three figures above show that SHA-1 is no longer resistant to length extension attacks. SHA-3 was used to hash the 'key+data+padding' in the same case. The results of the ten experiments showed that the last digest differed from the second digest. Table 3 shows the results of the second and third digests. SHA-1 resulted in the same digest, which implies that it was broken with a length extension attack. SHA-3 demonstrates a different result, which suggests that SHA-3 is resistant to length extension attacks.

Table 3. Length extension attack operation.

Input data	SHA-1	SHA-3
Second Digest	6ba03cd6379c088ed32ec984 04f783bf7b2d0db4	682820e67e769ec9bba0a11664e929 dca1e4839156e7a800cf670cbc9c212afd
Third Digest	6ba03cd6379c088ed32ec984 04f783bf7b2d0db4	b09f99085b9f16171399315b9d30f13a 27406014d7fcaca01174aa8457a6f90c

Based on the experiments involving collision and length extension attacks, SHA-3 satisfies the specifications of the hash function criteria and outperforms SHA-1. SHA-3 currently cannot be broken by the two attacks. It can be used to secure the Mobile IPv6 environment, especially the signalling process. However, the impact of the implementation of SHA-3 in Mobile IPv6 must be analysed. The next subsection points out the effect of SHA-3 on the network latency of Mobile IPv6.

4.3. Handover time

The handover time of an MN is calculated by adding movement detection time and the signalling time, as formulated in [27]. Movement detection time is the time it takes for the MN to discover a new wireless region in which it can receive a Router Advertisement message. Signalling time consists of the address configuration and registration time. Most signalling time is consumed by the authentication of the BU and BA messages during the registration phase. In this research, handover time was measured to understand the impact of SHA-1 and SHA-3 on the signalling process. Longer handover time means more signalling time needed, which raises network latency. Figure 9 demonstrates the handover time on average. Figure 9 shows that SHA-3 has a longer handover time than does SHA-1. These experiments were conducted to recognize the significant influence of SHA-3 on the handover time. To better understand the impact of SHA-3 and SHA-1 on Mobile IPv6 signalling, the percentage of discrepancies between the two algorithms has been calculated.

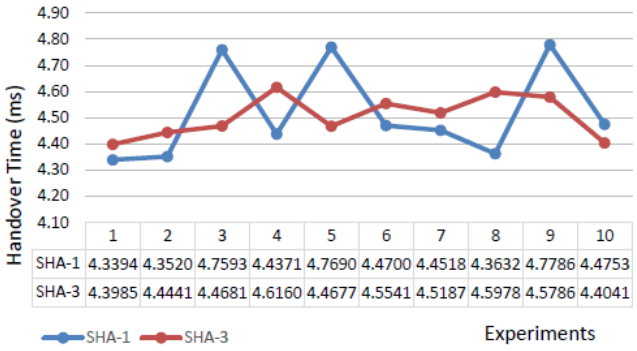

Fig. 9. Mobile IPv6 handover time.

Overall, the authentication algorithm used affects the signalling time since it mainly consists of authentication time in Mobile IPv6. Figure 9 shows a little of a gap between SHA-1 and SHA-3 when used to secure the signalling process. Table 4 reports the percentages of the differences between the two algorithms. The BU signalling message authentication using SHA-3 takes 11.42% longer than does that which uses SHA-1.

In contrast, the BA signalling message authentication shows a lower time of 2.43%. The overall handover times in the Mobile IPv6 handover process of the two hash algorithms are similar. The use of SHA-3 does not significantly affect signalling time. While SHA-3 takes more time than SHA-1, the difference is only 0.33%. The SHA-3 implementation should not impact the Mobile IPv6 handover. This inference is drawn when the two algorithms are implemented in the same setting as described in Section 3 with the distance between the access point is 30 meters.

Table 4. Authentication times.

Signalling Message	Hash Algorithm		Percentage of difference
	SHA-3	SHA-1	
Binding Update	29.88549 ms	26.82232 ms	11.42
Binding Acknowledgment	19.24674 ms	19.71468 ms	-2.43
Handover Time	4.51961 s	4.50482 s	0.33

It can be seen in Table 4; the authentication time of the BU message is higher than BA messages for the two algorithms. This difference is due to message size issues. Based on [29], the BU message with IPsec has a size of 161 bytes , and the BA message has a size of only 145 bytes. The hash algorithm calculates a signalling message based on a byte per byte operation. The larger message will require a longer processing time.

5. Conclusion

Mobile technology continues to grow exponentially, and as a result, securing handovers to Mobile IPv6 deserves serious consideration. The handover of Mobile IPv6 must remain resistant to any malicious activity to be connected all the time and everywhere. During the handover, an MN is required to generate a new CoA, which depends on information obtained from a foreign network. False information could cause the generation of an address to fail or cause a wrong address to be generated. The key step in the handover is the signalling process, which involves registering the newly generated CoA to the HA. Failure to complete the registration means that the MN cannot communicate with other nodes. Although IPsec is

mandatory to secure the network layer of Mobile IPv6 communication, the existing authentication algorithm used in IPsec, SHA-1, has been broken by collision and length-extension attacks. A new SHA-1 replacement algorithm must be found.

Replacement candidates must be resistant to both of these attacks. SHA-3, the winner of the NIST hash function competition, is considered a viable replacement for SHA-1 for Mobile IPv6 signalling. Experiments were conducted to compare the authentication performance of the two algorithms during the signalling process. The results showed that SHA-3 met the requirements for collision resistance and length extension attacks. The comparison also revealed that the implementation of SHA-3 did not affect the handover time required by Mobile IPv6. As the significant growth of mobile device continues, the security should be taken into consideration to researchers. Fast and secure handover could be a challenge for the future.

Abbreviations

AES	Advanced Encryption Standard
AUTH	Authentication
BA	Binding Acknowledgement
BU	Binding Update
CN	Correspondent Node
CCM	Cipher Block Chaining-Message
CGA	Cryptographically Generated Address
CPU	Central Processing Unit
CTR	Counter Mode
CoA	Care of Address
DAD	Duplicate Address Detection
DHCPv6	Dynamic Host Control Protocol version 6
ESP	Encapsulating Security Payload
ENCR	Encryption
FN	Foreign Network
FPGA	Field Programmable Gate Array
GCM	Galois / Counter Mode
GMAC	Galois Message Authentication Code
HA	Home Agent
HMAC	Hash Message Authentication Code
HoA	Home Address
IP	Internet Protocol
ICV	Integrity Check Value
ISP	Internet Service Provider
IETF	Internet Engineering Task Force
IPSec	Internet Protocol Security
IPv6	Internet Protocol version 6
KMAC	Keccak Message Authentication Code
MN	Mobile Node
MANET	Mobile Ad Hoc Network
NIST	National Institute of Standards and Technology
NS2	Network Simulator 2
RFC	Request for Comments
RADVD	Router Advertisement Daemon

SLAAC	Stateless Address Auto Configuration
SHA-1	Secure Hash Algorithm-1
SHA-3	Secure Hash Algorithm-3
UMIP	Universal Mobile IP
3DES	Triple Data Encryption Standard

References

1. Deering, S.; and Hinden, R. (2017). Internet protocol, version 6 (IPv6) specification, it obsoletes RFC 2460. Retrieved March 1st, 2020, from https://datatracker.ietf.org/doc/html/rfc2460.
2. Bogdan-Martin, D. (2019). Measuring digital development facts and figures 2019. Retrieved March 15, 2020, from https://news.itu.int/measuring-digital-development-facts-figures-2019/
3. Perkins, C.; Johnson, D.; and Arkko, J. (2011). Mobility support in IPv6. Retrieved March 15, 2020, from https://tools.ietf.org/html/rfc6275.
4. Perkins, C. (2010). IP mobility support for IPv4, revised. RFC 5944.. Retrieved August 30, 2020, from https://tools.ietf.org/html/rfc5944.
5. Praptodiyono, S.; Santoso, M.I.; Firmansyah, T.; Abdurrazaq, A.; Hasbullah, I.H.; and Osman, A. (2019). Enhancing IPsec performance in mobile IPv6 using elliptic curve cryptography. *6th International Conference on Electrical Engineering, Computer Science and Informatics*, Bandung, Indonesia, 186-191.
6. Ullah, S.; Choi, J.; and Oh, H. (2020). IPsec for high speed network links: Performance analysis and enhancements. *Future Generation Computer Systems*, 107, 112-125.
7. Chandrana, N.R.; and Manuel[b], E.M. (2016). Performance analysis of modified SHA-3. *Procedia Technology*, 24, 904-910.
8. Stevens, M.; Bursztein, E.; Karpman, P.; Albertini, A.; and Markov, Y. (2017). The first collision for full SHA-1. *Proceedings of the Annual International Cryptology Conference*, 570-596.
9. Al-Odat, Z.; and Khan, S. (2019). The sponge structure modulation application to overcome the security breaches for the MD5 and SHA-1 hash functions. *43rd Annual Computer Software and Applications Conference*, 1,. 811-816.
10. Cortez, D.M.A.; Sison, A.M.; and Medina, R.P. (2020). Cryptographic randomness test of the modified hashing function of SHA256 to address length extension attack. *Proceedings of the 2020 8th International Conference on Communications and Broadband Networking*, 24-28.
11. Ramya, P.; and SairamVamsi, T. (2019). Securing MANETs using SHA3 Keccak algorithm. *International Conference on Intelligent Computing and Communication Technologies*, 328-335.
12. Prachi.; and Jora, N. (2015). Mobile IP and comparison between mobile IPv4 and IPv6.*Journal of Network Communications and Emerging Technologies*, 2(1). 72-77.
13. Ahmed, N.; Sadiq, A.; Farooq, A.; and Akram, R. (2017). Securing the neighbour discovery protocol in IPv6 state-ful address auto-configuration. *2017 IEEE Trustcom/BigDataSE/ICESS*. Sydney, Australia, 96-103.
14. Shah, J.L.; and Parvez, J. (2016). IPv6 cryptographically generated address: Analysis and optimization. *Proceedings of the International Conference on Advances in Information Communication Technology & Computing*, 1-6.

15. Kumar, G.; and Tomar, P. (2020). IPv6 addressing scheme with a secured duplicate address detection. *IETE Journal of Research*, 1-8.
16. Lee, S.; Jeong, J.P.; and Park, J. (2016). DNSNA: DNS name autoconfiguration for internet of things devices. *2016 18th International Conference on Advanced Communication Technology* , 410-416).
17. Ahmed, A.S.A.M.S.; Hassan, R.; and Othman, N.E. (2017). IPv6 neighbor discovery protocol specifications, threats and countermeasures: A survey. *IEEE Access*, 5, 18187-18210.
18. Al-Ani, A.K.; Anbar, M.; Manickam, S.; Wey, C.Y.; Leau, Y.B.; and Al-Ani, A. (2019). Detection and defense mechanisms on duplicate address detection process in IPv6 link-local network: A survey on limitations and requirements. *Arabian Journal for Science and Engineering*, 44(4), 3745-3763.
19. Wouters, P.; Migault, D.; Mattsson, J.; Nir, Y.; and Kivinen, T. (2017). RFC 8221, Cryptographic algorithm implementation requirements and usage guidance for encapsulating security payload (ESP) and authentication header (AH). Retrieved from August 30, 2020, from https://www.rfc-editor.org/info/rfc8221
20. Stevens, M.; Bursztein, E.; Karpman, P.; Albertini, A.; and Markov, Y. (2017). The first collision for full SHA-1. *Annual International Cryptology Conference*, 570-596).
21. Komargodski, I.; Naor, M.; and Yogev, E. (2018). Collision resistant hashing for paranoids: Dealing with multiple collisions. *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, 162-194).
22. Leurent, G.; and Peyrin, T. (2019). From collisions to chosen-prefix collisions application to full SHA-1. *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, 527-555.
23. Kelsey, J.; Chang, S.J.; and Perlner, R. (2016). *SHA-3 derived functions: cSHAKE, KMAC, TupleHash, and ParallelHash* (NIST Special Publication 800-185). Gaithersburg: National Institute of Standards and Technology.
24. Buchanan, W.J.; Li, S.; and Asif, R. (2017). Lightweight cryptography methods. *Journal of Cyber Security Technology*, 1(3-4), 187-201.
25. UMIP (Usagi-Patched Mobile IPv6 stack). Retrieved March 1st, 2020, from https://ns-3-dce-umip.readthedocs.io/en/latest/getting-started.html
26. Pieterse, J. (2015). *Comparative Evaluation of the mobile internet protocol 6 suite*. Degree Master Thesis. University of Stellenbosch.
27. Praptodiyono, S.; Firmansyah, T.; Alaydrus, M.; Santoso, M.I.; Osman, A.; and Abdullah, R. (2020). Mobile IPv6 vertical handover specifications, threats, and mitigation methods: A Survey. *Security and Communication Networks*, 2020.
28. Perez, L.J.D.; Trujillo, L.M.G.; Cortés, N.C.; and Henríquez, F.R. (2019). On the impact of the SHA-1 collider on Mexican digital signatures with legal binding. *Computación y Sistemas*, 23(4).
29. Jara, A.J.; Lopez, D.F.P.; Zamora, M.A.; and Skarmeta, A.F. (2013). Lightweight MIPv6 with IPSec support a mobility protocol for enabling transparent IPv6 mobility in the internet of things with support to the security. *2013 IEEE Global Communications Conference.* Atlanta, USA, 2791-2797.