Enhancing IPsec Performance in Mobile IPv6 Using Elliptic Curve Cryptography

Supriyanto Praptodiyono
Electrical Engineering Department
Universitas Sultan Ageng Tirtayasa
Banten, Indonesia
supriyanto@untirta.ac.id

M. Iman Santoso
Electrical Engineering Department
Universitas Sultan Ageng Tirtayasa
Banten, Indonesia
iman.santoso@untirta.ac.id

Teguh Firmansyah
Electrical Engineering Department
Universitas Sultan Ageng Tirtayasa
Banten, Indonesia
teguhfirmansyah@untirta.ac.id

Ali Abdurrazaq
College of Education for Pure Sceince
University of Mosul
Nainawa, Iraq
aliabd@uomosul.edu.iq

Iznan H. Hasbullah
National Advanced IPv6 Centre
Universiti Sains Malaysia
Penang, Malaysia
iznan@usm.my

Azlan Osman
School of Computer Sciences
Universiti Sains Malaysia
Penang, Malaysia
azlan@usm.my

Abstract — **Internet has become indispensable to the modern society nowadays. Due to the dynamic nature of human activities, the evolving mobile technology has played a significant role and it is reflected in the exponential growth of the number of mobile users globally. However, the characteristic of the Internet as an open network made it vulnerable to various malicious activities. To secure communication at network layer, IETF recommended IPsec as a security feature. Mobile IPv6 as the successor of the current mobile technology, Mobile IPv4, also mandated the use of IPsec. However, since IPsec is a set of security algorithm, it has several well-known weaknesses such as bootstrapping issue when generating a security association as well as complex key exchange mechanism. It is a well-known fact that IPsec has a high overhead especially when implemented on Mobile IPv6 and used on limited energy devices such as mobile devices. This paper aims to enhance the IPsec performance by substituting the existing key exchange algorithm with a lightweight elliptic curve algorithm. The experiments managed to reduce the delay of IPsec in Mobile IPv6 by 67% less than the standard implementation.**

Keywords—IPsec, Security, Mobile IPv6, Key Exchange, ECP

I. Introduction

Based on the Internet world statistic published in [1], 56.1% of the world population is connected to the Internet in 2019. Since the year 2000, Internet users have gone up by 1,104%. In March 2019, there are 4,346,561,853 people communicating through the Internet. They may communicate with other people, either using fixed devices as well as mobile devices. The number of mobile broadband subscription has reached about 4.3 billion subscriptions globally [2]. This mean almost all Internet users use mobile technology to connect to the Internet. One of the reasons for the exponential growth of mobile users is because the cost of mobile broadband has become more affordable than fixed broadband. Mobile infrastructure usually utilizes wireless technology to enable quick connection for mobile devices.

Being an open network, the internet is also vulnerable to malicious activities. In the case of wireless communication, especially Mobile IPv6, the vulnerability is greater. It is because the message exchange between devices is conducted via broadcasting. The 2016 Norton cybercrime [3] reported that 87% of consumers have in-home Wi-Fi, and they engage in dangerous behaviors. However, 66% of their home connections are not protected. Hence, the condition leaves them vulnerable to hackers eavesdropping on the network and intercepting their information. Within the last year, 689 million people in 21 countries were impacted by cybercrime. Furthermore, about $126 billion were spent globally in dealing with cybercrime. It has conclusively been shown that an increasing number of wireless devices could increase the illicit cybercriminal activities that may include, but not limited to, computer hacking, malicious attacks, data forging and financial information theft.

All standard on Mobile IPv6 mandated the use of IPsec to secure the mobility support on IPv6 such as RFC 3775 and RFC 6275. The RFC 6275, the latest standard of mobility support in IPv6, has mandated the use of IPsec on establishing security association (SA) to assure the integrity and authenticity of mobility messages as the essential information [4]. The standard specifies the usage of IPsec by mandating the use of Encapsulating Security Payload [5] header in transport mode. The ESP could authenticate the data origin, provide the connectionless integrity as well as replay attack protection.

IPsec is a set of security protocol that is mandatory on the implementation of IPv6 as well as Mobile IPv6. The IPsec was standardized in RFC 4301 [6] that combines three main security protocols which are Authentication Header (AH) [7], Encapsulating Security Payload (ESP) [5] and Internet Key Exchange (IKE) [8, 9]. The primary function of AH is to assure the connectionless integrity as well as to authenticate the source of transmitted data. Also, it can be used to provide an optional service such as replay attack protection. This protocol could be implemented by itself, or in combination with ESP. The ESP itself is used to provide all functions of the AH plus the confidentiality of the data transmitted through the network.

Based on RFC 7296 [9], the IKE is a key exchange mechanism that performs mutual authentication between communication parties. It is also used to establish SA which is a set of key and policy used to secure information. In order to make the SA establishment on both ESP and AH more efficient, a shared secret information could be included. Fig. 1 shows a block diagram of information exchange between initiator and responder to initiate establishment of a SA on IKEv2. There are two pairs of messages for initiating communication (IKE_SA_INIT Request and IKE_SA_INIT Response) and authenticating identities as well as certificates (IKE_AUTH Request and IKE_AUTH Request). All messages are cryptographically protected including the keys negotiated in the first pair of initiation message.

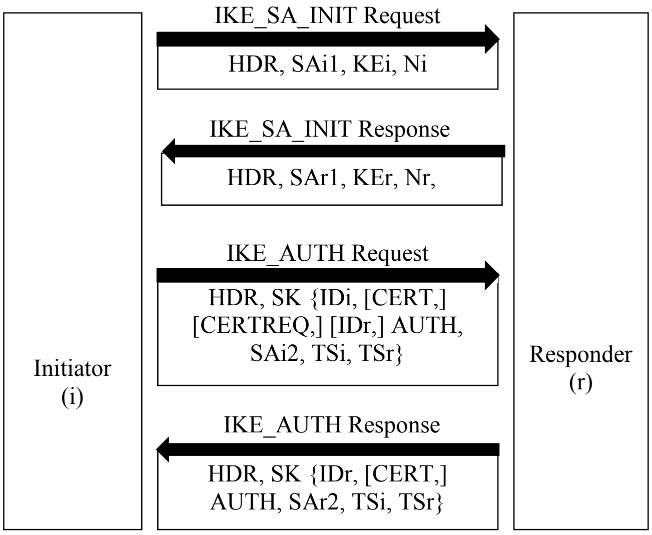


Fig. 1 Messages Exchange for Establishing SA in IKEv2

The first pair contains IKE header (HDR), SA, key exchange (KE) and nonce. The KE payload includes a Diffie Helman value. Once the responder receives the request message, it completes the Diffie Helman key exchange by sending its KE and nonce. Using the second message pair, both the responder and initiator can independently generate keying information that supports the IKE SA. The messages include a certificate containing the public key used.

A number of researchers had evaluated the use of IPsec to secure Mobile IPv6 such as [10], [11], and [12]. Jara et al. [10] analyzed the suitability of Mobile IPv6 and IPsec for resource-constrained devices. They designed, developed, and evaluated a lightweight mechanism for the integration of Mobile IPv6 with IPsec as its security feature. Their proposal considered the use of IPsec for resource-constrained device such as IoT by adding header compression as well as reduced the footprint requirements. The authors implemented a Lightweight Mobile IPv6 over Contiki OS. Their evaluation highlighted a successful offering of mobility with a handover in under two seconds. However, they also stated that IPsec introduced high latency due to the additional time required to encrypt and to send the over headed packet.

The authors of [11] surveyed the usage of IPsec in Mobile IP, especially on Mobile IPv6. It provides a study of security issues in Mobile IPv6 and the role of IPsec on securing mobile communication. As it is known, IPsec provides security to the transport layer and network layer. The study found that the security suite has 80% impact on mobile IP communication. This is because of the use of AH and ESP as the primary security protocols on IPsec which add a heavy computation task on the operation of IPsec. Both requires using internet key exchange algorithm to establish a SA. However, it is still susceptible to threats and attacks. On transport mode, even though IPsec secures host to host communication, it lacks encryption to the IPv6 header. The tunnel mode on the other hand, although does encrypts the IPv6 header as well and assigns a new header, it is not able to deliver end to end secure connection.

Performance analysis of the usage of IPsec on Mobile IPv6 was also done by Faigl et al. [12]. This paper focused on the use of IPsec on protecting Mobile IPv6 signaling. The signaling is done between Mobile Node and its Home Agent by transmitting Binding Update Message as well as Binding Acknowledgment message. The author described the overheads that were caused by the mechanism of signaling protection. They analyzed the overheads based on the queuing theory. The total response time for the mobility process in the network resulted in a high value of up to 18.5 ms.

Based on the previous studies, we can conclude that the use of IPsec to secure Mobile IPv6 introduces some overhead as well as long delay. One of the contributors to the overhead is the IKE algorithm that manages the security association establishment. The existing IPsec mandates the use of IKEv2 on the implementation of IPsec as standardized in RFC 7296 [9]. The standard defined Diffie Helman algorithm with 768-bit and 1024-bit MODP to get a shared secret key. However, the newer standard, RFC 8268 [13] stated that the usage of MODP group less than 2048-bit is no longer suggested.

This paper aims to enhance the performance of IPsec by replacing the existing key exchange algorithm with a better algorithm. We propose an algorithm based on elliptic curve algorithm [14], ECP 384-bit as the new replacement. The rest of this paper is an overview of the internet key exchange and Mobile IPv6 operation in Section 2, and methodology in Section 3. Section 4 provides result and discussion. The last part of this paper is the conclusion that will be provided in Section 5.

II. Overview of Internet Key Exchange and MIPV6

A. Internet Key Exchange on IPsec

IPsec is a security suite that integrates several security protocols as well as provides both confidentiality and integrity services. In order to ensure confidentiality, it usually uses an encryption mechanism. Based on the standard (RFC 7296), IPsec uses symmetry cryptography that requires a key exchange algorithm. The internet key exchange (IKE) is needed to define the key generation as well as to establish a secure environment for the key distribution process. The IKE consists of three protocols: Internet Security Association and Key Management Protocol (ISAKMP), a protocol that is required in establishing a SA; OAKLEY protocol to describe a series of key exchange and services provided; and SKEME, a key exchange method that provides repudiability and fast key refreshment.

There are two phases in the implementation of IKE in IPsec according to its functionality [15]:

1. Phase 1: establishing a security association
   In this phase, the two parties involved in the communication build a SA using the ISAKMP protocol. They create a virtual network that can share parameters after the SA has been established. The SA control data traffic in one direction, and hence, it needs to establish another SA to control data traffic in the opposite direction. Thus, there is a need to create a SA pair to each IPsec. It then stores the SA established in a security association database.
2. Phase 2: negotiation on providing security services
   Phase 2 involved negotiation on IPsec services such as key material as well as parameters needed. It is done

using a Quick Mode that is initiated after phase 1 is completed. Finally, the IKE defines some features in the SA that includes the encryption algorithm, hash algorithm, authentication method, and the group for the Diffie Hellman (DH) exchange.

Based on RFC 7296, the current IPsec mandated IPv6, including the Mobile IPv6 to use IKEv2. The IKEv2 consists of three phases that can be described as follows:

1. Phase 1
   In IKEv2, phase 1 begins with the initiation of IKE SA that consists of only two packets containing all the information of the four packets in IKEv1. All the packets transmitted are encrypted and authenticated by the IKE.
2. Phase 1.5
   This phase manages the IKE authentication that consists of:
   - The authentication payloads and ISAKMP identifier
   - The authentication method (RSA, PSK, ECDSA, or EAP)
   - The IPsec SA parameters
3. Phase 2
   The IKEv2 does not use Quick Mode on the negotiation between peers as in IKEv1. Once the SA has been established, phase 2 is done to negotiate the child SAs to generate a new key of the SA.

As shown in Fig. 1, the process of IKEv2 always consists of a request-response pair. The requester is responsible for ensuring the reliability and thus it sets a timeout interval. If a response is not received within the preset interval, it should retransmit the request. To deliver its function, the IKEv2 uses several cryptographic algorithms, including four transforms types: encryption algorithm, pseudorandom functions, integrity algorithm, and Diffie-Helman Groups.

B. Mobile IPv6

IPv6 (Internet Protocol Version 6) was developed by Internet Engineering Task Force (IETF) in the 90s by introducing RFC 2460 [16] that was obsoleted by RFC 8200 [17]. It includes some advantages such as offering a large IP addresses pool as well as mobility support [4]. The mobility support on IPv6 was then called Mobile IPv6 (MIPv6) that were introduced to address some weaknesses of the current Mobile IP technology (MIP) [18, 19].

One of the problems on MIP is the triangle routing mechanism that requires a long time to complete. The triangle includes mobile node (MN), home agent (HA) and correspondence node (CN). The actual communication is between the MN and CN. However, in the triangle mechanism, all message exchange between MN and CN should be routed through the HA [20]. In order to address this problem, MIPv6 introduced a route optimization mechanism that makes a direct communication between MN and CN without disturbing the HA as shown in Fig. 2.

Fig. 2 shows the communication between MN and CN without the assistance of the HA. Once MN connects to a new network, it will generate a care of address (CoA) that binds with its original address, home address (HoA). However, it should register the new CoA to its HA and CN by sending a Binding Update (BU) message. When the CN receives the BU message, it will check its binding cache to know the availability of the received CoA. If the new CoA is not in the entry, it will create an entry accordingly and then reply with a Binding Acknowledgement (BA) message.

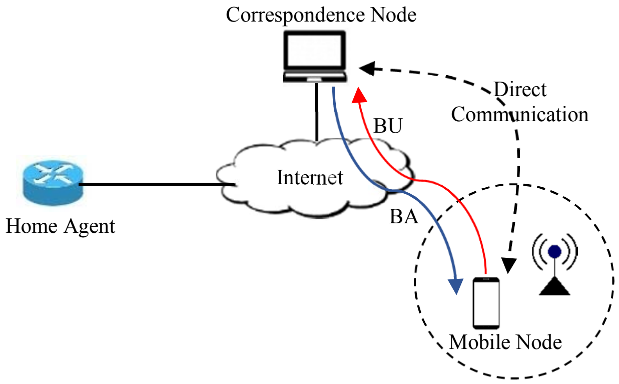


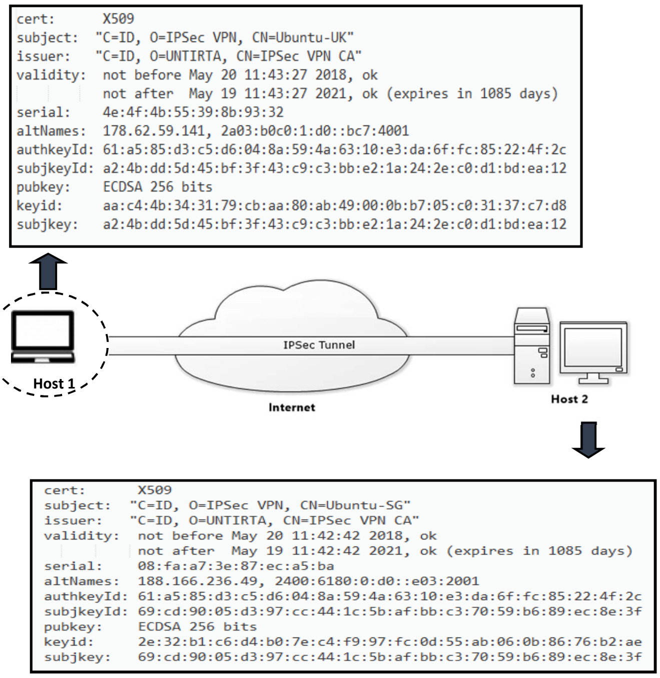
Fig.2 Route Optimization in MIPv6

The role of BU and BA message in Fig. 2 are very significant since the binding address will be used for communication. False address information will result in miscommunication. In addition, some general attacks could also manipulate these messages to perform malicious activity such as DoS attacks, Man-in-the-middle attacks, and replay attacks [21]. Thus, a security mechanism is required to protect these messages. As mandated in RFC 7296, the security of binding information should use IPsec. Hence, the performance of IPsec including key exchange algorithm must be at least favorable.

The challenge of securing BU and BA messages have attracted a number of researchers to propose various security improvements such as [22] and [23]. However, this paper focuses on the improvement of IPsec since it is the mandatory security support for MIPv6. The improvement is on the performance of the key exchange algorithm without adding a significant overhead or degrading the network performance.

III. Methodology

An experimental isolated IPv6 network testbed was set up and IPsec based on IKEv2 protocol was implemented using strongSwan software. Fig. 3 shows the network topology of the testbed including the certificate of each host. The certificate is X509 that uses elliptic curve digital signature algorithm (ECDSA) 256 bits as the public key. Once the establishment of IPsec system has been completed, further tests are conducted on the usage of the key exchange cryptography algorithm used in IKEv2 especially on the Diffie Helman Group on the key exchange process. The first test uses the existing algorithm (MODP 1024-bit), and the second test uses two candidates which are MODP 3072-bit and ECP 384-bit. The experiments measure several parameters including the time required to establish the SA and the entire delay time of IPsec implementation. This is done to find the most suitable algorithm to be implemented on Mobile IPv6.



```
cert:      X509
subject:  "C=ID, O=IPSec VPN, CN=Ubuntu-UK"
issuer:   "C=ID, O=UNTIRTA, CN=IPSec VPN CA"
validity:  not before May 20 11:43:27 2018, ok
           not after  May 19 11:43:27 2021, ok (expires in 1085 days)
serial:    4e:4f:4b:55:39:8b:93:32
altNames:  178.62.59.141, 2a03:b0c0:1:d0::bc7:4001
authkeyId: 61:a5:85:d3:c5:d6:04:8a:59:4a:63:10:e3:da:6f:fc:85:22:4f:2c
subjkeyId: a2:4b:dd:5d:45:bf:3f:43:c9:c3:bb:e2:1a:24:2e:c0:d1:bd:ea:12
pubkey:    ECDSA 256 bits
keyid:     aa:c4:4b:34:31:79:cb:aa:80:ab:49:00:0b:b7:05:c0:31:37:c7:d8
subjkey:   a2:4b:dd:5d:45:bf:3f:43:c9:c3:bb:e2:1a:24:2e:c0:d1:bd:ea:12
```

```
cert:      X509
subject:  "C=ID, O=IPSec VPN, CN=Ubuntu-SG"
issuer:   "C=ID, O=UNTIRTA, CN=IPSec VPN CA"
validity:  not before May 20 11:42:42 2018, ok
           not after  May 19 11:42:42 2021, ok (expires in 1085 days)
serial:    08:fa:a7:3e:87:ec:a5:ba
altNames:  188.166.236.49, 2400:6180:0:d0::e03:2001
authkeyId: 61:a5:85:d3:c5:d6:04:8a:59:4a:63:10:e3:da:6f:fc:85:22:4f:2c
subjkeyId: 69:cd:90:05:d3:97:cc:44:1c:5b:af:bb:c3:70:59:b6:89:ec:8e:3f
pubkey:    ECDSA 256 bits
keyid:     2e:32:b1:c6:d4:b0:7e:c4:f9:97:fc:0d:55:ab:06:0b:86:76:b2:ae
subjkey:   69:cd:90:05:d3:97:cc:44:1c:5b:af:bb:c3:70:59:b6:89:ec:8e:3f
```

Fig. 3. Network Topology of Testbed and Host's Certificate

Similar with the previous experiment conducted in [24], several scenarios were conducted to select one of the two candidates of key exchange cryptographic algorithms running on an IPsec system to replace the current one. Furthermore, three algorithms, as follows, were tested:

1. MODP 1024-bit, the currently used algorithm
2. MODP 3072-bit, an algorithm with longer key length as recommended by RFC 8268
3. ECP 384-bit, a lightweight elliptic curve algorithm

IV. Result and Discussion

An analysis on the Diffie Helman algorithm is done prior to the experiments. The important step on the Diffie Helman algorithm is the selection of a prime n umber. For the two candidates, their primes are shown in Equation 1 for 3072-bit MODP group and Equation 2 for 384-bit ECP group, respectively. Based on the prime calculation equation, the MODP group is more complex than the ECP group.

$$P = 2^{3072} - 2^{3008} - 1 + 2^{64}\{[2^{2942\pi}] + 1690314\} \quad (1)$$

$$p = 2^{384} - 2^{128} + 2^{96} + 2^{32} - 1 \quad (2)$$

The ECP group uses integer arithmetic modulo as in Equation 2, which is more efficient compared to binary field arithmetic used in MODP group. The number 384 means the ECP uses elliptic curve, as shown in Equation 3 with field size of 384. The values of Group Prime, Group Curve and Group Order for this field are from RFC 5903 [25]:

Group Prime:

```
FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE
FFFFFFFF 00000000 00000000 FFFFFFFF
```

Group Curve:

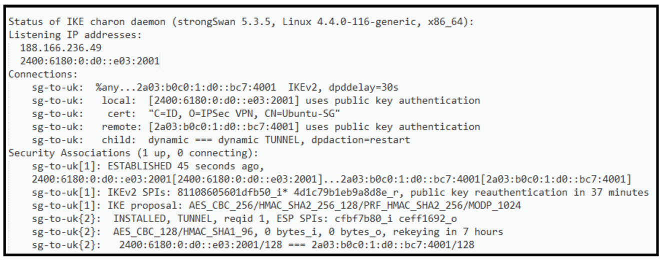
```
B3312FA7 E23EE7E4 988E056B E3F82D19
181D9C6E FE814112 0314088F 5013875A
C656398D 8A2ED19D 2A85C8ED D3EC2AEF
```

Group Order:

```
FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF
FFFFFFFF FFFFFFFF C7634D81 F4372DDF
581A0DB2 48B0A77A ECEC196A CCC52973
```

$$y^2 = x^3 - 3x + b \quad (3)$$

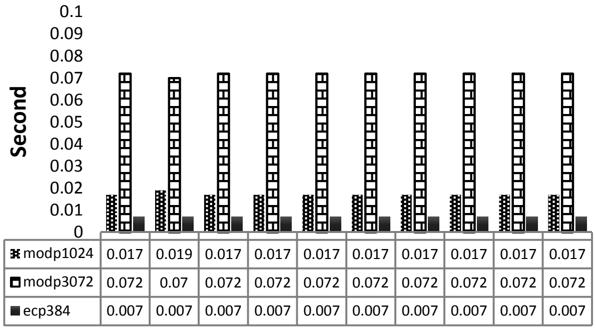
Experiments were done by implementing IPsec, including IKEv2 with three algorithms listed in Section 3. This section shows the results of the experiments. To compare the performance of the three algorithms, two-time parameters were recorded, including time required to establish SA and the IPsec delay. Since one of the well-known weaknesses of IPsec is the long delay due to the complex cryptographic algorithm, a lightweight algorithm is expected to improve this aspect. Fig. 4 shows the IPsec status of one of the hosts involved in the communication.



```
Status of IKE charon daemon (strongSwan 5.3.5, Linux 4.4.0-116-generic, x86_64):
Listening IP addresses:
  188.166.236.49
  2400:6180:0:d0::e03:2001
Connections:
    sg-to-uk:  %any...2a03:b0c0:1:d0::bc7:4001  IKEv2, dpddelay=30s
    sg-to-uk:   local:  [2400:6180:0:d0::e03:2001] uses public key authentication
    sg-to-uk:    cert:  "C=ID, O=IPSec VPN, CN=Ubuntu-SG"
    sg-to-uk:   remote: [2a03:b0c0:1:d0::bc7:4001] uses public key authentication
    sg-to-uk:   child:  dynamic === dynamic TUNNEL, dpdaction=restart
Security Associations (1 up, 0 connecting):
    sg-to-uk[1]: ESTABLISHED 45 seconds ago,
    2400:6180:0:d0::e03:2001[2400:6180:0:d0::e03:2001]...2a03:b0c0:1:d0::bc7:4001[2a03:b0c0:1:d0::bc7:4001]
    sg-to-uk[1]: IKEv2 SPIs: 81108605601dfb50_i* 4d1c79b1eb9a8d8e_r, public key reauthentication in 37 minutes
    sg-to-uk[1]: IKE proposal: AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_1024
    sg-to-uk{2}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: cfbf7b80_i ceff1692_o
    sg-to-uk{2}:  AES_CBC_128/HMAC_SHA1_96, 0 bytes_i, 0 bytes_o, rekeying in 7 hours
    sg-to-uk{2}:   2400:6180:0:d0::e03:2001/128 === 2a03:b0c0:1:d0::bc7:4001/128
```

Fig. 4. IPsec Status on the Host

Fig. 4 shows the IPsec status of host that is connected to the IPv6 network. From the IPsec status, several information related to the connection can be seen, such as the authentication that is used by the host with a public key that indicates the use of digital signatures; there is also IKE_SA_INIT information of Internet Key Exchange (IKE) proposal containing AES_CBC_256/HMAC_SHA1_96 as the encryption algorithm and MODP-1024 as Diffie-Hellman's key exchange algorithm for the first scenario. The second and third scenarios use MODP-3072 and ECP-384, respectively, as the key exchange algorithm. Fig. 5 demonstrates the time required by each algorithm on generating itself.



▨ modp1024	0.017	0.019	0.017	0.017	0.017	0.017	0.017	0.017	0.017	0.017
□ modp3072	0.072	0.07	0.072	0.072	0.072	0.072	0.072	0.072	0.072	0.072
■ ecp384	0.007	0.007	0.007	0.007	0.007	0.007	0.007	0.007	0.007	0.007

Fig. 5. The time required to generate the key exchange algorithm

The experiments on generating key exchange algorithm were repeated 10 times. ECP-384 shows a constant time (0.007 s) for all experiments. It performed the fastest compared to other algorithms based on MODP group. A faster process on generating key exchange algorithm could reduce the potential threat for DoS attacks. Typically, DoS attacks are done by bombarding the target with many requests to overwhelm the processing task of the target. The more complex the process, the higher the chance of the attack to succeed, and vice versa. If the generation time is shorter, then more time and resources will be needed by the attacker to succeed.

Once the key exchange algorithm is generated, the IKEv2 establishes an SA using the corresponding algorithm. Table 1 shows the time required by each key exchange algorithm to create an SA. Theoretically, the time it takes for key generation correlates to the time for SA establishment; the faster the key generation, the faster the SA establishment. The experiments were repeated 10 times. The table includes the average time, minimum time, maximum, and deviation. The results show that on average, ECP-384 requires the least amaunt of time to complete. It requires 67% less time compared to MODP-1024. On the other hand, the completion time increased by 123% when using MODP-3072.

TABLE 1. THE TIME REQUIRED TO ESTABLISH A SECURITY ASSOCIATION

Time required	MODP-1024	MODP-3072	ECP-384
Average (s)	0.398	0.887	0.132
Minimum (s)	0.311	0.763	0.092
Maximum (s)	0.488	1.026	0.187
Deviation	0.057	0.063	0.036

In term of deviation of the algorithms, ECP-384 also outperformed the other algorithms. The deviation of 0.036 for ECP-384 is the smallest of the three, which means it has the highest stability. From the result, it is clear that ECP-384 is the fastest on the SA establishment. Since the establishment is done inside IPsec, it should positively influence the overall delay of the IPsec implementation on Mobile IPv6. This is clearly presented in Fig. 6 which shows the IPsec delay using the three algorithms.

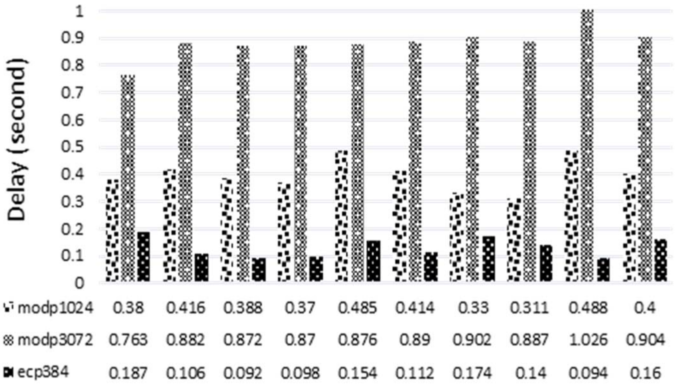


Fig. 6. Delay on IPsec Implementation

The experiments to measure the delay of IPsec implementation, including the key exchange as well as SA establishment were conducted and repeated 10 times. The results showed that ECP-384 has the lowest delay compared to the others. It is evident that the elliptic curve algorithm performed better than the existing algorithm used currently by IPsec. Based on the results, the ECP-384 is the most suitable candidate to be implemented in IPsec to secure Mobile IPv6. Any resource-constrained device using Mobile IPv6 could gain increased lifetime by reducing its energy consumption with faster IPsec configuration. However, it is worth noting that the key exchange is not the only overhead contributor in IPsec. There are also other cryptographic algorithms in IPsec implementation such as encryption algorithm to provide confidentiality and to hash MAC to ensure the integrity of messages.

V. CONCLUSION

Most Internet standards mandated the use of IPsec to secure the Internet layer for both IPv6 and Mobile IPv6. IPsec as the security protocol involves some complex cryptographic computation, including the key exchange mechanism. The latest standardized algorithm on the key exchange is IKEv2 that is used to establish an SA. The IKEv2 uses Diffie Helman Group algorithm to do the key exchange. Since IPsec has been well-known and well-documented to require heavy computation for use in Mobile IPv6, especially on resource constrained device, it needs a lightweight key exchange algorithm. The selection of key exchange cryptography is required. This paper proposes two candidates to replace the current algorithm, which are MODP-3072 and ECP-384.

Results of the experiments confirmed that ECP-384 is less complex and thus more lightweight than MODP-3072. The 384-bit cryptography of Elliptic Curve Group Modulo a Prime (ECP) can offer the best result in terms of key generation and cryptographic performance when applied to IPsec. Furthermore, if it is implemented on the Mobile IPv6 environment, the enhancement of its security can be reached. In addition, it will enhance the network performance in general, compared to other cryptographic algorithms as suggested by NSS.

AKNOWLEDGMENT

This research was supported by the Directorate General of Higher Education, Ministry of Research, Technology and Higher Education, the Republic of Indonesia in collaboration with National Advanced IPv6 Centre, Universiti Sains Malaysia and the University of Mosul, Iraq.

REFERENCES

[1] Internet World Statistics. http://www.internetworldstats.com/, last accessed 2019/03/31.

[2] Sanou, B., ICT Facts and Figures 2017, I.T.D. Bureau, International Telecommunication Union, 2017.

[3] Norton, Semantec, "2016 Norton Cyber Security Insights Report," [Online], http://now.symassets.com/. 2018.

[4] Perkins, C., D. Johnson, and J. Arkko, "Mobility Support in IPv6," RFC 6275, 2011, [Online]. Available: http://www.rfc-editor.org/info/rfc6275.

[5] Kent, S., "IP encapsulating security payload (ESP)," RFC 4303. 2005. [Online]. Available: http://www.rfc-editor.org/info/rfc4303.

[6] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol," RFC 4301, 2005, [Online]. Available: http://www.rfc-editor.org/info/rfc4301.

[7] Kent, S., "IP authentication header," RFC 4302. 2005, [Online]. Available: http://www.rfc-editor.org/info/rfc4302.

[8] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol," RFC 4306. 2008, [Online]. Available: http://www.rfc-editor.org/info/rfc4306.

[9] Kaufman, C., “Internet Key Exchange Protocol Version 2 (IKEv2),” RFC 7296, 2014, Available: http://www.rfc-editor.org/info/rfc7296.

[10] Antonio J. Jara, David Fernandez, Pablo Lopez, Miguel A. Zamora, and Antonio F. Skarmeta, Lightweight MIPv6 with IPsec support, Mobile Information Systems, 2014, Vol. 10, pp. 37–77.

[11] Khan, R. A., & Mir, A. H. IPsec in Mobile IP: A Survey. Network Journal, 2012, 4(6).

[12] Faigl, Z., Fazekas, P., Lindskog, S., & Brunstrom, A. Performance analysis of IPsec in mobile ipv6 scenarios. In: 2007, 16th IST Mobile and Wireless Communications Summit 2007, (pp. 1-5).

[13] M. Baushke, “More Modular Exponentiation (MODP) Diffie-Hellman (DH) Key Exchange (KEX) Groups for Secure Shell (SSH),” RFC 8268, 2017. [Online]. Available: http://www.rfc-editor.org/info/rfc8268.

[14] Miller, V. S. Use of elliptic curves in cryptography. In Conference on the theory and application of cryptographic techniques 1985, pp. 417-426. Springer, Berlin, Heidelberg.

[15] Caldera, J., De-Niz, D., & Nakagawa, J. “Performance analysis of IPsec and IKE for mobile IP on wireless environments”. Information Networking Institute, Carnegie Mellon University. 2000.

[16] Deering, S. and R. Hinden, “Internet Protocol Version 6 (IPv6) Specification”, RFC 2460, 1998, [Online]. Available: http://www.rfc-editor.org/info/rfc2460.

[17] Hinden, R., “Internet protocol, version 6 (IPv6) specification”. RFC 8200, 2017, [Online]. Available: http://www.rfc-editor.org/info/rfc8200.

[18] Perkins, C.E., “Mobile ip*”.* IEEE Communications Magazine, 1997, **35**(5): pp. 84-99.

[19] Calhoun, P. and C. Perkins, “Mobile IP network access identifier extension for IPv4”, RFC 2794, 2000, [Online]. Available: http://www.rfc-editor.org/info/rfc4301.

[20] Koo, J.-D. and D.-C. Lee, “Extended ticket-based binding update (ETBU) protocol for mobile IPv6 (MIPv6) networks”. IEICE transactions on Communications, 2007, **90**(4): pp. 777-787.

[21] Mankin, A., “Threat models introduced by Mobile IPv6 and requirements for security in mobile IPv6”. IETF draft-ietf-mipv6-scrty-reqts-02. txt, 2001.

[22] Rajkumar, S., M. Ramkumar Prabhu, and A. Sivabalan, “Securing binding updates in routing optimizaton of mobile IPv6*”.* Research Journal of Applied Sciences, Engineering and Technology, 2012. **4**(12): pp. 1633-1636.

[23] Mathi, S. and M. Valarmathi, “An enhanced binding update scheme for next generation internet protocol mobility”. Journal of Engineering Science and Technology, 2018. **13**(3): pp. 573-588

[24] Praptodiyono, S., Furqon, M., Maulana, A., Hasbullah, I. H., & Rehman, S. U. “Performance Analysis of Internet Key Exchange Algorithms on IPsec Security Association Initiation”. In: MATEC Web of Conferences 2018, Vol. 218, p. 03001. EDP Sciences.

[25] Fu, D. E., and Solinas, J. A. “Elliptic curve groups modulo a prime (ECP Groups) for IKE and IKEv2”. RFC 5903, 2010, [Online]. Available:http://www.rfc-editor.org/info/rfc5903.