DOI: https://doi.org/10.33103/uot.ijccce.22.3.14

The Techniques of Based Internet Key Exchange (IKE) Protocol to Secure Key Negotiation

Zainab Kareem Mahyob[1], Raheem AbdulSahib Ogla[2], Suhiar Mohammed Zeki[3]
[1,2,3]Computer Sciences Department, University of Technology, Baghdad, Iraq
[1]cs.19.16@grad.uotechnology.edu.iq, [2]110137@uotechnology.edu.iq, [3]110121@uotechnology.edu.iq

Abstract *— The Internet is a massive network that connects millions of users from all over the world and the data transmitted via it needs great protection, especially since that are in the age of big data. To solve part of this problem, IPsec was utilized, which is a set of protocols necessary to offer security to units of the Internet in general and the IP layer in particular. It is mostly based on major exchange protocols. The most frequent mechanism for transferring key materials and establishing security linkages between two entities is Internet Key Exchange (IKE). In the present work, it is proposed to use a public key that works together with Diffie-Hellman cryptography and the main advantages of a single-stage contribution (as opposed to the two-stage in standard IKE) it is better in terms of improved transfer and time (more time for the corresponding negotiation) to make the proposed IKE more secure with Simple account constraints*

Index Terms— *IPsec; Internet Key Exchange (IKE) protocol; Security Association (SA).*

I. INTRODUCTION

The Internet has become a giant network that connects millions of people around the world today [1]. However, there are risks associated with this medium, including loss of privacy, data security, impersonation, and denial-of-service attacks Internet Protocol Security (IPsec) provides a wide range of services, including data integrity, authentication, confidentiality, and access control, to address most of these issues [2].

Diffie-Hellman cryptography depends on the keys exchanged between two parties, as each party will exchange the secret key to encrypt a message, as well as it depends on the symmetric key exchange for both encryption and decryption [3].

In the present work, an encrypted public key with Diffie-Hellman was used to make IKE more secure and efficient. With fewer computational complications. The paper will be organized as follows: the first section is an introduction; the second section is about the background IPsec and IKE. The third section explains the literature survey, the fourth section explains the proposed protocol, the fifth section contains security analysis against attacks, the sixth section contains the experimental results, and the seventh section explains the discussions and the seventh conclusion of the paper.

II. BACKGROUND IPSEC AND IKE

IPsec is an IETF protocol suite that provides Internet Protocol (IP) security [4] IPsec has two protocols, Authentication Header (AH) [5] which provides data integrity and authentication, while the second protocol is Encapsulating Security Payload (ESP) [6] which provides data confidentiality as well as data integrity and authentication as well as by using cryptographic key management techniques and protocols (IKE) .The IPsec security association is done through IKE. To get started, there must be a mutual authentication between the two IPsec parties. It creates a shared secret key. And in the end it negotiates the parameters of IPsec SA [7] as shown in *Fig. 1*.

The IKE is often based on the NSA-designed ISAKMP (Internet security association and key management protocol) (National security agency) [8] To perform mutual authentication between two

Received 26/December/2021; Accepted 29/January/2022
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.22.3.14

IPsec peers, a secure IPsec association is provided by IKE [9] Two communication entities/security gateways connect with each other to execute mutual authentication, produce shared secret session keys, and negotiate and exchange confidential settings in the security association (SA). Key-related materials, cryptographic methods, and other parameters are among those exchanged as a part of the SA life cycle, as well as the security parameter index (SPI) [10] Phase 1 and phase 2 of the IKE are key negotiation phases [11] Phase 1 establishes the IKE SA, and Phase 2 establishes the IPsec SA. Since IKE SA is protecting Phase 2 negotiations, Phase I negotiations are a major concern. Phase 1 of IKE has eight different variations. As a result Main and Aggressive modes of exchange are available, however in many circumstances, phase II of IKE is implemented in a single-mode known as "quick mode," which employs three messages to establish the IPsec protocol's SA in a single step [12].

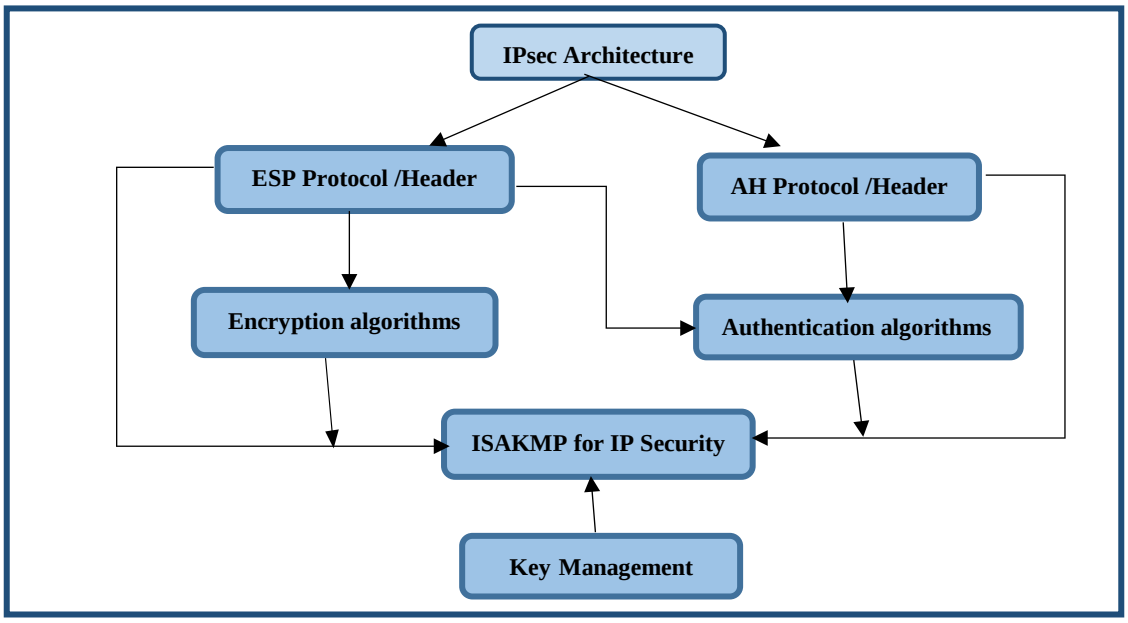

FIG. 1. STRUCTURE OF IPSEC [13].

III. LITERATURE SURVEY

As shown in Table I, this section presents the comparison of prior thoughts and research connected to the IKE Internet Key Exchange. The researchers used a variety of Internet key exchange strategies, as revealed in our analysis of their study.

TABLE I. SUMMARY OF LITERATURE REVIEW

Title	Authors	Research Concept(s)
Formal analysis of efficiency and safety in IPSec based on internet key exchange protocol	In 2015 M. Ahmim et al. [14]	Suggested the development of an efficient and high-security IKE protocol by using the Elliptic Curve Cryptography (ECC). Automated Validation of Internet Security Protocols and Applications (AVISPA) tools reveal that our contribution can withstand attack types such as DoS and man-in-the-middle based on our security analysis and formal verification.
Impact of IPSec on Real Time Applications in IPv6 and 6to4 Tunneled Migration Network	In 2015 J.L .Shah et al. [15]	IPSec implementation in IPv6 and 6to4 Tunneled Migration Networks is empirically investigated in this study. The study is important because it examines how security affects performance and how it can be mitigated. OPNET Simulator ver. 14.5 is used for simulations and measurements.

Received 26/December/2021; Accepted 29/January/2022
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.22.3.14

Proposed Pseudo Random Generator Based on RC5 Block Cipher	In 2017 A.T. Hashim et al. [16]	Fast and accurate 64-bit random number generators can be generated by applying RC5 encryption round functions with minor adjustments in the key usage, where two keys are employed with an initial vector to start the sequence generator
Performance Analysis of Internet Key Exchange Algorithms on IPSec Security Association Initiation	In 2018 S. Praptodiyono et al .[17]	All vulnerabilities of the IKE protocol have been addressed Some encryption algorithms were used and evaluated in IPv6 network to find out the best encryption algorithm for IPsec
Formal verification of the Internet Key Exchange (IKEv2) security protocol	In 2020 Ninet et al. [18]	The unbounded model's non-injective agreement and injective agreement guaranties of IKEv2 have been discussed in detail using ProVerif and Tamarin. The Deviation Attack, a new sort of Denialof-Service attack that targets IKEv2, is enabled by the penultimate authentication weakness, which was previously thought to be safe.
A Comparative Study of Researches Based on Magic Square in Encryption with Proposing a New Technology	In 2021 I.M.ALattar et al .[19]	A new cryptographic algorithm based on the order five magic square method with multiple message lengths is being developed in this paper in an effort to increase the algorithm's complexity

IV. PROPOSED IKE PROTOCOL

The purpose of this research is to create a safe IKE protocol with low computational complexity by combining the DH protocol and public key cryptography.

To create an IKE protocol that is more secure than the prior protocol. So that the suggested protocol can withstand a variety of attacks, including (Dos, Man In The Middle). The Table II lists the parameters needed to calculate computational complicity.

TABLE II. NOTATION USED

ID_I : Identity of Initiator.
ID_R : Identity of Responder.
SA_i: List of Suggestions for Initiator Cryptography (IKE Security Association Suggestions)
SA : From the list of protocols given by the initiator, a respondent has selected a set of encryption protocols (the security link is specified by IKE)
$SA_{ipsec\ 1}$: The initiator's list of cryptographic suggestions (security association proposals of IPsec).
$SA_{ipsec\ 2}$: Responses to the initiator's list of cryptographic protocols (security association selected of IPsec).
H(.):Hash function.
K_{IR}: The two-party derived session key : utilizing symmetric cryptography with a key K_{IR}.

The following data can be utilized in any type of cookie of either the Initiator (C_I) or the responder (C_R):

- A protocol hash value, an IP address, and a port number
- The initiator is access to a secret random number, (or responder).
- A timestamp

In messages 1 and 2 , Cookies are sent by both initiators and responders in the headers of subsequent messages. <C_I, C_R>.

A- The proposed algorithms

Internet Key Exchange Protocol between initiator and transponder is depicted in Table III and includes six phases.

Received 26/December/2021; Accepted 29/January/2022

 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.22.3.14

TABLE III. DEDICATE THE PHASES OF INTERNET KEY EXCHANGE PROTOCOL

Phase 1: Initiator → Responder: SA , C_I **The initiator creates a cookieC_I and sends the responder a SA proposition series of cryptographic proposals**
Phase 2: Responder → Initiator: C_I, C_R, SA_r **The respondent selects the SA_r from the appropriate SA_i and sends the SA_r to the initiator as well as the cookie pairs, It has the ability to reject the entire SA chain. and send an error message if the SA_r does not approve it.**
Phase 3: Initiator → Responder: C_I, C_R, X{g. p}{HASH($CERT_I$)} $PUBKEY_R(N_I)$, $PUBKEY_R(ID_I)$ **There are many operations that the initiator performs:** **The initiator sets the identity, both are encrypted with the public key of the responder in addition to the use of DH cryptography .Through the HASH, the initiator identifies a valid respondent if it reduces the appropriate values for the initiator's authentication.**
Phase 4: Responder → Initiator: C_I, C_R, Y, $PUBKEY_I$, (ID_R) **The initiator's public key is used to encrypt the responder's identification before it is send it back to the initiator.**
Phase 5: Initiator → Responder : E {$SA_{ipsec\ 1}$, H(SA_{ipsec1})} **The initiator calculates the K_{IR}, encrypts the $SA_{ipsec\ 1}$, send it to the responder, and encrypt it using the K_{IR} key.**
Phase 6: Responder → Initiator : E_{KIR} {$SA_{ipsec\ 2}$, H($SA_{ipsec\ 2}$)} **The respondent performs the following operations upon receiving the initiator's message: It decodes the received and encrypted messages by using the K_{IR} key, it chooses the appropriate SA. If the respondent does not approve, then the entire is rejected. Otherwise, it sends E {$SA_{ipsec\ 2}$, H ($SA_{ipsec\ 2}$) to the initiator again.**

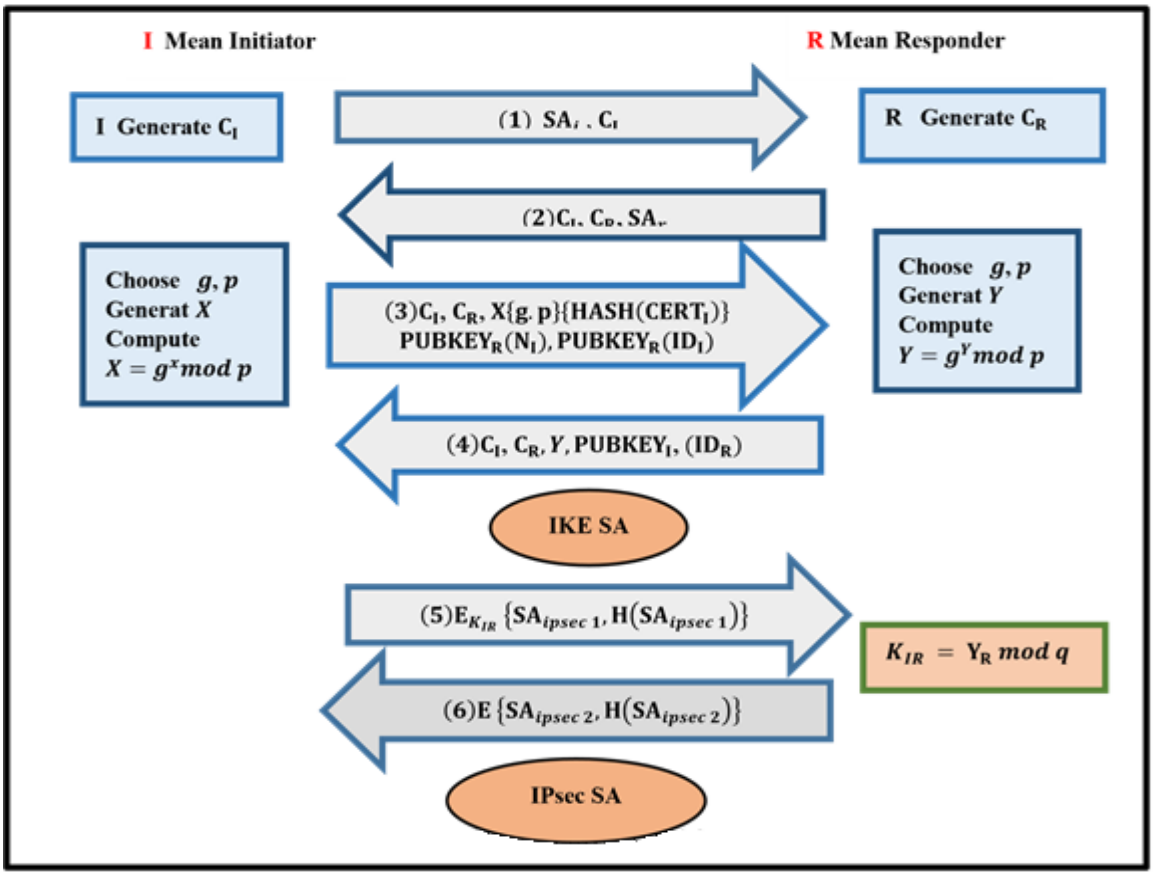

FIG. 2. I. PROPOSED IKE PROTOCOL.

Received 26/December/2021; Accepted 29/January/2022

 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.22.3.14

V. ANALYSIS OF SECURITY

This section discusses the susceptibility of the proposed protocol to counteracting some attacks

A- Replay attack

In the proposed protocol for message exchange contains the initiator/cookie responder's (C_I/C_R), an IP address, port number, protocol, as well as a secret random number known only to the parties involved, are utilized to generate this hash code. This means that an attacker can easily find the timestamp of a prior cookie and replicate a previous message. This means that a replay attack will be prevented by the suggested protocol.

B- Man-in-the-middle Attack

To prevent man-in-the-middle attacks, the proposed IKE protocol uses a public key certificate for authentication in phase 1. For this reason, the attack is thwarted in *Fig. 2* by authenticating messages 3 and 4 that include the responder and initiator's identities as well as symmetric public keys.

C- Denial-of-service (DoS) attack

To prevent a denial of service attack, the initiator's cookies are included in every payload sent. (C_I) and responder (C_R). Due to the fact that the sender will not receive a reply message if an attacker uses a bogus IP address as an initiator, he cannot return the same cookie. As a result, A DoS attack may not be achievable using the suggested IKE protocol.

D- The attack of the man in the middle

The flexibility to address it Through the N1 used in the proposed protocol, where which is refer to the confidential information between the initiator and the responder, and N1 can be effective to authenticate both parties in the face of a man in the middle attack.

E- Identification privacy

Since messages 2 and 3 of the proposed phase I protocol are encrypted with the public key, the identities of (I) and (R) are hidden.

F- Key control

Any pre-shared secret to generate a new shared session key that hasn't been used in the proposed protocol and allows the initiator/responder key control.

G- Efficiency

There are three exchanges of messages in the six-stage proposed protocol, the first four messages are utilized to generate the IKE SA, and the remaining two are used to create $SAipsec$, which is protected with the shared session key.

VI. EXPERIMENTAL RESULTS

In comparison to the proposed system, it depicts the number of sent messages during the first and second stages of the IKE protocol *Fig. 3*.

Received 26/December/2021; Accepted 29/January/2022

 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.22.3.14

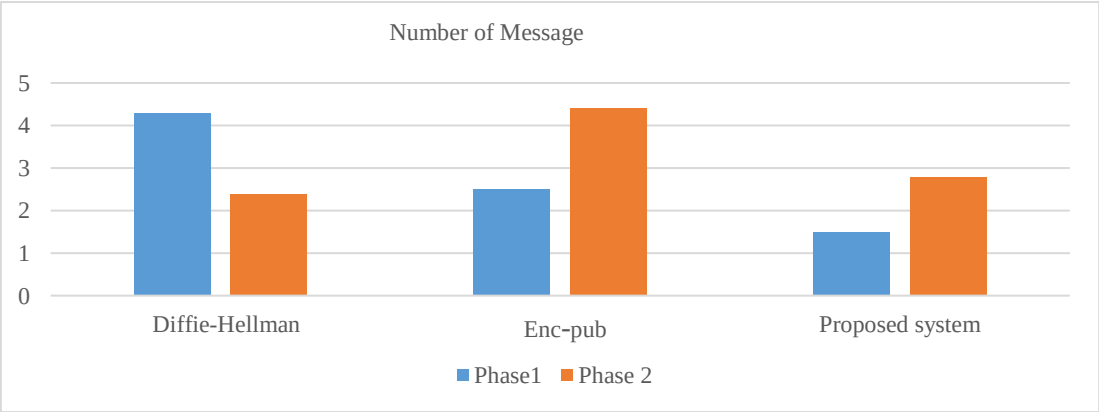

FIG. 3. NUMBER OF MESSAGE.

VII. DISCUSSIONS

Here in this section, Many results that appeared in the proposed protocol are discussed, which are the speed of complexity analysis key exchange.

A. key exchange generation speed

The suggested algorithm's performance was compared to other strategies in *Fig. 4* by exchanging one pair of keys and measuring the time it took to generate a new key. Only then can the algorithm's performance be evaluated on a platform that does not yet support IPsec. Key creation experiments are provided in Table III for DH, encrypted Public key and the suggested algorithm. The proposal took less than 0.01 seconds, followed by DH and then the public key, as evidenced by the table's findings.

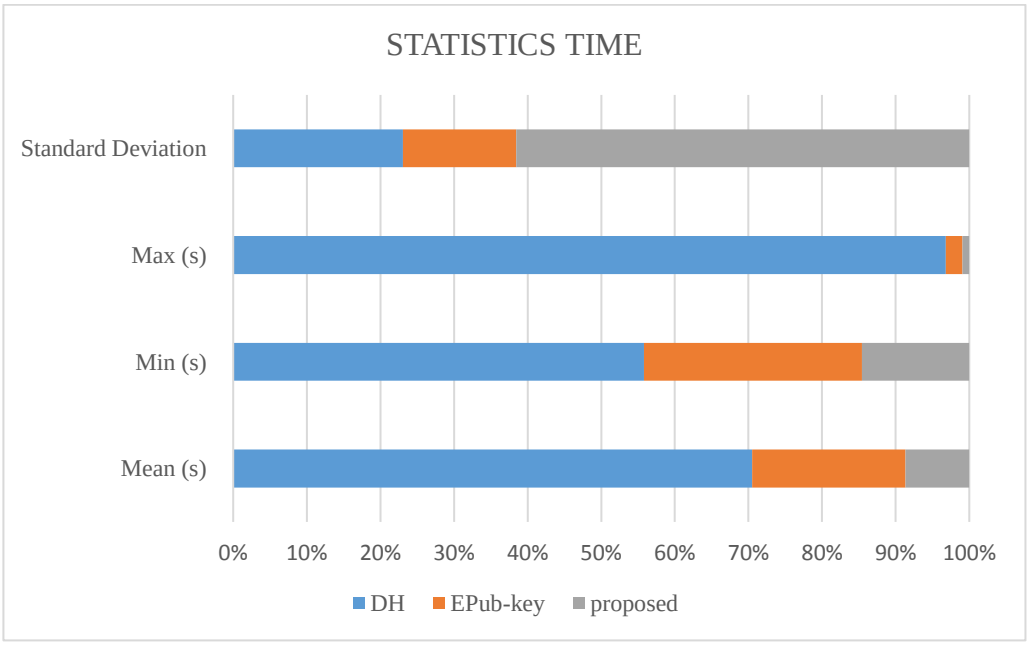

FIG. 4. STATISTICS TIME FOR KEY EXCHANGE GENERATION.

Received 26/December/2021; Accepted 29/January/2022

 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.22.3.14

B. Complexity analysis

The following operations are used to evaluate the complexity of the IKE protocol: message number key decryption, hash function and digital message encryption in the first stage or/and in the second stage. Some operations will be compared to illustrate the complexity of the proposed protocol and these operations: (Hash function, input/decryption confidentiality, public key input/decryption, decryption number in the first stage and the message number in the second stage),The proposed protocol uses two messages to generate IPsec-SA, Four messages for mutual authentication and shared key generation. IKE-SA generation, two hash functions and so on, the proposed protocol provides simple computational complexity that can compute the number of message, efficiency and processing speed with a high level of security. The proposed IKE significantly enhances processing speed by using symmetric encryption rather than the EPub-key, DH approaches as it is used in the current ways. As a result, the efficiency of the proposed protocol is reduced as shown in Table IV.

TABLE IV. COMPLEXITY ANLYSIS

Parameters	EPub-key	DH	Proposed
No.of msg exchange in phase 1	6	4	4
efficiency	0.0054	0.0037	0.112
Processing speed	0.0031	0.0011	1.001

VIII. CONCLUTIONS

The Internet consists of network layer security protocol, which is IPsec, therefore this protocol consists of secondary and necessary protocols to achieve security, which are AH, ESP and IKE .This paper proposes a method of using the public key encrypted with the DH to make the IKE more safe and has a secret to face attacks, in addition to, this method has many advantages, including the ability to respond to attacks by the man in the center and denial of service as well as the ability to analyze many of the various other attacks.

REFERENCES

[1] K. Amadasun, M. Short, J. Agajo, K. U. Osigwelem, and J. O. Egwaile, "A Secured Network Prototype for Enhanced Connectivity in Hospital Environment for Remote Patient Monitoring," *J. Commun. Comput.*, vol. 16, pp. 6–18, 2021.

[2] H. Haddad, M. Berenjkoub, and S. Gazor, "A proposed protocol for internet key exchange (IKE)," in *Canadian Conference on Electrical and Computer Engineering 2004 (IEEE Cat. No. 04CH37513)*, 2004, vol. 4, pp. 2017–2020.

[3] N. A. Lal, "A Review Of Encryption Algorithms-RSA And Diffie-Hellman," *Int. J. Sci. Technol. Res.*, vol. 6, no. 07, 2017.

[4] M. Maryanto, M. Maisyaroh, and B. Santoso, "Metode Internet Protocol Security (IPSec)
Dengan Virtual Private Network (VPN) Untuk Komunikasi Data," *PIKSEL Penelit. Ilmu Komput. Sist. Embed. Log.*, vol. 6, no. 2, pp. 179–188, 2018.

[5] S. Raza, C. Keppitiyagama, and T. Voigt, "Security and Privacy in the IPv6-Connected Internet of Things," *Secur. Cyber-Physical Syst.*, vol. 241, 2015.

[6] M. Hellsing and O. Albin, "Efficient Multi-Core Implementation of the IPsec
Encapsulating Security Payload Protocol for a Single Security Association." 2018.

[7] W. Easttom, "Virtual Private Networks, Authentication, and Wireless Security," in *Modern Cryptography*, Springer, 2021, pp. 299–317.

[8] H. Tan, M. Ma, H. Labiod, A. Boudguiga, J. Zhang, and P. H. J. Chong, "A secure and authenticated key management protocol (SA-KMP) for vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 9570–9584, 2016.

[9] G. Lopez-Millan, R. Marin-Lopez, and F. Pereniguez-Garcia, "Towards a standard SDNbased IPsec management framework," *Comput. Stand. Interfaces*, vol. 66, p. 103357, 2019.

Received 26/December/2021; Accepted 29/January/2022

 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.22.3.14

[10] S. Pérez, D. Garcia-Carrillo, R. Marín-López, J. L. Hernández-Ramos, R. Marín-Pérez, and A. F. Skarmeta, "Architecture of security association establishment based on bootstrapping technologies for enabling secure IoT infrastructures," *Futur. Gener. Comput. Syst.*, vol. 95, pp. 570–585, 2019.

[11] I. Cisco Systems, "Internet Key Exchange for IPsec VPNs Configuration Guide," no. 6387, pp. 2–7, 2018.

[12] T. Kivinen, "Minimal Internet Key Exchange Version 2 (IKEv2) Initiator Implementation," *Internet Requests Comments, RFC Ed. RFC*, 2016.

[13] Y. Zhu and D. Zhou, "Security Technology of Wireless Sensor Network Based on IPSEC," in *The International Conference on Cyber Security Intelligence and Analytics*, 2020, pp. 92–97.

[14] M. Ahmim, M. Babes, and N. Ghoualmi-Zine, "Formal analysis of efficiency and safety in IPSec based on internet key exchange protocol," *Int. J. Commun. Networks Distrib. Syst.*, vol. 14, no. 2, pp. 202–218, 2015.

[15] J. L. Shah and J. Parvez, "Impact of ipsec on real time applications in IPv6 and 6to4 tunneled migration network," in *2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*, 2015, pp. 1–6.

[16] A. T. Hashim and Z. M. Radeef, "Proposed Pseudo Random Generator Based on RC5 Block Cipher," *IRAQI J. Comput. Commun. Control Syst. Eng.*, vol. 17, no. 1, 2017.

[17] S. Praptodiyono, M. Furqon, A. Maulana, I. H. Hasbullah, and S. U. Rehman, "Performance Analysis of Internet Key Exchange Algorithms on IPsec Security
Association Initiation," in *MATEC Web of Conferences*, 2018, vol. 218, p. 3001.

[18] T. Ninet, "Formal verification of the Internet Key Exchange (IKEv2) security protocol." Université Rennes 1, 2020.

[19] I. M. ALattar and A. M. S. Rahma, "A Comparative Study of Researches Based on Magic Square in Encryption with Proposing a New Technology," *IRAQI J. Comput. Commun. Control Syst. Eng.*, vol. 21, no. 2, 2021.

Received 26/December/2021; Accepted 29/January/2022

 ISSN (Print) 1811-9212 *ISSN (Online) 2617-3352*