Mutual Friendly Force Identification Protocol based on Hash-Chain for Personal Combat Systems

Jongkwan Lee*
Department of Computer Science, Korea Military Academy
Seoul, 01805 – Republic of Korea
[e-mail: jklee64@kma.ac.kr]
*Corresponding author: Jongkwan Lee

Received January 6, 2020; revised February 17, 2020; revised May 31, 2020; accepted July 9, 2020; published September 30, 2020

Abstract

In this paper, we propose a hash-chain based friendly force identification protocol for personal combatants equipped with a personal combat system in a tactical wireless network. It is imperative in military operations to effectively and quickly identify friendly forces. If the identification of friendly forces is not correct, this can cause friendly fire. In current ground operations, the identification of friendly forces by personal combatants is neither secure nor safe. To address this issue, the proposed protocol uses a hash-chain to determine if a detected person is friendly. Only friendly forces with the same materials that are assigned before they deploy can construct an initial hash-chain. Moreover, the hash-chain is changed at specific times. The performance of the proposed protocol is evaluated on the assumption that the secret key is leaked, which is the worst scenario in the security research field. We verify that the proposed protocol is secure for the various attack scenarios, such as message replay attack, fabrication attack, and Denial of Service attack.

Keywords: Mutual Identification Protocol, Hash-Chain, Friendly Force Identification, Tactical Wireless Networks, Personal Combat System

1. Introduction

The personal combat system is a kind of weapon system that combines combat equipment, such as the personal equipment and clothes of a combatant, with advanced technology, to maximize the capability of each soldier. It has been actively researched for personal combat systems, due to the reduction of troops, and the emergence of advanced technologies. Personal combat systems will utilize a variety of state-of-the-art technologies, such as Iron Man in the movies, to provide new capabilities that can overcome human physical and mental limitations.

The most basic and most important information for effective combat for the individual soldier is where we, our friendly force, and our enemy. A critical function in military operations is also to be able to distinguish whether a detected object is friendly or not. It is because the actions after recognizing of the opponents are significantly different, depending on whether the opponent is friendly.

In modern warfare, Identification Friend or Foe (IFF) identifies whether detected weapons, such as fighters, war vessels, and tanks, are friendly or not. IFF is a radar-based identification system, a kind of transponder that listens for a request signal, and then sends a response consisting of a unique signal [1]. Unlike what the name implies, IFF can only positively identify friendly objects, not hostile ones. It is challenging to distinguish between enemy forces and friendly forces. The distinction is only between friendly and non-friendly. The reasons why a detected object did not respond appropriately in the identification of friend or foe can be very diverse. However, it is significant to identify the detected entity as friendly. It is because it helps avoid friendly fire, which is an attack by a friendly personal combatant.

Then, personal combatants performing near-field operations identify friendly forces in a relatively primitive way. In general, the way a personal combatant identifies whether a detected person is friendly or not is either to make a specific mark promised in advance or to require an appropriate response to a question at close range. The first method is easy and straightforward, but it has the disadvantage that it can easily be exposed to the enemy, as well as the friendly force. In other words, the enemy can easily pretend to be friendly. The second method is not exposed easily to the enemy, but it can be hazardous if the unidentified person is not friendly, because it must be within the effective range of personal weapons. Thus, conventional identification, which is primarily used in ground combat operation, is not adequate to safely and quickly identify friendly forces. Therefore, in this paper, we propose a mutual identifying protocol based on a hash-chain to identify friendly forces unambiguously.

The contribution of this paper is threefold. First, we propose a mutual friendly force identification protocol that does not require a separate authentication server required in many existing authentication protocols. Considering a battlefield environment where wireless channels cannot always be guaranteed, a separate authentication server cannot be operated. Second, we defined the operation model and threat model for friendly force identification, considering the battlefield environment's characteristics. Third, in terms of security, the proposed protocol is mathematically analyzed to provide guidelines for adjusting protocol parameters according to security requirements.

This paper is composed as follows. Section 2 reviews related works. Section 3 explains the system model and the threat model. Section 4 describes the proposed identification protocol in detail, while Section 5 analyzes its performance. Finally, Section 6 concludes the paper.

2. Related Work

The problem of identifying a friendly force in a military operation is similar to a general authentication problem. Many researchers have studied effective authentication protocols considering specific operation environments, such as the Internet of Things (IoT), sensor networks, and Vehicular Ad-hoc Networks (VANET) [2–6]. On the other hand, few studies have considered military operations. However, existing authentication protocols can be used to identify friendly forces. In this section, we review typical researches related to the proposed protocol.

In general, the authentication protocols for sensor networks or IoT devices have focused on lightweight schemes due to resource limitations [7, 8]. A continuous authentication protocol for the Internet of Things in [9] is presented based on the Shamir (t, n) secret sharing scheme. Only hash and MAC algorithms are employed for the protocol, and only two transactions are required. Thus, the protocol provides efficient authentication in terms of computation cost compared to conventional protocols based on the symmetric and asymmetric key operations. However, nodes participating in the authentication procedure must store a secret material securely used as a basis for authentication. If the secret material is exposed for any reason, the protocol is no longer secure. The mutual authentication method for sensors in IoT environment was proposed applied by S/Key technology based on a hash –chain [10]. This method is robust against replay attacks and man-in-the-middle attacks but requires an intermediate node to relay messages between the base station and the sensor. It is not suitable for military operational environments.

The basic structure of VANET is composed of Trusted Authority (TA), Road-Side Units (RSUs), and vehicles. TA is responsible for registration and secret key distribution for all RSUs and vehicles, while RSU is a communication relay between TA and vehicles [11]. The vehicle must transmit and receive data from the remote TA via the nearby RSU for authentication. In other words, long-distance communication should be guaranteed. RSU in VANET acts as a communication infrastructure so that the long-distance communication is possible. Thus, this is not a full *ad hoc* network. Also, if there are problems with the TA, the entire authentication system will not function properly. Moreover, vehicle-to-vehicle authentication is usually not considered.

Vijayakumar et al. proposed the dual authentication protocol in VANETs, divided into three phases [12]. To join VANET, a vehicle sends an authentication material to TA through RSU to demonstrate its legitimacy. The material is double encrypted with the vehicle secret key and the RSU secret keys. On receiving the encrypted material, TA decrypts and authenticates the vehicle. After that, TA sends an authentication code (AC) to the vehicle through the RSU. AC is a kind of token to indicate that the vehicle has legitimately joined the VANET. Although the authentication protocol is computationally efficient, it is designed for VANET, so the inherent drawbacks described above cannot be overcome.

Cryptographic hash functions are widely used in the authentication protocol because of their inherent useful properties. The hash function is deterministic and quickly computes the hash value of a given message. It is also practically impossible to predict a message that generates a given hash value. Some studies have used a hash-chain as an authentication material, taking advantage of the property that it is impossible to invert the previous hash value from the current hash value.

Some protocols, such as TESLA [13] and TAM [14], use a one-way hash-chain to authenticate a message source. Identifying the source of the message is the same as identifying friendly forces in a military operation. The authentication code is attached to

messages, and the authentication key to be verified is delivered separately, after the message is delivered. That is, there is the disadvantage that the authentication request cannot be processed in real-time, and a delay time occurs. The inability to identify friendly forces within a short time can be a fatal drawback due to the time-sensitive nature of military operations. Lamport suggested the use of hash-chains as password authentication in an insecure environment [15]. The method is easy to implement and provides sufficient security for distributed client/server interactions. However, it is not suitable for peer-to-peer authentication environments.

It is not appropriate to use existing authentication protocols to identify friendly forces in military operations. Authentication protocols that consider sensor networks or IoT devices cannot satisfy all security requirements for military operations because they cannot use sufficient computation power with limited resources. Since the authentication protocol considering the VANET environment requires a centralized TA to perform the authentication and assumes the infrastructure, such as RSUs, it is challenging to apply it to military operations, a full *ad hoc* network. Therefore, we propose a friendly force identification protocol considering the characteristics of military operations.

3. System Model and Threat Model

In this section, we explain the military operation environment of the personal combatants, attack scenarios, and security requirements we consider in this paper.

3.1 Military operation environment of the personal combatants

We define three types of range: maximum communication range (MCR), maximum surveillance range (MSR), and maximum effective range (MER). First, MCR means the maximum range that combatants with portable communication equipment can transmit a message without error. Second, MSR is defined as the range for which combatants with portable surveillance equipment can recognize an unidentified object as a person. Note that the combatants are not sure whether the found person in the range is a friendly force or not, due to lighting or climate conditions. Third, MER means the maximum range that an average soldier can score 50 % hits with a portable weapon on a person.

We assume that the MER is the smallest, the MSR is larger than the MER, and the MCR is the largest. This is because weapons cannot be used without the detection of a target, and the communication distance is generally longer than the surveillance distance. Since the unidentified object is not even detected outside the MSR, it is impossible to identify a friendly force outside the MSR. On the other hand, if the identification process for friendly forces is performed within the MER, that process can be attacked by the unidentified person, which is very dangerous. Therefore, the identification process should be performed outside MER and inside MSR.

Meanwhile, it is natural that the MSR is a part of the MCR. It means that communication with the detected objects is possible at the point. Therefore, it is possible to identify whether the person who is detected but unidentified is friendly or not, by data exchange.

Fig. 1 shows the relationship between MER, MSR, and MCR. The figure shows that the person outside MSR is hidden because the personal combatant has no way of recognizing the other's existence. The person inside MSR can be detected, but is unidentified, due to several reasons. As described above, the identification process must be completed within the area indicated in the dark color in **Fig. 1**.

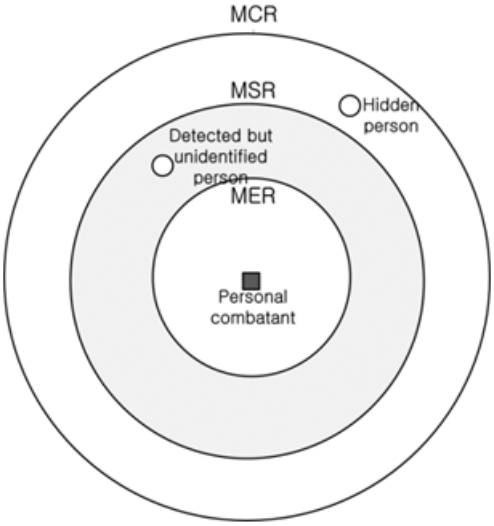

Fig. 1. The Relationship between MER, MSR and MCR

Table 1. The notations used in this paper

Symbols	Description
r_1, r_2	Pre-shared secret keys
T	Period the new hash is added to the hash-chain
L	Maximum length of the hash-chain
n	Number of times the identification process is performed during the period of T
$E(M, k)$	Encrypt message M with key k
$H(M)$	Hash message M
B_i^j	Identifier of hash that is added from the beginning by j^{th} and added by i^{th} in currently valid hash-chain
$i\|\|j$	Concatenation of i and j

3.2 Attack scenarios and security requirements

In this paper, we assume that an enemy located within the signal transmission and reception range of the personal combatant can receive all signals between the transmitter and the receiver. In other words, the enemy can receive all the messages transmitted for the identification process between the personal combatant and the detected person. Therefore, the following types of attack scenarios are possible.

First, the enemy can perform a message replay attack. It is a type of network attack in which the transmission of a legitimate message is maliciously repeated or delayed. This attack allows personal combatants to identify the enemy as a friendly force. Second, the enemy can perform a message fabrication attack. The attacker can extract meaningful data from the received signal and modify it, which may interfere with the normal identification procedure. Third, Denial of Service (DoS) attacks can be performed by repeatedly requesting

identification procedures. The personal combatants cannot carry out the normal identification procedure, due to unnecessary identification procedures by the enemies.

The following security requirements are needed to address the attack scenarios described above. The first security requirement is to be safe from the message replay attack. The best way to respond to the attack is to prevent the reuse of data used, such as employing the one-time password (OTP). Another way is that the message used in the identification procedure should only be valid for a certain period. The second security requirement is that all messages must be encrypted, and the integrity of the received message must be assured. It should not be possible for the enemy to extract meaningful data from the received signal, and legitimate participants in the identification procedure must be able to assure that the received message is error-free. The third requirement is to be able to respond to the DoS attack. To achieve the requirement, fraudulent participants should not be able to participate in the identification procedure repeatedly. For this purpose, mutual identification should be made.

4. Proposed Scheme

In this section, we describe the detail of the proposed identification protocol. **Table 1** shows the notation used in this paper to explain the proposed protocol.

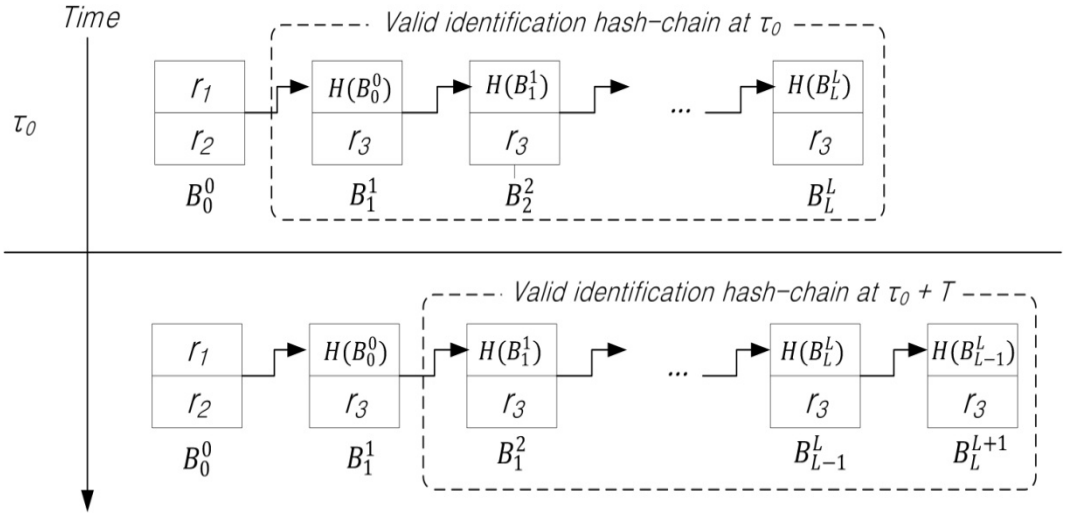

Fig. 2. The architecture of the proposed identification hash-chain

4.1 Hash-chain

The random numbers r_1 and r_2 are assigned equally to all combatants before field deployment. Note that combatants stand by at a safe zone where enemy threats do not exist before being committed to the battlefield. In other words, r_1 and r_2 are initially assigned without the risk of exposure. All items of communication equipment of the valid combatants generate the origin block by concatenating r_1 and r_2. They generate identification hash blocks independently, using the previous block every time interval T. The i^{th} block consists of the hash value of the previous block and r_3, which is the combination of the first half of r_1 and the second half of

r_2. Thus, the blocks are connected with the hash value. The r_3 and i^{th} block can be expressed as follows:

$$r_3 = upper(r_1) \vee lower(r_2) \tag{1}$$

$$B_0 = r_1 \vee r_2 \tag{2}$$

$$B_{i+1} = H(B_i) \vee r_3 \tag{3}$$

An identification block is added every time interval T, but the maximum length of a valid hash-chain is kept at L. That is, when the length of the hash-chain becomes larger than L, the first block in the current hash-chain is deleted, and the length of the chain is maintained at L.

From now on, we express a specific hash block with a superscript and a subscript. The superscript and subscript of block identifiers represent absolute block indices and relative block indices, respectively. The absolute block index indicates the order in which blocks are generated after the initial block. On the other hand, the relative block index indicates the order in which blocks are generated in the current valid identification block chain.

If the length of the hash-chain is less than L, the absolute and relative indices are the same. However, if the length of the chain is equal to L, every time a new block is added, the first block of the current hash-chain is deleted, and the index of all blocks is decremented by one. The relative index of the newly added block is always L. **Fig. 2** represents the architecture of the proposed identification hash-chain.

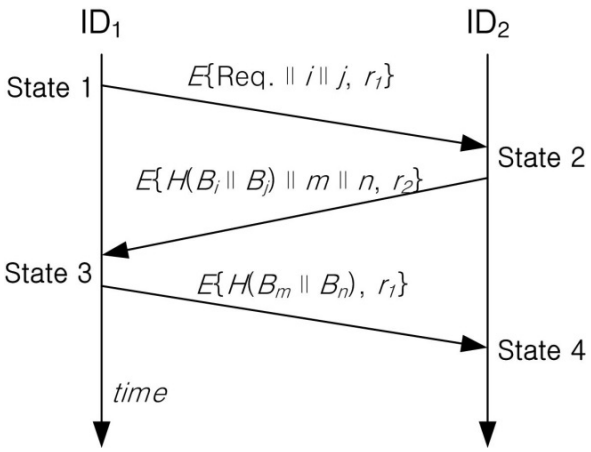

Fig. 2. Message flow diagram in the proposed protocol

4.2 Identification process

In the proposed identification protocol, two combatants (ID_1 and ID_2) are mutually identified by exchanging three messages in four stages. To make it easy to understand the identification process, we assume that two integers are used for the identification query. Depending on the security requirements, more than two integers can, of course, be used.

- Stage 1: ID_1 encrypts a request message with two integers (i, j) less than L, and transmits it to start the identification process. The integers are an identification query for ID_2.

- Stage 2: ID_2 who receives the request message decrypts it with r_1, and verifies the two integers, i and j. Then, ID_2 generates hash value of the concatenation of the i^{th} and j^{th} hash blocks, which is a response to the identification query. The hash value and two integers (m and n) that differ from the received integers are encrypted with r_2. The encrypted message is then transmitted to ID_1. The integers in the encrypted message are an identification query for ID_1.

$$E\{H(B_i||B_j)||m\,||n,\ r_2\} \tag{4}$$

- Stage 3: ID_1 who receives the message from ID_2 decrypts it with r_2, and verifies the hash values and two integers. If the received hash value matches the expected value, ID_1 identifies ID_2; otherwise, the identification process ends. After the identification of ID_2, ID_1 generates a hash value of the concatenation of the m^{th} and n^{th} hash blocks. The hash value encrypted with r_1 is transmitted to ID_2, which is a response to the identification query.

$$E\{H(B_m||B_n), r_1\} \tag{5}$$

- Stage 4: ID_2 decrypts the received message, and verifies the hashed value. If the received hash value matches the expected value, ID_2 identifies ID_1. Finally, the mutual identification process ends successfully for the two personal combatants, ID_1 and ID_2.

5. Security Analysis

In this section, we analyze the security of the proposed protocol for brute-force attack, message replay attack, fabrication attack, and DoS. The results of the mathematical analysis provide guidance for adjusting protocol parameters according to security requirements.

5.1 Brute-force attack

We assume that enemies obtain r_1 and r_2, and they response authentication queries without block chain. The total number of possible responses to a specific identification query is determined by L and α. The number is expressed as $\prod_{i=0}^{\alpha-1}(L-\alpha)$. If t is the time it takes to respond to the query, the number of times an enemy can attack during T is T/t. Therefore, the probability of a brute-force attack being successful is as follows:

$$P_s^{(BF)} = \frac{T}{t\prod_{i=0}^{\alpha-1}(L-\alpha)} \tag{6}$$

As we can see from the Eq. (6), the probability increases as T increases, and decreases as t, L and, α increase.

We can design the success probability small enough by adjusting the system parameters such as T, t, L, and α. Besides, if an incorrect response to the identification query is repeated, it can be considered an enemy and defend against the brute-force attack. Therefore, the proposed scheme is not vulnerable to brute-force attacks.

5.2 Message replay attack

The proposed scheme changes the state of the hash-chain at every period T. In other words, the hash-chain does not change state for T. Therefore, the messages used in the identification procedure are only valid for, at most, T.

An enemy who obtains r_1 and r_2 must know the identification queries and corresponding hash values used during period T to perform identification. Note that the enemy who obtains r_1 and r_2 can decrypt all messages related to the identification process, so using the same identification queries for T may allow the attacker to exploit the messages.

Let $P_s^{(MR)}$ be the probability that the same identification query is used several times during period T. The period that the authentication block chain lasts unchanged is T. During period T, there can be as many identification attempts as T/t times, and up to n ($2 \leq n \leq T/t$) identification queries are used. Note that two identification queries are used in the one identification process. It is assumed that nodes select the identification query composed of several integers randomly with a uniform distribution. Each integer indicates the hash's identifier in the current identification hash-chain. Let α be the number of integers used in the identification query. Then the number of available identification query is L^{α}, and the identification process can be performed T/t times during the period of T. Therefore, calculating the probability P is equivalent to finding the probability that the same ball will come out two or more times when L^{α} balls are taken out randomly $2 \cdot n$ times in the jar. The probability P can be expressed as follows:

$$P_s^{(MR)} = 1 - \frac{L^{\alpha}}{L^{\alpha}} \times \frac{(L^{\alpha}-1)}{L^{\alpha}} \times \frac{(L^{\alpha}-2)}{L^{\alpha}} \times \ldots \times \frac{(L^{\alpha}-2n+1)}{L^{\alpha}} = 1 - \frac{L^{\alpha}!}{L^{2n\alpha}(L^{\alpha}-2n)!} \tag{7}$$

where t is a constant determined by the frequency bandwidth and modulation method of the wireless communication device. However, T, L, and α are parameters that can be adjusted variably in system design. So we observe the value of P with changes in T, L and α.

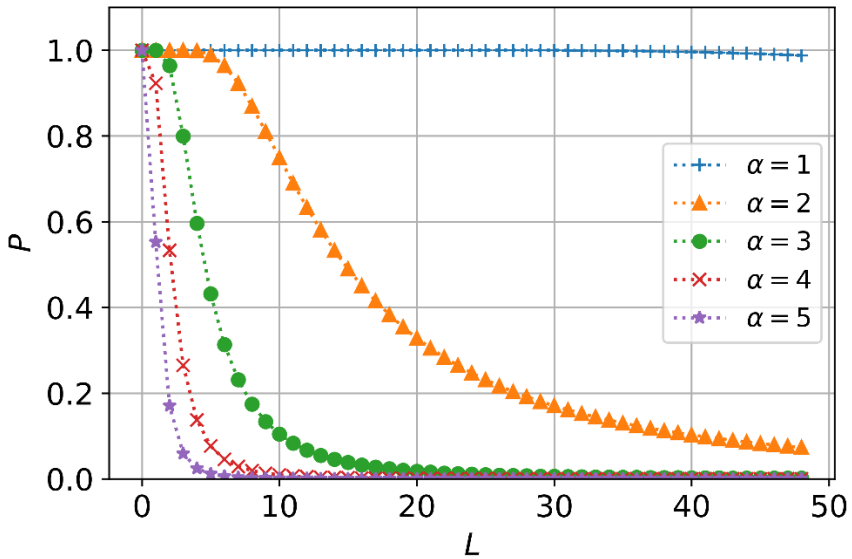

Fig. 4. The values of P with change in α and L values (T=10, t=1)

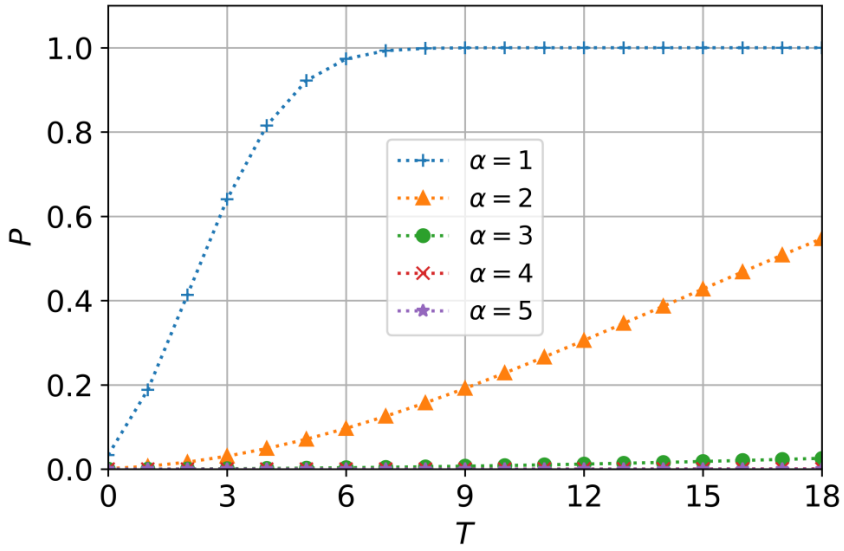

Fig. 5. The values of P with change in α and T values (L=30, t =1)

Fig. 4 shows the value of P with changes in α and L values. T and t in **Fig. 4** are set to 10 and 1, respectively. Therefore, n becomes 10. As L increases, P decreases. It is because the larger L means that the hash-chain is long enough to avoid selecting the same integer values. In addition, it is not surprising that P decreases with increasing α. It is because the larger α, the greater the number of integers to select.

Fig. 5 shows the value of P with changes in α and T values. L and t in **Fig. 5** are set to 30 and 1, respectively. As T increases (that is, as n increases), P increases. It is because the longer T means that the hash-chain remains unchanged for a longer period, and during period T, the number of times the identification query is exposed is increased by that much.

Fig. 4 and **Fig. 5** show that if the parameters α, L, and T are properly chosen, P is very small. Also, since the selection of identification query can be easily designed not to use the same query for T without random selection, the proposed protocol is safe for message replay attack.

5.3 Fabrication attack and DoS

The enemies who have obtained the secret keys can decrypt all the messages shown in **Fig. 3**, and extract information about the hash values and the integers used in the identification process. However, since the currently valid hash-chain is not exposed, the correct response to the identification query is not possible. In other words, they cannot pretend to be friendly.

However, the enemies can correctly construct the identification query that is the first message in the identification protocol. It will lead to a response message that is valuable information to reconstruct the hash-chain. Therefore, the enemies can obtain hash values corresponding to a specific integer pair by transmitting various identification queries. If they transmit sufficient identification queries, they will be able to obtain the complete information about the valid hash-chain. It also has the effect of a DoS attack. Then, the enemies who receive the response message to the identification query cannot respond to the received message, because they do not have the complete information about the currently valid hash-chain. Note that the same identification query is never used for T.

If the expected response message is not received, the opponent who had transmitted the first identification query is not convinced by a friendly force. Then, the surveillance will be enhanced, and their existence and position can be exposed. It is not what the enemy wants. Nevertheless it would be possible in a battlefield that an attacker can take the risk of exposing one's location to achieve the operational goal of disrupting communication. We can apply a basic security policy to neutralize the DoS attack, such as considering the initiator of the authentication as an enemy or ignoring the identification query for a certain period if the expected response message is not received continuously. The DoS attacks can be easily blocked. Moreover, the re-constructed hash-chain by the enemy is only valid for the period of *T*. As a result, the proposed protocol is secure for fabrication attacks and DoS attack, in terms of the operational and technical aspects.

6. Conclusion

In this paper, we proposed mutual friendly force identification protocol for the personal combatant equipped with a personal combat system in tactical wireless networks. In future warfare, the personal combatant will be able to overcome human physical and mental limitations, thanks to personal combat systems. They will be able to surveil longer, hit targets precisely, and communication effectively with others. Even if their capability improves dramatically, a military operation will not be successful if its forces cannot efficiently identify their friendly forces. It is because wrong identification causes friendly fire. The proposed protocol constructs a hash-chain that is changed at specific times, and uses a combination of hash values in the currently valid hash-chain. If the chain is not generated from the beginning, it is impossible to re-construct a valid hash-chain in limited time. The performance of the proposed protocol was evaluated on the assumption that the secret key is leaked, which is the worst scenario in the security research field. We verified that if appropriate parameters are selected, the proposed protocol is secure for the various attack scenarios, such as message replay attack, fabrication attack, and Denial of Service attack.

References

[1] Lijia Chen, Jintao Xiong, Liangchao Li, Zongjie Cao, and Jianyu Yang, "Research on a novel method for identification friend or foe based on fuzzy c-means and dynamic Bayesian network," in *Proc. of 2011 IEEE CIE International Conference on Radar*, pp. 1656-1659, 2011. Article (CrossRef Link).

[2] El-hajj, M. Chamoun, A. Fadlallah, and A. Serhrouchni, "Analysis of authentication techniques in Internet of Things (IoT)," in *Proc. of 2017 1st Cyber Security in Networking Conference (CSNet)*, pp. 1-3, 2017. Article (CrossRef Link).

[3] Chang and H. Le, "A Provably Secure, Efficient, and Flexible Authentication Scheme for Ad hoc Wireless Sensor Networks," *IEEE Transactions on Wireless Communications*, vol. 15, no. 1, pp. 357-366, Jan. 2016. Article (CrossRef Link).

[4] Rasheed and R. N. Mahapatra, "The Three-Tier Security Scheme in Wireless Sensor Networks with Mobile Sinks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 5, pp. 958-965, May 2012. Article (CrossRef Link).

[5] E. A. M. Anita and J. Jenefa, "A survey on authentication schemes of VANETs," in *Proc. of 2016 International Conference on Information Communication and Embedded Systems (ICICES)*, pp. 1-7, 2016. Article (CrossRefLink) .

[6] Meddeb-Makhlouf, N. Meddeb and M. A. B. Ayed, "An Enhanced Multilevel Authentication Protocol for VANETs," in *Proc. of 2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA)*, pp. 1232-1238, 2017. Article (CrossRefLink) .
[7] S. V. Nesteruk, V. Y. Kovalenko, and S. V. Bezzateev, "A Survey on Localized Authentication Protocols for Wireless Sensor Networks," in *Proc. of 2018 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF)*, pp. 1-7, 2018. Article (CrossRefLink).
[8] Liu, Jing, Yang Xiao, and CL Philip Chen, "Authentication and access control in the internet of things," in *Proc. of IEEE 32nd International Conference on Distributed Computing Systems Workshops (ICDCSW)*, pp. 588-592, 2012. Article (CrossRefLink).
[9] Bamasag, Omaimah Omar, and Kamal Youcef-Toumi, "Towards continuous authentication in internet of things based on secret sharing scheme," in *Proc. of the WESS'15: Workshop on Embedded Systems Security*, pp. 1-8, 2015. Article (CrossRefLink).
[10] K.H. Lee and J.S Lee, "Mutual authentication method for hash chain based sensors in IoT environment," *Journal of the Korea Academia-Industrial cooperation Society*, vol. 19, No. 11, pp. 303-309, 2018. Article (CrossRefLink).
[11] H. Liu, Y. Chen, H. Tian, T. Wang, and Y. Cai, "A novel secure message delivery and authentication method for vehicular ad hoc networks," in *Proc. of 2016 First IEEE International Conference on Computer Communication and the Internet (ICCCI)*, pp. 135-139, 2016. Article (CrossRefLink).
[12] P. Vijayakumar, M. Azees, A. Kannan, and L. Jegatha Deborah, "Dual Authentication and Key Management Techniques for Secure Data Transmission in Vehicular Ad Hoc Networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 1015-1028, April 2016. Article (CrossRefLink).
[13] A. Perrig, R. Canetti, J. D. Tygar, and Dawn Song, "Efficient authentication and signing of multicast streams over lossy channels," in *Proc. of 2000 IEEE Symposium on Security and Privacy*, pp. 56-73, 2000. Article (CrossRefLink).
[14] M. Younis, O. Farrag, and B. Althouse, "TAM: A Tiered Authentication of Multicast Protocol for Ad-Hoc Networks," *IEEE Transactions on Network and Service Management*, vol. 9, no. 1, pp. 100-113, March 2012. Article (CrossRefLink).
[15] Lamport, Leslie, "Password authentication with insecure communication," *Communications of the ACM* vol. 24, no. 11, pp. 770-772, 1981. Article (CrossRefLink).

Jongkwan Lee received the B.S. degree in electronic engineering from Korea Military Academy, Seoul, Korea in 2000, the M.S. degree in electronic engineering from Korea Advanced Institute of Science and Technology (KAIST), Daejeon, Korea in 2004, and the Ph.D. degree in Network Centric Warfare (NCW) engineering with the Ajou University, Suwon, Korea, in 2014. He has served as a military officer since 2000. Currently, he is an assistant professor at the Korea Military Academy. His research interests include network security, machine learning for military systems.