applied sciences

MDPI

Article

A Study on the Concept of Using Efficient Lightweight Hash Chain to Improve Authentication in VMF Military Standard

Dohoon Kim [1], Sang Seo [1], Heesang Kim [1], Won Gi Lim [2] and Youn Kyu Lee [3,*]

[1] Department of Computer Science, Kyonggi University, Suwon-si, Gyeonggi-do 16227, Korea; karmy01@kgu.ac.kr (D.K.); tjtkd8271@kgu.ac.kr (S.S.); victoriousian@kgu.ac.kr (H.K.)
[2] Agency for Defense Development (ADD), Seoul 05661, Korea; wklim@add.re.kr
[3] Department of Information Security, Seoul Women's University, Seoul 01797, Korea
* Correspondence: younkyul@swu.ac.kr

Received: 23 November 2020; Accepted: 14 December 2020; Published: 16 December 2020

Abstract: Authentication algorithms in the form of cryptographic schemes, such as the Secure Hash Algorithm 1 (SHA-1) and the digital signature algorithm (DSA), specified in the current variable message format (VMF) military standard have numerous reliability-related limitations when applied to tactical data link (TDL) and multi-TDL networks (MTN). This is because TDL and MTN require maximum tactical security, communication integrity, and low network overhead based on many protocol header bits for rapid communication with limited network resources. The application of such authentication algorithms to TDL and MTN in a rapidly changing battlefield environment without reinforcement measures will lead to functional weaknesses and vulnerabilities when high-level digital-covert activities and deception tactics are implemented. Consequently, the existing VMF authentication scheme must be improved to secure transmission integrity, lower network transaction, and receive authentication tactical information in VMF-based combat network radio (CNR) networks. Therefore, in this study, a tactical wireless ad hoc network topology, similar to that of the existing CNRs, is considered, and a lightweight multi-factor hash chain-based authentication scheme that includes a time-based one-time password (T-OTP) for network overhead reduction and terminal authentication is proposed, coupled with exception handling. The proposed method enhances the confidentiality of tactical message exchanges and reduces unnecessary network transactions and transmission bits for authentication flows between real-time military terminals owned by squads, while ensuring robustness in limited battlefields. Based on these approaches, in the future, we intend to increase the authentication reliability between wireless terminals in the Korean variable message format (KVMF)-based CNR networks based on the Korean Army Corps network scenarios.

Keywords: military; VMF; hash chain; T-OTP; lightweight secure hash (LSH); CNR

1. Introduction

The variable message format (VMF) [1] is a military digital information exchange standard established by the Joint Interoperability of Tactical Command and Control Systems (JINTACCS) program under the United States Joint Chiefs of Staff. It provides common interoperability standards, including command data elements and protocol standards for information transfer in command, control, communications, computer and intelligence (C4I) systems over limited battlefield networks. Further, it enables the real-time exchange of digital tactical information in surveillance systems, command and control (C2) systems, and striking systems in a limited resource-based network-centric operational environment (NCOE) using both wired and wireless

military communications. These VMF-based tactical information transmissions involve the transmission of only the required command data to minimize the message size. This technique enables faster message transmission compared to that of previous systems and presents the minimum essential technical parameters in the form of a mandatory system standard and optional design objectives for interoperability and compatibility among digital message transfer devices.

1.1. Limitations of the Authentication Process within the Existing VMF Military Standard and Importance

However, because the VMF-based tactical communication uses the Secure Hash Algorithm 1 (SHA-1)-based digital signature algorithm (DSA) as the primary authentication process without reinforcement measures, this can lead to potential limitations owing to major challenges, such as practically proven hash collision vulnerability [2–5], network overhead-based protocol format, and low transmission integrity. This will be problematic within the combat network radio (CNR) in tactical data link (TDL) networks that require maximum tactical security, communication integrity, and low network overhead based on several protocol header bits. In addition, such vulnerabilities will become limitations when high-level adaptive digital-covert activities and deception tactics are successfully implemented in hierarchical corps communication-based network-centric warfare (NCW) because of the unnecessary network transactions required for authentication. Furthermore, RSA encryption, which is primarily used for VMF authentication, will cause a slow processing speed and computational overhead when transferring secure tactical information in rapidly changing unstable battlefield networks with limited resources. Therefore, the existing VMF authentication must be improved to support the reliable transmission and reception of authentication information in limited CNRs, satisfying the requirements for military tactics, strategies, and interoperability.

To improve the overall terminal authentication scheme in VMF-based CNR networks, it is vital to introduce simplified approaches to enable rapid authentication and realize an authorization network connecting the terminals of the CNRs. In addition, a lightweight modification detection and authentication scheme with multiple exception handling processes to quickly generate small robust hash values and reduce authentication flows must be applied. To maintain communication robustness and realize network migration in a limited network environment, the following are vital: reducing unnecessary network transactions for authentication between military terminals owned by squad members; introducing advanced methods to enhance the confidentiality of tactical information exchange; and securing network transmission integrity.

However, in most VMF-based studies and related documents, the efficiency of VMF message transfer for application in the Force XXI Battle Command Brigade and Below (FBCB2)-based embedded ground weapon systems, aerospace trace tracking systems, and tactical mobile platooning communication systems for infantry position reporting has been analyzed only in terms of specialization in obtaining the interoperability and adaptability to alert propagation, fire control, tracking and striking, detection, identification, and defense systems. Differentiated research supporting authentication and data integrity between terminals in a VMF-based operating environment has not been officially reported. Therefore, with increasing cybersecurity threats and a changing NCW system, it is essential to secure military authentication based on the VMF standard.

1.2. Security Requirements for Enhancing VMF Authentication and Research Contribution

As such, the following approach to improving the VMF authentication scheme in a military CNR network based on a wireless terminal device is required.

- The feasibility of implementing a lightweight authentication and integration scheme to improve the existing VMF terminal authentication, such as a hash chain, must be analyzed. The network configuration in CNRs with hash chain-based authentication schemes must be similar to that of the dynamic military ad hoc network-based mobile ad hoc network (MANET) and vehicle ad hoc network (VANET) in the cell planning area.

- Cryptographic hash chain-based authentication and transmission integrity approaches must be considered. Interoperability within the next-generation NCW system, and technical adaptability and continuity in CNR networks with TDL, should also be ensured, and there should not be any deviations from the specifications of the existing VMF military standard.
- Rather than simply assembling the conceptual technology suggested by previous hash chain-based studies, a comparative analysis based on the pros and cons, differences, and limitations of each study should be considered to suit VMF-based CNR networks.
- Active security requirements that consider various military network scenarios must be established. Examples include a hash chain-based authentication, including a time-based one-time password (T-OTP) keyless point, low latency and transaction, robustness to external and internal auth attacks, a specialization of various FBCB2-based All-IP CNR network types, the introduction of re-authentication and revocation steps in the authentication scheme, and deep interoperability. Functional support and availability for rapidly changing battlefield environments and secure lightweight communication for covert activities are also required.

Accordingly, in this study, an authentication scheme to be employed in rapidly changing VMF-based environments is proposed. It is based on the cryptographic hash chain-based authentication technology that includes T-OTP. In particular, assuming a flexible CNR network environment, the hash chain structure is applied to various military ad hoc networks in dynamic cell planning areas, and its effectiveness is analyzed. Based on the final established authentication scheme within the military ad hoc network and the multi-factor hash chain structure, an improved lightweight authentication scheme is proposed to satisfy the demands of a rapidly changing battlefield network and any additional security requirements based on VMF standards.

1.3. Paper Organization

This hash chain-based lightweight authentication method with T-OTP, including comparative analysis of related studies and tactical network scenarios in CNR networks, is organized as follows. In Section 2, the research and standards related to the hash chain, ad hoc network, and VMF standard are introduced. In Section 3, the unique features and limitations, the advantages and disadvantages, and the applicability of the most relevant prior hash chain-based studies to VMF-based CNR networks are compared and analyzed. In addition, ad hoc network studies on utilizing and assembling such processes in the construction of a VMF-based lightweight authentication scheme are also described. In Section 4, a lightweight authentication scheme applicable to CNRs based on flowcharts and related simulation parameters is proposed. Finally, in Section 5, concluding remarks are provided. Further, the tactical background and technical limitations of the lightweight authentication scheme proposed in this study, as well as future military authentication research directions based on the Korean variable message format (KVMF) in the Korean Army Corps network, are described.

2. Background and Related Studies

2.1. VMF Authentication Improvements Based on MIL-STD-2045-47001

In the existing VMF standard applied to CNRs with TDL, the MIL-STD-2045-47001 standard defines the VMF network protocol and application header, security parameter information (SPI), and group parameter (GP). The purpose of the MIL-STD-2045-47001 standard is to stipulate the technical parameters and procedures, such as application header generation, message packaging and unpackaging, data segmentation, and assembly, which are essential for the message exchange and communication of digital tactical information between the digital message transfer (DMT) equipment and C4I systems in All-IP-based CNRs with limited bandwidth, resources, and device energy. It also presents the VMF message header, RSA-based encryption, and SHA-1-based DSA authentication rules. This determines the DSA-based authentication according to the SPI value in a VMF binary message header, which falls within the scope of this study.

The existing protocols and authentication schemes in the VMF standard have several unique characteristics.

- **Variability**—Variability minimizes message transmission and processing time by dynamically selecting only required real-time tactical messages and information when performing various operations in a limited resources-based network;
- **Bit-coded transmission**—Bit-coded transmission subdivides the transmission unit of a tactical message containing military operation information into bit and octet. It can maximize the transmission efficiency of the operational information and tactical data and ensure integrity;
- **Applicability of multiple layers**—The VMF standard is independent of arbitrary network structures applied in various types of military tactical networks. The MIL-STD-188-220 standard was applied for the physical and link layers, and the MIL-STD-6017 and MIL-STD-2045-47001 standards were applied in the application layer based on CNR networks. Therefore, the multi-layer applicability enables a configuration for the independence of the form of military tactical network and the handling of each squad's platooning behavior and related networks;
- **Integration and interoperability**—The integration of VMF is an essential feature in the design, development, testing, certification, and continuous operation of the automated tactical data system (that is, it satisfies the necessary requirements for promptly transmitting command and control information through joint boundaries). In addition, an integration is required to exchange tactical data and situation awareness information between heterogeneous weapon systems, and to exchange the command system within the allied operation in real-time through an interlocking of the joint tactical data link system (JTDLS). Currently, this is being applied, with a focus on FBCB2-based platooning networks in cell planning areas and mosaic warfare.

However, these protocols and authentication systems used in the VMF standard can cause several issues and limitations.

- **Weak authentication process by SHA-1 cryptographic hash function:** In the existing VMF military standard, the SHA-1-based DSA authentication and modification detection process is performed according to the SPI setting in a dynamic limited CNR network without additional encryption. However, SHA-1 currently has theoretical collision vulnerability and exploits a practical proof of concept (PoC). Thus, to protect confidential military information from leakage and theft in a tactical CNR network under the VMF standard, cryptographic hash-based authentication algorithms (e.g., SHA-2, SHA-3, and LSH of Korean cryptographic hash standard) that are more robust than SHA-1 are urgently required. In addition, although the SPI setting is immediately applied, it is only assumed that authentication in the current VMF-based CNR networks is safe from the perspective of the closed military network. Therefore, it is difficult to protect consistent security in CNR networks from parameter tampering because no separate encryption process in the modification detection and authentication scheme is applied (RSA public encryption may be applied in a separate protocol header area for tactical message encryption, but this may cause additional overhead on network performance and calculation).
- **Lack of factor robustness:** The existing VMF standard includes variables from a rapidly changing battlefield environment (e.g., information loss from environmental changes, latency, jitter, and authentication delay), enemy types (e.g., active and passive internal and external attackers and masqueraders), and operational environments (e.g., bandwidth, energy, frequency, squad, and resources by limited CNRs) that are not well defined. Therefore, it is necessary to introduce additional requirements and establish parameter-based measures.
- **Undefined re-authentication and revocation scheme**: The existing VMF standard does not suggest a continuous authentication scheme when it is necessary to re-establish the reliability of the participating nodes because it takes a certain amount of time after the initial authentication for the operation of the squad to be completed. In addition, processes related to authentication rejection and exclusion as well as the elimination of hostilities are not considered. Therefore, to support a

consistent authentication system in a rapidly changing VMF-based CNR network, definitions of re-authentication and revocation schemes for all nodes are urgently required.

- **Non-existent exception process:** The existing VMF standard does not provide any method for the detection, tolerance, and attenuation of node malfunctioning caused by dynamic changes in the network or enemy nodes corrupting operational data and stealing confidential information. Therefore, it is necessary to establish a variety of exception handling methods to satisfy the unique information exchange demand in the battlefield, and support both functional and structural stability. This can also be related to the following challenges: low speed and low bandwidth in real-time VMF-based CNR, the deployment of military base stations for constructing the cell planning area, guaranteeing the availability of authentication for low-spec networks, and the network delay and tolerance related to the establishment of the initial FBCB2-based CNR in mosaic warfare networks, which requires rapidity.

As described above, SHA-1 was proposed by the National Security Agency (NSA) based on message digest 4 (MD4) and adopted in DSA. However, concerns regarding the collision attack vulnerabilities of the SHA-1-based cryptographic hash function were raised in 2005. In 2017, the PoC for generating collision pairs for the SHA-1 hash function was fully released, thereby verifying its theoretical and practical vulnerabilities. As such, owing to the existing vulnerabilities of SHA-1, the VMF standard for executing the authentication scheme between terminals through the SHA-1-based DSA in CNR networks also has limitations. Applying this method to the VMF authentication scheme without overcoming these vulnerabilities can result in the exposure of operational information and the exchange of tactical data to unauthorized nodes in real-time. Even during normal confidential operations, indiscriminate intrusions by enemy forces related to authentication in a tactical network can occur without preventative and detective measures. Thus, the cryptographic hash function must be transitioned into a function with guaranteed robustness, such as SHA-2, SHA-3, or LSH, the Korean cryptographic hash standard [6].

As indicated in Table 1, when the SPI is 0, the data in the VMF-based communication channel do not go through separate one-way encryption types in the authentication and transmission processes, but do undergo one-way encryption based on the weak cryptographic hash function standard, SHA-1. This aspect can also be observed in Tables 2 and 3.

Table 1. Security parameter information type codes.

Code	Reference
0000 (0)	Authentication (using SHA-1 and DSA)/No Encryption
0001–1111 (1–15)	Undefined

Table 2. Typical SPI field sizes.

Field Name	Size (Bits)
Keying Material ID	0–64
Cryptographic Initialization	0–128
Key Token	0–512
Authentication Data (A)	320–1024
Authentication Data (B)	320–1024
Message Security Padding	0–128

Table 3. Digital signature.

Octet	Field Identification	Value
1	Block Number: Identifies specific data block.	15
2	Length: Indicates the length of the Address Designation Parameters block in octets.	Variable length: 13 + size of Digital Signature
3	Hash Algorithm: Used to produce the hash.	0 = MD5 1 = SHA-1
4	Crypto Algorithm: Identification of the crypto algorithm used to encrypt the hash to produce the digital signature.	0 = Not encrypted 1 = RSA 2–255 User defined
5–13	Key ID: signer's public key.	8 octet binary field
14-Length field	Digital Signature: Authentication of the sender of the message.	

2.2. Related Research and Improvements for Introduction of Hash Chain-Based Authentication in VMF

To overcome the limitations related to the authentication and integrity of VMF-based CNR networks, a hash chain-based lightweight authentication scheme including T-OTP should be introduced. The primary considerations of hash chain-based authentication are the security extension protocol (SEP)-related security requirements, computation and network transmission overhead, latency issues, maximum tactical security, and communication integrity. Moreover, to establish a hypothesis for these issues and provide a clear basis for further studies, the potential possibilities of applying a hash chain-based authentication structure, including T-OTP steps, proactive re-initialization for efficient network transactions, specialization of existing military ad hoc networks in cell planning areas, and the configuration of processes related to misbehaving node detection and anomaly auditing, are considered. Therefore, the unique features, advantages, and limitations described in previous related studies based on hash chain and ad hoc must be compared and analyzed for the construction of lightweight authentication in VMF-based CNR networks.

A hash chain-based one-time password, as proposed by Lamport, uses the hash values of a hash chain by applying the same cryptographic hash function in reverse order, thereby preventing the calculation of the hash value used in the next authentication session and addressing the vulnerability of a simple password [7–11]. The S/Key standard proposed by Haller et al. addresses the difficulty of reducing the calculation weight when generating and re-registering the root hash values in a hash chain structure. In addition to enhancing the efficiency in a limited network environment, this standard also prevents reuse attacks [12–14].

The timed efficient stream loss-tolerant authentication (TESLA) protocol proposed by Perrig et al. used a multi-factor method, involving message authentication code chaining and the concepts of time-delayed key disclosure and loose time synchronization. This would mitigate any vulnerabilities to theft or abuse that might arise from a non-combination with other authentication schemes, as well as overhead problems related to the hash chain initialization that were not addressed by S/Key [15–18]. Zhu et al. proposed a lightweight hop-by-hop authentication protocol (LHAP) specialized for MANET networks and related authentication based on TESLA [19,20]. Akbani et al. proposed the hop-by-hop efficient authentication protocol (HEAP) to be employed in wireless networks [21,22], thereby ensuring scalability.

In addition, Zhang et al. proposed a self-renewable hash chain (SRHC) [23], Hamdy et al. proposed an OTP-based two-factor authentication [24], and Bittl et al. proposed an efficient construction of infinite-length hash chains with perfect forward secrecy using two independent cryptographic hash functions [25], further alleviating problems related to initialization, root re-registration, and overhead in existing hash chains. Subsequently, in a T/Key study, a two-factor authentication based on T-OTP and S/Key structure was proposed that further reduced the computational overhead, compared to those in previous studies, while avoiding the storage of the client's secret key in the server [26]. Yin et al. proposed a binary hash tree-based Merkle tree structure to solve potential issues, such as the

management of the finite hash chain length, the complexity of computation according to the hash chain length, the lack of a self-reinitialization scheme, and security problems dependent on the hash chain length, related to the efficiency of T-OTP generation and verification in T/Key. Consequently, it was possible to use less storage than T/Key, lower network transactions, and maximize the efficiency of OTP generation and verification time [27].

However, despite these unique features and advantages, previous studies related to hash chain-based authentication have not presented specific exception handling concepts at an algorithmic level for functional problems that potentially arise in a rapidly changing limited battlefield network, such as VMF-based CNRs. In particular, in a low-resource wireless CNR network, where the bandwidth varies according to the layers because of dynamic operational environments, a method for specialized authentication has not been clearly described. An existing hash chain authentication approach in poor communication environments causes several restrictions to network-centric operations, and the performance of the entire network potentially deteriorates when the traffic increases rapidly, such as during wartime. In addition, these naïve hash chain-based authentications have a limitation in that their parameters do not consider the structure or functional aspects under such limited tactical circumstances. In particular, when topology update messages are periodically transmitted to prevent VMF-based CNR networks from disconnecting when the squad commander and related members perform combined platooning operations, poor communication environments may increase the corruption of the authentication status of each squad member, causing network overhead owing to transactions that are required to establish authentication.

Therefore, rather than utilizing the same existing hash chain-related authentication scheme in this military ad hoc network that focuses on cell planning areas and mosaic warfare networks, an alternative approach is necessary to identify and analyze unique features that can be optimized for All-IP or non-All-IP-based CNRs. Accordingly, a comparative analysis of the pros and cons of existing hash chain-based approaches is required.

3. Comparative Analysis of the Existing Hash Chain-Based Authentication Approaches

As described in Section 2, improvements to the DSA-based VMF message authentication processes of the existing SHA-1 are necessary, and their integrity and availability must also be secured for various limited battlefield networks. Therefore, additional requirements must be satisfied, including authentication-related elements provided in the SPI of the existing VMF authentication header; that is, data origin authentication (whether the data transmitted by the sender have been forged along the path), connectionless integrity (limited connectionless configuration for detecting any modifications or retransmissions of the tactical data while preventing hostile nodes from analyzing VMF messages, thereby preventing the identification of the sender's or receiver's tasks), and non-repudiation with proof of origin and proof of delivery. In addition, adaptability to other constraints, such as operational security (covertness), intermittent connectivity, risk of capture and compromise, and limited resources based on low bandwidth, frequency, and device energy, is required in order to operate in rapidly changing tactical network environments [28].

Accordingly, additional security requirements specific to VMF-based CNR networks for a hash chain-based authentication scheme including T-OTP are preemptively defined so as to achieve functional authentication stability over a certain level and high tactical and strategic diversity. Based on these requirements, this approach contains a comparative analysis of prior studies related to hash chains in terms of their differences, unique features, advantages, and limitations, as well as their potential for being applied to VMF-based limited tactical networks.

3.1. Definitions of Additional Tactical Security Requirements in VMF

The following additional security requirements are predefined and analyzed based on general requirements in the existing VMF standards and various national defense documents [29,30]:

- **Configuration of keyless point (CKP) (①)**—Because the hash chain-based authentication with a T-OTP value is used in a rapidly changing battlefield environment, authentication in a VMF-based CNR must be able to verify friendly tactical ad hoc networks in reliable cell planning areas and warfare networks, thereby necessitating robustness against authentication data loss. In addition, to reduce the regular authentication flow, related network overhead and the security cost of server storage after adjusting the initial tactical network, the system is configured to exclude the key ownership stage in one of the two terminals using the authentication algorithm and scheme side. Interference from a variety of environmental variables and wireless jitter must also be considered [31,32];
- **Low latency (LL) (②)**—To rapidly conduct tactical operations and insert this scheme in wireless static terminals, the entire initial authentication process of VMF must be quickly completed. Moreover, to secure the robustness of military-based adaptive strategies [33] in line with developing network technology trends, components of latency-related requirements, such as time-to-transmit, time-to-preprocessing, time-to-retransmission, and bias or noise in battlefield [34,35], based on general parameters in VMF, are reflected and must be defined [36–39];
- **Robustness to authentication attack (RA) (③)**—Security against active and passive internal and external authentication attacks on random nodes in VMF-based CNRs is necessary, which can be achieved using various defensive mechanisms, such as preventing the reuse of keys in hash chain- and state-based exception handling. In particular, the hash chain-based authentication system including a T-OTP value must be configured to minimize the impact of various ad hoc network-based wireless authentication attacks, such as rushing attacks [40] wormhole, blackhole and sinkhole attacks, jellyfish, flooding and fragmentation attacks, man-in-the-middle (MITM), eavesdropping and sniffing [41–45]. Specifically, considering the military security requirements, the resistance capabilities should focus on replay, MITM, and Byzantine authentication attacks.
- **Low authentication overhead in limited networks (LAO) (④)**—To secure interoperability across hierarchical limited-resource CNRs and connected tactical terminals with low specifications, it is necessary to minimize the authentication overhead of the computation and network transactions based on the purpose of VMF standards. In addition, unnecessary transmission and energy consumption must be reduced through exception handling, punishment, and the monitoring of participating nodes in VMF-based closed CNRs, thereby achieving higher efficiency in limited battlefields. Furthermore, it is necessary to enable rapid decision-making and provide high-quality real-time combat environment features [46];
- **Re-authentication and revocation for operations (RR) (⑤)**—Re-authentication and topology updation processes must be provided to ensure that new nodes continue to participate as legitimate nodes even after the initial authentication is completed, re-establish the reliability of internally authenticated nodes, and prevent authentication attacks in an environment where intrusions from enemy forces can lead to theft and damage. It is also necessary to develop immediate authentication rejection and routing-based removal processes for the detected hostile nodes in hash chain-based authentication, including a T-OTP value, and identify internal malfunctioning nodes through an online-based culprit recognition and detection mechanism. Furthermore, more realistic military scenarios related to authentication in VMF must be established to ensure consistent authentication capabilities in actual CNRs. These scenarios must be standardized based on previously proposed military features, such as heterogeneous velocity, tactical areas, optimal paths, obstacles, and unit join and leave scenarios [47,48];
- **Deep interoperability in authentication scheme (DI) (⑥)**—The US Army plans to employ the VMF standard for data exchange in most of its TDL- and CNR-based systems, and the US Navy uses VMF-based TDL to satisfy the tactical requirements of information exchange between ground and maritime operations. According to the unit-specific operability described in US military materials [49] published in 2008, in an actual combat environment in which 64 vehicles and one unmanned aerial vehicle are active, it is possible to observe the movement of nodes constituting

squads without disconnections. When one squad moves safely through a specific operational area, other squads often follow, confirming the presence of mobility through group units. On this basis, if multiple nodes forming a squad receive similar command data while moving as a squad, platooning at the same speed and in the same direction, it is necessary to maintain the authentication robustness of the squad CNRs at a high level to ensure the security of not only a given CNR, but also of the overall tactical environment. In addition to forming a smooth C4I between squads within the same country, it is necessary to establish combined operations with the militaries of other nations. As such, any hash chain-based authentication applied in CNRs must adhere to the interoperability demands based on the purpose of VMF standards.

3.2. Applicability Analysis of VMF-Based CNRs in Previous Studies on Hash Chain-Based Authentication

A hash chain is a cryptographic hash function-based one-way chain structure originally devised by the mathematician Lamport. By continuously calculating the hash value using a one-time password and a random value as the initial seed determined by the client, the cryptographic hash function has a preimage resistance. Therefore, it is impossible to recover the original message from the arbitrary hash value of a given message. Because one hash-based password contains both the actual data value and the hash value for the next hash-based password, it is used in the authentication process, which utilizes the continuity and sequentiality of the passwords formed in the chain structure. Therefore, by the comparative analysis of various prior authentication studies using this hash chain structure with the security requirements presented in Section 3.1, its applicability in a VMF-based CNR network in a pre-built cell planning area is determined as follows. The functional satisfaction scores in each study, presented in Table 4, are the key points required in VMF standards. In particular, to logically distinguish the satisfaction of these qualitative requirements, it is necessary to express them as relative indexes, such as weak, slightly weak, slightly strong, and strong, compared to the proposed research method.

Table 4. Taxonomy of hash chain research applicable to VMF authentication process.

	CKP (①)	LL (②)	RA (③)	LAO (④)	RR (⑤)	DI (⑥)
Haller et al. [12]	X	X	△	△	△	△
Perrig et al. [15]	X	△	▲	▲	▲	△
Zhu et al. [19]	X	△	▲	▲	▲	▲
Zhang et al. [23]	X	△	△	△	▲	△
Hamdy et al. [24]	X	△	X	▲	▲	△
Bittl et al. [25]	X	△	O	X	△	△
Kogan et al. [26]	O	△	O	△	▲	O
Yin et al. [27]	O	▲	O	▲	▲	▲

[Functional Satisfaction Score] (X = weak, △ = slightly weak, ▲ = slightly strong, O = strong).

First, Haller et al. [12] proposed "S/Key," an authentication scheme that uses an exclusive OR and a one-way chain structure based on a cryptographic hash function. This technique makes it difficult for attackers to use old message exchange information, despite the existence of all previous communications and related messages between the client and server. Moreover, because this scheme does not allow for duplicate hash values in the chain and establishes overall security based on the preimage resistance, it is suitable for lightweight authentication environments. In the S/Key standard, however, because all hash values in the one-way chain are sequential, unless a random one-time hash value is used, the hash value is valid for an indefinite amount of time and is also vulnerable to theft, abuse, race condition, loop, MITM, and small-n attacks. Therefore, the widespread use of other cryptographic protocols that can secure an entire session, and not only the password, can render S/Key insignificant if mainly used by itself. Despite these limitations, applying such features of the S/Key standard to the authentication process in VMF-based CNR networks will achieve the following:

- The basic verification and re-authentication processes can be standardized using only one S/Key structure-based hash chain without needing multiple independent keys to periodically identify normal nodes in a resource-limited tactical network;
- S/Key has an extensible structure that is easiest to employ in multi-factor authentication without duplication for a randomly exposed key or hash value;
- To transit to a joint operation front with other squads during a combined operation, interoperability is achieved by applying the S/Key-based one-way chain structure used in the previous squad unit to the new squad unit, and based on the sequential hashing process, a rapidly lightweight tactical message transmission and authentication scheme can be secured according to the VMF-based information control. Thus, the existing authentication schemes and related parameters presented in VMF standards can be satisfied and further strengthened based on S/Key as an initial interface for the construction of a lightweight authentication scheme.

Next, Perrig et al. [15] proposed "TESLA", based on the S/Key standard. Despite a recipient knowing the specific signature, the signature for the next sequence cannot be computed in advance until it is disclosed in the next time interval; therefore, malicious nodes in the network are prevented from sending packets after they have been declared false through packet theft and abuse. Thus, by applying the loosely time synchronization concept, this process handles situations in which a specific hash value for authentication is valid for an indefinite period, while reducing the overhead in generating and verifying authentication information, as compared to S/Key (aspects of network transactions and computations), expanding the recipient nodes, and preparing for a packet loss [16]. However, the TESLA authentication has limitations, including the non-guaranteed problem of non-repudiation, and the problem of storage space if packets transmitted during a specific time interval before the release of a random secret key must be continuously buffered in the receiver. Other limitations include the delayed authentication of buffered packets until the secret key is disclosed, the use of the same cryptographic hash function as that in the S/Key, and the inadequate exception handling of malicious nodes. Despite these limitations, applying the features of the TESLA standard to the authentication process in VMF-based CNR networks will achieve the following:

- TESLA is an authentication method for adding the calculated message authentication code (MAC), including a secret key generated through a hash function, to a packet based on a one-way chain. Therefore, based on the act of revealing the hash value owing to the loose time synchronization between the sender and the receiver, it is possible to minimize the exposure of information to the attacker and block false packet attacks. In addition, when there are multiple recipients in a multicast environment, quick and accurate individual authentication for each recipient can also be performed;
- The TESLA standard that was first proposed did not support non-repudiation, but TESLA++, an improved version, can secure a higher non-repudiation function than the elliptic curve digital signature algorithm (ECDSA). Through the TESLA-based VAST combined with the existing ECDSA, it is possible to derive specialization for authentication in military ad hoc networks such as VMF-based CNRs, including MANET and VANET [50];
- In addition to protection from valid authentication values that have not been used for long periods of time in VMF-based CNRs, a system can be established to monitor and identify spoofed nodes using such valid authentication keys. Moreover, hash chain-based authentication schemes can be constructed for an update and expansion of the squad member authorization list for long-term operations.

Zhu et al. [19] proposed "LHAP", which uses a TESLA-based bootstrap trust structure and a one-way chain for traffic and device authentication. As a protocol concept specialized in ad hoc networks based on MANET, this study implemented a network access control scheme while preventing unauthorized nodes from injecting traffic into a given MANET. To implement this process, each node in the network applied token-based hop-by-hop authentication before specific neighboring nodes one

hop away transmitted a random packet, thereby deleting abnormal packets. To achieve this, a structure was adopted that combined one-way chain-based authentication and trust management between nodes. Based on this lightweight structure, issues with a buffering-based authentication delay and a large-capacity storage demand owing to delayed key disclosure and loose time synchronization in the existing TESLA could be addressed. Moreover, issues related to securing independence and transparency for multiple routing protocols, increasing the authentication and computational efficiencies compared to those of TESLA, and abnormal node exception handling that was not well defined in TESLA could be addressed through a standardization based on a trust relationship. However, the limitations of the LHAP must be considered, including a central management problem in which all nodes in the network had to share the secret key in advance, a limited key maintenance package, and the increased complexity of the authentication process owing to a larger number of keys, latency caused by one node performing duplicate hashing for verification of abnormal packets and nodes, and authentication delays that could not be fully resolved owing to vulnerabilities to basic intrusion attacks such as wormhole and MITM [20,21]. Despite these limitations, applying the features of the LHAP to the authentication process in VMF-based CNR networks will achieve the following:

- LHAP was proposed to overcome the vulnerability of basic TESLA standards applied to multi-hop ad hoc networks such as MANET. Therefore, the network and computational overhead can be reduced by reducing the number and capacity of requests for nonce and hash values for initial authentication and re-initialization, and removing authentication information based on each node participating in or leaving the VMF-based ad hoc network.
- The concept of hop-by-hop access control can be realized for the behavior of malicious nodes and collaborative hostile nodes that have personal channels. In addition, the issues of exception processing for authentication delay and disconnection according to changes in the ad hoc network can be alleviated by generating a separate control packet. Furthermore, an additional lightweight authentication for distributed VMF-based WSNs can be calculated.
- Beyond filtering invalid authentication keys and packets at the authentication algorithm level, by establishing a system to authenticate and identify legitimate squad nodes and punish enemy nodes, a small-scale VMF-based CNR network specialized for more realistic battlefield environments can be constructed. Establishing trust relationships through specific keys will mitigate issues with authentication delays and network disconnections that arise in limited tactical networks and low-spec military wireless terminals.

Various studies supplementing the weaknesses of the hash chain-based authentication, including the T-OTP value, must also be analyzed, including the problems of the server-side re-registration and initialization after the hash values in the hash chain are exhausted [22], and the client-side overhead based on multiple hash calculations when the hash values are stored beforehand.

Zhang et al. [23] proposed an "SRHC" that does not require a separate re-registration, despite all hash chains being exhausted after registering the root value of the first hash chain in the Lamport's OTP. Here, during the authentication process, the bits constituting the root value of the new hash chain are transmitted to the server in advance, whereas a random hash value is transmitted through the OTP. A one-time signature (OTS) based on a cryptographic hash function standard is also applied as a secondary modification detection and authentication technique for protection against abnormal nodes and attackers during this transmission process. Consequently, all hash values in the current hash chain are exhausted, and the root value of the new hash chain is automatically registered based on a four-way protocol. However, further strategies to improve the SRHC are required owing to other limitations, such as a lack of exception handling in the case of mismatches between specific hash values of the client and server, and the computational and network overhead caused by the increasing length of the transmitted messages. Despite these limitations, applying the features and advantages of the SRHC structure to the authentication in VMF-based CNR networks will achieve the following:

- The central system will automatically mitigate the problem of separate re-initialization owing to the exhaustion of the root keys used for node confirmation, identification, and updation in VMF-based closed CNRs when conducting independent operations for long periods of time [51];
- When applying this hash chain-based authentication in CNR networks, issues such as the potentially limited operational time and resources, unnecessary network transactions associated with checking the remaining hash values, and securing independence owing to specificity in the military environment can be overcome.

Hamdy et al. [24] proposed "OTP-based two-factor authentication," an infinitely superimposed hash chain structure that applies a two-factor authentication-based multi-hash function to address the cost, time, and performance limitations of the authentication process. In this study, the hash chain generation and usage processes are applied in the forward direction, as opposed to the existing Lamport method. In addition, when the server side sends a specific index value to a client based on the hash chain generated in the forward direction, the client responds with an OTP. As such, because the cryptographic hash function operates in the forward direction rather than in the reverse direction, as in other hash chain structures, a re-registration owing to the exhaustion of the hash values is not required. However, specific strategies to improve the two-factor authentication-based infinitely superimposed forward hash chain structure are required owing to various limitations, such as the existing simple-password problem owing to the seed value being secret information immediately shared by the client and server, as well as the inability to realize the advantages of the OTP. Despite these limitations, applying the features of a two-factor authentication-based infinitely superimposed forward hash chain structure to the authentication in VMF-based CNRs will achieve the following:

- The re-initialization problem occurring from the exhaustion of keys used for authentication and updation when performing independent operations over a long period of time will be simply resolved. The performance cost owing to the participation of multiple new squad and member nodes and the establishment of a joint operation with other squads will also be minimized.

Similar to other advanced studies, to solve the problem of hash chain re-registration, an infinite hash chain technique based on the double independent hash function proposed by Bittl et al. [25] was designed such that a client had to apply a specific cryptographic hash function to a random seed value and another hash function shared by only the client and server to the output value, which was used as an OTP. Compared to the techniques used in previous studies, this technique enabled the realization of robust security at higher levels of OTP. However, this technique had a limitation in that the client and server had to share secret information, such as seed, in advance. Thus, prior studies on improving the hash chain-based OTP assumed that the secret key, cryptographic hash function, and digital signature, among other factors, were shared between the client and the server in advance. Owing to this limitation, they could not be efficiently established compared to other cryptographic primitives, which were fundamental advantages of a hash chain structure. Specific strategies to address this issue are necessary. Despite these limitations, applying the features of a double independent hash function-based infinite hash chain to the authentication process in VMF-based CNR networks will achieve the following:

- The security of the authentication in each closed CNR network will be further strengthened, and the scheme will be more robust than those in other methods against the issues of limited key maintenance, authentication delays from duplicate hashing, wormhole attacks, and MITM;
- Application of this approach also enables the conversion of the authentication scheme into one that is specialized for changing battlefields in which enemy forces employ active confusion tactics based on the network.

Kogan et al. [26] proposed a "T/Key" based on a multi-authentication scheme that combines the S/Key and T-OTP and does not store the secret key on the server. T/Key uses independent hash functions to address any potential security instabilities that arise from deriving hash values through

the same cryptographic hash function in the S/Key. In addition, regarding the vulnerability to phishing attacks owing to the indefinite validity of the hash value by applying the concept of the time interval length, the validity of a specific hash value can be limited up to only a predetermined period of time. Furthermore, to alleviate the ripple effects of preprocessing attacks, an independent salt value is assigned to each cryptographic hash function in the hash chain, thereby verifying the lower limit of the hash value for each function and establishing proper security. However, because the hash values in the T/Key structure are time-limited, the structure is significantly longer than the existing S/Key structure, thereby leading to potential structural vulnerabilities. Moreover, other potential issues, such as the management of finite hash chain length, the complexity of computation according to hash chain length, the lack of a self-reinitialization scheme, the security problems dependent on hash chain length, and the efficiency of T-OTP generation and verification, remain. Therefore, possible designs to be employed in limited-resource CNRs as well as a specific authentication formulation based on T/Key are required. Despite these limitations, applying these features of the T/Key to the authentication process in VMF-based CNR networks will achieve the following:

- Limiting the lifetime of valid authentication keys that have not been used for long periods based on a predefined time span will enable the preparation of functional countermeasures to prevent, identify, and attenuate the continuous collection of information by specialized enemy nodes and conspirator nodes;
- Laying the foundation for military cyber agility [52,53] in a limited-resource CNR, based on independent cryptographic hash functions that can be deployed at any given time for each node in a tactical network, will facilitate the development of an authentication scheme that proactively prevents intrusions from specialized hostile nodes in a battlefield environment;
- Establishing a multi-factor hash chain-based authentication process including T-OTP will secure high levels of robustness and responsiveness against any initial reconnaissance attempts by enemy nodes, maintain tactical covert activities, and maximize the covert activities of friendly forces based on a scheme specialized for low-spec and low-speed closed squad networks;
- Furthermore, the ability to easily establish joint operation systems with other squad members and foreign militaries by synchronizing the hash functions will help satisfy various interoperability-related scenarios.

Based on these potential possibilities, introducing the T/Key concept is vital for schemes related to the multi-factor hash chain-based authentication scheme including T-OTP in VMF-based CNRs.

4. Proposed Lightweight Authentication Based on Multi-Factor Hash Chain with T-OTP in VMF

This section describes the design principle, initialization and registration, authentication and verification, re-authentication and revocation, exception handling flow processes based on tactical scenarios, and multi-factor hash chain-based authentication with T-OTP that satisfy the predefined requirements of the VMF-based CNRs. In addition, the conditions and additions satisfied by the final proposed scheme are compared with those in the methods in previous studies.

4.1. Design Principle

The DSA authentication used with the existing VMF standard faces severe challenges, such as collision vulnerabilities of the SHA-1-based cryptographic hash function. In the CNR networks, any confidential tactical messages, such as situation reports, location reports, and reconnaissance reports, are exchanged in real-time according to the VMF standards. Therefore, VMF standards should be robust against cryptographic problems using strong cryptographic hash functions such as SHA-2, SHA-3, and LSH. In addition, it is also vital to secure inter-message operability for low-spec connected wireless terminals, such as position reporting equipment based on infantry communication devices, armored terminals in tank and helicopter types, and limited networks used in NCW-based tactical operations that change in real-time as well as adding a re-authentication procedure based on sudden

unexpected military operational scenarios. The concepts of our proposed processes were improved based on the multi-factor hash chain and T-OTP proposed by Kogan and Yin. The related authentication scheme, with multi-factor hash chain and T-OTP values that satisfy the overall requirements of the existing VMF standards, is illustrated in Figure 1.

① Initialization and registration phases: The OTP seed hash generation in an LSH-based multi-factor hash chain between the administrator (the military authority or the commander of squad) and the user (the connected wireless device or squad member) in CNRs.

② Authentication and verification phases: Rapid authentication and verification with time-stamp-based clock synchronization values for T-OTP, and the limitation of the lifetime of arbitrary hash values in a hash chain that have not been used for a long time.

③ Re-authentication and revocation phases: Tactical scenario-based network regularization of authentication status and exception handling for CNRs, including wireless terminals.

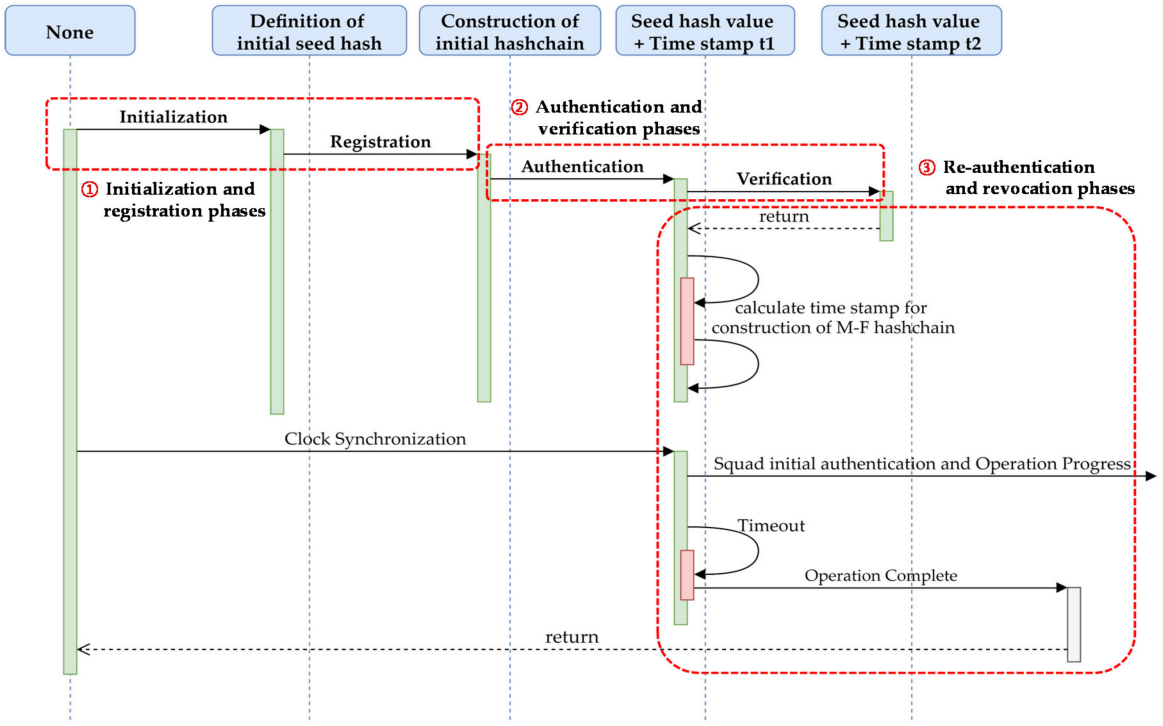


Figure 1. Proposed overall authentication scheme with multi-factor hash chain and T-OTP in VMF.

The proposed processes included three specific phases: initialization and registration, authentication and verification, and re-authentication and revocation. The scheme proposed in this study used the hash value of the LSH-based hash chain with T-OTP in the CNR networks, including wireless military devices and internal terminals. After the initial authentication, the status of the current authentication progress was reflected in a real-time value, such as the serialization of a QR code, and the participating tactical equipment nodes were updated based on static transmission rules in CNR networks in cell-planning areas. Subsequently, if an internal or external malfunctioning node or hostile node was detected and re-authentication was required, an additional authentication scheme could be easily executed at any time through clock synchronization of the hash functions in the LSH-based multi-factor hash chain of combined operation.

4.2. Lightweight Authentication Processes Based on Hash Chain

4.2.1. Initialization and Registration Phases

The processes proposed in this study were improved by applying the existing multi-factor hash chain and T-OTP authentication proposed by Kogan and Yin. The one-time initialization and registration phases similar to the hash chain-based OTP method are depicted in Figure 2.

① Fetch user information: Execution of the initialization and registration phases.
② Challenge/Reject: Initial settings of the range of the time slot length for the configuration of T-OTP values in the multi-factor hash chain structure by the administrator.
③ Key matching: Clock synchronization (periodic linkage of time between the user and administrator in CNR networks within a predetermined time-error range).
④ Establish session: Delivery of the seed hash value on T-OTP by the administrator to the user.

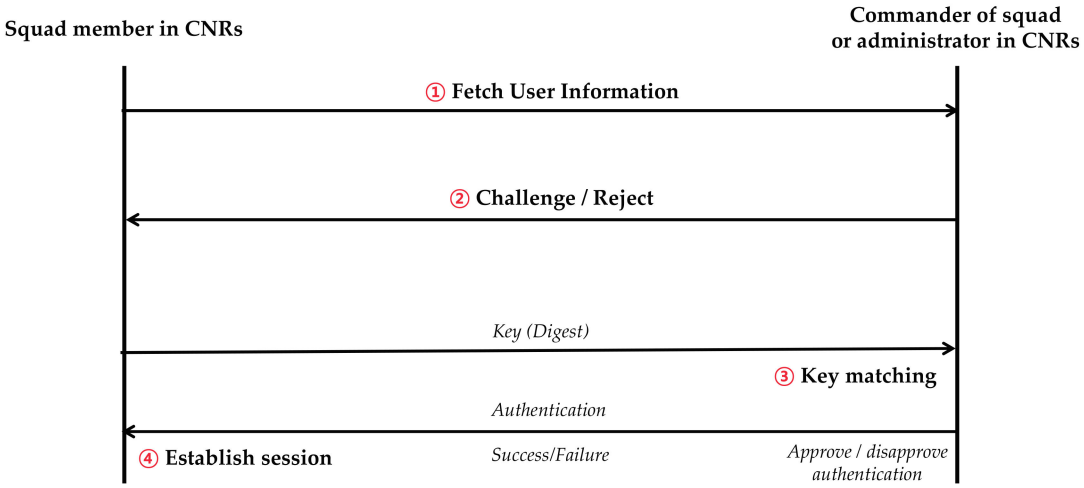


Figure 2. Initialization and registration phases.

The administrator was defined as the operation control authority or commander of the squad in any military operation, and the user was defined as a connected device or squad members that executed the operations under the received tactical messages. During the initialization and registration phase, the hash value of the hash chain was used as the T-OTP to execute the authentication phase. A user shared a bit-length seed to calculate the hash chain used as the OTP, after which the hash chain $h(x)$ was continued up to length i of the repetitive hash chain. The hash chain length was defined as 2×10^7 to 2×10^8 owing to the 2^{114} or 2^{224} based minimum security strengths and open multi-factor standard, and the length of the key used for certification was dynamically composed of values within the range of 130–224 bits because of protocol header storage limitations in VMF standards. In contrast to the Kogan method, a periodic clock synchronization process existed between the user and the administrator within a predetermined time-error range. In addition, for the authentication and verification phases that directly followed the initialization and registration phases, the user and administrator did not have to share secret keys, cryptographic hash functions, or digital signatures during the T-OTP authentication process based on the hash value of the hash chain. They had to share only pre-built abstract hash chain structures in wireless military terminals at the time of creation of the VMF-based CNR networks.

4.2.2. Authentication and Verification Phases

After the initialization and registration phases, the user utilized the T-OTP in an LSH-based multi-factor hash chain structure that used the hash values generated by applying the same

cryptographic hash function in reverse order to prevent the calculation of the hash value used in the next authentication session, thereby addressing the vulnerability of a simple password.

The objective of this phase was to deliver to the administrator the seed hash value of the LSH-based hash chain that the user would apply as the T-OTP. During the previous phase, authentication was performed using the time-based multi-factor method, utilizing the seed during the clock synchronization process. In the S/Key, because all hash values in the hash chain were sequential, they were indefinitely valid and vulnerable to theft and abuse. To mitigate this vulnerability, prior studies on improving a hash chain-based OTP assumed that a secret key, cryptographic hash function, and digital signature, among other factors, were shared, in advance, between the client and the server, resulting in limitations compared to other cryptographic primitives. However, through time-stamp-based clock synchronization, our proposed authentication process utilized hash values and related T-OTP values by applying a predefined time slot length between nodes participating in the VMF message exchange in the operation execution in CNRs. As such, the lifetimes of the hash values and T-OTPs of valid authentication keys that have not been used for long periods of time were limited to prevent, identify, and attenuate the continuous collection of information by specialized hostile nodes. The related phases are illustrated in Figure 3.

① Definition of initial seed hash: The initial seed hash of T-OTP, in which clock synchronization is executed and defined based on static transmission rules in military corps scenarios.

② Clock synchronization: The real-time authentication-based squad interoperability between the user and administrator within a predetermined time-error range is confirmed from the perspective of the operation start time in CNRs in cell-planning areas.

③ Sharing and calculating based on time slot length: The calculated hash values between the administrator and user within the range of the dynamic time slot length is verified. Next, authentication is performed based on T-OTP in the LSH-based hash chain structure.

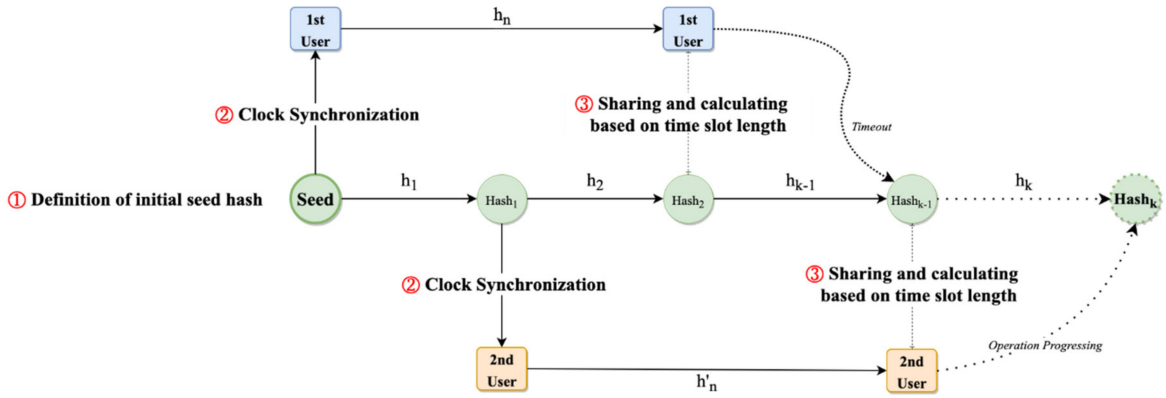


Figure 3. Authentication and verification phases.

The significant advantage of the LSH-based hash chain with multi-factor seed management was the independence of the T-OTP table between the administrator and the user in CNRs. Security was ensured because the administrator did not know the user's secret key. In terms of the feature securing availability in a mobile environment, such as ad hoc networks, by applying a finite dynamic time slot length, the validity of a specific hash value was limited up to the moment a predetermined period of time had passed. Thus, the proposed hash chain-based T-OTP yielded better computational and utilization efficiency compared to other cryptographic primitives. In addition, an independent salt value was assigned to each cryptographic hash function in the hash chain to verify the lower limit of the hash value of each function, thereby establishing the level of security. Here, the administrator could change the predetermined period for each operation group; as such, the clock synchronization process did not cause any issues owing to a low influence on real-time operation.

4.2.3. Re-Authentication and Revocation Phases

This phase included security considerations for the initial operation of various VMF-based closed CNRs and the rapid additional authentication of new squad nodes based on an extension of secure communication and authentication sessions. In addition, it was necessary to maintain an authenticated connection between squad members in the command system who were conducting squad operations and refresh the new authentication status with legitimated squad members after a certain amount of operation time had elapsed. The related phases are shown in Figure 4.

① Identify the state: The current authentication state of each squad member node in VMF-based CNR networks and a tactical system is identified.
② Check if a failure session occurs within this arbitrary time: The re-authentication variable-based military scenario in dynamic battlefields is recognized.
③ Whether a user has already achieved authentication within this arbitrary time is checked: The squad node authentication and re-authentication are executed in CNR networks for refreshing.
④ Setting of a time scheduler for clock synchronization: The re-authentication time scheduler for a configuration of the dynamic time stamp is set.
⑤ Re-configuration of time slot length: The slot length for clock synchronization is configured.
⑥ Phase execution: The re-authentication and execution of this overall phase is awaited.
⑦ Phase repetition: The authentication and verification phases with the re-authentication scheduler (if necessary) are repeated.

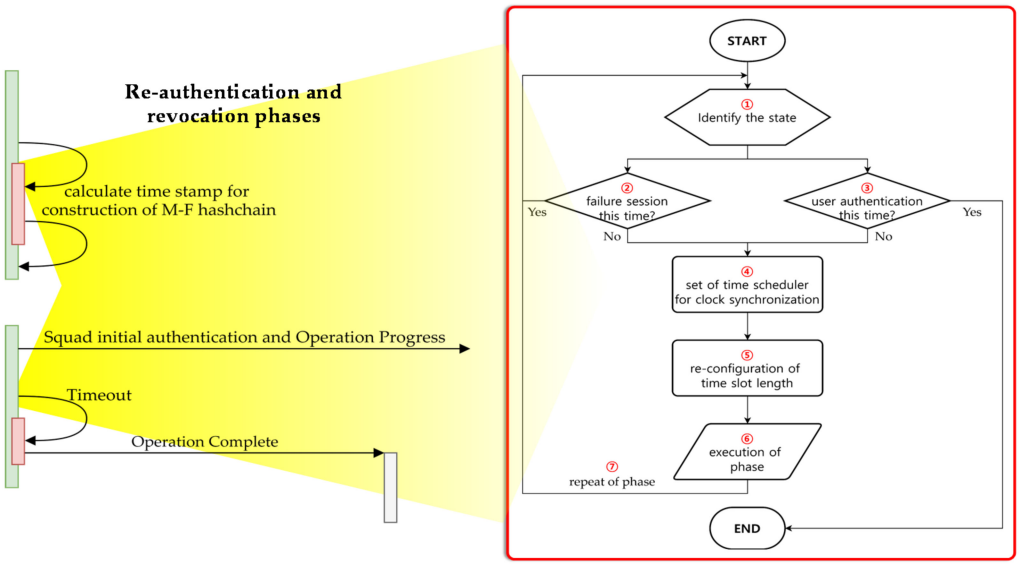


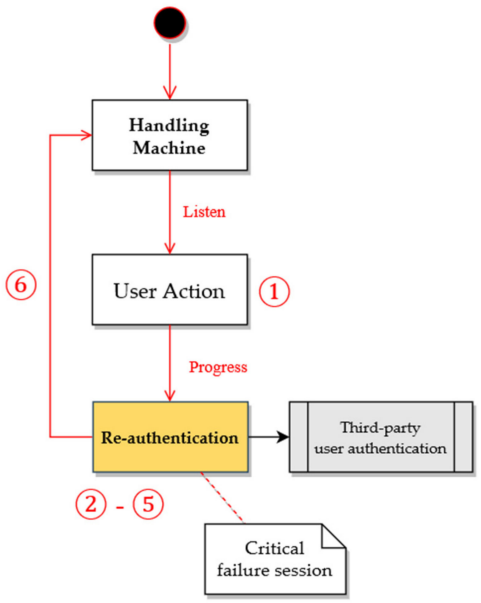
Figure 4. Re-authentication and revocation phases.

During the re-authentication and revocation phases, a scenario-based theoretical scheme was proposed to improve the robustness of each operation phase, the responsiveness and speed of each squad, the robustness and agility of the authentication for rapidly changing battlefield environments, the maximization of allied nodes and minimization of potential enemy nodes in CNRs related to digital-covert activities, and the independence of seed hash re-initialization based on securing transmission integrity, lower network transaction, and the reception of tactical information.

4.2.4. Testing of Exception Handling Flows in Specialized Military Scenarios in VMF-Based CNRs

This phase involved testing to prove the reliability of the LSH-based multi-factor hash chain with T-OTP value schemes in CNRs, including specialized military scenarios. Certain example scenarios to test exception handling flows are as follows.

- **Scenario 1**: Masquerading hostile nodes for exfiltration of tactical information (Figure 5).
- **Scenario 2:** Internal friendly nodes deliberately or accidentally conspiring with malicious outsiders based on deceptive collusion attacks (Figure 6).
- **Scenario 3:** Selfish friendly nodes monopolizing limited network resources with an enemy node that has been compromised (Figure 7).



[Scenario 1]

When an enemy node deceives a friendly node.

Example: Enemy nodes disguised as allies.

① Detection of abnormal behavior of unspecified nodes during military operation in a dynamic battlefield.

② Situational awareness of critical failure session-based state machine.

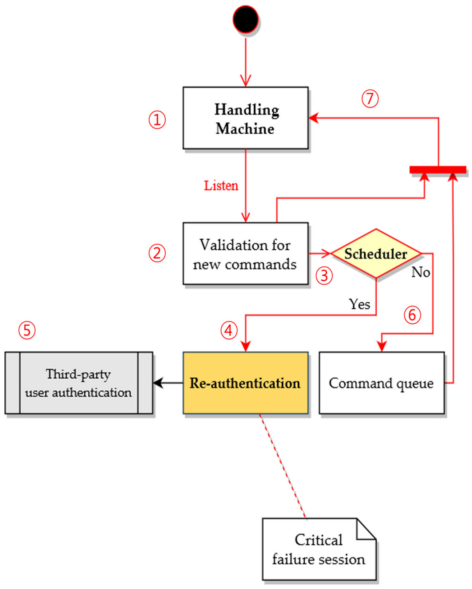
③ Instant node authentication based on hash chain with T-OTP and each node authentication in third-party environments, such as central control systems.

④ Early execution of identification and authorization.

⑤ Elimination of a node from the network when it is identified as an enemy node.

⑥ Reflection of the variation state value and related time slot length for clock synchronization in the hash chain.

Figure 5. Scenario 1—based exception handling flows.



[Scenario 2]

When an enemy conspires maliciously with friendly nodes.

Example: Friendly node intentionally or unintentionally conspiring with outsiders.

① Validation if a node in VMF-based CNRs is online.

② Pass when no exception occurs with tactical inspection.

③ Parameterization of clock cycles in re-authentication.

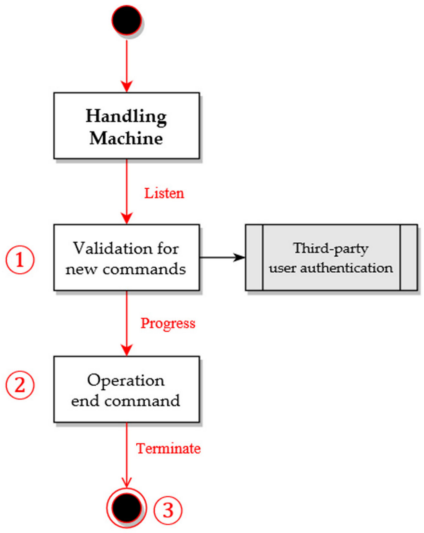
④ Re-authentication according to scheduler parameters during communication; elimination of a node from the network if it is identified as an enemy node when a critical failure session is recognized during the re-authentication process.

⑤ Early execution of identification and authorization.

⑥ Waiting for a message to be received when the scheduler is not required.

⑦ Reflection of the variation state and the related time slot length for clock synchronization in the hash chain.

Figure 6. Scenario 2—based exception handling flows.



[Scenario 3]

When a friendly node is terminated and removed under the administrator's authorization owing to a problem occurring during a tactical operation.

Example: Termination of existing nodes for efficient processing of restricted resources.

① Awaiting new commands and user authentication of each squad in third-party environments.

② Activation of operation activity termination, such as operation end command.

③ Elimination of nodes that are no longer used for a tactical combat network.

Figure 7. Scenario 3—based exception handling flows.

Scenario 1 checked the maintenance power of tactical confidentiality and fraud detection of an occupied hostile node or an enemy node disguised as a friendly node (that is, when abnormal behavior is detected and recognized as a critical failure session, the LSH-based hash chain including T-OTP was used to conduct an emergent authentication between the commander of the squad and the squad members in CNR networks). In addition, when a specific abnormal node was identified as an enemy, it was removed from the tactical squad status, and the change was reflected in the CNR. Scenario 2 checked the detection and prevention of internal nodes that might conspire with unspecified hostile nodes. While the inter-connection was maintained, re-authentication was performed according to the re-authentication scheduler (periodic). Depending on the resilience of the operation, the clock cycle for the re-authentication scheme was dynamically configured according to the purpose of the tactical operation (non-periodic). When a critical failure session was recognized during the re-authentication process, the corresponding enemy node was removed from the network, and the state of the belonging squad nodes was reflected in the VMF-based CNRs. Scenario 3 checked the robustness of the network structure when removing abnormal nodes that occupied limited resources, such as low transaction for lightweight authentication or nodes that were currently not required for additional allied operations. In the event that member nodes in the squad network were changed to conduct additional tactical operations, unwanted nodes were safely removed.

In addition to the aforementioned three scenario-based exception handling flows, attack scenarios that can be considered in limited military ad hoc-based CNR networks should reflect the characteristics of military communication environments in small-scale combat situations, for example, hierarchical high-capacity transmitter radio-net (HCTR) communication for independent battalions above brigade levels, low capacity transmitter radio-net (LCTR) communication below battalion levels, tactical mobile communication system (TMCS), and master–slave-based swarm communication. These include malicious radiowave interference in wideband network waveforms (WNW), spoofing and meaconing-based GPS jamming, advanced DoS-based operation availability violations, deceptions, and other cyber threats that can significantly impact limited tactical networks.

4.3. Configuration of Experimental Environments and Related Variables Based on VMF-Based CNR Networks

The configuration of related experimental environments and variables focused on comparative analysis combined with compound military metrics and wireless tactical operation scenarios based on Korean Army Corps networks in VMF-based CNRs. An overview of the NS-3- and MATLAB-based

co-testbed with limited resources in military ad hoc, cell-planning areas, and mosaic warfare networks is depicted in Figure 8.

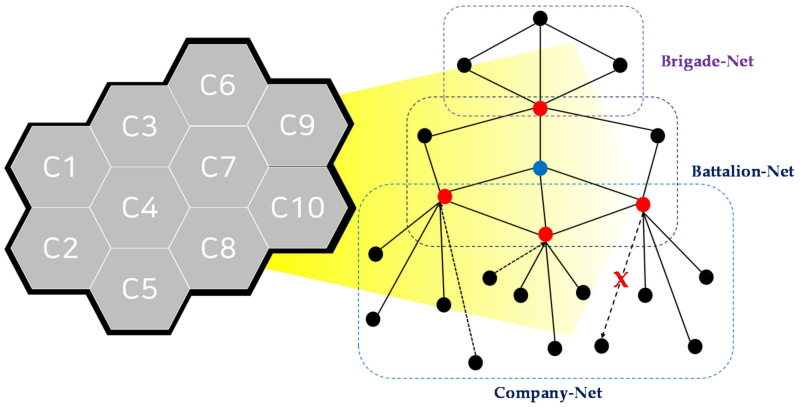


Figure 8. Overview of VMF-based CNR testbed with ad hoc and static cell-planning concepts.

Here, the red dot is the commander node in the CNRs and is the only one involved in establishing a communication channel between the upper and lower military ad hoc networks based on VMF. The blue dot is a communication forwarding node and exists to ensure the level of communication tolerance according to regional changes in CNRs and cell planning areas. In general, for VMF-based CNRs and related military ad hoc networks, communication environments and related configurations and structures are determined, in advance, before the operation is performed. However, because the communication structure of the VMF-based military ad hoc networks may change according to changes in operations, such as performing combined operations with other squads, the situation, such as the participation and withdrawal of nodes, is also reflected.

In addition, as shown in Figure 9, VMF-based CNR networks have different ad hoc structures for each wireless communication device, such as FM- or All-IP-based radio. The green dot is the transmitter node of the upper network when configuring the cluster swarming communication network types related to the ground and aerial unmanned systems, such as drones, Unmanned Aerial Vehicle (UAV) and Unmanned Ground Vehicle (UGV). The orange dot is a master or leader node constituting a cluster swarming communication network.

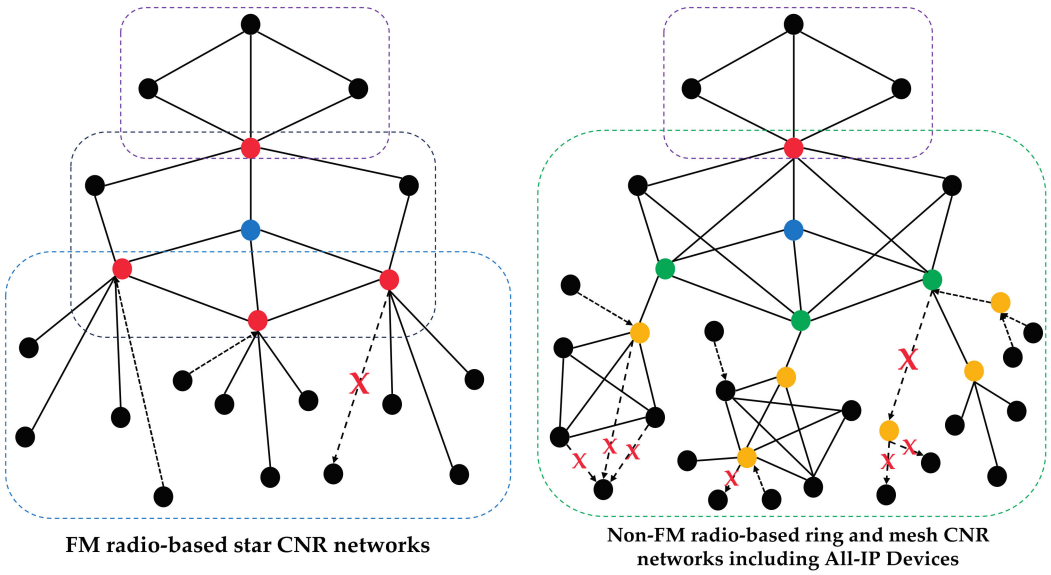


Figure 9. VMF–CNR network architecture based on FM radio and All-IP next-generation radio.

The overall experimental variables related to the VMF-based CNR network co-testbeds are presented in Tables 5–8, and Figure 10. In addition, when configuring related experimental variables, the following major tactical perspectives are considered.

① Currently, the VMF-based CNR networks, to which the LSH-based multi-factor hash chain with a T-OTP authentication system is applied, are considered to support a maximum bandwidth of approximately 2 Mbps and BPSK modulation. The primary goal is to transfer messages as quickly and with as low an overhead as possible, while ensuring low-transaction-based authentication and integrity within the CNRs. Therefore, preferentially, based on the extreme configuration from a minimum of 2.4 kbps bandwidth to a maximum of 192 kbps bandwidth, additional variables such as transmission rate, transmission and reception electric power, modulation and demodulation, maximum transmit time (MTT), and jitter should be variably defined.

② There are differences in the communication power specifications of wireless devices for each squad class and military specification in the VMF-based CNRs. In addition, there is a difference in the equipment used for mixed voice and multi-media transfers. In other words, the wireless communication for infantry in a small squad network does not have an amplifier; as such, the bandwidth is low owing to small energy resources. However, the pieces of wireless communication terminal equipment mounted on tanks, corps helicopters, and corps unmanned vehicles have an amplifier, resulting in high radio energy emissions; as such, the bandwidth is higher. Therefore, all these aspects should be applied within the VMF-based military ad hoc network for each communication environment such as MANET and VANET, and the concepts of mobility variations and ground device specifications to simulate rapidly changing battlefields and limited network resources should be defined and calculated.

③ The VMF-based CNR networks are largely classified into an FM radio-based communication type and an All-IP-oriented non-FM radio-based communication type. The FM radio environment includes a hierarchical star cluster network such as "brigade–battalion–company–platoon," and each commander-specific communication uses different frequency bands. The All-IP-based non-FM radio environment includes a ring-type network, determines upper, lower, and unmanned swarming communication based on WAN-LAN, and uses different frequency bands for each operation or set of military occupational skills (MOS). Therefore, by applying all these aspects, isolated closed radio networks within VMF-based CNRs and related ad hoc networks should be constructed.

④ The communication nodes are physically separated from the network, and only commander nodes, such as the brigade commander, battalion commander, company commander and platoon commander, can perform hierarchical sequential communication. In other words, in the FM radio environment, commander nodes other than the rank of platoon commander use two static radio channels instead of one, and squad members can communicate only to commanders in the same squad networks. Commander nodes in an All-IP-based non-FM radio environment have two IP classes themselves, such that they can simultaneously configure closed or open radio channels. All radio channels or IP addresses in FM and non-FM radio environments are not dynamically assigned, but are statically injected and maintained until the end of the operation. In addition, when an arbitrary commander node belonging to the lower cluster network requests communication from the upper commander, the lower node must directly join the upper network and change to the frequency of the upper cluster network. Therefore, all these aspects should be considered and applied.

⑤ The authentication variable values related to the LSH-based multi-factor hash chain with the T-OTP system are obtained in a form that is injected before the start of the tactical operation. In addition, wireless communication authentication in the cell-planning areas based on corps ground and air control stations is similarly considered. Therefore, all these aspects should be considered and applied.

Table 5. Examples of message variables in CNR networks based on infantry networks.

Message	Generation Cycle (s)	Generation Length (Bit)	Importance	Allocation
Location reporting	10	200, 400, 600	Routine	Broadcast
Reconnaissance reporting	1000–2000	2000, 4000, 12,000	Priority	Multicast
Volley ordering	1000–2000	150	Urgent	Unicast

Table 6. Examples of communication parameters in physical layer-related VMF standards.

Parameter	Value	Description
Number of static cells	1–7	Number of cell clusters with center
Number of nodes	8–1200	Number of participating nodes in CNRs
Execution time (s)	120–259,200 (3 days)	Operation time in VMF-based CNRs
Join nodes	0–200	Number of join nodes in ad hoc
Withdrawal nodes	0–30	Number of withdrawal nodes in ad hoc
Bandwidth (kbps)	2.4–192	Frequency band size
Frequency	Declared according to bandwidth	Frequency band
Power (w)	0.01–0.2	Transmit and receiver power
Coverage	Declared according to power	Device communication coverage
Distance (m)	1–3000	Distance of transmission
Number of channels	1–3	Number of sessions for communication
Modulation	BPSK, QPSK	Modulation method
Data rate (bps)	2400–7200	Data transfer rate
MTT	0.0–0.02	Maximum transmit time
PER	0.0–0.1	Packet error rate
BER	0.0–0.1	Bit error rate

Table 7. Configuration of parameters in LSH-based multi-factor hash chain with T-OTP scheme.

Parameter	Value
Hash algorithm	LSH-256, LSH-512
Size of nonce (bit)	224, 256, 384, 512
Minimum security length (bit)	112 (NIST), 224 (BSA), 256 (NSA)
Execution time based on hash chain (s)	128–1024
Time slot length for T-OTP (s)	5, 10, 30, 60, 300, 600
Message digest (bit)	150, 200, 400, 600, 2000, 4000, 12,000
Crypto period (year)	1, 2, 3

Table 8. Configuration of authentication testbed environment (not military spec).

Element	Value
Processor 1 for central administration	Intel Xeon E series, Intel i7-10700
Processor 2 for commander	Intel i7-10875H, Samsung Exynos 8890 (virtual)
Processor 3 for member	Qualcomm Snapdragon 805 (virtual)
Type of communication nodes	Producer, Interpreter, Forwarder, Consumer, and Noise node (Declared according to number of nodes)
Enabling jitter nodes for causing overhead such as PDV, PER, and BER	True (0–20)
Type of communication packets	Voice, Data, Image, and Video
Type of ACK	TWOACK and S-ACK
Re-transmission of max count-based ACK	0–3
Type of wireless radio-based SDR	HF (AM), VHF (AM), and UHF (AM/FM)
Enabling cell-planning node	True (0–10)/False
Enabling terrain information	False

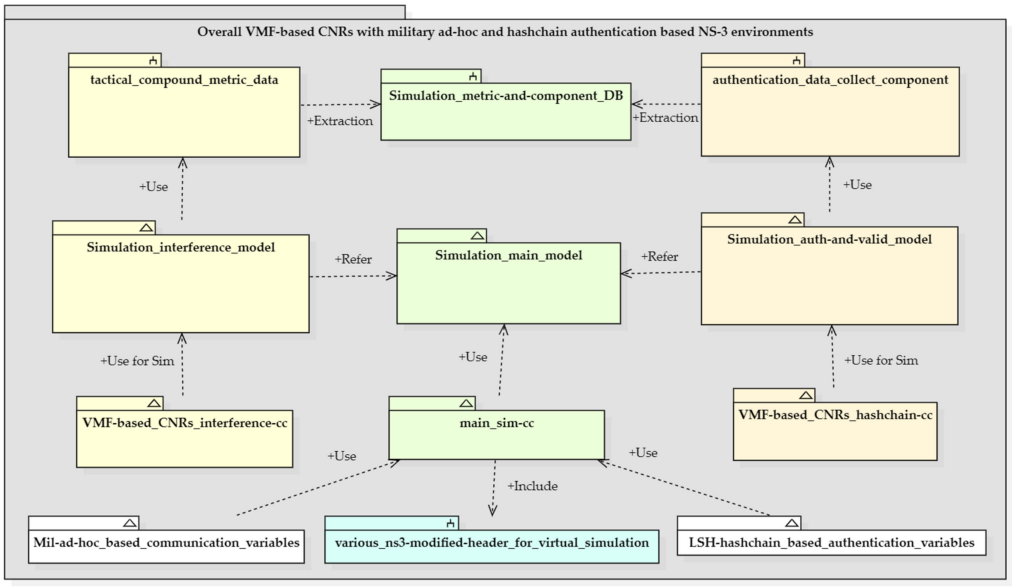


Figure 10. Overview of overall VMF-based CNR testbed architecture with hash chain authentication.

4.4. Comparison between Overall Proposed Model and Previous Studies

The existing hash chain-based studies required improvements owing to network operation constraints as a result of the poor communication environment in rapidly changing VMF-based wireless CNR networks. The proposed authentication model addressed these limitations through a four-phase process of initialization and registration, authentication and verification, re-authentication and revocation, and various exception handling flows. The related comparison results and the taxonomy of the 112 bit-based minimum security strengths are presented in Figure 11 and Table 9, respectively.

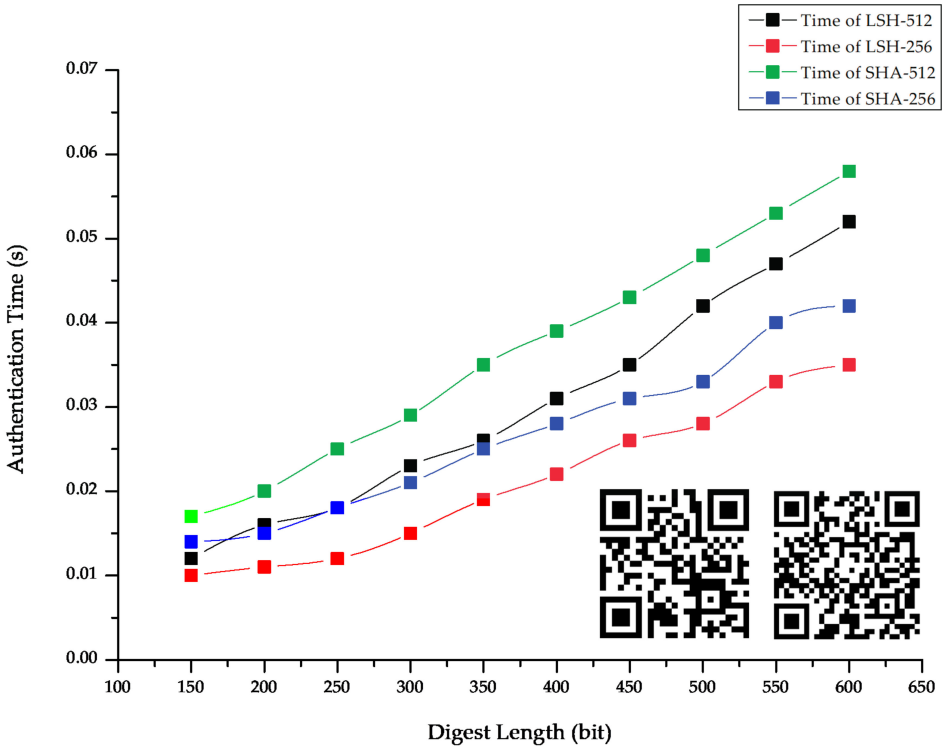


Figure 11. Brief comparative result of LSH and SHA hash functions based on each QR code.

Table 9. Taxonomy of existing LSH hash chain-based authentication and proposed model.

	CKP (①)	LL (②)	RA (③)	LAO (④)	RR (⑤)	DI (⑥)
VMF [1]	O	O	O	O	X	X
Haller et al. [12]	X	X	△	△	△	△
Perrig et al. [15]	X	△	▲	▲	▲	△
Zhu et al. [19]	X	△	▲	▲	▲	▲
Zhang et al. [23]	X	△	△	△	▲	△
Hamdy et al. [24]	X	△	X	▲	▲	△
Bittl et al. [25]	X	△	O	X	△	△
Kogan et al. [26]	O	△	O	△	▲	▲
Yin et al. [27]	O	▲	O	▲	▲	▲
Our proposed authentication model	**O**	▲	**O**	▲	**O**	**O**

[Functional Satisfaction Score] (X = weak, △ = slightly weak, ▲ = slightly strong, O = strong).

During the initialization and registration phases, for the conditions of LL (②), the entire initial authentication process of the VMF-based tactical CNR networks based on wireless terminals and squad devices was completed within a short period of time, allowing the operations to be rapidly conducted and the multiple squads to be quickly input into the battlefield environment. In terms of LAO (④), smooth communication and message transmission were ensured for hierarchical low-speed, low-bandwidth networks and the low-spec connected equipment with limited resources. Because the authentication process was an improvement over existing processes in VMF standards, it also secured interoperability, satisfying the DI (⑥) conditions based on military ad hoc networks, such as MANET and VANET, with pre-built cell planning areas. During the authentication phase, by satisfying the CKP (①) conditions, the authorization of friendly squad nodes in arbitrary tactical networks could be verified at a reliable level, even in a rapidly changing limited network. In addition, to maintaining a regular authentication process and reducing the overhead, the system was configured to exclude the key ownership stage in one of the two terminals from the authentication algorithm, while satisfying the RA (③) conditions. Thus, security against overall wireless attacks in a CNR was achieved by activating various defensive mechanisms, such as preventing the reuse of random keys and exception handling. The RR (⑤) conditions were satisfied during the verification phase, which ensured that any new nodes continued to participate as legitimate nodes even after the initial authentication was completed. An environment in which theft and damage might occur owing to intrusions from unforeseen hostile enemy forces during combined operations was considered when designing this scheme.

5. Conclusions

In this study, for the first time, a multi-factor hash chain-based lightweight authentication scheme including T-OTP values applicable to VMF-based CNR networks was proposed. The existing military tactical message system using the VMF standard has potential vulnerabilities in terms of message integrity and authentication, which arise from the use of a digital signature algorithm based on SHA-1- and RSA-based encryption. Accordingly, through comparative analysis of previous studies based on pros and cons, in this study, a lightweight authentication scheme was proposed. This model could enhance the integrity of tactical message exchanges and reduce unnecessary network transactions and transmission bits for authentication flow in VMF-based CNR networks, while ensuring robustness with limited resources. In addition, by considering the actual limited military communication environment, such as HCTR, LCTR, TMCS, and unmanned ground and aerial system-based swarm communication, and presenting functional exception handling flows that are not implemented in the existing VMF military standard as a basis for possible cyber threats, military authentication processes applicable to small-scale combat situations can be practically constructed.

In the future, we intend to increase the reliability between wireless devices in the KVMF, and apply it in-depth as lightweight authentication in Korean Army network scenarios. Finally, the limitations of this study and plans for future research are as follows.

- Because this hash chain-based study focused on the design and analysis of a lightweight authentication for a VMF standard, future studies will assess its quantitative performance through network load tests in TDL based on the Korean Army Corps network scenarios with related equations, pseudo codes, and compound All-IP- or non-All-IP-based wireless topologies.
- During the re-authentication and re-validation phases, aiming to take advantage of the dedicated hash chain configured using the Byzantine fault tolerance property among other failure models in a distributed system, specific scenario-based schemes and attack graphs will be presented. In addition, they will be judged on their ability to be classified into specific tactical scenarios, including state machines for critical failure between actual operations.
- To obtain a dynamic adaptation of the proposed authentication process for a rapidly changing battlefield environment, the responsiveness of each squad must be considered for the rapid deployment of various nodes and the successful execution of various tactics and strategies. Therefore, by further devising a process for applying concrete state-based conditional exception handling modeling, a military communication system-based VMF message transfer standard will be produced that can also consider real-time authentication situations.

Author Contributions: Conceptualization, D.K., S.S., and H.K.; methodology, S.S. and H.K.; software, D.K., Y.K.L., and W.G.L.; validation, D.K., S.S., and Y.K.L.; formal analysis, S.S. and H.K., investigation, D.K., Y.K.L., and H.K.; resources, D.K., W.G.L., and S.S.; data curation, D.K., S.S., H.K. and Y.K.L.; writing—original draft preparation, Y.K.L., D.K., and W.G.L.; writing—review and editing, S.S. and D.K.; visualization, D.K. and S.S.; supervision, W.G.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the ADD project, the Defense Acquisition Program Administration and the Agency for Defense Development under the contract UD200023ED.

Acknowledgments: The authors gratefully acknowledge the financial support provided by the Defense Acquisition Program Administration and the Agency for Defense Development under the contract UD200023ED.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. MIL-STD-2045/47001D (w/CHANGE 1), Department of Defense Interface Standard: Connectionless Data Transfer Application Layer Standard. June 2008. Available online: http://everyspec.com/MIL-STD/MIL-STD-2000-2999/MIL-STD-2045_47001D_CHANGE-1_25098 (accessed on 1 November 2020).
2. The FIPS 180-1 Secure Hash Standard. April 1995. Available online: https://nvlpubs.nist.gov/nistpubs/Legacy/FIPS/fipspub180-1.pdf (accessed on 1 November 2020).
3. Wang, X.; Yin, Y.; Yu, H. Finding collisions in the full SHA-1. In *Advances in Cryptology—CRYPTO 2005, Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 14–18 August 2005*; Springer: Berlin/Heidelberg, Germany, 2005; Volume 3621, pp. 17–36.
4. Wang, X.; Yin, Y.L.; Yu, H. Finding Collisions in the Full SHA-1. In *Advances in Cryptology–CRYPTO 2005*; CRYPTO 2005; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2005; Volume 3621. [CrossRef]
5. Stevens, M.; Bursztein, E.; Karpman, P.; Albertini, A.; Markov, Y. The first collision for full SHA-1. In *Proceedings of the 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, 20–24 August 2017*; Springer: Berlin/Heidelberg, Germany, 2005; Volume 10401, pp. 570–596.
6. Lee, J.; Kim, J. LSH: A new fast secure hash function family. In *Proceedings of the 17th International Conference on Information Security and Cryptology, Seoul, Korea, 3–5 December 2014*; Springer: Berlin, Germany, 2005; Volume 8949, pp. 286–313.
7. Lamport, L. Password authentication with insecure communication. *Commun. ACM* **1981**, *24*, 770–772. [CrossRef]

8. Eldefrawy, M.H.; Khan, M.K.; Alghathbar, K. One-time password system with infinite nested hash chains. In *Security Technology, Disaster Recovery and Business Continuity*; Communications in Computer and Information Science: Berlin, Germany, 2010; Volume 122, pp. 161–170.
9. Hu, Y.C.; Perrig, A. A survey of secure wireless ad hoc routing. *IEEE Secur. Priv.* **2004**, *2*, 28–39.
10. Hyun, S.; Ning, P.; Liu, A.; Du, W. Seluge: Secure and DoS-resistant code dissemination in wireless sensor networks. In Proceedings of the International Conference on Information Processing in Sensor Networks, St. Louis, MO, USA, 22–24 April 2008; pp. 445–456.
11. Deng, J.; Han, R.; Mishra, S. Secure code distribution in dynamically programmable wireless sensor networks. In Proceedings of the 5th International Conference on Information Processing in Sensor Networks, Nashville, TN, USA, 19–21 April 2006; pp. 292–300.
12. Haller, N.M. The S/Key™ one-time password system. In Proceedings of the Internet Society Symposium on Network and Distributed System, San Diego, CA, USA, 1 January 1994; pp. 151–157.
13. Zhang, Y.; Chen, Y.; Sun, Y.; Chen, M. Training demand analysis for airlines safety manager based on improved OTP model. In *Proceedings of the International Conference on Human-Computer Interaction, as Vegas, NV, USA, 15–20 July 2018*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 334–342.
14. Mitchell, C.J.; Chen, L. Comments on the S/KEY user authentication scheme. *ACM SIGOPS Oper. Syst. Rev.* **1996**, *30*, 12–16. [CrossRef]
15. Perrig, A.; Canetti, R.; Tygar, J.D.; Song, D. The TESLA broadcast authentication protocol. *RSA CryptoBytes Tech. Newsl.* **2002**, *5*, 2–13.
16. Perrig, A.; Song, D.; Canetti, R.; Tygar, J.; Briscoe, B. Timed Efficient Stream Loss-Tolerant Authentication (TESLA): Multicast Source Authentication Transform Introduction. *Req. Comments* **2005**, RFC-4082. Available online: https://tools.ietf.org/html/rfc4082 (accessed on 12 December 2020).
17. Jakobsson, M. Fractal hash sequence representation and traversal. In Proceedings of the IEEE International Symposium on Information Theory, Lausanne, Switzerland, 30 June–5 July 2002; p. 437.
18. Hu, Y.-C.; Jakobsson, M.; Perrig, A. Efficient constructions for one-way hash chains. In Proceedings of the International Conference on Applied Cryptography and Network Security, New York, NY, USA, 7–10 June 2005; pp. 423–441.
19. Zhu, S.; Xu, S.; Setia, S.; Jajodia, S. LHAP: A lightweight hop-by-hop authentication protocol for ad-hoc networks. In Proceedings of the 23rd International Conference on Distributed Computing Systems Workshops, Providence, RI, USA, 19–22 May 2003; pp. 749–755.
20. Lu, B.; Pooch, U.W. A lightweight authentication protocol for mobile ad hoc networks. In Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'05), Las Vegas, NV, USA, 4–6 April 2005; pp. 546–551.
21. Akbani, R.; Korkmaz, T.; Raju, G.V.S. HEAP: Hop-by-hop efficient authentication protocol for mobile ad-hoc networks. In Proceedings of the 2007 Spring Simulaiton Multiconference, Norfolk, VA, USA, 25–29 March 2007; pp. 157–165.
22. Goyal, V. How to re-initialize a hash chain. *IACR Cryptol. ePrint Arch.* **2004**, *97*, 1–9.
23. Zhang, H.; Li, X.; Ren, R. A novel self-renewal hash chain and its implementation. In Proceedings of the IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, Shanghai, China, 17–20 December 2008; pp. 144–149.
24. Eldefrawy, M.H.; Alghathbar, K.; Khan, M.K. OTP-based two-factor authentication using mobile phones. In Proceedings of the Eighth International Conference on Information Technology: New Generations, Las Vegas, NV, USA, 11–13 April 2011; pp. 327–331.
25. Bittl, S. Efficient construction of infinite length hash chains with perfect forward secrecy using two independent hash functions. In Proceedings of the 11th International Conference on Security and Cryptography (SECRYPT), Vienna, Austria, 28–30 August 2014; pp. 213–220.
26. Kogan, D.; Manohar, N.; Boneh, D. T/Key: Second-factor authentication from secure hash chains. In Proceedings of the ACM SIGSAC Conference on Computer and Communications, Dallas, TX, USA, 30 October–3 November 2017; pp. 983–999.
27. Yin, X.; He, J.; Guo, Y.; Han, D.; Li, K.C.; Castiglione, A. An efficient two-factor authentication scheme based on the Merkle tree. *Sensors* **2020**, *20*, 5735. [CrossRef] [PubMed]
28. Burbank, J.L.; Chimento, P.F.; Haberman, B.K.; Kasch, W.T. Key challenges of military tactical networking and the elusive promise of MANET technology. *IEEE Commun. Mag.* **2006**, *44*, 39–45. [CrossRef]

29. Tang, H.; Salmanian, M.; Chang, C. *Strong Authentication for Tactical Mobile Ad Hoc Networks*; Defence R & D Canada: Ottawa, ON, Canada, 2007.
30. Lee, K.; Lee, S.; Kim, Y.; Kwon, K.; Lim, W. A study for hop count on the ad-hoc of wireless communication. In Proceedings of the 14th International Conference on Advanced Communication Technology (ICACT), PyeongChang, Korea, 19–22 February 2012; Volume 176, pp. 931–935.
31. Tu, W.; Lai, L. Keyless authentication and authenticated capacity. *IEEE Trans. Inf. Theory* **2018**, *64*, 3696–3714. [CrossRef]
32. Jiang, S. Keyless authentication in a noisy model. *IEEE Trans. Inf. Forensics Secur.* **2014**, *9*, 1024–1033. [CrossRef]
33. Kong, J.; Luo, H.; Xu, K.; Gu, D.L.; Gerla, M.; Lu, S. Adaptive security for multilevel ad hoc networks. *Wirel. Commun. Mob. Comput.* **2002**, *2*, 533–547. [CrossRef]
34. Ji, H.; Park, S.; Yeo, J.; Kim, Y.; Lee, J.; Shim, B. Ultra-reliable and low-latency communications in 5G dwnlink: Physical layer aspects. *IEEE Wirel. Commun.* **2018**, *25*, 124–130. [CrossRef]
35. Ji, H.; Park, S.; Shim, B. Sparse vector coding for ultra reliable and low latency communications. *IEEE Trans. Wirel. Commun.* **2018**, *17*, 6693–6706. [CrossRef]
36. Parvez, I.; Rahmati, A.; Guvenc, I.; Sarwat, A.I.; Dai, H. A survey on low latency towards 5G: RAN, core network and caching solutions. *IEEE Commun. Surv. Tutorials.* **2018**, *20*, 3098–3130. [CrossRef]
37. Gao, P.X.; Narayan, A.; Karandikar, S.; Carreira, J.; Han, S.; Agarwal, R.; Ratnasamy, S.; Osdi, I.; Gao, P.X.; Narayan, A.; et al. Network Requirements for Resource Disaggregation. In Proceedings of the 12th USENIX Symposium on Operating Systems Design and Implementation, Savannah, GA, USA, 2–4 November 2016; pp. 249–264.
38. Seok, B.; Sicato, J.C.S.; Erzhena, T.; Xuan, C.; Pan, Y.; Park, J.H. Secure D2D communication for 5G IoT network based on lightweight cryptography. *Appl. Sci.* **2019**, *10*, 217. [CrossRef]
39. Vladyko, A.; Khakimov, A.; Muthanna, A.; Ateya, A.A.; Koucheryavy, A. Distributed edge computing to assist ultra-low-latency VANET applications. *Future Internet* **2019**, *11*, 128. [CrossRef]
40. Hu, Y.C.; Perrig, A.; Johnson, D.B. Rushing attacks and defense in wireless ad hoc network routing protocols. In Proceedings of the 2nd ACM Workshop on Wireless Security, San Diego, CA, USA, 19 September 2003; pp. 30–40.
41. Wu, B.; Chen, J.; Wu, J.; Cardei, M. A survey of attacks and countermeasures in mobile ad hoc networks. In *Wireless Network Security*; Springer: Berlin/Heidelberg, Germany, 2007; pp. 103–135.
42. Aad, I.; Hubaux, J.P.; Knightly, E.W. Impact of denial of service attacks on ad hoc networks. *IEEE/ACM Trans. Netw.* **2008**, *16*, 791–802. [CrossRef]
43. Abdul-Ghani, H.A.; Konstantas, D.; Mahyoub, M. A comprehensive IoT attacks survey based on a building-blocked reference model. *Int. J. Adv. Comput. Sci. Appl.* **2018**, *9*, 355–373.
44. Ponsam, J.G.; Srinivasan, R. A survey on MANET security challenges, attacks and its countermeasures. *Int. J. Emerg. Trends Technol. Comput. Sci.* **2014**, *3*, 274–279.
45. Alani, M.M. MANET security: A survey. In Proceedings of the IEEE International Conference on Control System, Computing and Engineering (ICCSCE), Batu Ferringhi, Malaysia, 28–30 November 2014; pp. 559–564.
46. Bar-Noy, A.; Cirincione, G.; Govindan, R.; Krishnamurthy, S.; Laporta, T.F.; Mohapatra, P.; Neely, M.; Yener, A. Quality-of-information aware networking for tactical military networks. In Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), Seattle, WA, USA, 21–25 March 2011; pp. 2–7.
47. Aschenbruck, N.; Gerhards-Padilla, E. A survey on mobility models for performance analysis in tactical mobile networks. *J. Telecommun. Inf. Technol.* **2008**, *2*, 54–61.
48. Suri, N.; Benincasa, G.; Lenzi, R.; Tortonesi, M.; Stefanelli, C.; Sadler, L. Exploring value-of-information-based approaches to support effective communications in tactical networks. *IEEE Commun. Mag.* **2015**, *53*, 39–45. [CrossRef]
49. Lu, X.; Chen, Y.-C.; Leung, I.; Xiong, Z.; Liò, P. A novel mobility model from a heterogeneous military MANET trace. In Proceedings of the International Conference on Ad-Hoc Networks and Wireless, Sophia-Antipolis, France, 10–12 September 2008; Volume 5198, pp. 463–474.
50. Studer, A.; Bai, F.; Bellur, B.; Perrig, A. Flexible, extensible, and efficient VANET authentication. *J. Commun. Netw.* **2009**, *11*, 574–588. [CrossRef]

51. Chefranov, A.G. One-time password authentication with infinite hash chains. In *Novel Algorithms and Techniques in Telecommunications, Automation and Industrial Electronics*; Springer: Berlin/Heidelberg, Germany, 2008; pp. 283–286.
52. Mitchell, W. *Three C2 Models for Military Agility in the 21st Century*; Royal Danish Defence College Press: Copenhagen, Denmark, 2012.
53. Alexeev, A.; Henshel, D.S.; Levitt, K.; McDaniel, P.; Rivera, B.; Templeton, S.; Weisman, M. Constructing a science of cyber-resilience for military systems. In Proceedings of the NATO IST-153 Workshop on Cyber Resilience, Munich, Germany, 23–25 October 2017; pp. 23–25.