Journal of KIIT. Vol. 19, No. 11, pp. 13-28, Nov. 30, 2021. pISSN 1598-8619, eISSN 2093-7571 
http://dx.doi.org/10.14801/jkiit.2021.19.11.13

# 전투무선망 내 경량 인증 수행을 위한 멀티팩터 해시체인 인증 연구

서상*, 김도훈**, 임원기***

# A Study on Multi-factor Hashchain-based Authentication for Lightweight Authentication in Combat Network Radios

Sang Seo*, Dohoon Kim**, and Won-Gi Lim***

이 연구는 국방과학연구소의 지원(계약번호: UD200023ED)을 받아 수행되었습니다.


## 요 약

현재 기존 VMF 표준 내 인증 프로세스는 SHA-1 기반 해시충돌 취약성, 높은 네트워크 통신 부하, 낮은 채널 무결성, 전술 환경 내 다양한 공격의 접점이 늘어나면서 이를 감쇄하기 위한 보안적 기술의 한계성 검토가 필요하다. 즉, 이러한 문제점을 최소화하고 네트워크 통신이 극도로 제한된 작전 기동 환경에 적합한 지휘통신 운용 개념 수립이 필요하다. 본 논문은 전투무선망의 시공간적 운용 개념을 고려한 T-OTP 기반 LSH 경량 해시체인 인증 모델을 신규 제안한다. 이는 군집형 다종 애드혹 전투무선망을 NS-3 기반으로 모의실험을 수행하여, 기존 VMF 인증 대비 향상된 인증 효율성을 입증함과 함께, 급변하는 전장 환경을 고려한 점진적인 통신 강건성 및 복원성 역시 추가 확보하였다.

## Abstract

Currently, the existing VMF standard authentication process requires a review of the limitations of security technologies to attenuate SHA-1-based hash collision vulnerabilities, high network communication loads, low channel integrity, and increased contact points of various attacks in tactical environments. In other words, it is necessary to minimize these problems and establish a concept of command and communication operation suitable for an extremely limited operational management environment. To this end, an independent authentication process based on a real-time unique authentication value with limited communication validity is required. This paper proposes a new T-OTP-based LSH lightweight hashchain authentication method, including the concept of spatiotemporal operation of combat wireless networks. This demonstrated improved authentication efficiency compared to the existing VMF certification by conducting simulations based on NS-3 of the clustered multi-species ad hoc combat wireless network. In addition, we have additionally secured gradual communication robustness and resilience in consideration of the rapidly changing battlefield environment. In the end, the proposed model can be used as a structure to ensure terminal authentication and data integrity of advanced combat wireless networks in the future.



Keywords

variable message format, combat network radios, hashchain, time-based one-time password, lightweight secure hash, ad-hoc



* 경기대학교 AI컴퓨터공학부 석사과정
- ORCID: https://orcid.org/0000-0003-1524-3710
** 경기대학교 AI컴퓨터공학부 교수 (교신저자)
- ORCID: https://orcid.org/0000-0001-6370-9744
*** 국방과학연구소 제 2기술연구본부
- ORCID: https://orcid.org/0000-0003-4155-9807



· Received: Oct. 22, 2021, Revised: Nov. 05, 2021, Accepted: Nov. 08, 2021


· Corresponding Author: Dohoon Kim
Department of Computer Science, Kyonggi University, Suwon 16227, Gyeonggi-do, Korea
Tel.: +82-31-249-1364, Email: karmy01@kyonggi.ac.kr

# Ⅰ. 서 론

군사혁신으로 지휘통신체계 및 독립형 무인체계 등이 도약적으로 기술 발전함에 따라, 현대전의 작전 패러다임과 기술적 군사 생태계는 급변하고 있으며, 군 현대화 요구에 근거한 다종 무기체계와 전술정보통신체계의 실질 성능 개선 역시 활발히 진행 중이다. 이러한 추세에 근거하여 대한민국 지상군 역시 현재 제한된 대역폭 환경 내에서 실시간적 전술정보 송수신을 보장하는 미군의 VMF(Variable Message Format) 전술정보 교환 표준[1]을 개량하여, 기존 전투무선망(Combat network radios)의 장비-통신 운용성을 개선하여 과업 단위제대별 잠재적 단말기 보안 취약성을 최소화하면서 신속한 전장상황 공유 및 지휘통제를 추가 보장하여 총체적인 전투효율성을 향상시키는 전략화를 상세 수행하고 있다.

하지만 기존 전투무선망 내 적용된 VMF 표준은 SHA-1(Secure Hash Algorithm-1) 기반 전자서명(Digital signature) 개념을 주된 인증 스킴으로 채택하고 있기에, 이에 따라 높은 해시충돌 취약성[2]과 네트워크 통신 부하, 채널 무결성 미보장 이슈 등이 발생할 수 있으며, 군 운용 체계의 전반적인 스마트화 및 네트워크화에 따른 대항군의 시공간 우위적인 비대칭 공격 표면 극대화 등의 잠재적인 한계성 역시 유발될 수 있다. 또한 VMF 전자서명 인증 내 파라미터 정의 여부에 기인하여 부수적으로 구성 가능한 RSA(Rivest‐Shamir‐Adleman) 기반 공개키 암호화 스킴 역시, 높은 인증 트랜잭션 요청 횟수와 페이로드 길이에 따라 극한의 전장 통신 환경과 은밀한 작전 기동 과업 등에는 적합하지 못한 기능성을 가지며, RSA-1024 기반 초기의 개념적 인터페이스를 어떠한 추가적인 예외처리 고려 없이 그대로 VMF 내에 함양했기에, 실질적으로 PoC(Proof of concept)된 인수분해 공격[3] 등에도 취약함을 보이며 비-인가된 외부자 접속이나 대항군 공격에도 대응하지 못하는 보안 한계점 역시 초래할 수 있다.

이러한 기존 VMF 내 기능적-보안적 한계성을 모두 감쇄하기 위한 개선된 체계 운용 개념과 개량된 인증 프로세스 등이 시급히 정립되지 않는 경우, 급변하는 전장 환경에서 기동 중인 전투무선망 내 지휘전술통신의 기밀성 및 가용성, 대응성을 신속히 확보하고 유지할 수 없을 것이며, 통신 품질 저하에 근거하여 총체적 작전 수행 효율성 역시 급격히 감소할 것이다. 또한 스마트-네트워크화된 VMF 전투무선망 내 영상통화 및 데이터 송수신과 관련된 통신 서비스의 복원성과 민첩성을 향상시키기 위한 사전예방적 사이버 보안 개념도 명확히 심층화되지 않음에 따라, 대항군에 의해 발생 가능한 인증 위협을 사전 차단하면서 대응방책을 적시 수립하기 위한 운용 영역도 제한될 것이며, 송수신 데이터의 무결성 보장 범위 역시 한정될 것이다.

이에 본 논문에서는 기존 VMF 기반 전투무선망 내 SHA-기반 전자서명 인증 프로세스의 한계성을 완화하고 극한의 전장 통신 환경에 적합한 신규 인증 개념을 수립하기 위해, 분대원별 독립적인 LSH (Lightweight Secure Hash)[4] 경량 해시체인 구조에 기반한 T-OTP(Time-based One-Time Password) 인증 아키텍처를 최초로 제안하도록 한다. 그리고 NS-3 [5] 네트워크 시뮬레이터와 공개된 군 장비-통신 제원 정보들을 활용하여 대대급 이하 군집기동 시나리오 기반 성형-링형 중앙 집중 무선 애드혹을 분대형-차량형-드론형 기준으로 모의하여, 제안 인증 아키텍처와 타 인증 간 성능 비교와 주요 메트릭별 민감도 분석을 모두 수행하고, 기존 대비 향상된 인증 효율성과 통신 강건성을 검증하도록 한다.

이에 따른 본 논문의 기여도를 정리하면 다음과 같다. 첫째, VMF 기반 전투무선망 인증 프로세스에 적합한 T-OTP 기반 LSH 경량 해시체인 인증 아키텍처를 최초로 신규 제시함으로서, 현 지상군이 운용 중인 기존 전투무선망 내에 잠재적으로 잔류하는 인증 및 전술통신 관련 기능적-보안적 한계성을 즉각 완화 가능함을 보였다. 둘째, 공식적으로 제정된 해시 함수 및 인증 표준과 관련 오픈소스 라이브러리에 기반한 인증 아키텍처의 테스트베드 구조를 제시함으로서, 구현 용이성과 실질성, 확장성 등을 도출하였다. 셋째, 실질 군 제원 정보, 작전 과업 및 태스크, 토폴로지 구조 등에 모두 기반한 무선 애드혹 통신과 관련 인증 프로세스 모의를 통해, 타 인증 및 가용 함수 대비 향상된 인증 성능 및 효율성, 통신 강건성 및 복원성 등을 총체적으로 입증하였다. 넷째, 향후 진보된 VMF 기반 전투무선망 내 표준화에 입각한 적응형 군 단말기 인증 및 데이터

무결성 보장 스킴으로서 응용 가능하며, 추가 개량 연구 역시 수행 가능함을 보였다.

본 논문의 구성은 다음과 같다. 먼저 2장에서는 기존 VMF의 한계성을 완화하기 위한 해시체인 인증과 관련된 대표 선행 연구들을 비교 분석, 분류한다. 3장에서는 전투무선망의 시공간적 운용성과 중앙 통신 구조에 입각한 T-OTP 기반 LSH 경량 해시체인 인증 아키텍처를 제시하고, 단계별 상세 프로세스와 주요 활용 라이브러리 역시 기술한다. 4장에서는 NS-3 기반으로 분대-차량-드론 군집형 전투무선망 애드혹 모델을 모의한 후 성능 비교를 수행한다. 마지막 5장에서는 본 연구의 활용성과 향후 연구방향성을 제시하고 결론에 대해 기술한다.

## II. 관련 연구

### 2.1 VMF의 한계성 분석 및 관련 개선안 정립

가변 메시지 형식 (VMF) 군사 표준은 미국 합동참모본부 산하의 JINTACCS에 의해 제정된 군사 서비스 기반 디지털 정보 교환 표준으로, 제한된 전장 네트워크 내 C4I 체계의 정보 전송을 위한 전술 데이터 요소 및 관련 프로토콜 표준을 포함한 복합 공통 상호 운용성 군사 표준식을 제공한다. 또한 유선 및 무선 군사 통신을 모두 사용하는 제한된 전술 통신 자원에 기반한 네트워크 중심 운영 환경(NCOE)에서 감시체계, 지휘통제체계, C2 체계, 화력 투사 및 지원 타격체계 등에서 디지털 전술 정보를 실시간으로 교환 하는데 있어, 상황별로 유의미한 전술 명령 데이터만 취사선택하여 전송하도록 구성된다. 즉 해당 군사 표준을 통해 이전 고정크기 메시지 처리 시스템 대비 신속한 전술통신 메시지 전송이 실현 가능하며, 지상전술데이터링크 내 디지털 메시지 전송 장치 간 상호운용성 및 호환성 확보를 위한 최소한의 필수 통신 매개 변수를 함양하도록 선택적 전술통신 설계 목표 형태 역시 유의미하게 제시할 수 있다[1]. 현재 이러한 VMF 표준에 입각하여 지상군 내 대대급 이하 전투무선망과 중소규모 다종 무기체계에 주요로 구체화 되었으며, 수립된 작전 과업과 태스크에 기반하여 군단형 항공 및 함정 운용체계에도 고도화 중에 있다.

하지만 이러한 VMF에 대한 선행 연구들 중, 단말기 인증 및 데이터 무결성 지원을 위한 보안성 향상 연구는 현재 공식적으로 보고된 바 없다. 즉 군 현대화 요구에 따라 급변하는 전투무선망에서 잠재적으로 발생 가능한 사이버 보안 위협과, 폭발적으로 증대될 것으로 예상되는 공격 표면 변화와도 관련지어, VMF 운용 개념에 기반한 인증 및 보안성 향상 연구가 시급히 요구될 것이다.

특히 현 전투무선망 내 적용된 VMF 표준은 그림 1과 같이 강화 조치 없이 SHA-1 기반 전자서명을 기본 인증으로 차용하고, RSA-1024 암호화 기반으로 선택적인 데이터 암호화를 예외 처리 없이 순수히 수행하기 때문에, 약한 해시 강건성에 기반한 높은 해시 충돌 취약성, 높은 네트워크 통신 부하로 인한 인증 처리 지연, 낮은 채널 전송 무결성, 불필요한 추가 인증 트랜잭션 및 페이로드-플래그 오버헤드, 방어자 열위적인 공격 및 탐사 표면의 폭증, 높은 전투무선망 리소스 활용에 따른 은폐 및 은닉화 실현 불가, 제한된 통신 채널 유지와 복원성 확보를 위한 마이그레이션 미존재 등의 다양한 기능적-보안적 한계성이 여전히 잔존할 것이다.

| Code<br>MSB - LSB | Reference |
|---|---|
| 0000<br>(0) | Authentication (using SHA-1 and DSA) / No Encryption |
| 0001 – 1111<br>(1 – 15) | Undefined |

| 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 |

그림 1. MIL-STD-2045-47001[1] 군사 표준 내 SHA-1 기반 전자서명 기반 VMF 인증 수행 정보
Fig. 1. Information on performing SHA-1-based DSA for VMF authentication in MIL-STD-2045-47001 standard

이에 따라 극한의 전장 통신 환경과 시공간적 전투무선망 운용 교리 등에 최적화된 경량 보안 인증 아키텍처를 신규 제시함으로서, 기존 VMF 내 데이터 인증 및 기밀성, 무결성, 가용성 확보를 모두 수행함과 함께, 총체적인 군 인증 보안성 역시 향상시켜야 할 것이다.

이에 본 논문은 VMF 기반 전투무선망 내 하위 분대원 및 관련 단말기 인증을 위한 불필요한 네트워크 트랜잭션을 최소화함과 함께, 지휘관 입회 하 중앙집중형 인증-인가 프로세스를 극한의 저속 전장 통신 환경에서도 강건히 유지하면서 효율적인 암호화 통신 역시 보장하기 위한 개념적 아키텍처로서, 전투무선망 내 지휘관과 분대원 모두가 동적 보유할 수 있는 T/Key 기반 해시체인 인증 아키텍처를, 주요 VMF 인증 개선안으로 선정한다.

그리고 해시체인 내 해시함수는 취약한 SHA-1이 아닌, 대한민국 독자 표준의 암호학적 해시 함수인 LSH를 적용하고, 해시 상태별 적재되는 고유값은 시공간적 변화에 따른 절대적 타임스탬프에 기반한 T-OTP로서 정형화한다. 이때 LSH 해시 함수의 정립을 통해 기존 SHA-1의 약한 해시 안정성에 따른 해시 충돌 취약성 문제와 채널 전송 무결성 이슈 등을 원천 방지할 수 있으며, 시공간적 타임스탬프 기반으로 유효성이 제한된 T-OTP 적용을 통해서는 높은 네트워크 인증 트랜잭션 및 통신 부하, 인증-처리 지연, 공격 및 탐사 표면, 낮은 채널 유지력 및 복원성 이슈 등을 역시 완화할 수 있을 것이다.

## 2.2 VMF 개선을 위한 해시체인 인증체계 분석

먼저 Lamport가 제안한 해시체인 기반 일회용 암호(OTP)[6]는 동일한 해시함수를 연속적으로 적용하여 생성된 해시체인 내 해시값들을 역순 구성함으로서, 다음 인증 세션에서 활용될 해시값의 계산을 역상 저항성 기반으로 불가능하도록 최초 조성하여 단순 패스워드의 재생 공격 기반 취약성을 방지하였다. Haller 등이 제안한 S/Key 표준[7]은 해시체인 내 루트 해시값의 생성과 재등록이 요구됨에 따른 태생적인 해시체인 경량화 이슈의 한계성을 최초로 해결하였으며, 제한된 리소스를 함양한 네트워크 통신 환경 내 인증 효율성을 향상시킴과 함께 재사용 공격 역시 방지하였다.

Perrig 등이 제안한 TESLA[8]는 선행된 S/Key에서 해결하지 못한 해시체인 초기화 오버헤드 이슈와 타 인증체계 간 결합 불가 한계성에 따른 도난 및 악용 취약성 문제 등을, 타임스탬프 내 고정된 시간 간격 기반 키 공개 지연 개념과 느슨한 시간 동기화 스킴, 메시지 인증 코드(MAC)와 같은 다요소 구조를 총괄 부여하여 완화하였다. 그 후 이러한 TESLA를 기반으로 하여 동적 애드혹에 특화된 인증 체계로서 Zhu 등이 제안한 LHAP[9]와 Akbani 등이 제안한 HEAP[10] 등의 응용 인증 프로토콜 개념이 제시되어 이동 노드별 채널 확장성과 실질 구현성을 추가 확보했으며, Zhang 등이 제안한 SRHC [11], Eldefrawy 등이 제안한 이중 OTP[12], Bittle 등이 제안한 무한중첩 해시체인 연구[13] 등을 통해, 해시체인 초기화 및 루트 재등록과 오버헤드 이슈를 높이 완화하였다.

Kogan 등은 S/Key 표준과 T-OTP 스킴을 결합하여 서버에 클라이언트의 비밀키를 저장하지 않는 다중 인증 체계로서 T/Key[14]를 제안하였고, 동적 애드혹 등의 모바일 분산 환경 내 노드별 보안성과 가용성, 신속성을 선행 해시체인 구조 대비 높이 확보하기 위한 상세 개념들을 추가 정립하였다. 즉 T/Key는 동일 해시 함수 사용에 따른 보안 불안정성을 완화하기 위해, 계층적으로 각각 독립적 해시 함수를 적용하여 인증 해시값을 동적 구성하였고, 시간 간격 길이 개념 역시 절대적 타임스탬프 기반 적응적 동기화 서브루틴으로 추가 정의함으로서 해시값의 무기한적 유효성으로 인한 공격 가능성도 제한하였다.

또한 사전 공격(Dictionary attack) 등을 위한 공격자의 비대칭적 우위성 기반 전처리 행위의 부정적 파급 효과를 최소화하기 위해, 해시체인 내 각 해시 함수에 독립적인 솔트 값을 할당하여 각 함수에 대한 해시 값의 하한을 검증하여, 조직별로 운용 중인 애드혹 내 확보 가능한 암호학적 최소 보안성을 기존 S/Key 및 TESLA 대비 랜덤 오라클 모델 기반으로 4배 넘게 크게 향상시켰다. 관련된 상세 개념도는 그림 2와 같이 정리된다.

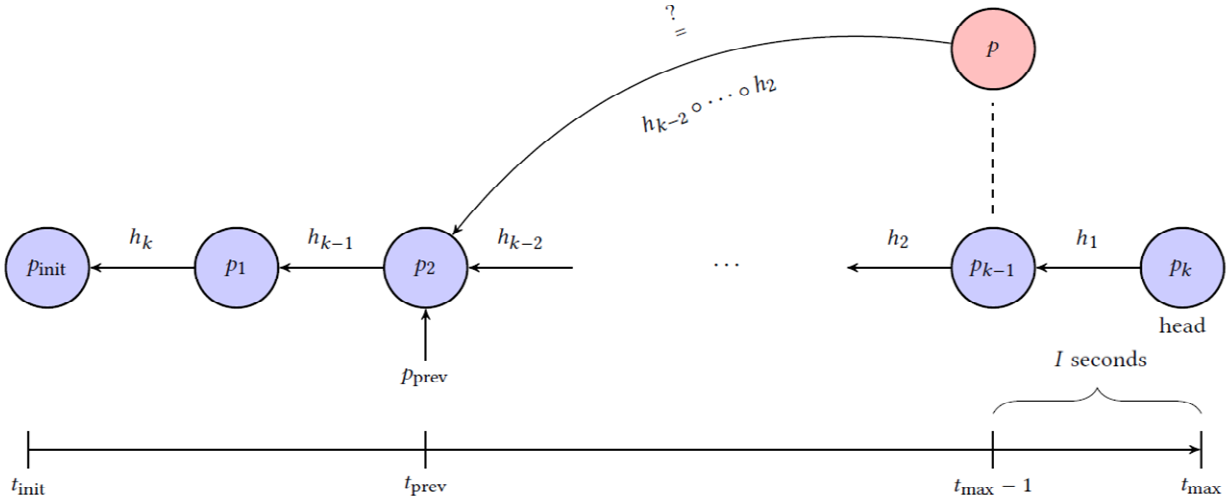


그림 2. T/key 개념도 및 주요 인증 성능 비교
Fig. 2. Conceptual diagram of T/key and comparison of authentication performance

Yin 등은 이진 해시 트리인 머클 트리(Merkle tree) 기반 MOTP[15] 인증 아키텍처를 신규로 제안하여, T/Key 대비 소량의 서버 스토리지를 활용하면서 급변하는 트래픽 통신 내 동적 애드혹 노드별로 불필요한 인증 트랜잭션 수와 클라이언트 스토리지 비용 등은 절감하고, T-OTP 생성 및 검증 시간의 효율성 역시 향상시키는 기능성을 도출하였다.

즉 MOTP는 머클 트리 내 상위 부모 노드가 하위 자식 노드를 대표하는 특질에 근거하여, 머클 트리와 T/Key 알고리즘을 결합한 응용 인증 아키텍처로서, 시간 동기화에 극히 민감한 OTP 개념을 부가해 이중 보안성을 추가 확보하고 중복 계산의 제거 및 트리 루트 등을 통한 대량의 계산량 감쇄 역시 실현하여, 기존 다요소 인증 체계 내 잔존한 지연 문제와 정보 노출 문제 등을 완화하였다.

## 2.3 선행 연구별 비교 분석

T/Key 이전 선행된 해시체인 연구들은 대부분 해시체인 인증 단계가 단독으로 존재하기에, 대항군의 적극적 혹은 수동적 위협이나 급격한 통신 환경 변화 등에 따른 부정적 파급력을 잠재적으로 높이 내포한다. 이에 T/key는 S/Key와 T-OTP를 결합한 다중 인증 구조를 함양함으로서, 동일 해시 함수 사용에 따른 보안 불안정성 문제와 무기한적 인증 해시 유효성 유지에 따른 공격자의 비대칭적 우위 관계 이슈, 전처리 공격 행위의 효율성 증대 문제 등을 모두 해결하였으며, 타 인증체계 간 암호학적 최소 보안성 역시 높이 향상시켰다. 하지만 T/Key는 내부의 모든 해시값들이 시간 제한적인 사용성에 따른 단계별 접근제어 개념을 가지기에 기존 S/Key보다 긴 체인 길이를 함양하며, 이에 따른 유한 체인 길이 관리와 계산량 증폭 문제가 유발될 수 있다.

또한 총체적인 인증 보안성 보장과 OTP 생성-검증 등의 작업 등이 여전히 유한 해시체인 길이에 의존하며 장기 운용을 위한 자가-재초기화 스킴 역시 부재하고, 통신 환경별로 더 많은 해시 작업이 요구됨에 따라 T-OTP 생성 및 검증의 효율성이 급락하는 기능적 한계성 역시 여전히 잔존한다. 관련 후속 연구로서 머클 트리 기반 MOTP가 제안되었고, 극한 통신 환경 내 부하를 유발하는 인증 트랜잭션 수와 페이로드 길이, T-OTP 계산 및 스토리지 사용 비용 등을 모두 감쇄함과 함께, 지연 및 정보 노출 이슈로 인한 보안적 한계성 역시 완화하였다. 선행 연구들을 고려하여, Kim[16]은 멀티팩터 해시체인 인증 기반 VMF 인증 개량과 관련된 개요 연구를 수행하였고 성능 비교 분석 역시 수행하였다.

이러한 서술에 기반하여 선행 연구들과 제안 인증 아키텍처별 비교 분석은 표 1과 같이 정리된다. 이를 통해 본 논문에서 제안하는 인증 아키텍처가 메트릭별 가장 높은 인증 효율성을 보일 수 있음을 산출하였다. 이는 후술될 3장과 4장에서 언급한다.

표 1. 선행 연구와 제안한 인증 개념 간 주요 분류표
Table 1. Taxonomy about our proposed authentication (충족 기준 - X : 낮음, △ : 약간 낮음, ▲ : 약간 높음, O : 높음)

| Property / Existing study | Key independence and integrity | Low latency and high reliability | Responsiveness and robustness | Compatibility in battlefield | Ease of recertification and renewal | Interoperability and Interoperability |
|---|---|---|---|---|---|---|
| Haller et al. | X | X | △ | △ | △ | △ |
| Perrig et al. | X | △ | ▲ | ▲ | ▲ | △ |
| Zhu et al. | X | △ | ▲ | ▲ | ▲ | ▲ |
| Zhang et al. | X | △ | △ | △ | ▲ | △ |
| Eldefrawy et al. | X | △ | X | ▲ | ▲ | △ |
| Bittl et al. | X | △ | O | X | △ | △ |
| Kogan et al. | O | △ | O | △ | ▲ | O |
| Yin et al. | O | ▲ | O | ▲ | ▲ | ▲ |
| **Proposed models** | O | ▲ | O | ▲ | O | O |

## III. T-OTP 기반 LSH 해시체인 인증 아키텍처

### 3.1 설계 원칙

기존 VMF 인증 프로세스는 SHA-1 기반 전자서명을 기본 인증 개념으로 차용하고 RSA-1024 암호화 기반으로 선택적인 데이터 암호화를 수행하기에, SHA-1 기반 높은 해시 충돌 취약성, 많은 네트워크 통신 부하, 높은 인증 및 처리 지연율, 낮은 채널 전송 무결성, 과다한 네트워크 트랜잭션 오버헤드와 같은 기능적-보안적 한계성들을 내포한다.

이러한 한계성들을 모두 완화 및 해결하기 위해, VMF 기반 전투무선망 내 지휘관과 분대원 모두가 동적 보유할 수 있는 S/Key 및 T/Key 기반 일방향 해시체인 개념을, 제안 아키텍처 내 주요 인증값 초기화 및 저장, 검증을 위한 스토리지 구조로서 1차 채택한다. 그리고 취약한 SHA-1이 아닌, 대한민국 표준의 LSH 해시 함수를 적용하여 인증에 활용하고자 하는 해시 값들을 경량화하고, 지상군의 전투무선망 운용 현황에 근거한 시공간적 타임스탬프 기반 T-OTP를 핵심 분대원 인증 요소로 적용함으로서, 임의 시간 간격 내에서 부설된 인증 통신 채널의 제한된 유효성을 지휘관 입회 하에 제어하도록 정형화한다. 이러한 세부 원칙들을 기반으로 그림 3과 같이 아키텍처화하여, VMF 기반 전투무선망 내 지휘관 기반 중앙집중형 폐쇄적 군 인증 프로세스에 유효한 'T-OTP 기반 LSH 경량 해시체인 인증 아키텍처'로서 명명한다.

이 때 이러한 'T-OTP 기반 LSH 경량 해시체인 인증 아키텍처'는 다음과 같은 세부 프로세스를 통해 전투무선망 내 분대원 인증을 수행한다.

1) [작전 수행 전 VMF 기반 전투무선망 통신 개설 후 분대원별 고유식별번호 생성 및 보고]: 작전 수행 직전, VMF 기반 전투무선망 내 지휘관과 분대원들 간 통신 채널이 신규 개설됨과 함께, 분대원은 자신의 고유식별번호를 지휘관에게 보고함. 이 때 고유식별번호는 미군 VMF 표준 내 URN(Unit Reference Number) 개념에 기반하여 타임스탬프 기반 패턴화된 IPv4로서 평문화함

2) [지휘관 입회 하 분대원별 고유식별번호 기반 LSH 시드 해시 생성 및 적재]: 지휘관은 각 예하 분대원들의 고유식별번호를 LSH 해시함수 내 평문으로, 타임스탬프는 키로서 고려하여, 해시체인 내 시드 해시를 구성함. 즉 지휘관 휘하의 하위 분대원이 총 10명인 경우, 지휘관은 LSH 기반 독립적인 시드 해시 총 10개를 보유하는 것임. 활용되는 고유식별번호의 크기는 32bit에서 256bit 사이 크기의 평문이나, 작전 과업 및 운용 환경에 따른 기밀성의 추가 고려가 요구될 시 고밀화된 암호학적 별도 해시 함수를 부가하여 256bit에서 512bit 사이의 해시값으로 구성함. 이렇게 평문 또는 해쉬화된 고유식별번호를 원전(Origin)으로 구성한, 분대원별 LSH 시드 해시의 최종 크기는 256bit에서 512bit 사이 크기로 정형화함

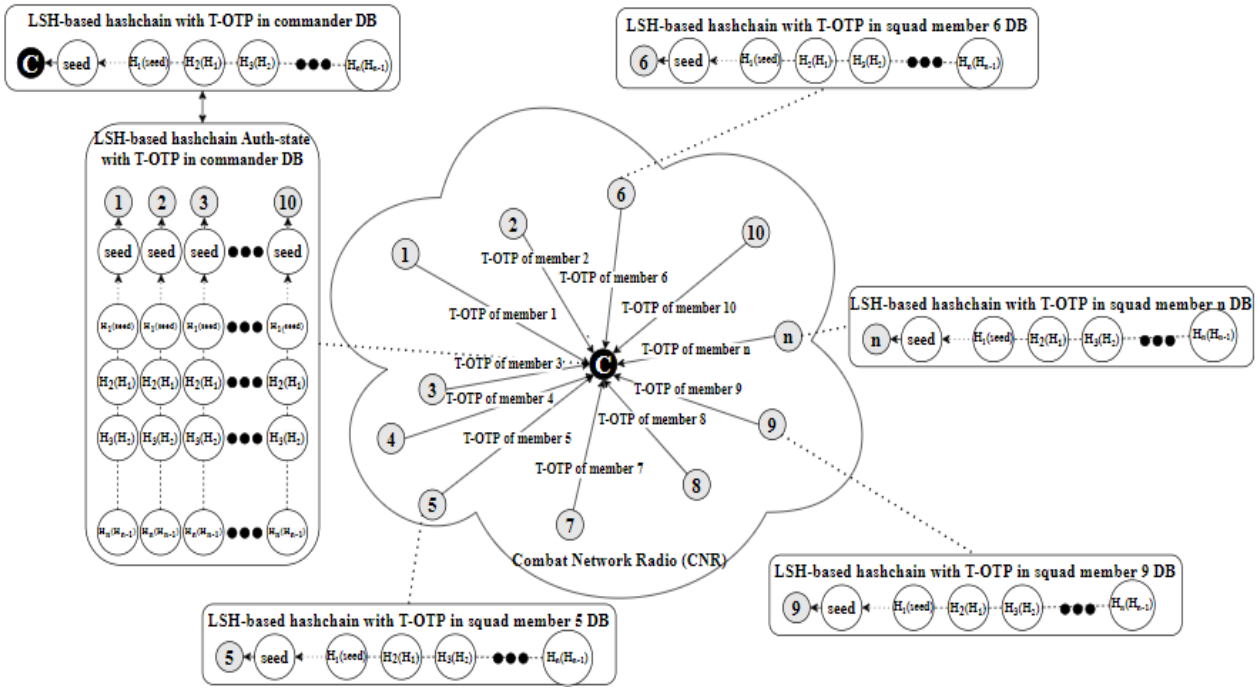


그림 3. T-OTP 기반 LSH 경량 해시체인 인증 아키텍처 개념도
Fig. 3. Overview of LSH-based lightweight hashchain architecture with T-OTP authentication

3) [분대원별 LSH 시드 해시 기반 T-OTP 생성 및 LSH 해시체인 기반 구조화 수행]: 시간 경과에 따라 유효성이 제한되는 동적 인증을 위해, 지휘관은 기 보유한 분대원별 시드 해시를 활용하여 절대적 타임스탬프 기반 T-OTP를 생성함. 그리고 T-OTP의 유효성을 한정하기 위해 정의한 주기적 시간 간격에 따라 다수의 T-OTP를 순차적으로 생성하고, 이를 각각의 LSH 해시체인 구조에 적재함. 이 때 지휘관은 하위 분대원으로부터 주기적으로 전달받거나 비주기적으로 송수신할 수 있는 작전 과업 및 관련 군 운용 시나리오에 근거하여, 분대원별 인증 및 적법 권한 인가를 수행해야 하므로, 이전에 구성한 분대원별 시드 해시들로서 모든 해시체인들을 정형화하고 각각의 별개 DB들로서 분산관리를 수행함. 지휘관과 달리, 하위 분대원들은 임의 시점에서 통신 채널 사용에 대한 권한 인가만 적법하게 획득하면 되기에, 자신의 시드 해시에 근거한 T-OTP 해시체인만을 보유함. 이러한 T-OTP들은 곧 송수신 표준인 BASE64로서 최종 인코딩된 LSH 해시들이며, 이 역시 시드 해시에 근거하여 LSH-256 또는 LSH-512 해시 함수가 순차적으로 적용됨

4) [분대원에 대한 T-OTP 기반 주기적 또는 비주기적 동적 인증 진행 및 적법 권한 인가]: 제시된 시간 간격 길이와 시나리오 등에 근거하여, 해시체인 내 적재된 T-OTP를 활용하여 지휘관은 분대원별 동적 인증을 수행함. 주기적 관점에서, 시공간 변화에 따른 지휘관의 위치 보고 요청에 따라 분대원은 현 시점에서 자신이 유효하다고 판단되는 T-OTP를 위치 보고 전술메시지와 함께 전달함. 지휘관은 특정 분대원이 전달한 T-OTP와, 자신이 보유한 해당 분대원의 해시체인 내 현 시간 간격에 속하는 T-OTP와의 일치 여부를 비교하여, 적법한 분대원임을 그림 4와 같이 확인함. 이때 특정 T-OTP를 획책한 대항군이 재사용하거나 기만 및 교란하는 것을 방지하기 위해, 지휘관은 분대원별 해시체인에 존재하는 모든 T-OTP에 대한 이전 사용 여부를 2차 카운트 기반으로 기록함. 그리고 이전 사용되지 않은 임의 T-OTP가 통신 문제 또는 위협 발생 등으로 인해 뒤늦게 수신될 시에는, 관련 분대원에게 2차 Health check를 수행함. 비주기적 관점에서, 임의 애드혹 통신 환경 내 무선위협이 발생하거나 노드 조인 및 탈퇴가 발생할 시, 지휘관은 하위 분대원들에게 브로드캐스팅 기반으로 현 시점의

T-OTP를 재요청하고, 예하 분대원별 인증 여부가 모두 갱신되기 전까지는 작전 수행을 중단함

5) [LSH 해시체인 내 T-OTP 고갈에 따른 재초기화 및 갱신 수행]: 만일 장시간의 작전으로 지휘관 및 분대원들이 보유한 해시체인 내 T-OTP가 모두 고갈될 시, 현 과업을 일시중단하고 초기화를 수행함. 먼저 기존의 모든 T-OTP 인증 카운트를 초기화한 후, 지휘관은 분대원 고유식별번호 기반 시드 해시를 신규 발급함. 그 후 이전에 사용한 총 인증 정보는 백업한 후, 휘하의 적법한 모든 분대원들에게 시드를 재송신하여 ②의 과정을 반복함. 이 때 작전을 처음 수행할 때의 폐쇄 환경의 보안성보다, 현재 재초기화를 수행하는 전장 환경의 보안성이 더 낮기에, 잠재적으로 노출된 T-OTP로 인한 대항군의 예측 공격 및 부채널 공격 가능성을 최소화하기 위해, 시간 간격 길이를 이전과 상이하게 구성함

6) [작전 및 시간 종료 후 초기화 및 종료]: VMF 기반 전투무선망 분대에게 부여된 작전 과업이 완료되거나, 총 시뮬레이션 시간이 만료될 시 모든 인증 정보를 초기화하고 정상적으로 종료함

### 3.2 인증 테스트베드 구성

제안 인증 아키텍처는 전투무선망 이외 기타 다양한 군 무선통신환경에 대한 확장성을 지원함과 함께, 구현 용이성과 향후 개량을 위한 실질성 역시 추가 확보하기 위한 방안으로서, 공식적인 해시 함수 표준과, 관련 인증 스킴, 부가적인 오픈소스 라이브러리에 기반하여 그림 5와 같은 테스트베드로서 구체화하였다. 대표적으로 LSH 해시함수는 대한민국 국가보안기술연구소의 응용 라이브러리[17]를, SHA 해시함수와 해시체인 구조는 OpenSSL 산업계 표준 라이브러리[18]와 NIST 표준[19]에서 주력 참조한 후, VMF 기반으로 개량되어 고도화되었다.

## Ⅳ. 전투무선망 모의 및 인증 성능 실험

### 4.1 NS-3 기반 군집 전투무선망 애드혹 설계

상술한 T-OTP 기반 LSH 경량 해시체인 인증 아키텍처의 성능을 비교 검증하고 탑재하기 위한 전투무선망을 NS-3 기반으로 모의한다. 이때 해당 모의환경은 분대, 차량, 드론 기반 엔터티가 노드로서 정의된 군집형 동적 애드혹 네트워크 모델에 기반하며, 대대급 이하 단일 지휘관에 다수의 하위 분대원이 성형 또는 링형 토폴로지 구조 기반으로 정적 할당되는 계층적인 망분리 형태로서 정의된다.

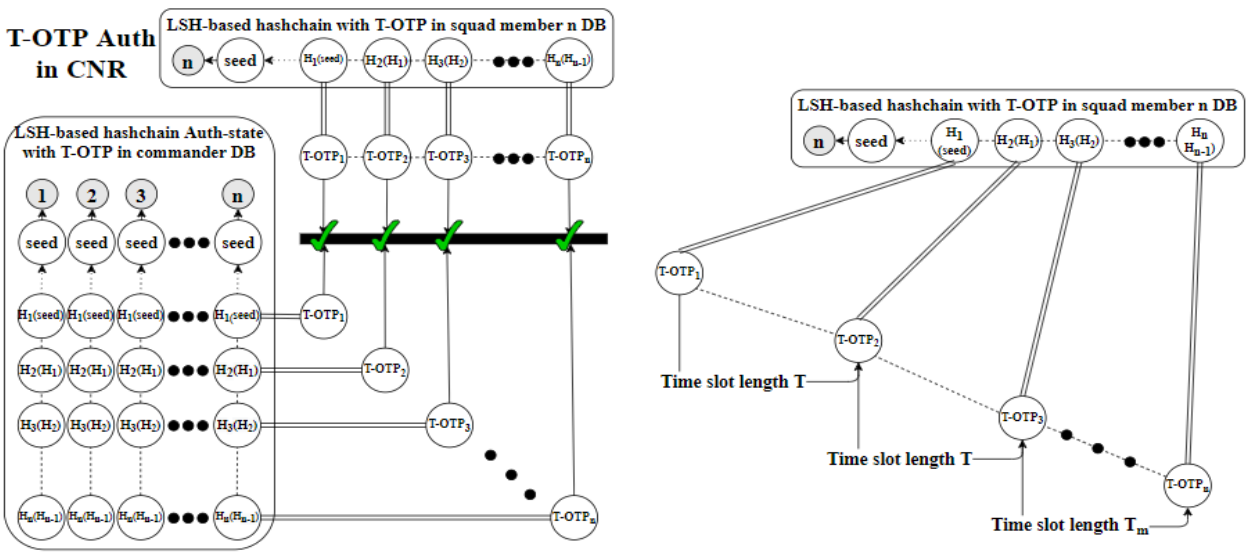


그림 4. 전투무선체계 내 T-OTP 기반 LSH 경량 해시체인 인증 수행 개념도

Fig. 4. Sub-overview of LSH-based lightweight hashchain with T-OTP in VMF-based combat network radios

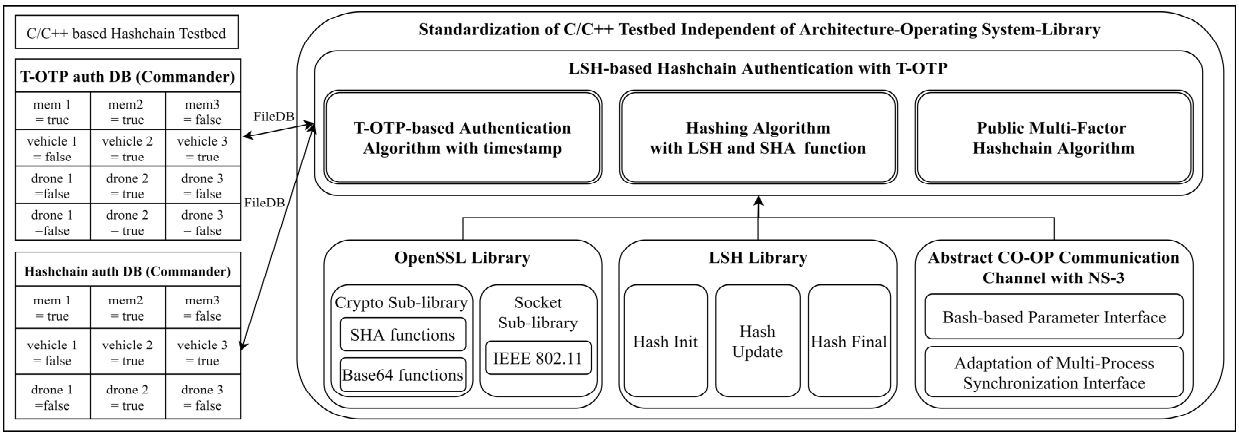


그림 5. 세부 모듈 및 라이브러리 기반 제안 인증 테스트베드 구성도

Fig. 5. Configuration diagram of authentication testbed based on detailed modules and libraries

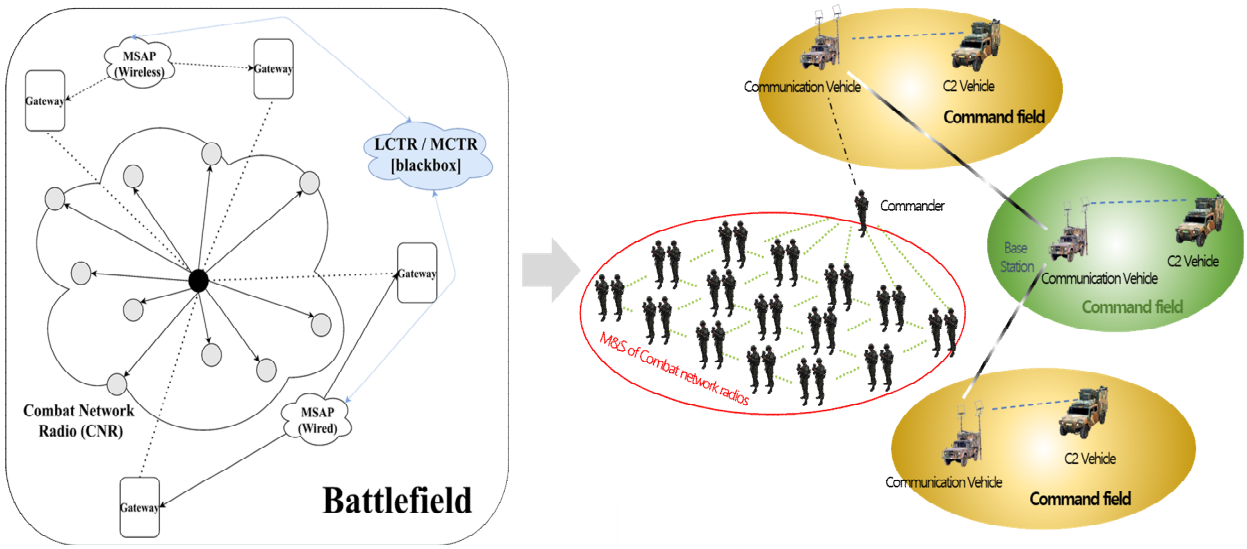


그림 6. NS-3 기반 단일 분대형 전투무선망 토폴로지

Fig. 6. Topology of single squad-type combat network radios with NS-3

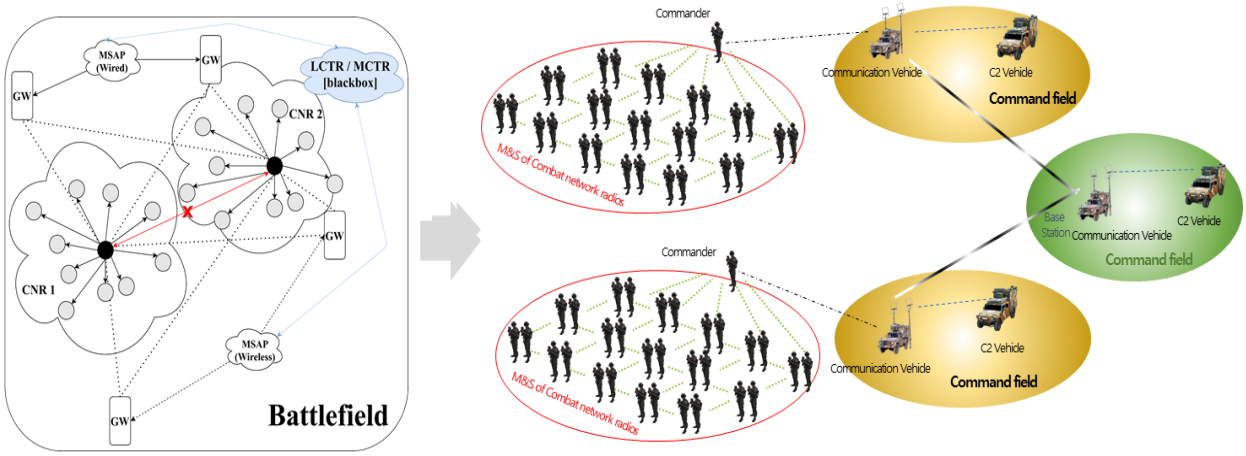


그림 7. NS-3 기반 다중 분대형 전투무선망 토폴로지

Fig. 7. Topologies of multiple squad-type combat network radios with NS-3

즉 대대급 성형 망에서는 대대장을 지휘관으로, 중대장을 분대원으로 노드화하고, 중대급 성형 망에서는 상급망 내 분대원이었던 중대장을 지휘관으로, 예하 소대장을 분대원으로 노드화하는 Top-Down 구조로 구성한다. 또한 군용 FM 무전기 기반 군 무선단말기의 장비-통신 제원을 활용하는 과업 수행 시에는 지휘관 중점의 성형 토폴로지 구조로 정형화하고, All-IP 기반 군용 SDR(Software-Defined Radio) 무전기 등의 차세대 군 무선단말기의 장비-통신 제원을 활용하는 작전 시나리오 적용 시 광범위한 무선 커버리지 및 기동 영역 보장을 위한 운용 교리에 따라, 링형 토폴로지 구조로서 논리화한다.

이에 대한 NS-3 기반 단일 및 다중 전투무선망 모의 개념도는 그림 6의 단일형과, 그림 7의 다중형으로서 기초한다. 여기서 지휘관 노드는 물리적인 성형 구조로서 추상화된 전투무선망 내 하위 분대원을 관리하며, 예하 분대원 노드에 대해 인증을 요청하고 검증할 시 중앙화된 관리 주체로서 동작한다. 그리고 대항군의 공세적 무선 위협이 발생하거나 전장 통신 환경의 급변에 따른 통신 노이즈 발생 시에도 예외 처리 기반으로 전투무선망 내 통신 품질을 임계치 이상으로 보장하기 위해 자동 개입하는 동적 모니터링 체계로서도 수행한다.

물론 같은 전장 환경 내에서 기동 중인 타 전투무선망 간 통신은 상위 부대 입회 하에만 가능하도록 독자적인 무선통신 채널 부설 권한이 제한된다. 분대원 노드는 전투무선망 내에서 지휘관 입회 하에만 적법한 통신을 수행하고 관련된 과업을 달성하도록 명령을 하달받는 수동적 객체로서, 향후 인증 요청에 따른 T-OTP 전달 매개체로서 동작한다. 즉 작전 수행을 위한 목적 외에는 전투무선망 내 통신 및 작전 목표 등에는 어떠한 개입도 불가능하도록 권한이 제한된다는 특징을 역시 가진다. 마지막으로 게이트웨이 노드는 군용 FM 무전기와 차세대 SDR 무전기 기반 무선 패킷 송수신을 위한 커버리지 확보와 릴레이 통신 무결성 보장 역시 수행하고자 도입된 중간자 객체로서, IEEE 802.11 또는 IEEE 802.16e (WiMAX) 기반 실질 애드혹 프로토콜 스택 인터페이스를 확장 제공하는 역할을 담당한다.

그에 따라 이러한 토폴로지, 시나리오, 인터페이스 구성에 근거하여, 정의된 전투무선망 내 애드혹 통신 관련 NS-3 파라미터는 표 2와 같이 총체적으로 산정되며, 군 고유 장비-통신 제원, 시나리오 및 작전 과업에 근거하여 상이하게 구성된다.

그에 따라 이러한 토폴로지 및 시나리오, 인터페이스 구성에 근거하여, 정의된 전투무선망 내 IEEE 802.11 및 802.16e 기반 애드혹 프로토콜 통신 관련 NS-3 파라미터 정보들은 표 2와 같이 총체적으로 정리된다. 이때 정의된 파라미터들은 산정된 군 고유 장비-통신 제원에 따라 상이하게 구성된다.

표 2. NS-3 기반 전투무선망 애드혹 구성을 위한 주요 파라미터
Table 2. Experimental parameters for configuration of ad-hoc-based combat network radios with NS-3

| Parameter (1/2) | Value | Parameter (2/2) | Value |
|---|---|---|---|
| Execution time (s) | 600 ~ 7,200 | Delay model | Constant speed propagation |
| Number of runs | 10 | Loss model | Friis, Okumura - Hata, Cost231 |
| Size of scenario (m) | 100x100 ~ 8,000x8,000 | TCP/IP stack | IEEE 802.11b, IEEE 802.11p |
| Number of nodes | 1:10 ~ 10:100 | Power (dBM) | 27 ~ 60 |
| Number of gateways | 1 ~ 10 | Interval routing (s) | 15 ~ 30 |
| Channel model | DSSS, OFDM (WNW) | Guard interval (ns) | 1600 |
| Channel capacity (bps) | 75 ~ 16,000 | Retransmission count | 3 |
| Bandwidth (kbps) | 256 ~ 2048 | RTT (s) | 9 |
| Frequency (MHz) | 30 ~ 512 | Protocol | AODV, OLSR, DSR, DSDV |
| Packet size (byte) | 300 ~ 1000 | VMF auth algorithm | proposed architecture, ECDSA[20] |
| Velocity of nodes (m/s) | 2 ~ 16 | mission-waypoint | 1, 50 ~ 100 |

표 2 내에서 시나리오 크기는 모의된 전투무선망의 기동 범위, 즉 전체 전장 영역을 나타내며, 애드혹 채널 모델은 All-IP 기반 차세대 전투무선망 내 WNW(Wideband Network Waveform)[21]이 기초로 한 OFDM(Orthogonal Frequency Division Multiplexing)을 중점으로 특성화한다.

또한 채널 용량과 대역폭, 주파수, 송수신 전력 세기 등은 공식적으로 보고된 군용 FM 무전기 등의 일부 제원 정보에 입각하여 정의하고, 지연 모델, 손실 모델, 라우팅 모델은 현 지상군의 전투무선망의 시공간적 운용과 관련된 파라미터로 근사화(Approximation)하여 고도화한다.

### 4.2 전투무선망 기동 시나리오 다종 구성

NS-3 기반으로 모의된 분대-차량-드론 엔터티 기반 전투무선망 내 제안 인증 아키텍처의 향상된 인증 성능을 실질 평가 검증 및 비교 분석하기 위해서는, 현 지상군의 전투무선망 운용 현황에 근거한 시나리오 산정이 요구된다. 이에 따라 하나의 임무점(Mission point)과 다수의 경로점을 중점으로 기동하는 군집형 분대 시나리오를 초기 구성함과, 산정된 엔터티 속성을 중점으로 표 2 내 파라미터를 재정의한다. 즉 엔터티 속성이 지상전술차량형이면, 그에 따라 송수신 전력과 대역폭, 주파수, 채널 용량, 기동 속도, TCP/IP 스택 등의 주요한 장비-통신 제원들의 값을 분대형보다 높게 변경하고, 드론형이라면 NLOS(Non-Line-Of-Sight propagation) 환경 지수를 더 높이 산출하는 지연 및 손실 모델이나 라우팅 프로토콜을 가지도록 재정립한다.

이에 따라 정형화 가능한 시나리오 개념도는 그림 8과 그림 9와 같이 도식화된다. 그림 8은 지상전술차량과 릴레이 통신용 드론이 노드화된 동적 애드혹 통신 환경을 중점으로 전투무선망 내 기동 태스크를 적용한 것으로, 두 개의 차량형 애드혹(VANET) 사이의 무선 통신 NLOS를 최소화하는 작전 과업을 나타낸다. 그림 9는 단일 및 군집통신 드론이 노드화된 항공형 애드혹(FANET) 통신 환경 내 기동 태스크와 관련된 작전 과업을 의미한다.

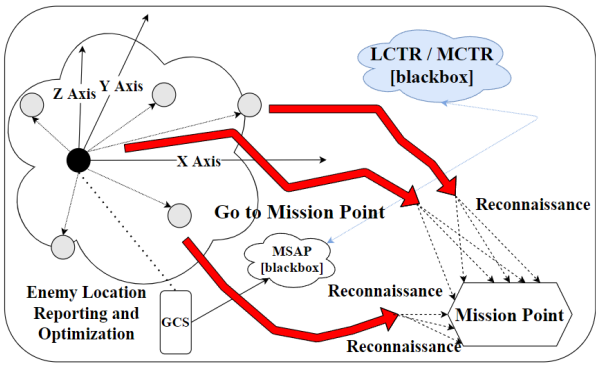


그림 9. NS-3 기반 드론형 전투무선망 기동 시나리오
Fig. 9. Maneuvering scenario of swarmming drone-type combat network radios with NS-3

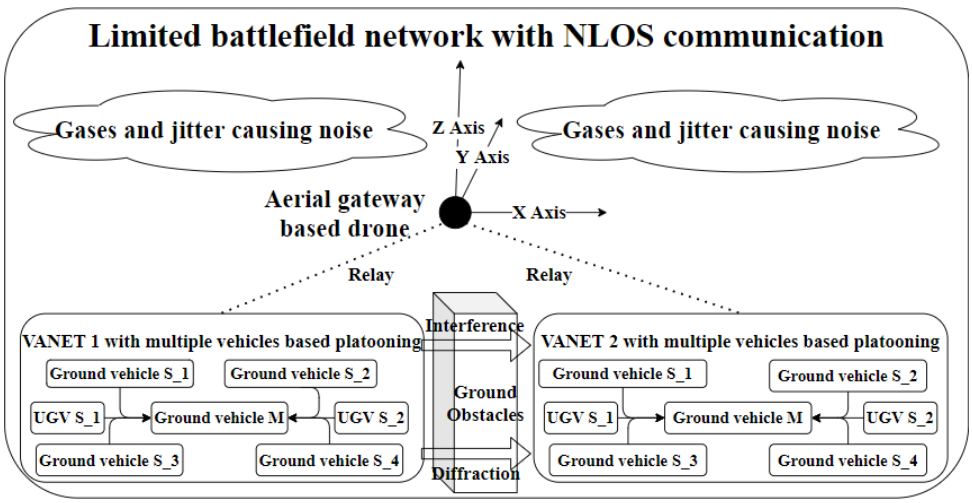


그림 8. NS-3 기반 차량형 전투무선망 기동 시나리오
Fig. 8. Maneuvering scenario of vehicle-type combat network radios with NS-3

### 4.3 주요 성능 평가

본 장에서는 제안한 T-OTP 기반 LSH 경량 해시체인 아키텍처의 VMF 전투무선망 내 향상된 인증 성능을 평가 검증하고, 타 인증체계 간 비교 분석을 수행한다. 이 때의 전투무선망은 대대급 이하 보병 지휘관 1명당 3명의 분대원으로 구성된 계층적인 분대 성형 망으로 정의하고, 관련 작전 과업은 하나의 임무점과 50개의 경로점에 기반한 기동 시나리오를 중점으로 한다. 그리고 성능 비교 실험과 관련된 동적 애드혹 통신, 기능, 손실, 환경 파라미터는 상술한 표 2에 기반하고, 제안 인증 아키텍처 내 주요 파라미터는 표 3으로 정립한다. 표 3 내 구성된 인증 파라미터를 기반으로, 그림 10과 같은 지휘관 및 분대원별 해시체인 T-OTP가 생성(10개)된다.

표 3. 분대형 전투무선망 해시체인 인증 파라미터 구성
Table 3. Configuration of hashchain-based authentication parameters in squad-type combat network radios

| Authentication parameter | Value |
|---|---|
| Hash function | SHA-256, SHA-512<br>LSH-256, LSH-512 |
| Minimum security strength (bit) | 128 |
| Length of URN (byte) | 32 ~ 512 |
| T-OTP size (byte) | 256 ~ 512 |
| Time slot length (s) | 30 |
| Length of hashchain | 20 ~ 240 |
| Number of keys | 1 |
| Standard of message encoding | BASE64 |

1) LSH-256 해시함수를 통해 생성된 T-OTP 해시체인

```
OhOG8Q6VoczG+lH9TKhBHH9s7MIEj8wvaL3ADDnbT5c=
VBodW9NBAHhlW7RjSdHtx5MK9vA8JFWoGCDZYDuenLY=
vgFaLDOk0RxPClJfCTa96OnoTE4/8fUoMPIQ2HZ9/g8=
egrA15d75rSWvRLFoRYbnFOfki0S9ubZlaGCi4cykio=
6mzcOKqCz++SDTdAWi0DqI7iRN0LgM4C9EnOWOFv1MQ=
G41C9iUejDc9tSKKI+xxfCrCV+3wTuvSTPOdRjYYHy8=
j/52W+Ri84VcKZXHoe9qNiBf2wZTLx89iwW+hzb3iV8=
NffqH/C+PhtiDtS4eT9hmQVdeXm12rAMffOyxNC19Aw=
gk+q8dxSxWcwMJb0AMOzedQvKhg0OW4xY43nT+waFCQ=
6S5rhRzV1/pw7M8tJiaz/LKG5ENEtFX+KhuR3zPN+b0=
```

2) SHA-256 해시함수를 통해 생성된 T-OTP 해시체인

```
Qkd0uc5Zc7147nrEMf+eEJUjO8u2Oz+X4K5OewMClT4=
hUrst1JVpPfQa+QeZHnahjwhcJ/Gn2e8O6g/HEe2SE8=
j++neSEPn2RU3BF6uhzHY9xvKA1IxpjuRYZdGxeqVPU=
dcwLUTQ5pCPtb5m8v5lPdLL5MCxD2WtRfd8IlWDjnfI=
Dp23pb72q7/Q5KcpfK1y1jmEpdysR6nnze89R8NMEL4=
CQ8eKlG3bEVHsRsBaMO8MTPu65tXER3Uu+W2jx5nP8Y=
uCi//WVDz8EF3GErRSF7Y251DVeW+/d32i4nHQ3noY0=
jfNh8udevAaUVDoyhLS7HfE8uixPBG82GF1d+uciYCo=
e6uUnCvasvfT9CcbArfuz5zfVEntCs1u+pDF+vjkXKQ=
I2BB5607ll/+vXYQuKbP24excXs/9mr3P+2yHoA+SmE=
```

그림 10. T-OTP 기반 LSH 해시체인 인증값 예시
Fig. 10. Example value of LSH-based hashchain authentication with T-OTP in combat network radios

관련된 비교 실험 결과 집합 (result set)은 그림 11부터 그림 15까지로 간략 정리된다. 먼저 그림 11은 극한의 전장 통신 환경 내에서의 SHA 또는 LSH 기반 타원곡선 전자서명 (ECDSA) 인증체계 간 비교 분석을, 트랜잭션 오버헤드 메트릭 기준으로 수행한 결과이다. 해당 그래프를 통해, T-OTP 기반 LSH 경량 해시체인 인증 아키텍처가 ECDSA 인증체계 대비 작전 수행 시간이 증가할수록 최소 18%에서 최대 263% 정도의 오버헤드 감쇄 효율성을 발휘함을 확인할 수 있다.

이러한 경향은 곧 주기적인 시간 간격에 기반하여 특정 분대원 통신 채널의 인증 유효성 범위를 제한하는 제안 인증 아키텍처 내 T-OTP의 직접적 인증 수행 개념이, 매번 송수신되는 요청-응답 패킷 내 메시지 서명에 기반하는 ECDSA의 간접적 인증 수행 개념보다 인증 성공을 위해 요구되는 트랜잭션이 더 적으며, 동시에 그림 12 내 총 네트워크 부하율 관련 메트릭 기준과 같이, 인증을 위해 해시화되는 난스(Nonce) 또는 다이제스트 역시 T-OTP가 ECDSA보다 더 작다는 사실에 기인함을 보여준다.

다음으로 그림 13과 그림 14는 동일한 제안 인증 아키텍처 내에서 LSH 또는 SHA 해시함수를 선택적으로 적용했을 시의 비교 분석을, 무선 애드혹 상에서의 총 인증 소요 시간과 하위 분대원 노드별 소요 시간 메트릭 기준으로 수행한 결과들이다.

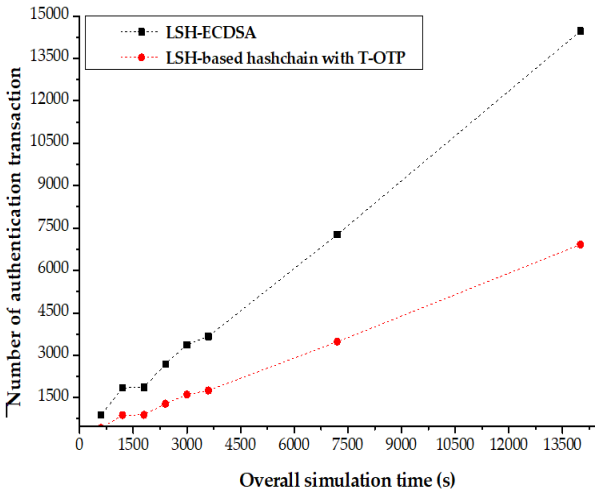


그림 11. 트랜잭션 오버헤드 기반 인증 성능 비교 분석
Fig. 11. Comparative analysis of authentication performance based on transaction overhead

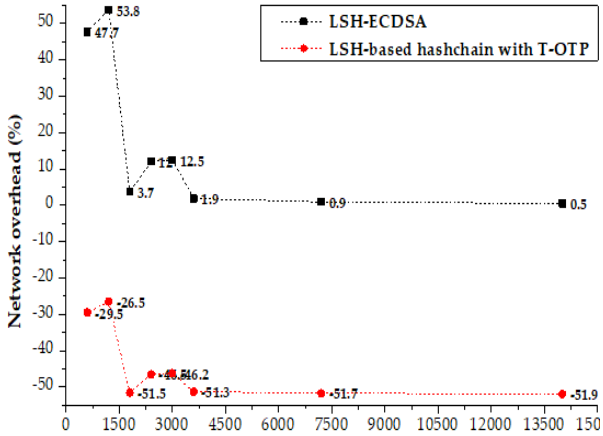


그림 12. 총 네트워크 부하율 기반 인증 성능 비교 분석
Fig. 12. Comparison analysis of authentication performance based on total network load ratio

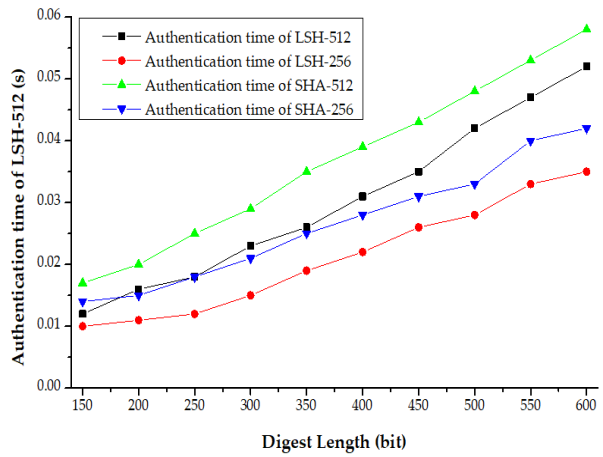


그림 13. 해시 함수 간 총체적 인증 소요 시간 비교 분석
Fig. 13. Comparison analysis of total authentication time between hash functions

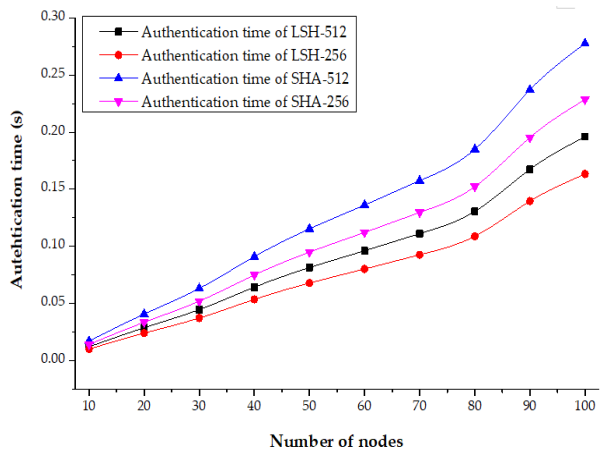


그림 14. 소속 노드 개수별 인증 소요 시간 비교 분석
Fig. 14. Comparison analysis of authentication time required by number of squad nodes

해당 그래프들을 통해, 임베디드 운용 경량화를 목적으로 연구개발된 대한민국의 LSH 표준이 기존 국제 표준인 SHA 대비 최소 3%에서 최대 42% 정도의 인증 소요 시간 감쇄 효율성을 산출함을 확인할 수 있다. 하위 분대원 노드 갯수 관련 결과 역시 노드 증가에 따라 각 인증 소요 시간 역시 선형적으로 증가하나, LSH가 SHA 대비 최소 2%에서 최대 57% 정도의 소요 시간 감쇄를 보인다. 이러한 경향은 곧 더 작은 길이의 고유식별번호 및 난스를 적용해도, 동일한 최소 보안성을 가진 T-OTP 인증값을 도출할 수 있는 LSH 해시함수 고유성이, 기존 SHA보다 효율적이라는 사실에 기인함을 보여준다.

마지막으로 그림 15는 인증 트랜잭션 비율과 키 관리 및 배포 비율, 송수신 패킷 크기 비율, 노이즈 감쇄를 위한 플래그 점검 비율 등의 세부 구성 메트릭들의 합계로서 정의한, 총 네트워크 오버헤드 메트릭이라는 기준을 중점으로, 동일 제안 인증 아키텍처 내 LSH와 SHA 간 비교 분석 결과이다.

이러한 그래프를 통해서도 전술된 그래프들과 동일하게, LSH가 SHA보다 낮은 네트워크 인증 오버헤드를 가짐을 재차 확인할 수 있다.

이로서 만일 극한의 전장 환경에서의 대대급 이하 분대형 전투무선망 내 분대원 및 단말기 인증과 데이터 무결성 보장이 요구될 시, 기존 VMF 인증에서 제안된 SHA-1 기반 전자서명 인증이나, 보다 개량된 SHA 또는 LSH 기반 ECDSA 인증체계보다, 제안한 T-OTP 기반 LSH 경량 해시체인 인증 아키텍처가 효율적임을 최종적으로 정리할 수 있다.

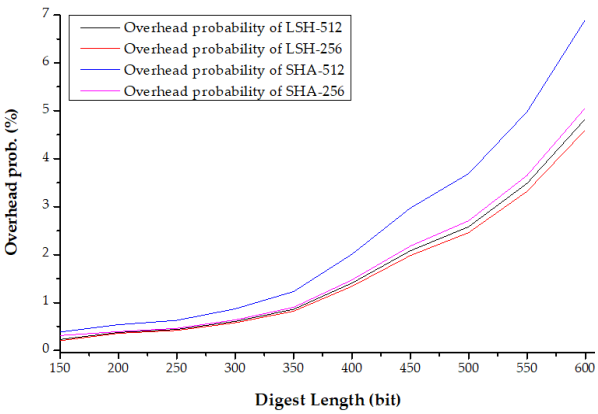


그림 15. 해시별 총 네트워크 오버헤드 기반 비교 분석
Fig. 15. Comparison analysis based on overall network overhead by hash function

이에 따라 분류 가능한 제안 인증 아키텍처의 Taxonomy는 표 4로 최종 정형화 가능하다.

표 4. 제안 인증 아키텍처와 ECDSA 간 Taxonomy
Table 4. Taxonomy between the proposed LSH-based hashchain authentication with T-OTP and ECDSA

| Property | Proposed architecture | ECDSA |
|---|---|---|
| Authentication strategy | T-OTP based direct authentication | indirect authentication based on signature and public key sharing |
| Key considerations | authentication and integrity assurance in CNRs | |
| Unit of authentication | T-OTP in hashchain | message hash |
| Minimum security strength and number of keys | 128bit, 1 | 512bit, 2 or more (private-public key) |
| Reliability and versatility | high, slightly high | slightly high, high |
| Major function | authentication, integrity, communication availability, non-repudiation, Non-forgery and non-reusable | user authentication, integrity, non-repudiation, Non-forgery and non-reusable, unaltered |
| Network overhead | greatly attenuated | slight increased, Significant increased when encryption is applied |
| Goal | securing lightweight authentication and integrity in CNRs | Securing the signature of tactical messages in CNRs |

## Ⅴ. 결론 및 향후 과제

본 논문에서는 급변하는 극한 전장 통신 환경 내 VMF 기반 전투무선망 보안 인증 한계성과 기능적 확장성을 확보하기 위해, T-OTP 기반 LSH 경량 해시체인 인증 모델을 개량된 VMF 프로토콜 인증 개념으로서 최초로 신규 제안하였다.

그리고 이를 위해 공식 제정된 해시 함수 및 인증 표준과 관련 오픈소스 라이브러리를 활용하여 제안 인증 아키텍처를 구체화하였으며, 실질 군 장비 및 통신 제원 정보와 작전 과업, 통신 교범 등에 모두 기반한 군집형 다종 무선 애드혹 통신 모델을 NS-3 기반으로 모의하고, 전투무선망의 내부 인증 통신 역시 추가 구현하였다. 이를 통해 타 인증체계 대비 개선된 인증 성능 효율성과 보안성, 통신 강건성 및 복원성의 향상 역시 군 기동 시나리오 기반으로 모두 검증하였으며, 동일 보안성 대비 감쇄된 네트워크 인증 트랜잭션의 수와 부하 비율, 소요 시간 및 오버헤드 등을 기록함을 역시 보였다.

그러나 산출된 비교 분석 결과들이 단순 네트워크 시뮬레이터 내에서 모의 구현된 전투무선망의 인증 통신 모의에 한정되었기에, 제안 인증 아키텍처가 실제 군 무선 단말기와 상세 통신 장비에 탑재되었을 시의 신뢰성은 완전히 확보하지 못함과 함께, 기동 과업 이외의 정찰 및 화력 투사 등의 추가적인 작전은 시나리오 내에서 정의하지 않았다는 한계점 역시 내포할 것이다. 따라서 향후에는 진보된 VMF 기반 전투무선망 내 제안 인증 아키텍처의 표준화를 중점으로, 실제 분대원 단말기 인증 및 데이터의 무결성 보장 스킴으로서 활용하고자 하며, 추가 개량 연구 역시 실질 군 무선 단말기와 통신 장비를 중점 테스팅을 기준으로 수행하고자 한다.

## References

[1] MIL-STD-2045/47001D (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: Oct. 21, 2021]

[2] Wang, Xiaoyun, Yiqun Lisa Yin, and Hongbo Yu. "Finding collisions in the full SHA-1", Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, pp. 17-36, Aug. 2005.

[3] ROCA Vulnerability (CVE-2017-15361), National Vulnerability Database, NIST. October 2017. Available online: https://nvd.nist.gov/vuln/detail/CVE-2017-15361. [accessed: Oct. 21, 2021]

[4] K. Dong-Chan, et al. "LSH: A new fast secure hash function family", International Conference on

Information Security and Cryptology (ICISC), Seoul, Korea, pp. 286-313, Dec. 2014.

[5] NS-3, Available online: https://www.nsnam.org. [accessed: Oct. 21, 2021]

[6] Lamport, "Password authentication with insecure communication", Communications of the ACM, Vol. 24, No. 11, pp. 770-772, Nov. 1981. https://doi.org/10.1145/358790.358797.

[7] Haller, "The S/Key™ one-time password system", Proceedings of the Internet Society Symposium on Network and Distributed System, pp. 151-157, Jan. 1994.

[8] Adrian Perrig, Ran Canetti, J. D. Tygar, and Dawn Song, "The TESLA broadcast authentication protocol", Rsa Cryptobytes, Vol. 5, No. 2, pp. 2-13, Nov. 2002. http://dx.doi.org/10.1007/978-1-4615-0229-6_3.

[9] Sencun Zhu, Shouhuai Xu, S. Setia, and S. Jajodia "LHAP: A lightweight hop-by-hop authentication protocol for ad-hoc networks", Proceedings of the 23rd International Conference on Distributed Computing Systems Workshops, Providence, RI, USA, pp. 749-755, May 2003. https://doi.org/10.1109/ICDCSW.2003.1203642.

[10] Rehan Akbani, Turgay Korkmaz, and G. V. S. Raju, "HEAP: Hop-by-hop efficient authentication protocol for mobile ad-hoc networks", Proceedings of the 2007 Spring Simulaiton Multiconference, Norfolk Virginia, USA, pp. 157-165, Mar. 2007.

[11] Haojun Zhang, Xiaoxue Li, and Rui Ren, "A novel self-renewal hash chain and its implementation", Proceedings of the IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, Shanghai, China, pp. 144-149, Dec. 2008. https://doi.org/10.1109/EUC.2008.74.

[12] Eldefrawy, et al., "OTP-based two-factor authentication using mobile phones", Proceedings of the Eighth International Conference on Information Technology: New Generations, Las Vegas, NV, USA, pp. 327-331, Apr. 2011. https://doi.org/10.1109/ITNG.2011.64.

[13] Bittl, "Efficient construction of infinite length hash chains with perfect forward secrecy using two independent hash functions", Proceedings of the 11th International Conference on Security and Cryptography (SECRYPT), Vienna, Austria, pp. 213-220, Aug. 2014.

[14] Dmitry Kogan, Nathan Manohar, and Dan Boneh, "T/Key: Second-factor authentication from secure hash chains", Proceedings of the ACM SIGSAC Conference on Computer and Communications, Dallas Texas USA, pp. 983-999, Nov. 2017. https://doi.org/10.1145/3133956.3133989.

[15] Yin, et al., "An efficient two-factor authentication scheme based on the Merkle tree", Sensors, Vol. 20(20), No. 5735, Oct. 2020. https://doi.org/10.3390/s20205735.

[16] Kim, et al., "A Study on the Concept of Using Efficient Lightweight Hash Chain to Improve Authentication in VMF Military Standard", Applied Sciences, Vol. 10 (24), No. 8999, Dec. 2020. https://doi.org/10.3390/app10248999.

[17] Korea Internet & Security Agency (KISA), Available online: https://seed.kisa.or.kr/kisa/Board/22/detailView.do. [accessed: Oct. 21, 2021]

[18] OpenSSL, Available online: https://www.openssl.org/. [accessed: Oct. 21, 2021]

[19] Dang, "Secure Hash Standard, Federal Inf. Process. Stds. (NIST FIPS)", National Institute of Standards and Technology (NIST), 2015, Available online: https://doi.org/10.6028/NIST.FIPS.180-4. [accessed: Oct. 21, 2021]

[20] National Institute of Standards and Technology (NIST), "Digital Signature Standard (DSS) - FIPS 186-5 (Draft)", 2019, Available online: https://csrc.nist.gov/publications/detail/fips/186/5/draft. [accessed: Oct. 21, 2021]

[21] Shahzad, Kashif, et al., "A novel hybrid narrowband/wideband networking waveform physical layer for multiuser multiband transmission and reception in software defined radio", Physical Communication, Vol. 36, No. 100790, Oct. 2019. https://doi.org/10.1016/j.phycom.2019.100790.

## 저자소개


### 서 상 (Sang Seo)

2020년 2월 : 경기대학교
AI컴퓨터공학부 (공학 학사)
2020년 3월 ~ 현재 : 경기대학교
AI컴퓨터공학부 석사과정
관심분야 : 사이버 기만, 능동적 이동 변이, 인증, 군사 보안

### 김 도 훈 (Dohoon Kim)

2005년 2월 : 고려대학교
수학/컴퓨터과학과 (이학 학사. 이중전공)
2007년 8월 : 고려대학교
컴퓨터과학과 (이학 석사)
2012년 2월 : 고려대학교
컴퓨터·전파통신학과 (공학 박사)
2018년 2월 : 국방과학연구소 선임연구원 (사이버 방호 & 정보보호 업무수행)
2018년 3월 ~ 현재 : 경기대학교 AI컴퓨터공학부 교수
관심분야 : 네트워크 보안, 봇넷, 리스크 분석

### 임 원 기 (Won-Gi Lim)

1994년 2월 : 건국대학교
전자계산학과 (공학 학사)
1996년 2월 : 건국대학교
컴퓨터공학 (공학 석사)
1996년 1월 ~ 현재 :
국방과학연구소 제2기술연구본부 책임연구원
관심분야 : 정보보호, 전술통신, 내장형 시스템