JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지 Vol. 26, No. 12: 1863~1871, Dec. 2022

사물인터넷 환경을 위한 경량화 키 위탁 기법

뚜언[1] · 이민우[2*] · 임재성[2]

Lightweight Key Escrow Scheme for Internet of Battlefield Things Environment

Vu Quoc Tuan[1] · Minwoo Lee[2*] · Jaesung Lim[2]

[1]Graduate Student, Department of Military Digital Convergence, Ajou University, Suwon, 16499 Republic of Korea
[2*]Professor, Department of Military Digital Convergence, Ajou University, Suwon, 16499 Republic of Korea

요 약

4차 산업혁명 시대에는 보안 네트워킹 기술이 국방 무기 체계에서 필수적인 역할을 하고 있다. 정보보안을 위해 암호 기술을 사용한다. 암호 기술의 안전성은 케르크호프의 원칙(Kerchoff's principle)에서 강조하듯 암호 기술 알고리즘이 아닌 암호 기술의 안전한 키 관리에 기반한다. 그러나, 전장 환경에서 무기체계의 잦은 이동으로 인해 네트워크 구조가 변하며 전통적인 중앙 집중식 키 관리 방법을 사용하기가 어렵다. 또한 IoBT(Internet of Battlefield Things) 환경에서 사용되는 각 노드의 시스템 자원은 크기, 용량, 성능이 제한되므로 기존의 키 관리 알고리즘보다 계산량과 복잡도가 적은 경량화 키 관리 시스템이 필요하다. 본 논문은 IoBT 환경을 위한 경량화 방식의 새로운 키 위탁 방식을 제안한다. 제안된 기법의 안전성과 성능을 수치 분석과 시뮬레이션을 통해 검증하였다.

ABSTRACT

In the era of Fourth Industrial Revolution, secure networking technology is playing an essential role in the defense weapon systems. Encryption technology is used for information security. The safety of cryptographic technology, according to Kerchoff's principles, is based on secure key management of cryptographic technology, not on cryptographic algorithms. However, traditional centralized key management is one of the problematic issues in battlefield environments since the frequent movement of the forces and the time-varying quality of tactical networks. Alternatively, the system resources of each node used in the IoBT(Internet of Battlefield Things) environment are limited in size, capacity, and performance, so a lightweight key management system with less computation and complexity is needed than a conventional key management algorithm. This paper proposes a novel key escrow scheme in a lightweight manner for the IoBT environment. The safety and performance of the proposed technique are verified through numerical analysis and simulations.

키워드 : 키 위탁, 전장 사물 인터넷, 경량화 암호, 샤미르 알고리즘

Keywords : Key Escrow, Internet of Battlefield, Lightweight Encryption, Sharmir Algorithm

Received 29 September 2022, **Revised** 12 October 2022, **Accepted** 24 October 2022

*** Corresponding Author** Minwoo Lee(E-mail:iminu@ajou.ac.kr, Tel:+82-31-219-3810)
Professor, Department of Military Digital Convergence, Ajou University, Suwon, 16499 Republic of Korea

Open Access http://doi.org/10.6109/jkiice.2022.26.12.1863 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

국방 분야에서 4차산업혁명 기술을 이용한 많은 첨단 무기체계가 게임 체인저(game changer)로써 등장하고 있다. 이 중에서 전장 사물인터넷(IoBT: Internet of Battlefield Things) 기술은 소형 센서와 정보통신 기술이 결합하는 사물인터넷 기술을 전장 환경에서 군의 감시정찰 체계로 운영하는 것이다.[1][2]

IoBT 기술에서는 각 노드 간 안전한 통신을 위해 암호 기술이 사용된다. 암호 기술의 안전성은 케르크호프의 원칙(Kerchoff's principle)에서 강조하듯 암호 기술 자체의 은닉보다는 암호 기술의 안전한 키 관리에 기반한다.

보안 통신에 사용되는 키를 안전하게 관리하기 위해, 일반적으로 별도의 키 관리 서버를 운영한다. 이러한 키 관리 서버는 키를 효율적으로 관리할 수 있지만, 키 관리 서버의 중앙관리 특성으로 인해 단일실패점(SPOF: Single Point of Failure) 위협이 있다. 그래서 키를 분산 보관하기 위해 키를 나누어 공유하는 키 위탁(key escrow) 방법이 사용된다.

이때 키를 나누어 안전하게 분산 보관하고, 필요할 때 키를 복원하기 위해 샤미르(Shamir) 비밀 공유 알고리즘이 사용된다.[3] 하지만, IoBT 환경에서 샤미르 비밀 공유 알고리즘으로 키를 위탁 관리하기 위해서는 다음과 같은 문제점을 해결해야 한다.

첫째, IoBT 환경에서는 수십 개에서 수백 개의 많은 수량의 노드가 사용된다. 그래서, 많은 노드를 대상으로 키를 효율적으로 분배하고, 동시에 공격자로부터 키를 안전하게 보호할 수 있어야 한다.

둘째, IoBT 환경에서 사용되는 각 노드의 시스템 자원은 크기, 용량, 성능 면에서 제한된다. 그래서 기존의 키 공유 알고리즘보다 계산량과 복잡도가 적은 경량화 암호 기술이 필요하다.

따라서 본 논문에서는 IoBT 환경에서 전치 암호(transposition cipher) 기술을 응용한 경량화된 암호 기술을 이용해서 샤미르 비밀 공유 알고리즘으로 나눈 키 조각(share, 이하 '쉐어')을 암호화하고, 암호화된 키 조각과 키 복구 정보를 드론들에 분산하여 위탁하고, 필요할 때 키를 복원할 수 있는 경량화 키 위탁 기법을 제안한다.

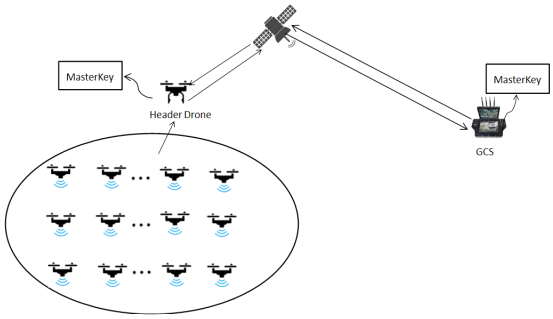

Fig. 1 Example of IoBT with drone swarming

본 논문의 구성은 다음과 같다. 2장에서는 군집 드론을 이용하는 IoBT 환경과 이러한 환경에 적용할 수 있는 키 위탁과 분산 보관 기술을 소개한다. 3장에서는 IoBT 환경에서 사용하기 위해, 전치 암호 기술을 응용하여 쉐어를 암호화하는 경량화 키 위탁 기법을 제안한다. 4장에서는 제안 기법의 처리 속도와 안전성을 수학적으로 검증하고, 시뮬레이션을 통해 샤미르 비밀 공유 알고리즘과 제안 기법의 성능을 비교한다. 그리고 5장에서 본 연구의 결론을 맺는다.

Ⅱ. 시스템 환경 및 관련 연구

2.1. 군집 드론을 활용한 IoBT 환경

그림 1은 수십 개의 소형 드론(drone)이 군집으로 운용되는 IoBT 환경을 보여준다. 이러한 환경에서는 군집 드론을 효율적으로 운용하기 위해, 헤더 드론(Header Drone)을 지정하고, 이 헤더 드론이 지상통제국(Ground Control Station)과 통신하는 방식이 사용된다. 헤더 드론과 지상통제국은 사전에 공유한 키를 가지고 보안 통신을 한다. 그리고, 헤더 드론은 이 키를 가지고 군집에 속한 다른 드론들과 보안 통신에 필요한 세션 키를 만든다.

만약 헤더 드론이 적의 공격으로부터 손실되면, 군집 드론들 사이에서 헤더 드론을 새로 지정해야 한다. 이 경우 새로운 헤더 드론은 지상통제국과 보안 통신을 하기 위해 기존에 사용 중이던 키를 복원할 수 있어야 한다.

2.2. 키 위탁과 분산 보관 기술

그림 1 환경에서 키를 복원하기 위해, 샤미르 비밀 공유 알고리즘이 사용될 수 있다. IoBT 환경에서는 드론

의 잦은 이동으로 인해 네트워크 구조가 변하며, 지상통제국과 드론 사이의 통신이 끊길 수도 있으므로, 중앙집중식 방법으로 키를 관리하는 것이 어렵다.

샤미르 비밀 공유 알고리즘은 키를 여러 개의 쉐어로 나눠서 위탁하고, 필요할 때 키를 복원할 수 있는 알고리즘이다. 이 알고리즘은 초기화 과정, 쉐어 분배 과정, 키 복원 과정의 3단계로 이뤄진다. 초기화 과정에서, 키를 n 개의 쉐어로 분할하고, 쉐어 분배 과정에서 쉐어를 n 명의 참가자에게 분배하여 쉐어를 위탁 관리한다. 키 복원 과정에서는 n 개의 쉐어 중에서 t 개 이상의 쉐어를 모아 원래의 키를 복구할 수 있다.

샤미르의 비밀 공유 알고리즘은 수식 (1)과 같이 서로 다른 t 개의 점을 갖는 t-1차 다항식의 해는 유일하다는 것을 이용한다. 예를 들어 서로 다른 점 3개가 있으면, 이 점들을 지나는 유일한 2차 다항식을 결정할 수 있다.

$$q(x) = a_0 + a_1 x + a_2 x^2 + ... + a_{t-1} x^{t-1} \quad (1)$$

수식 (1)과 같은 다항식에 존재하는 n 개의 점을 (t_1, q(t_1)), (t_2, q(t_2)..., (t_n, q(t_n))이라고 하면, 이들 n 개의 점들이 위탁 보관하는데 사용되는 쉐어가 된다. n 개의 쉐어 중에서 t 개 이상의 쉐어를 갖게 되면 다항식 보간법을 통해 원래의 다항식 q(x)를 알 수 있고, 최종적으로 원래의 키값인 a_0를 찾음으로써 키를 복원하게 된다.

2.3. 키 위탁 및 분산 보관 관련 연구

Drummond Reed는 키를 분산 관리하기 위한 DKMS (Decentralized Key Management System) 키 위탁 모델을 제안했다.[4] 키를 분실했을 때 키를 복원하기 위해, 샤미르의 비밀 공유 알고리즘으로 사전에 키를 나누어 백업하고 복원하기 위한 것이다. 하지만 이 모델에서는 쉐어에 대한 별도의 보호 절차 없이 평문 상태로 위탁기관에 전달하므로, 전달 과정에서 중간자 공격으로 키가 노출될 위험성이 높다.

Yoon의 연구는 공개키 알고리즘의 개인키를 안전하게 보관하고 복원하기 위한 방안을 제시하였다.[5] 개인키의 노출 방지를 위해, 키를 분할하여 쉐어를 보관할 수 있는데, 쉐어의 내용이 보호되지 않아 위임자 간 결탁의 위협이 있다.

Guojia의 연구는 위임자 간 결탁 위협을 해소하기 위해 키 소유자의 생체인증 정보를 사용하여 쉐어를 암호화하는 방안을 제안하였다.[6] 하지만 키 소유자의 생체인증 정보와 같은 고유 정보를 활용하기 어려운 경우에는 활용이 어렵다.

TakuNoguchi는 시스템 자원이 제한되는 MQTT (Message Queueing Telemetry Transport) 환경을 고려하여, 샤미르 알고리즘 기반의 경량화 키 공유 기법을 활용하는 방안을 제안하였다.[7] 하지만 이 연구에서도 쉐어에 대한 보호 대책이 없어서 중간자 공격이나 도난으로 인해 키를 노출 위험성이 높다.

드론이 지상통제국과 통신하기 위해 민간에서 사용하는 가장 대표적인 통신 프로토콜 중 하나는 MAVLink (Micro Air Vehicle Link)이다. 하지만 MAVLink는 경량화에 중점을 두어 보안이 다소 취약하다.[8][9]

이외에도 군집 드론 환경에서 안전한 통신을 보장하기 위해 디피-헬만 키 교환(Diffie-Hellman Key Exchange) 방법을 사용하여 무인기와 지상통제국 사이에서 키를 교환하는 방법에 관한 연구도 있다.[10][11] 하지만 D-H 키 교환할 때 중간자 공격 위협이 있고, D-H 키 생성을 위한 계산량 부담으로 인해 IoBT 환경에 적용하기는 적합하지 않다.

Ⅲ. 제안 기법

샤미르의 비밀 공유 알고리즘에 의하면, 키를 n개의 쉐어로 나누고, n명의 위탁 관리자(본 논문에서는 IoBT 단말)에게 하나씩 분배한다. 이 중에서 t개 이상의 쉐어를 갖고 있으면 키를 복구할 수 있다.

이때, 쉐어를 평문으로 분배하거나 IoBT 단말에 평문으로 보관하게 되면 중간자 공격이나 탈취로 인해 키가 복구될 위험이 있으므로, 이 연구에서는 새롭게 제안하는 전치 암호 기반의 경량화 암호화 기법을 사용해 쉐어를 암호화하는 방안을 제안한다. 표 1은 제안 기법에 사용된 기호에 대한 설명이다.

Table. 1 Notations used throughout the scheme

Notation	Description
M	Length of share
L	Length of nonce
S_i	i-th share
s_i	i-th share divided by d from Si

Notation	Description
t	Threshold value for recovery
n	Number of committee peer
d	Number of divisor
X_j	j-th location information
x_j	j-th location in nonce

3.1. 전치 암호 기법 기반 쉐어 암호화 기법

전치 암호(transposition cipher)는 평문의 문자 위치를 변경하여 암호문을 만드는 암호화 기법이다. 평문과 암호문의 문자(또는 문자열)가 일대일로 대응하기 때문에 암호문의 문자로 조합되는 경우의 수가 충분히 크면 암호문의 확산성을 높이기 때문에 안전성을 제공할 수 있다.

제안하는 쉐어 암호화 기법은 전치 암호 기법의 보안성을 향상시키기 위해 넌스(Nonce) 값을 기존의 쉐어와 결합하여 그림 2와 같이 확장 쉐어를 만든다. 이때 넌스는 키 소유자가 키를 위탁 관리하기에 앞서 임의적으로 만든 난수 값이다. 제안하는 기법은 다음과 같은 4가지 단계로 수행된다.

① L 길이를 갖는 넌스 값을 생성한다.

② 임의적으로 선택한 정수 d개로 쉐어 S_i를 나누어, $S_i = \{s_1, \dots, s_d\}$를 만든다($1 \le d \le M$). (단, s_d의 길이가 다른 s_i의 길이보다 짧은 경우에는 0으로 채운다.)

③ 넌스에서 서로 중복되지 않는 임의의 위치 값 d개를 만든다. $X_j = \{x_1, \dots, x_d\}$.

④ 임의적으로 $\{s_i, \dots, x_j\}$를 짝지어($1 \le i \le d$, $1 \le j \le d$), 나눠진 쉐어를 넌스의 x_j 위치에 삽입하여, 확장 쉐어 EXS_i를 만든다.

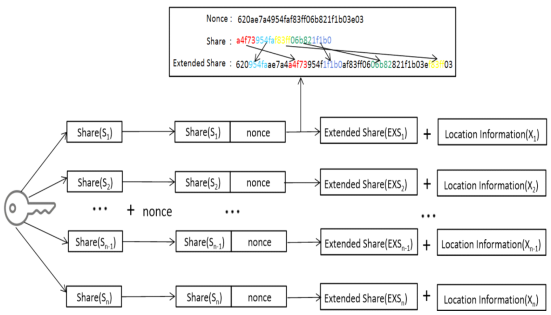

Fig. 2 Process for encrypting shares

3.2. 키 복원 과정

제안하는 기법을 통해 쉐어를 암호화하고 위탁된 확장 쉐어들로부터 원래의 키를 다시 복원하는 것은 그림 3과 같이 3단계 키 복원 과정으로 이뤄진다.

① t 개 이상의 확장 쉐어(EXS_i)와 위치 정보를 요청한다.

② t 개 확장 쉐어와 일치하는 짝의 위치 정보를 통해 쉐어(S_i)를 복원한다.

③ t 개 이상의 S_i를 이용하여 샤미르 비밀 공유 알고리즘을 통해 키를 복원한다.

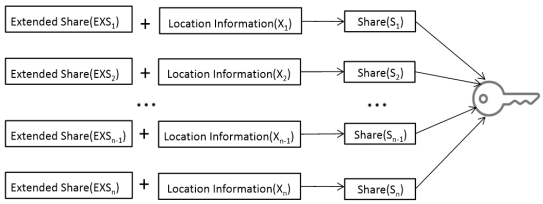

Fig. 3 Process of restoring a key

3.3. IoBT 환경 적용 예시

전장 상황에서 아군이 군집형 드론으로 구성된 IoBT를 이용하여 감시정찰 및 정보수집을 위한 임무에 사용할 수 있다.

그림 4는 군집 드론으로 이뤄진 IoBT를 대상으로 제안 기법을 적용한 예시이다. 전장에 배치되는 드론 중 헤더 드론이 있으며 이 드론은 나머지 드론들이 수집한 정보를 종합하여 위성을 통해 GCS에 전달한다. 그리고 안전한 통신을 위해 사전에 공유된 마스터 키를 사용해 암호화 통신한다. 마스터 키는 헤더 드론과 GCS만 갖고 있다. 만약 전장 상황에서 헤더 드론이 손실되면 나머지 드론 중에서 헤더 드론을 재선정한다. 재선정된 헤더 드론은 마스터 키가 있어야 GCS와 암호화 통신이 가능하다.

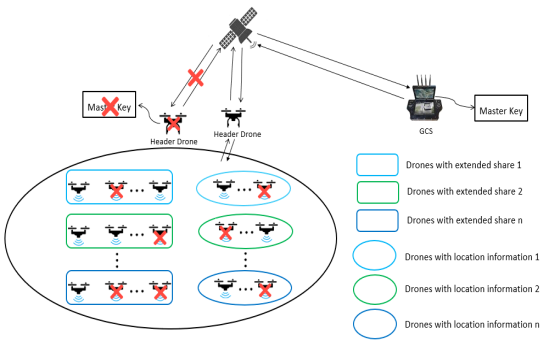

Fig. 4 Example of proposed scheme for IoBT

제안하는 키 위탁 기법으로 적용하면 마스터 키를 샤미르 알고리즘을 통해 여러 쉐어로 나누고, 제안된 암호화 기법을 통해 확장 쉐어와 쉐어의 위치 정보를 생성한다.

초기 설정되는 비율에 따라 확장 쉐어와 위치 정보를 IoBT 단말에게 할당한다. 이때 마스터 키를 복구하기 위해 재선정된 드론은 다른 드론들에게 확장 쉐어와 각각의 확장 쉐어의 위치 정보를 요청한다. 이를 통해 쉐어를 만들고 샤미르 알고리즘을 통해 t개 이상 쉐어를 이용해 마스터 키를 복구할 수 있다.

Ⅳ. 성능 검증

4.1. 제안 기법의 보안성

제안하는 알고리즘의 보안성은 다음과 같이 전수 공격(Brute force attack)의 어려움과 키 복원 정보(확장 쉐어, 위치 정보) 확보의 어려움을 통해 알 수 있다.

첫째, 길이가 L 인 넌스의 각 자리에 영문 소문자와 대문자, 숫자를 사용한다면, 넌스를 만들 수 있는 경우의 수는 62^L 개가 된다. 따라서, L의 길이가 충분히 길다면 전수 공격으로부터 키 노출을 보호할 수 있다.

둘째, 제안 기법 3.1의 ③번 단계에서 d에 의해 EXS_i가 만들어지는 조합의 경우 수는 ${}_LC_d$ 개이다. 따라서 전체 가능한 조합의 수는 수식 (2)와 같이 나타낼 수 있다. 하지만, d의 값은 키 소유자가 확장 쉐어를 만들 때만 필요하고, 외부로 전달되지 않으므로, 공격자는 d의 값을 알지 못한다.

$$\sum_{i=1_L}^{d} C_i = \sum_{i=1}^{d} \frac{L!}{i!\,(L-r)!} \tag{2}$$

수식 (2)의 값은 62^L에 비해 충분히 작은 값이므로, 본 제안 기법의 안전성은 L의 길이에 의존함을 알 수 있다. 그러므로 L의 길이를 충분히 길게(예, 256 bits) 사용하면 제안한 전치 암호 기반의 경량 암호 기법으로 보안성을 확보할 수 있다.

이와 함께, 제안하는 암호화 기법에서 넌스는 키 소유자가 확장 쉐어를 만드는 과정에서 한 번만 사용되기 때문에, 공격자는 키 복구를 위한 확장 쉐어 생성 정보를 직접 계산 할 수 밖에 없으므로, 키 복구 정보(확장 세어, 위치 정보)를 얻기 어렵다. 키를 복구하기 위해서는 샤미르 비밀 공유 알고리즘에 의해 t 개 이상의 확장 쉐어를 확보하고, 암호화를 풀기 위한 확장 쉐어에 대한 위치 정보가 필요하다.

따라서, 공격자는 전장에서 t개 이상 확장 쉐어를 확보해야 하며, 이와 동시에 t개 이상의 확장 쉐어에 대한 위치 정보도 확보할 수 있어야 한다. 그러므로, 공격자는 우선적으로 키 복원에 필요한 최소한의 드론을 탈취하기 위한 많은 노력(work factor)을 해야한다. 만약 2t 개 이상의 드론을 탈취하여도 키를 복원하기 위해서는 많은 계산량이 필요하다. 이에 대해서는 다음 절에서 성능 검증을 통해 확인한다.

4.2. 제안 기법의 효율성

제안 기법은 기존의 샤미르 비밀 공유 알고리즘을 대상으로 확장 쉐어를 만드는 과정이 추가되므로, 처리 효율성을 확인해야 한다. 이를 위해 표 2와 값으로 정의된 시뮬레이션 환경에서 쉐어의 길이(M)와 넌스의 길이(L)를 변화시키며 처리 속도를 확인하였다.

Table. 2 Notations used throughout the simulation

Notation	Description
T	Total of drones
E	Number of extended shares drones
l	Number of location information drones
T_s	Total of shares
H	Number of drones being hijacked
p	Quotient of H divided by 2

그림 5는 쉐어의 길이의 변화에 따른 알고리즘 처리 속도를 비교한 것이다. 넌스 값의 길이는 50비트로 설정하고 쉐어의 길이는 128비트부터 512비트까지 증가함에 따라 확장 쉐어를 생성하는데 소요되는 시간을 비교하였다. 최소 0.02밀리초에서 0.048밀리초가 소요되었다.

그림 6은 넌스의 길이의 변화에 따른 알고리즘 처리 속도를 비교한 것이다. 쉐어의 길이를 128비트로 고정하고 넌스의 길이를 128비트에서 512비트까지 증가함에 따라 확장 쉐어를 생성하는데 소요되는 시간을 비교하였다. 최소 0.031밀리초에서 0.071밀리초가 소요되었다.

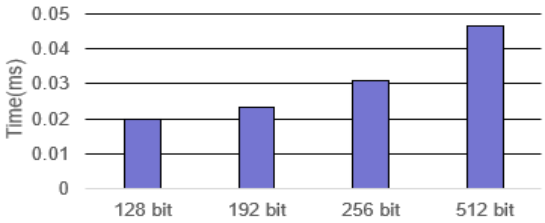

Fig. 5 Comparison of processing speed according to length of the share(M)

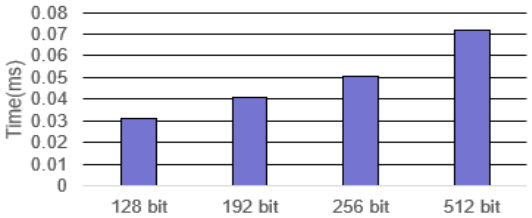

Fig. 6 Comparison of processing speed according to length of the nonce(L)

따라서, 이상의 시뮬레이션 결과를 보면, 드론과 같이 빠른 이동 속도로 임무를 수행하는 경우에도 제안 기법이 IoBT 환경에서 큰 영향 없이 적용될 수 있을 정도로 효율적이라고 볼 수 있다.

4.3. 공격자에 의한 키 복원 모의 공격 시뮬레이션

4.3.1. 키 복원 확률 수식 분석

제안 기법의 안전성을 검증하기 위해 공격자에 의한 키 복원 모의 공격 시뮬레이션을 수행하였다. 공격자에 의한 키 복원 확률은 확장 쉐어와 위치 정보를 갖고 있는 드론의 비율, 쉐어의 수, 키 복원에 필요한 쉐어의 개수(t)에 영향을 받는다.

모의 공격 시나리오에서는 기존에 사용되는 샤미르 비밀 공유 알고리즘만 적용할 때 탈취되는 드론 수에 따라 공격자에 의한 키 복원 확률을 비교하였다. 이를 위해 초기 변수를 표 3과 같이 설정하였다. 본 시나리오에서는 공격자가 키를 복원하기 위해서는, 공격자가 탈취한 드론 중에 겹치지 않는 3 개 이상의 쉐어(즉, t=3)가 있어야 한다. 이 경우 공격자에 의한 키 복원 확률은 다음과 같이 수식으로 분석할 수 있다.

Table. 3 Variables used throughout the simulation

Variable	Shamir Algorithm	Proposed scheme
T	100	100
E	Not Applicable	80
l	Not Applicable	20
T_s	5	5
t	3	3

먼저 100 개 드론 중에 H 개의 드론은 뽑을 수 있는 경우의 수는 ${}_{100}C_H$ 이다. 이 중에서 하나의 쉐어를 20 개씩 드론에 나누어 보관한다고 가정한다.

H 개의 드론이 탈취할 때 키를 복원할 수 없는 경우는 다음 2가지로 나눌 수 있다. 첫째는 탈취되는 H 개 드론 중에 같은 쉐어 종류만 있는 것이고, 둘째는 2개의 쉐어 종류를 갖고 있는 것이다. H 개 드론을 탈취했는데, 같은 쉐어의 종류만 있는 경우의 수는 $5\times{}_{20}C$ 가 된다.[1)]

공격자가 탈취한 H 개의 드론 중에 2가지의 쉐어가 있는 경우에는, 5가지 쉐어 중에 2가지의 쉐어를 선택하는 경우이므로, ${}_5C$개가 된다.

H개의 드론 중에 1가지의 쉐어를 갖는 i개의 드론이 있다고 가정하면, 나머지 드론에는 다른 종류의 쉐어가 H-i 개가 있다($1 \le i < H$).

H가 짝수 개가 아닌 경우에서는 H개 드론 중에서 2가지 종류의 쉐어로 나눌 수 있는 경우의 수는 2p 개이며, 각 경우에서 나올 수 있는 경우의 수는 ${}_{20}C_i \times {}_{20}C_{H-i}$ $(1 \le i < H)$이다. 따라서 키를 복원할 수 있는 확률은 다음 식 (3)과 같이 나타낼 수 있다.

$$1-\frac{5\times{}_{20}C}{{}_{100}C_H}-\frac{2\times{}_5C_2\sum_{i=1}^{p}({}_{20}C_i\times{}_{20}C_{H-i})}{{}_{100}C_H} \tag{3}$$

H가 짝수 개일 때 H개 드론 중에 쉐어가 2가지 종류인 경우의 수는 2p-1 개이며, 각 경우에서 나올 수 있는 경우 수는 ${}_{20}C_i\times{}_{20}C_{H-i}(1 \le i < H)$ 개가 된다. 따라서 이 경우에 키를 복원할 수 있는 확률은 수식 (4)와 같이 나타낼 수 있다.

$$1-\frac{5\times{}_{20}C}{{}_{100}C}-\frac{2\times{}_5C_2\sum_{i=1}^{p-1}({}_{20}C_i\times{}_{20}C_{H-i})+{}_5C_2\times{}_{20}C_p\times{}_{20}C_{H-p}}{{}_{100}C} \tag{4}$$

제안하는 기법에서 키를 복원할 수 있는 조건은 탈취

1) 여기에서는 쉐어의 갯수가 5개이므로 5를 곱한다.

되는 드론 수 중에 겹치지 않는 t개 이상의 확장 쉐어가 있어야 하고 확장 쉐어와 일치하는 위치 정보 쌍이 있어야 한다. 탈취되는 드론 수중에 t쌍 이상의 확장 쉐어와 위치 정보가 있으면 키를 복원할 수 있다. [2)]

탈취되는 드론 수가 증가하면 키를 복원할 수 있는 경우의 수가 증가하며, 각각의 경우마다 확률을 계산하는 수식 및 조건이 달라진다. 예를 들어, 만약 6개 드론이 탈취되면 키를 복원할 수 있는 확률이 다음과 같은 방식으로 계산할 수 있다.

100개 드론 중에 6개 드론을 뽑을 수 있는 경우는 ${}_{100}C$ 개가 된다. 6개의 드론을 가지고 키를 복원하기 위해 겹치지 않는 3개의 확장 쉐어와 위치 정보 쌍이 있어야 하며, 5개 종류의 쌍 중에 3개 종류 쌍을 뽑을 수 있는 경우 수는 ${}_5C_3$ 개다.

확장 쉐어를 가지고 있는 드론 수가 80개이고, 위치 정보를 가지고 있는 드론 수가 20개이면, 각각 한 종류의 확장 쉐어를 가진 16개의 드론이 있고 한 종류의 위치 정보를 가진 4개 드론이 있다.

따라서 하나의 쌍을 만들 수 있는 경우 수는 ${}_{16}C_1 \times {}_4C_1$ 개이다. 3개 쌍을 만들 수 있는 경우의 수는 ${}_5C_3 \times ({}_{16}C_1 \times {}_4C_1)^3$ 개다. 그러므로, 6개의 드론이 탈취되었을 때, 키를 복원할 수 있는 확률은 수식 (5)와 같이 나타낼 수 있다.

$$\frac{{}_5C_3 \times ({}_{16}C_1 \times {}_4C_1)^3}{{}_{100}C_6} \tag{5}$$

4.3.2. 키 복원 확률 시뮬레이션 분석

시뮬레이션을 통해 공격자에 의해 탈취된 드론의 수량에 따라 공격자가 키를 복원할 수 있는 확률을 평가했다. 각 환경에서 알고리즘을 100 만 번을 수행해 평균값을 계산했다.

먼저 확장 쉐어와 위치 정보를 갖고 있는 드론의 비율에 따라 공격자가 키를 복원할 수 있는 확률을 분석하였다. 드론 총 수량은 100개이고, 탈취되는 드론 수는 10개일 때, 샤미르 비밀 공유 알고리즘을 통해 5개의 쉐어를 만들고 키를 복원하는데 필요한 쉐어의 개수는 3개이다 (즉, T=100, T_s=5, H=10, t=3)

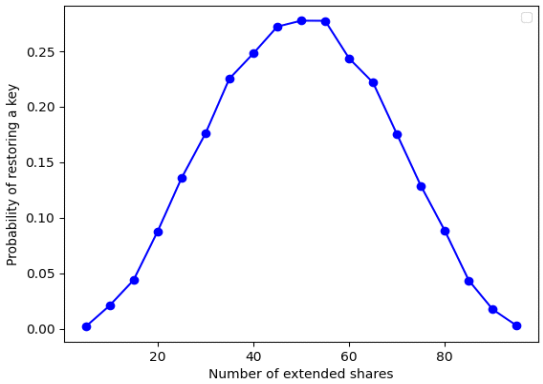

Fig. 7 Probability of key restoration according to the percentage of expansion shares

그림 7은 확장 쉐어를 가지고 있는 드론 수의 변경에 따라 공격자가 키를 복원할 수 있는 확률을 비교한 것이다. 이에 따르면 확장 쉐어의 수가 전체 드론 수 중에 25% 이하 또는 75% 이상 차지하면 10개 드론이 탈취되어도 키를 복원할 수 있는 확률이 10% 보다 더 작다. 따라서 제안 기법을 적용하면 전체 드론 중에서 확장 쉐어를 가지는 드론 수가 25% 이하 또는 75% 이상을 차지하는 경우 공격자가 키를 복원할 수 있는 확률은 낮아지므로 그만큼 안전하다고 볼 수 있다.

그림 8은 제안 기법과 기존에 사용되는 샤미르 비밀 공유 알고리즘에서 탈취되는 드론의 수에 따른 공격자의 키 복원 확률을 비교한 것이다. 이에 따르면 제안하는 키 위탁 기법이 기존에 있는 방법보다 공격자의 키 복원 확률이 훨씬 낮은 것을 확인할 수 있다.

다음은 제안 기법과 기존에 사용되는 샤미르 비밀 공유 알고리즘에서 임의값(t)을 변경하여, H개 드론이 탈취되었을 때 공격자가 키를 복원할 수 있는 확률을 비교하였다. 시뮬레이션에 사용된 변수는 표 4와 같다.

Table. 4 Variable for Fig. 9

Variable	Shamir Algorithm	Proposed Scheme
T	100	100
E	Not Applicable	80
l	Not Applicable	20
T_s	10	10
H	10	10

2) 예를 들어, 확장 쉐어를 가지고 있는 드론의 수가 80개이고, 위치 정보를 가지고 있는 드론의 수가 20개가 있을 때, 키를 5개 쉐어로 나누면 키를 복원하기 위해 3개 이상의 쉐어가 필요하다. 즉, 탈취되는 드론 수가 최소 6개 이상 되어야 키를 복원할 수 있다.

그림 9는 시뮬레이션을 통해 임의값 t가 증가함에 따라 공격자의 키를 복원할 수 있는 확률이 감소하는 것을 볼 수 있다. 기존의 샤미르 비밀 공유 알고리즘을 사용하는 경우 임의값을 6개 이하로 설정하면 키를 복원할 수 있는 확률이 거의 99%에 가깝고, 제안 기법을 적용하는 경우 임의값을 6개 이상으로 설정하면 키를 복원할 수 있는 확률이 매우 낮은 것을 확인할 수 있다.

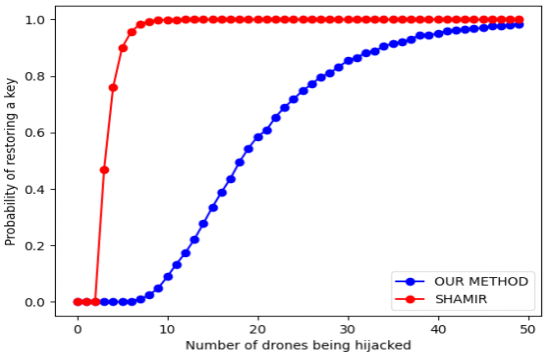

Fig. 8 Probability of key restoration according to the number of drones being hijacked

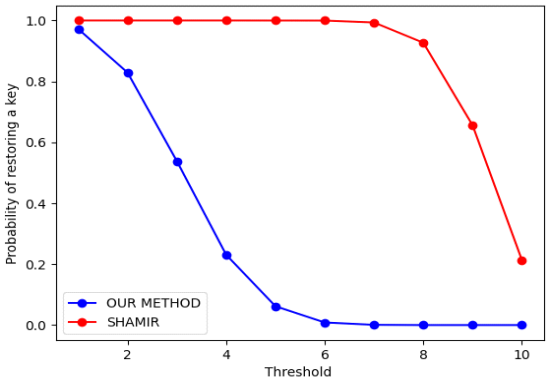

Fig. 9 Probability of key restoration according to the number of threshold value

Ⅴ. 결 론

본 논문은 IoBT 환경을 위한 경량화 키 위탁 관리 기법을 다루었다. 기존 샤미르 비밀 공유 알고리즘의 쉐어(키 조각)를 전치 암호 기술 기반의 경량 암호 기술로 새로운 확장 쉐어를 생성하고 복원하는 방법을 제안하였다. 그리고 제안 기법의 보안적 안전성을 수학적 분석과 시뮬레이션을 통해 검증하였다.

시뮬레이션 결과, 제안 기법이 기존 방법에 비해 키 길이가 길어지는 특성을 갖고 있지만, 전장환경의 전투 임무수행 시간을 고려해서 넌스 값을 50비트로 설정하면, IoBT 환경에서 수 시간 내의 임무 시간 동안 충분한 안전성을 제공할 수 있다. 향후 적정한 넌스 길이와 안전성, 그리고 드론 무선통신 링크 특성을 고려한 추가 연구를 수행할 예정이다.

ACKNOWLEDGEMENT

This paper is a basic research project conducted with the support of the Korean Research Foundation with the funding of the government (Ministry of Education) in 2021. (No. NRF2021R1I1A1A01047914)

References

[1] S. Russell and T. Abdelzaher, “The Internet of Battlefield Things: The Next Generation of Command Control, Communications and Intelligence (C3I) Decision-Making,” *IEEE Military Communications Conference*, Los Angeles: CA, USA, pp. 29-31, 2018.

[2] L. Zhu and S. Majumdar, “An invisible warfare with the internet of battlefield things: A literature review,” *Human Behavior and Emerging Technologies*, vol. 3, no. 2, pp. 255-260, Nov. 2020.

[3] A. Shamir, “How to Share a Secret,” *Communications of the ACM*, vol. 22, no. 11, pp. 612-613, Nov. 1979.

[4] D. Reed, J. Law, D. Hardman, and M. Lodder, “DKMS (Decentralized Key Management System) Designand Archite cture V3,” *U.S. Department of Homeland Security Science & Technology Directorate*, Apr. 2018.

[5] T. -Y. Yoon and J. -S. Moon, “Private Key Backup and Recovery Framework in Blockchain-based Service Environment,” *Journal of Digital Contents Society*, vol. 20, no. 12, pp. 2485-2493, Dec. 2019.

[6] G. Li, L. You, G. Hu, and H. Liqin, “Recoverable Private Key Scheme for Consortium Blockchain Based on Verifiable Secret Sharing,” *KSII Transactions on Internet And Information System*, vol. 15, no. 8, pp. 2865-2878, Aug.

2021.

[7] T. Noguchi, M. Nakagawa, M. Yoshida, A. G. Ramonet, “A Secure Secret Key-Sharing System for Resource-Constrained IoT Devices using MQTT,” in *Proceedings of International Conference on Advanced Communications Technology(ICACT)*, PyeongChang, Korea, pp. 147-153, 2022.

[8] A. Koubaa, B. Qureshi, M. -F. Sriti, A. Allouch, Y. Javed, M. Alajlan, O. Cheikhrouhou, M. Khalgui, and E. Tovar, “Dronemap Planner: A service-oriented cloud-based management system for the Internet-of-Drones,” *Ad Hoc Networks*, vol. 86, pp. 46-62, Apr. 2019.

[9] Y. M. Kwon, J. Yu, B. M. Cho, Y. Eun, and K. -J. Park, “Empirical Analysis of MAVLink Protocol Vulnerability for Attacking Unmanned Aerial Vehicles,” *IEEE Access*, vol. 6, pp. 43203-43212, Aug. 2018.

[10] M. Shin and S. Kim, “A Study on the Security Framework in IoT Services for Unmanned Aerial Vehicle Networks,” *Journal of Korea Multimedia Society*, vol. 21, no. 8, pp. 897-908, Aug. 2018.

[11] T. -W. Kim, S. -Y. Lee, S. W. Jung, H. Wi, and O. Yi, “A Research on the Security of Drone Control Data Using Quantum Entropy-Based Random Number Genera,” *Journal of The Korea Institute of Information Security & Cryptology*, vol. 31, no. 2, pp. 133-144, Apr. 2021.

뚜언(Vu Quoc Tuan)

2021년 2월 : 대한민국 공군사관학교 컴퓨터 공과 학사
2021년 3월~현재 : 아주대학교 국방디지털융합학과 석사
※관심분야 : 네트워크 보안, 사이버전

이민우(Minwoo Lee)

1998년 3월 : 한국항공대학교 항공통신정보공학과 학사
2013년 2월 : 아주대학교 일반대학원 NCW공학 박사
2019년 3월~현재 : 아주대학교 국방디지털융합학과 대우교수
※관심분야 : 위성통신, 네트워크보안, 사이버전자전

임재성(Jaesung Lim)

1983년 2월 : 아주대학교 전자공학 학사
1985년 2월 : KAIST 영상통신 석사
1994년 8월 : KAIST 디지털통신 박사
1995년 9월~1998년 2월 SK텔레콤 중앙연구원 책임연구원
1998년 3월~현재 : 아주대학교 국방디지털융합학과 정교수
2006년 8월~현재 : 아주대학교 국방전술네트워트 연구센터장
※관심분야 : 이동 및 위성통신, 무선네트워크, 국방전술통신