https://doi.org/10.33778/kcsa.2022.22.4.025

FANET에서의 비밀분산 기반 노드 인증

양 지 훈*, 이 수 진**

요 약

본 논문은 군집 드론, 무인기 편대 운용 시 자율적인 통신망 구축을 위해 활용 가능한 FANET(Flying Ad-Hoc Network)에 적용할 비밀분산 기반의 신속한 노드 인증 기법을 제안한다. FANET 환경에서 운용되는 각 노드는 필드에 전개되기 이전에 지수 분산비밀(share), 지수 원본비밀(secret) 및 PUF CRP(Challenge-Response Pair) 테이블 중 일부분을 저장한다. 필드에 배치된 이후 네트워크 형성 초기 단계에서 각 노드는 ID, 지수 분산비밀과 자신의 PUF Response 및 의사난수가 결합되어 해시 된 값을 네트워크로 브로드캐스트한다. 개별 노드는 이웃 노드들로부터 전송받은 지수 분산비밀을 이용, 지수 원본비밀의 복원 연산을 수행한다. 지수 원본비밀이 복원되면 연산에 사용된 지수 분산비밀을 전송한 모든 노드에 대한 동시 인증이 완료된다. 잘못된 지수 분산비밀을 전송하여 인증과정에서 원본비밀 복원을 방해하는 노드는 원본비밀 복원 연산을 수행하기 이전에 PUF 값을 검증하여 탐지하고, 복원 연산에서 배제한다.

Secret Sharing based Node Authentication in FANET

Yang Ji Hun*, Lee Soo Jin**

ABSTRACT

This paper proposes a secret sharing based fast node authentication technique applicable to Flying Ad-Hoc Network (FANET) that can be used to construct self-organized communication network in multi drones and drone squadrons operations. Before deployment, each node stores an exponential share, exponential secret and a portion of PUF CRP table. After being deployed in the field, in the early-stage of network formation, each node broadcasts its ID, exponential share and a hash value of PUF Response and pseudo-random number. Then each node performs a reconstruction of the exponential secret using the exponential shares transmitted from neighboring nodes. When the exponential secret is reconstructed, simultaneous authentication is completed for all nodes that have transmitted the exponential share used in the reconstruction. A node that transmits an incorrect exponential share to disturb the reconstruction of the exponential secret during the authentication process can be detected before performing the reconstruction through the verification of the hash value, and will be excluded from the reconstruction.

Key words : Flying Ad-Hoc Network, Authentication, Secret Sharing, PUF

접수일(2022년 09월 23일), 수정일(2022년 10월 27일), 게재확정일(2022년 10월 31일)

* 국방대학교/국방과학학과 (주저자)
** 국방대학교/국방과학학과 (교신저자)

1. Introduction

최근 드론 기술의 발전에 따라 다양한 분야에서 드론이 기존 모빌리티를 대체하거나 새로운 영역을 만들어내고 있다. 특히 군사 분야에서 드론은 현재 진행 중인 러시아-우크라이나 전쟁에서 보듯이 다양한 임무를 수행하면서 전장의 게임체인저로서의 역할을 확실하게 수행하고 있다. 전쟁에서 활용되는 드론은 소형 배회탄(Loitering Munition)부터 미사일을 발사할 수 있는 대형 공격 드론까지 스펙트럼이 넓다.

임무수행 과정에서 드론 대부분은 주로 1대씩 지상통제시스템을 이용하여 통제하는 방식으로 운용되고 있다. 그러나 넓은 전장 환경에서 다양한 임무를 수행하는 다수의 드론, 혹은 군집드론을 효율적으로 통제하기 위해서는 지상통제시스템의 개입을 최소화하는 방법이 필요하다.

이를 위해 최우선으로 고려해 볼 수 있는 방안은 Flying Ad-Hoc Network(이하 FANET) 기술이다. FANET은 Mobile Ad-Hoc Network(이하 MANET)를 기반으로 만들어진 통신기술로서, 사전에 구축된 기반구조가 없더라도 다수의 드론 또는 무인비행체가 동시에 상호 통신을 수행할 수 있도록 해준다. 그러나 FANET의 근간이 되는 MANET은 무선을 기반으로 하므로 다양한 보안취약점을 가질 수 있어 보안대책의 적용이 매우 중요하다. 특히 네트워크 형성 초기에 신뢰할 수 있는 노드들만으로 안전한 네트워크를 구성하기 위한 노드 인증이 반드시 수행되어야 한다.

MANET에서의 노드 인증과 관련된 선행연구들은 대부분 대칭키 암호를 기반으로 하며, 과도한 통신비용과 동일 비밀키의 계속된 사용으로 인한 비밀키 노출 가능성이 한계로 지적되어 왔다. 그리고 대칭키 암호를 이용한 인증은 일대일 방식으로 진행되기 때문에 이동성으로 인해 신속하게 네트워크 토폴로지가 변화하는 FANET 환경에 적용하기는 쉽지 않다. 공개키 암호를 기반으로 한 노드 인증의 경우에는 공개키 인증을 위한 인증기관의 구성이 제한된다는 결정적인 한계를 가진다.

이러한 문제를 해결하기 위해 본 연구에서는 비밀분산 기법을 적용하여 FANET에 참여하는 노드들이 필드에 배치되기 이전에 저장하는 분산비밀키와 원본비밀키를 이용하여 다수의 노드를 동시에 인증하는 기법을 제안한다. 그리고 원본 비밀키 복원을 위한 연산을 방해할 목적으로 잘못된 분산비밀을 전송하는 공격자를 조기에 탐지하기 위해 PUF(Physical Unclonable Function, 이하 PUF)를 기반으로 한 대응 방안을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 비밀분산의 개념과 MANET을 위해 제안되었던 인증기법에 대해 살펴본다. 3장에서는 제안하는 기법을 단계별로 설명하고, 4장에서는 제안 기법의 효율성과 안전성을 분석한다. 마지막으로 5장에서 연구 결과를 요약하고, 결론을 맺는다.

2. Preliminaries

2.1 비밀분산

비밀 공유(Secret Sharing)라고도 지칭되는 비밀분산은 일정 수 이상의 분산비밀이 모이면 원본비밀키나 코드를 복원할 수 있어 중요 정보의 분산 저장 및 권한의 분산 등을 위해 다양하게 응용되고 있다.

전통적인 비밀분산 기법을 보완하기 위해 반도체 공정특성을 이용한 PUF 기술을 활용하는 비밀분산 기법에 관한 연구도 진행되었다. Chen. S 등은 Shamir의 Secret Sharing을 활용한 PUF 기반의 인증 방법을 제안하였다[1]. Mahabub Hasan 등은 PUF 기반의 안전하고 가벼운 인증 및 무선 센서 네트워크를 위한 키 공유 방식을 제안하였다[2].

2.1.1 임계치 기반의 비밀분산 기법

(t, n) 임계치 비밀분산 기법에서, n은 비밀분산에 참여하는 전체 참여자의 수, 즉 생성될 분산비밀의 수를 의미한다. 원본비밀은 이를 복원하는 데 사용할 수 있는 n개의 분산비밀로 나누어진다. 임계치 t는 원본비밀을 복원하는데 필요한 최소한의 분산비밀 수를 의미하며, 임계치 이하의 분산비밀로는 절대 원본비밀을 복원할 수 없다. 대표적인 비밀분산 기법으로는 다항식을 이용한 Shamir의 기법[3], 평면과 교차점의

개념을 이용한 Blakley의 기법[4], 중국인의 나머지 정리를 이용한 기법 등이 있다.

2.1.2 검증 가능한 비밀분산 기법

분산비밀을 분배할 때 분산비밀의 유효성을 검증할 수 있는 추가적인 정보를 같이 분배하여 언제든지 참여자가 자신이 보유하고 있는 분산비밀이 일관성을 유지하고 있는지를 확인할 수 있는 기법이다. 비밀분산 기법에서는 분산비밀을 생성하는 분배자를 '신뢰할 수 있는' 것으로 가정하지만, 검증 가능한 비밀분산 기법에서는 분배자가 악의적인 행위를 하더라도 잘 정의된 원본 비밀이 존재하기 때문에 참여자들이 언제든 비밀을 복원할 수 있다. 대표적인 기법으로는 Feldman의 기법[5]과 Pedersen의 기법[6]이 있다.

2.2 대칭키 기반의 노드인증과 키관리 기법

지상통제소가 부재한 MANET에서의 인증 및 키관리 기법에 관한 연구들은 기반구조의 부재와 자원 제약적 특성을 고려하여 대칭키 암호 기반의 접근방법을 중심으로 연구가 진행되었다. 또한, 단일키 사용으로 인한 키 노출 문제를 해결하기 위해 다양한 기법들이 제안되었다.

LEAP은 다양한 상황에 따라 용도에 맞게 사용할 수 있도록 4개의 키(개인키, 일대일키, 클러스터키 및 그룹키)를 생성하여 운용한다[7][8]. TDKM은 Diffie-Hellman 키 교환 프로토콜을 기반으로 지수연산이 아닌 곱셈연산을 사용하여 비교적 적은 연산 요구량으로 효율적인 자원 사용이 가능하다[9].

확률적 키 공유 기법은 노드가 필드에 배치되기 전에 대량의 키들로 구성된 키 풀(Key Pool)에서 일정량의 키 집합(Key Ring)을 할당받은 후, 할당받은 키 집합에서 확률적으로 공유되는 키를 찾아 안전한 통신을 위한 키로 사용하는 접근방법이다[10].

2.3 공개키 기반의 노드인증과 키관리 기법

FANET은 기반구조 없이 네트워크가 구성되고 중앙집중적인 통제가 존재하지 않기 때문에, 공개키 암호 기반의 인증 및 키관리 연구들은 대부분 공개키 인증을 수행할 혹은 공개키 인증에 필요한 공개키인증서를 발급할 인증기관(CA, Certification Authority)을 어떻게 구성할 것인지를 중점적으로 연구하였다.

부분적으로 분산된 인증기관 구성 기법은 기본적으로 Shamir의 (t, n) 임계치 기법[3]을 이용하여 인증기관의 개인키를 분산비밀로 분배받은 노드들이 요청이 발생하였을 때 분산비밀을 이용해 부분 전자서명을 생성하고 이러한 부분 전자서명들을 하나의 노드가 모아서 공개키 인증을 유도한 전자서명을 생성한다. 분산비밀 탈취 공격에 대항하기 위해 다양한 기법들이 연구되었다[11][12].

완전히 분산된 인증기관 구성 기법은 부분적으로 분산된 인증기관 구성 기법과 같이 (t, n) 임계치 기법을 적용하고 있으나, 네트워크의 모든 노드가 인증기관 구성에 참여하는 접근방법이다[13].

인증서 체인을 이용하는 기법은 모든 노드가 자신의 공개키/개인키 쌍을 생성하고 자신들이 신뢰하는 노드들에 인증서를 발급하는 기법으로, 신뢰 관계가 계속 연결되어 확산하는 속성을 가진다[14].

2.4 PUF

PUF는 물리적으로 복제 불가능한 반도체를 개발하기 위한 기술로서, 반도체 제조 과정에서 발생하는 미세한 편차를 이용하여 반도체 칩 내부에서 예측하기 어려운 무작위 값을 생성하는 시스템을 의미한다[15][16].

각각의 PUF는 'Challenge'라고 불리는 입력값이 동일하더라도 서로 다른 출력값, 'Response'를 생성한다. 생성되는 출력값에 대해서는 예측 불가능성, 무작위성, 신뢰성이 보장되며, 이러한 특성들을 기반으로 물리적 복제 불가능성을 만족시킨다. PUF는 지연기반의 PUF(Mismatch-based PUF) 와 물리적 특성 기반의 PUF(Physical-based PUF)로 구분된다. 지연기반 PUF는 제작되는 소자 또는 회로의 특성이 반도체 제조 공정 과정에서 발생하는 공정 편차에 의해 각각의 고유한 특성을 갖게 되는 점을 이용한 PUF로 대표적으로는 Arbiter PUF가 있다.

2.5 기타 FANET의 보안에 관한 연구

FANET의 보안 위협에 관해 다양한 연구가 진행

되고 있으며, 이에 대응하기 위해 Arun Sekar Rajasekaran 등은 FANET에서 위치 정보를 활용해 End-User와 Drone 간 지상통제소 없이 상호 및 일괄적으로 익명 인증할 수 있는 기법을 연구하였다[17]. 또한 N. N. Shenets는 보안 비밀공유 기반의 FANET 보안 프로토콜을 다수 플랫폼에서 실험하였다[18].

3. 비밀분산 기반 노드 인증 및 키관리

비밀분산은 민감하고 중요한 정보 혹은 비밀을 다수의 분산비밀로 나누어 여러 참여자에게 분산 저장한다. 그리고 일정 수 이상의 분산비밀이 모이면 원본정보 혹은 비밀이 복원된다. 본 연구에서는 이러한 비밀분산의 특성을 활용하여 ElGamal 공개키 암호가 적용된 FANET 환경에서 다수 노드가 참여하여 원본비밀의 복원을 시도한 후 올바른 원본비밀이 복원되면 복원에 참여한 모든 노드를 동시에 인증한다. 본 논문에서 인증과정을 설명하기 위해 사용하는 표기법은 <표1> 에서 보는 바와 같다.

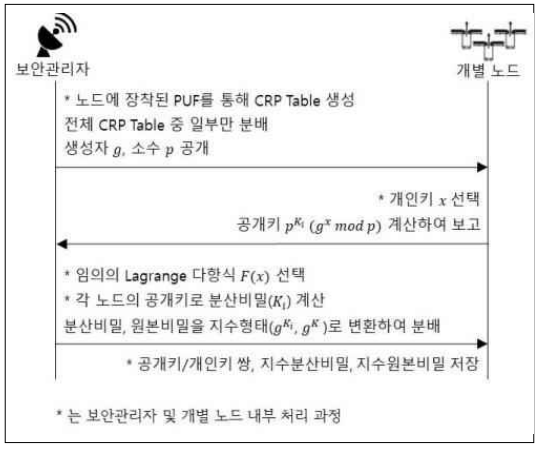
<표 1> Notation

g	생성자
p	소수
x	개인키
$p^{K_i}(g^x \bmod p)$	노드 i의 공개키
$F(x)$	임의의 Lagrange 다항식
K	원본비밀
K_i	노드 i의 분산비밀
g^{K_i}	노드 i의 지수 분산비밀
g^K	노드 i의 지수 원본비밀
C_i	노드 i의 PUF Challenge
R_i	노드 i의 PUF Response
RN	의사난수

3.1 필드 배치 전 준비단계

FANET에 참여하는 모든 노드는 기본적으로 PUF가 장착되어 있다. 보안관리자는 (그림 1)에서 보는 바와 같이 각 노드에 장착된 PUF를 통해 CRP (Challenge-Response Pair) 테이블을 생성한다. 그리고 FANET에 참여할 노드들이 사용할 생성자 g와 소수 p를 공개한다. 각 노드는 개인키로 사용할 x를 선택하고, 자신의 공개키 $pk_i(g^x \bmod p)$를 계산하여 보안관리자에게 보고한다.

보안관리자는 임의의 Lagrange 다항식 $F(x)$를 선택한 후, 각 노드로부터 보고받은 공개키를 이용하여 각 노드에 분배할 분산비밀(K_i)을 계산한다. 분산비밀의 계산이 완료되면 보안관리자는 분산비밀과 원본비밀을 지수 형태(g^{K_i}, g^K)로 변환한 후 각 노드에 분배한다. 이상과 같은 과정을 거쳐 각 노드는 공개키/개인키 쌍, 분산비밀 및 원본비밀을 가지게 되며, 작전에 투입될 노드들의 CRP 중 일부를 저장한다.



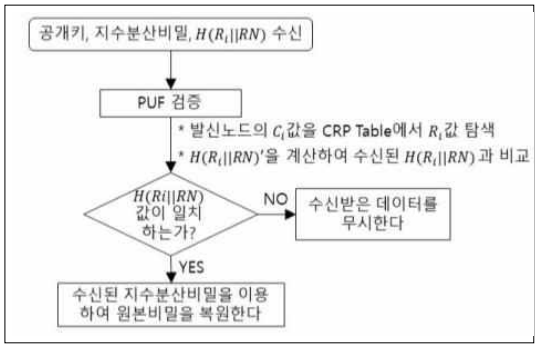
(그림 1) 필드 배치 전 준비단계

3.2 필드 배치 후 인증단계

필드에 배치된 노드들은 네트워크 형성 초기 단계에서 인증을 수행하기 위해 자신의 ID, 공개키와 지수형태의 분산비밀, 그리고 사전에 개별 노드에 저장된 PUF CRP의 Response 값(R_i)에 의사난수 생성 알고리즘에 의해 생성된 난수(RN)를 결합한 값의 해시값$[H(R_i \parallel RN)]$을 브로드캐스트한다.

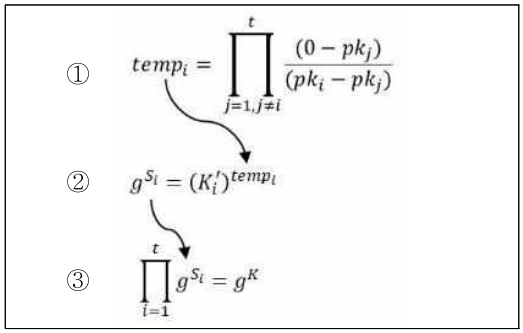
각 노드는 네트워크 내의 다른 노드들이 브로드캐스트한 데이터를 수신한 후, 먼저 각 노드에 해당하는

Challenge 값을 CRP 테이블에서 찾는다. 이후 매칭되는 R_i값과 난수를 결합한 값을 해시한 후 수신된 값과 비교하여 일치하는 노드들이 전송한 지수 분산 비밀만을 이용하여 지수 원본비밀의 복원을 시도한다. 이상의 과정을 도식화한 결과는 (그림 2)와 같다.



(그림 2) 데이터 수신 후 인증과정

원본비밀의 복원이 완료된 후 자신이 저장하고 있는 원본비밀과 일치할 때 원본비밀 복원에 참여한 모든 노드는 정당한 노드로 인증할 수 있게 된다. 수신된 데이터로부터 지수 원본비밀을 복원하는 과정은 (그림 3)에서 보는 바와 같다.



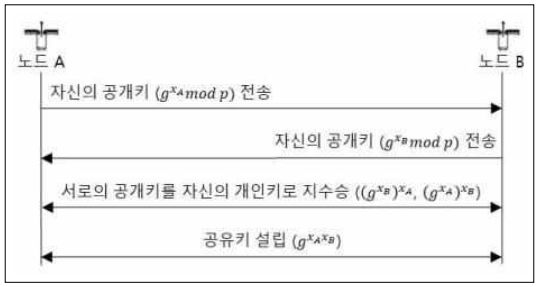
(그림 3) 지수 원본비밀 복원 과정

3.3 키 설립 및 운용단계

인증과정이 완료되면 신뢰할 수 있는 노드들로만 네트워크가 구성된다. 이후에는 각 노드가 저장하고 있는 공개키/개인키 쌍을 기반으로 ElGamal 암호시스템을 이용하여 안전한 통신을 진행할 수 있으나, 필요에 따라 대칭키 암호시스템을 사용해야 할 경우가 발생할 수 있다.

3.3.1 이웃 노드와의 일대일 통신

이미 신뢰 관계가 형성된 이웃 노드와의 통신에서 신속한 통신 및 배터리 소모량 감소를 위해서는 비교적 연산량이 적은 대칭키 암호시스템으로 전환하는 것이 유리할 것이다. 따라서 (그림 4)에서 보는 바와 같이 쌍방 간에 이미 보유하고 있는 정보(상대방의 공개키 및 자신의 개인키)를 이용한다면 신속한 대칭키의 설립이 가능해진다.

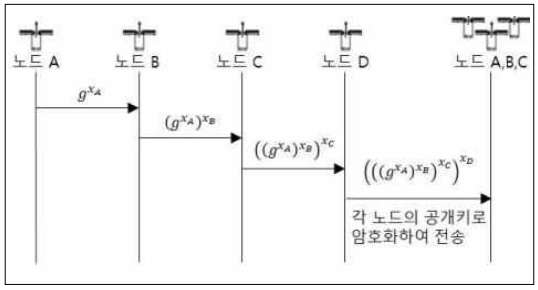


(그림 4) 두 노드 간의 대칭키 설립 절차

3.3.2 특정 노드 간의 그룹 통신

전체 노드 중 일부 노드에서 다른 작전을 수행하기 위해 소그룹 간의 새로운 통신채널을 구성하고자 할 때 Diffie-Hellman 키 교환 절차를 응용하여 그룹키를 손쉽게 설립할 수 있다.

(그림 5)에서 보는 바와 같이 작전에 참여하는 다른 노드로부터 전송받은 지수 분산비밀에 자신의 개인키를 지수승하는 과정을 반복하면서 전체 노드의 개인키 지수승이 완료되면, 최종 노드는 생성된 그룹키를 다른 노드들에 해당 노드의 공개키로 암호화하여 전송한다.



(그림 5) 다수 노드 간의 그룹키 설립 절차

3.3.3 전체 노드에 대한 명령 전송

전체 노드에 공통된 작전명령을 하달하는 상황이 발생하면 공개키 암호시스템을 기반으로 하는 전술 환경에서는 모든 노드가 공유하는 대칭키가 없어 네트워크 전체로 중요 메시지를 암호화하여 동시에 전송하기는 쉽지 않다. 그러나 전체 노드가 공유하는 대칭키를 설립하는 것 또한 비밀키 노출 가능성이 상당히 크며, 네트워크의 보안이 취약해지는 원인이 될 수 있다. 따라서 별도의 대칭키 설립 없이 각 노드가 사전에 저장한 정보만을 이용하여 전체 노드를 대상으로 작전명령을 하달하는 방법이 필요하다.

작전명령(M)은 명령하달자에 의해 원본비밀(K)을 이용하여 (그림 6)과 같이 암호화되어 암호문으로 브로드캐스트된다.

암호화
① 임의의 양의 정수 $r\,(0 < r < p-1)$ 선택 ② $(g^K)^r \bmod p$ 계산 ③ 암호문 $C = (g^r, Mg^{rK})$ 생성

(그림 6) 전체 노드에 대한 명령 암호화 과정

이를 수신한 노드들은 (t, n) 임계치 기법에 따라 다항식을 복원하는 것과 같은 절차로 t개의 노드 단위로 클러스터를 형성하여 (그림 7)과 같이 암호문에 대한 복호화를 동시에 수행한다.

복호화 (노드별 수행)
① 자신의 공개키, 지수분산비밀 브로드캐스트 ② $temp_i = \prod_{j=1, j\neq i}^{t} \frac{(0 - pk_j)}{(pk_i - pk_j)}$ 계산 ③ $g^{-S_i} = (K_i')^{-temp_i}$ 계산 ④ $\prod_{i=1}^{t} g^{-S_i} = g^{-K}$ 계산 ⑤ $Mg^K * g^{-K} = M$ // 복호화 완료

(그림 7) 전체 노드에 대한 명령 복호화 과정

4. 효율성 및 안전성 분석

효율성은 각 노드가 저장해야 할 정보의 크기, 인증과 키 설립과정에서 소요되는 통신비용을 중점적으로 분석한다. 연산성능의 경우 기존 비밀분산과 공개키 암호 기반의 접근방법들 모두가 거의 유사한 연산량을 요구하기에 구현 등을 통해 구체적으로 비교하는 과정은 생략한다. 안전성 분석은 발생 가능한 공격자 유형별 대처방안, 비밀분산의 비현실적 가정에 대한 안전성, 대칭키 설립과정의 안전성으로 구분하여 실시한다.

4.1 효율성 분석

배터리로 운용되는 FANET 노드의 특성상 한정된 자원을 효율적으로 활용하고 운용시간을 극대화하기 위해 효율성을 제고하는 것은 필수적이다. 특히 데이터를 송수신 하는 과정은 그 자체로 큰 배터리 소모를 야기하기에 통신횟수를 줄이는 것이 FANET의 인증과정에서 매우 중요하다.

4.1.1 저장하는 정보의 크기

저장하는 정보의 크기 측면에서 각 노드는 보안관리자가 생성한 지수 분산비밀과 지수 원본비밀 및 편집된 CRPs Table을 저장한다. 하나의 노드에 대한 해시값을 1로 간주했을 때 저장해야 할 해시값의 크기는 최소한 t 보다는 크다. 노드 인증이 진행되는 과정에서 임시 저장해야 할 정보의 크기는 $(t-1)$개 노드의 공개키와 지수 분산비밀로서, $2(t-1)$개의 정보를 추가로 저장해야 한다. 제안 기법은 중앙통제소 없이 최소 t개의 브로드캐스팅된 정보를 임시저장하여 연산을 하는 과정이 필요하기 때문에 기존 기법 대비 유사하거나 다소 많은 저장공간이 필요하다.

4.1.2 통신비용

통신비용 측면에서 기존 연구들은 기본적으로 다항식을 복원하는 작업을 모두 수행하여, 본 연구에서 제안하는 기법과 다항식 복원 및 원본비밀 계산 측면에서의 통신비용은 같다. 그러나 기존 접근방법들이 하

나의 노드를 인증하기 위해 같은 과정을 반복함에 반해 본 논문에서 제안하는 기법으로는 한 번의 통신만으로 $(t-1)$개의 노드를 동시에 인증할 수 있다. 또한 FANET을 기반으로 한 인증기법의 경우에 대다수의 접근방법에서 인증기관의 역할을 수행하는 지상통제소를 고려하여 별도의 인증기관 없이 운영되는 본 논문의 제안 기법과 운영환경이 달라서 직접적인 비교는 어렵다. 하지만 노드 간 뿐만 아니라 인증기관과의 통신이 별도로 요구됨으로 인해 제안기법 대비 상대적으로 통신비용이 증가한다.

저장정보의 크기와 통신비용 측면에서 기존 기법과 비교한 결과는 <표 2>에서 보는 바와 같다.

<표 2> 기존 기법과의 효율성 비교 결과

	저장정보 크기	통신비용
TDKM[9]	$N+1$	$\frac{2\times N^2}{k}$
LEAP[7][8]	$N+3$	$4\times d\times N$
Merkle Tree 기반[19][20]	$\log_2 N+1$	$N\times \log_2 N$
N.N.Shenets[18]	5 (CA : $5N$)	$4N$
제안 기법	$3t$	$2N-1$

4.2 안전성 분석

4.2.1 발생 가능한 공격자 유형별 안전성 분석

① 순수 외부 공격자

FANET에 한 번도 참가하지 않은 순수 외부 공격자는 필드에 배치되기 전에 지상통제소로부터 분배받아야 할 유효한 인증 정보를 가지고 있지 않으므로, 필드 배치 이후 곧바로 진행되는 인증과정에 참여할 수가 없다. 특히 각 노드의 고유한 PUF를 이용한 CRP값을 브로드캐스트 할 수 없으므로 순수 외부 공격자의 참여 시도는 충분히 차단할 수 있다. 만약 단순히 특정 노드의 브로드캐스트 데이터를 Replay 하는 공격도 지수원본비밀 복원에 영향을 주지 않으므로 인증과정 진행에 큰 영향이 없다. 게다가 본 논문에서 제안하는 기법은 이산대수문제의 어려움에 기초하여 지수형태로 변환된 분산비밀을 분배하기 때문에 외부 공격자가 지수 분산비밀을 확보하더라도 다항식을 복원하기는 매우 어렵다.

② 내부의 이동 노드가 공격자로 활동하는 경우

예를 들어 네트워크 내의 각종 활동에 적극적으로 참여하지 않는 방법으로 정상적인 운영을 방해하거나, 외부 공격자와 공모하여 네트워크 내부 정보를 외부로 유출 시도하는 경우가 있다. 이미 인증이 완료된 내부 공격자의 침해 행위는 추가 인증이나 다른 암호학적 수단으로 차단하는 것은 불가능하다. 이것은 본 논문의 연구범위를 벗어나는 부분으로 향후 침입탐지 및 침입방지 분야의 추가적인 연구가 필요하다.

③ 배치된 노드가 적에게 잠식된 경우

만약 인증과정 이전이라면 인증방해 외의 악의적 행위가 불가능하므로 충분히 대처할 수 있다. 본 논문에서 제안한 인증 방법이라면 의도적으로 인증을 방해하기 위해 초기 인증과정에서 조작된 데이터를 전송하더라도 PUF 및 의사난수값 확인을 통해 해당 노드를 배제하는 것이 가능하다.

하지만 인증과정이 완료된 노드가 포획되었다면 앞서 ②에서 살펴본 위협유형과 동일하거나 그보다 더 높은 위험성을 가진다. 중요 정보를 수집하거나, 수집된 정보를 외부로 전송할 가능성이 있으며, 정상 노드로 가장하여 침입탐지 메커니즘의 작동 임계치를 파악하고 침입탐지 임계치 내에서 지속적인 침해활동을 수행할 수도 있다. 이러한 경우에는 앞서 언급한 침입탐지 대책이 보다 정교하게 적용되어야 한다.

4.2.2 비밀분산의 비현실적 가정에 대한 안전성

비밀분산이 정상적으로 수행되기 위해 필요한 3가지 가정사항은 다음과 같다: ① 다항식을 이용해 분산비밀을 생성하는 분배자 또는 관리자를 믿을 수 있다. ② 정해진 임계치 이하의 정보로는 원본비밀에 대한 어떠한 정보도 얻을 수 없고, 공격자는 임계치 이상의 노드를 공격할 수 없다. ③ 다항식의 복원시 각 노드는 분산비밀 제공과정에서 부정행위를 하지 않는다. 이상 3가지의 가정사항은 대부분의 비밀분산 연구에서 비현실적인 가정사항으로 간주된다. 하지만 본 연구에서는 위의 가정사항들을 충족할 수 있다.

첫 번째 가정사항의 경우, 본 논문의 연구대상 네트워크가 군사용으로 많이 사용되는 무인기 군집비행을 위한 FANET임을 감안하였을 때, 운용기관의 특수성을 고려시 보안관리자에 대한 신뢰가 충분히 가능하다. 두 번째 가정사항은 본 논문에서 제안하는 기법이 이산대수 문제의 어려움에 기초하여 지수형태로 변환된 분산비밀을 전송하기 때문에 공격자는 원본비밀에 대한 어떠한 정보도 얻을 수 없다. 세 번째 가정사항은 이미 부정행위를 탐지하기 위한 다양한 기법들이 제시된 바 있으며, 본 연구에서 대책으로 제시한 PUF와 의사난수, 해시값을 이용한 데이터의 유효성 검증을 통해 충분히 극복 가능하다.

4.2.3 대칭키 설립과정의 안전성

본 논문에서 제시하는 기법은 각 노드가 필드에 배치되기 이전에 ElGamal 암호시스템에 사용할 공개키와 개인키를 이미 가지고 있기에 대칭키의 설립이 반드시 필요한 것은 아니다. 그러나 필요에 따라서는 신속한 암호화나 자원 사용의 효율을 위해 대칭키 암호시스템의 사용이 필요할 수 있다. 노드 간 일대일 통신을 위해 두 노드가 교환하는 정보는 서로의 공개키에 한정된다. 공개키를 이용해 생성된 분산비밀은 지수 형태로 변환되어 연관성을 파악하거나 원본비밀을 추정하는 것은 거의 불가능하다.

그룹키 설립과정 또한 정보 노출을 방지할 수 있는데, 순차적 키 설립과정에서 두 번째 노드부터 전송하는 값은 자신의 개인키가 지수승된 지수 형태이므로, 전송 간 노출되는 정보는 없다.

5. Conclusions

본 논문에서는 중요 정보의 분산저장이나 권한 분산에 활용됐던 비밀분산을 이용하여 FANET 환경에서 한 번의 통신만으로 $(t-1)$개의 노드를 동시에 인증할 수 있는 효율적인 인증기법을 제시하였다. 기존 기법들은 분산비밀을 취합하고 다항식의 복원을 통해 원본비밀을 계산함으로써 인증을 수행하는 방식을 이용하였으나 제시하는 기법은 최종 계산 값의 일치 여부만으로 다수 노드를 동시에 인증할 수 있도록 하였다. 그리고 원본비밀의 복원을 위한 계산을 수행하기 전에 PUF CRP값을 활용하여 인증과정을 방해할 수 있는 공격자를 탐지하고 비밀 복원 계산에서 배제하는 방안을 추가로 제시하였다.

제시된 기법의 효율성을 분석한 결과, 개별 노드의 인증 정보로 생성한 해시값을 임시로 저장해야 하므로 저장 정보의 크기가 다소 증가하는 것으로 분석되었다. 그러나 한 번의 통신만으로 다수 노드를 동시에 인증할 수 있어 통신비용 측면에서는 기존 기법들과 비교해 상당히 효율적인 것으로 분석되었다. 추가적으로 무인기 군집의 규모를 고려하였을 때 일정한 수의 노드로 클러스터 형성시 전체 노드 수에 상관없이 클러스터 수를 증가시키는 방법을 활용한다면 효율성에 미치는 영향은 미미할 것으로 판단된다.

본 기법의 안전성을 분석한 결과는 다양한 공격자 유형을 가정하였을 때 대부분은 안전성을 보장할 수 있는 것으로 확인되었으나, 이미 인증과정을 완료한 노드에 대해서는 추가적인 침입탐지 기법이 필요함을 식별하였다.

앞으로는 인증과정 중 임시저장이 필요한 데이터를 줄여서 저장공간이 효율적으로 관리될 수 있도록 기법을 개선하고, 이미 인증이 완료된 노드가 내부공격자가 되는 유형 등 다양한 공격에 대응하기 위한 침입탐지 기법에 관해서 추가 연구를 진행할 예정이다.

참고문헌

[1] Chen, S., Li, B., Chen, Z., Zhang, Y., Wang, C., Tao, C., “Novel Strong-PUF-based Authentication Protocols Leveraging Shamir’s Secret Sharing” IEEE Internet of Things Journal, 2021.

[2] Mahabub Hasan Mahalat, Dipankar Karmakar, Anindan Mondal, Bibhash Sen, “PUF based Secure and Lightweight Authentication and Key-Sharing Scheme for Wireless Sensor Network”, ACM Journal on Emerging Technologies in Computing Systems, Vol. 18, No. 9, pp. 1-23, 2022.

[3] Adi Shamir, “How to share a secret”, Lecture

Notes in Computer Science, pp. 371-375, 1983.

[4] G. R. Blakley, “Safeguarding cryptographic keys”, Proceeding of the 1979 AFIPS National Computer Conference, 1979.

[5] P. Feldman, “A practical scheme for non-interactive verifiable secret sharing”, IEEE Symposium on Foundations of Computer Science, pp. 427-437, 1987.

[6] T. Pedersen, “Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing”, CRYPTO 1991, pp. 129-140, 1991.

[7] S. Zhu, S. Setia, and S. Jajodia, LEAP : Efficient Security Mechanism for Large-Scale distributed Sensor Networks, in Proceedings of the 10th ACM Conference on Computer and Communications Security(CCS ’03), Washington D.C, Oct, 2003.

[8] Verma, Rakesh M., and Bailey E. Basile. "Modeling and analysis of LEAP, a key management protocol for wireless sensor networks." Security and Privacy of Mobile, Wireless, and Sensor Networks (MWSN), 2013 IEEE International Workshop on. IEEE, 2013.

[9] I. Chuang, W. Su, C. Wu, J. HSu and Y. Kou, “Two-layered Dynamic Key Management in Mobile and Long-lived Cluster-based Wireless Sensor Networks”, in Prpceedings of IEEE Wireless Communications and Networking Conference, pp.4145-4150, 2007.

[10] L. Eschenauer and V. Gligor, “A Key Management Scheme for Distributed Sensor Networks,” in the Proceedings of the 9th ACM Conference on Computing and Communication Security, 2002

[11] L. Zhou and Z. J. Haas, “Securing Ad Hoc Networks,” IEEE Network Mag., vol. 13, no.6, Nov./Dec. 1999, pp. 24-30, 1999.

[12] A. Herzberg et al., “Proactive Secret Sharing or: How to Cope with Perpetual Leakage,” Proc. Crypto’95, pp. 339-352, 1995.

[13] J. Kong et al., “Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks”, Proc. 9th Int’l. Conf. Network Protocols (ICNP’01), pp. 251-260, 2001.

[14] S. Capkun, L. Buttyán, and J. P. Hubaux, “Self-Organized Public-Key Management for Mobile Ad Hoc Networks”, IEEE Trans. Mobile Computing, vol. 2, no.1, pp. 1-13, 2003.

[15] Baek. Jong-Hak, Sin. Gwang-Jo, "Development and Application of Security Chip Technology Using PUF Technology", The Magazine of the IEIE, Vol. 43, No. 7, pp. 59-67, 2016.

[16] Sumin Kim, "A Study on the Development of Secure Communication Channel Using PUF Technology in M-IoT Environment," Journal of Information and Security, Vol. 19, No. 5, pp. 107-118, 2019.

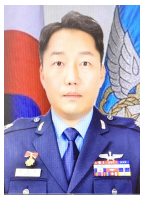
[17] Arun Sekar Rajasekaran, Azees Maria, Fadi Al-Turjman, Chadi Altrjman, Leonardo Mostarda, “Anonymous Mutual and Batch Authentication with Location Privacy of UAV in FANET”, Drones 6, No.1: 14, 2022.

[18] N.N.Shenets, “Security Infrastructure of FANET Based on Secret Sharing and Authenticated Encryption”, Automatic Control and Computer Science, Vol. 53, No. 8, 2019.

[19] Wenliang Du, "An Efficient Scheme for Authenticating Public Keys in Sensor Networks", 6th ACM International Symposium, 2005.

[20] R. Merkle, "Protocols for Public Key Cryptosystems", In Proceedings of the IEEE Symposium on Research in Security and Privacy, Apr 1980.

〔저자소개〕



양 지 훈 (Jihun Yang)
2006년 3월 공군사관학교 학사
2021년~현재 국방대학교
국방과학학과 석사과정
email : drain7@gmail.com

이 수 진 (Soojin Lee)
1992년 3월 육군사관학교 학사
1996년 2월 연세대학교 석사
2006년 2월 한국과학기술원 박사
2006년~현재 국방대학교
국방과학학과 교수
email : cyberkma@gmail.com