Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.29, NO.4, Aug. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.4.729

전술 무선 네트워크에서 무인체계를 위한 해시 충돌 기반의 양방향 인증 프로토콜*

이 종 관†‡
육군사관학교 컴퓨터과학과

A Two-Way Authentication Protocol Based on Hash Collision for Unmanned Systems in Tactical Wireless Networks*

Jong-kwan Lee†‡
Department of Computer Science, Korea Military Academy

요 약

본 논문에서는 채널 상태가 좋지 않아 장거리 통신이 보장될 수 없는 전술 무선 네트워크에서 무인체계 간의 양방향 인증 프로토콜을 제안한다. 모든 무인체계는 작전에 투입되기 전에 인증에 필요한 정보들을 안전하게 할당 받는다. 제안하는 프로토콜은 해시 충돌을 유발하는 임의의 데이터들을 사용하여 인증 코드를 생성한다. 인증 요청자는 생성한 인증코드, 무인체계의 ID와 시간정보 등으로 인증요청메시지를 구성한다. 그리고 인증요청메시지는 사전에 분배된 비밀키로 암호화하여 전송된다. 수신자는 인증요청메시지를 복호화하여 인증코드를 검증함으로써 인증요청자를 인증한다. 제안하는 프로토콜의 성능을 다양한 공격 시나리오를 대상으로 분석한 결과, 제안하는 프로토콜이 메시지 재전송, 위장, 메시지 변형 등 다양한 공격에 안전할 뿐 아니라, 장거리 통신이 요구되는 별도의 인증서버가 불필요하고 통신 오버헤드, 인증 소요시간 측면에서 효율적임을 확인하였다. 또한 제안한 프로토콜의 파라미터 값이 성능에 미치는 영향을 분석하여 보안 요구 수준에 따른 적절한 파라미터 값 선정 가이드를 제시하였다.

ABSTRACT

In this paper, we propose two-way authentication protocol between unmanned systems in tactical wireless networks in which long distance communications are not guaranteed due to a poor channel conditions. It is assumed that every unmanned systems have same random data set before they put into combat. The proposed protocol generates authentication code(AC) using random data that causes hash collision. The requester for authentication encrypts the materials such as their identifier, time-stamp, authentication code with the secret key. After then the requester transmits the encrypted message to the receiver. The receiver authenticates the requester by verifying the authentication code included in the request message. The performance analysis of the proposed protocol shows that it guarantees the security for various attack scenarios and efficiency in terms of communication overhead and computational cost. Furthermore, we analyzed the effect of the parameter values of the proposed protocol on the performance and suggest appropriate parameter value selection guide according to the level of security requirement.

Keywords: Authentication Protocol, Unmanned Systems, Hash Collision, Tactical Network

Received(05. 30. 2019), Modified(1st: 07. 16. 2019, 2nd: 08. 09. 2019), Accepted(08. 12. 2019)
* 본 연구는 한국연구재단 연구과제(No. 2019R1G1A11003030) 및 화랑대연구소 지원으로 수행하였습니다.
† 주저자, jklee64@kma.ac.kr
‡ 교신저자, jklee64@kma.ac.kr(Corresponding author)

I. 서 론

인구 감소에 따른 지속적인 병력감축, 보편화된 인명 중시 사상, 무기체계의 첨단과학화 등으로 현재 인력에 의해서 수행되는 많은 전투, 비전투 과업들이 점차 기계의 도움 하에서 적은 인력으로 수행되거나 더 나아가 인간의 개입이 최소화된 무인체계에 의해서 수행될 것이다. 또한 단위 무인체계가 수행하기에 복잡도와 난이도가 높은 임무들은 군집을 형성한 팀 단위의 무인체계들에 의해서 수행될 것이다. 한편, 수행하는 임무의 성격, 환경, 개별 무인체계의 능력에 따라 군집을 형성하는 무인체계들은 다양하게 구성될 수 있다. 또한 네트워크 환경이 매우 동적일 수밖에 없는 전장상황을 고려할 때 임무수행 중에도 무인체계들이 군집에 새롭게 추가되거나 또는 탈퇴하는 경우가 빈번할 것이다. 그리고 임무의 특성에 따라 무인체계들이 한 번에 투입되는 것이 아니라 축차적으로 투입될 수도 있다. 따라서 최초 군집이 형성된 이후 무인체계 구성원이 변경될 때 마다 무인체계간 상호인증 절차가 필요하다. 기만을 통해 정상적인 지휘통제 및 네트워크 운용을 방해하려는 적의 시도가 상존하는 전장 환경에서는 특히 안전한 인증절차가 필수적이라 할 수 있다.

인증은 정보보안을 구현하는 가장 기초적인 근간이다. 일반적으로 이용되는 사용자 인증수단은 알고 있는 것(something the individual knows), 소유하고 있는 것(something the individual possess), 정적 또는 동적 생물학적 특징(something the individual is) 등 크게 3가지로 나누어볼 수 있다[1]. 그리고 안전성을 보강하기 위해 2개 이상의 수단이 조합되어 인증에 사용되기도 한다. 그런데 인간이 인증절차에 개입하는 경우에는 앞서 언급한 3가지 인증수단에 포함되지 않는 매우 고차원적인 인증이 수행될 수 있다. 예를 들어, 전투상황에서 야간에 전투원이 신원미상자를 발견하여 암구어를 물었을 때 신원미상자가 암구어를 정확하게 제시하였다 하더라도 부자연스러운 목소리 또는 억양, 낯선 복장, 해당 시간에 그곳에서 등장하는 의외성 등을 종합적으로 고려하여 인증 여부를 판단한다. 반면, 무인체계간의 인증은 인간의 종합적인 상황인식, 이해, 추론 능력을 100% 활용할 수 없기 때문에 매우 엄격한 인증절차가 요구된다.

대부분의 인증 프로토콜에서 데이터의 무결성을 보장하기 위해 해시함수를 사용한다. 해시함수는 어떠한 입력값에도 항상 고정된 길이의 결과값을 출력하며, 입력값의 일부만 변경되어도 전혀 다른 결과값을 출력하고 결과값으로 입력값을 유추할 수 없다는 특징이 있다. 한편, 해시충돌은 해시함수가 서로 다른 입력값에 대해서 동일한 해시값을 출력하는 것을 의미한다. 한정된 범위의 해시값을 출력하는 해시함수는 비둘기집의 원리에 의해서 해시충돌이 항상 존재한다. 해시 충돌을 일으키는 임의의 두 값을 찾는 것을 충돌공격이라 하고, 주어진 값에 대해 그 값과 해시충돌을 일으키는 값을 찾는 것을 역상공격이라 한다. 일반적으로 완벽한 무결성을 보장하기 위해 인증 프로토콜에 충돌공격, 역상공격에 안전한 해시함수를 이용한다. 하지만 일부 연구에서는 역발상으로 해시충돌을 일으키는 데이터쌍을 특정 목적을 위해 활용하기도 한다[2].

본 논문에서는 장거리 통신이 원활하게 보장되지 않는 전술 무선 네트워크 환경에서 무인체계간의 안전한 양방향 인증 프로토콜을 제안한다. 제안하는 인증 프로토콜은 무인체계들이 동일하게 소유하고 있는 데이터들 중 해시충돌이 일어나는 데이터들의 조합을 인증코드로 사용한다. 이러한 방법을 통해 제안하는 인증 프로토콜은 원거리에 위치한 외부 인증서버 없이 무인체계간 양방향 인증을 수행한다.

본 논문은 다음과 같이 구성된다. 2장에서 관련 연구들을 살펴보고 3장에서 제안하는 기법에서 고려하는 시스템 모델과 공격 모델 등에 대해 설명한다. 4장에서 제안하는 인증 프로토콜에 대해 상세히 설명하며 5장에서 제안하는 프로토콜의 성능을 분석하고 6장에서 결론을 맺는다.

II. 관련 연구

사물인터넷, 센서 네트워크, 차량 애드혹 네트워크(VANET) 등에서 인간의 직접적인 개입이 없는 기기간의 인증 프로토콜에 대한 연구가 활발히 진행되고 있다. 본 장에서는 기기간의 인증 프로토콜을 제안한 대표적인 연구결과에 대해서 살펴본다.

BiBa 프로토콜은 생일 패러독스 (birthday paradox)를 이용하여 인증코드를 생성한다. 각 노드는 일방향 함수를 이용하여 SEAL (self authentication value)을 생성하고, 동일한 해시값을 갖는 SEAL들에 대한 정보를 인증코드로 사용한다. BiBa 프로토콜이 제안된 이후 인증코드의 용량, 인증을 위해 교환하는 메시지의 개수 또는 키의

크기 등을 줄이기 위한 다양한 변형 프로토콜이 제안되었다[2-4].

EG 프로토콜은 최초의 확률적 키 분배 기법이다[5]. 서버는 다수의 키들을 생성하고 키들 중 일부를 임의로 각 노드에게 할당한다. 센서가 배치된 후 두 개의 이웃 노드들은 확률적으로 최소 하나 이상의 키를 공유하게 된다. EG 프로토콜은 네트워크 규모가 커질수록 많은 키들을 보유해야하는 단점이 있다. 이는 저장공간 뿐 아니라 보안상에도 큰 단점이다. 이를 해결하기 위해 제안된 PKS-MP는 노드의 위치를 고려하여 키들을 분배한다[6].

센서 네트워크를 위한 계층적 키관리 프로토콜인 LEAP 계열의 프로토콜[7-9]은 마스터키를 인증수단으로 사용하며 기지국과의 통신, 인접 센서노드와의 통신, 그룹통신 등을 위한 키들을 모두 마스터키를 기반으로 생성한다. 센서 네트워크 운용에 필요한 키들이 모두 생성되면 (즉, 센서의 배치가 완료되면) 해당 센서노드는 마스터키를 삭제한다. 즉, 최초 인증 이후에는 추가적인 인증이 불가능하다. 따라서 동적으로 네트워크 환경이 변경되어 추가적인 인증이 필요한 경우에는 근본적으로 LEAP 계열의 프로토콜은 사용이 제한된다. 또한 마스터키가 공격자에게 노출되면 전체 네트워크 운용에 치명적일 수 있다는 단점이 있다.

한편 VANET 환경에서 차량의 인증을 위한 다양한 기법들이 연구되고 있다. 차량과 RSU(road side unit) 그리고 인증서버간에 공개키 암호화방식, 해시함수 그리고 시간정보 등을 이용하여 메시지 재사용 공격에 강인한 인증 프로토콜이 제안되었다[10]. 그리고 신뢰하기 어려운 RSU에 대한 의존성을 낮춘 CRT(chinese remainder theorem) 기반의 인증 프로토콜이 제안되었다[11]. VANET 환경을 고려한 인증 프로토콜들은 원거리에 위치한 인증 서버를 통해 인증이 수행된다. 즉, 인증서버와의 원활한 통신이 보장되는 것을 가정하고 있다.

기존 연구들은 센서 네트워크처럼 적은 배터리 용량과 제한된 계산력을 가정하거나, VANET 환경처럼 상시 접속이 가능한 인증서버의 존재 또는 정적인 네트워크 환경을 가정하였다. 하지만 전장에서 운용되는 무인체계는 단일 센서에 비해 배터리 용량과 계산력은 상대적으로 우월하지만 원활한 장거리 통신이 보장되지 않아 별도의 인증서버를 운용할 수 없고 무인체계의 이동성으로 인해 네트워크 멤버십이 매우 동적이다. 따라서 기존 인증 프로토콜들은 전장 무인체계에 적합하지 않으며 이러한 전술 환경에서의 무인체계의 특성을 고려한 인증 프로토콜에 대한 연구도 없는 실정이다. 따라서 새로운 인증 프로토콜에 대한 연구가 필요하다.

III. 전장 무인체계 운용 환경

3.1 시스템 모델 및 가정사항

무인체계들은 팀 단위로 활동하며 군사임무 수행의 특성상 반드시 리더 무인체계가 존재한다. 리더 무인체계가 정상적인 임무수행이 불가능할 경우에는 새로운 리더 무인체계가 선출된다. 그리고 고정형 센서들과는 달리 이동이 가능하여 네트워크 멤버십이 동적으로 변경될 수 있다. 이는 투입 전 무인체계들 간의 지휘관계의 변경 뿐 아니라 최초 투입 계획이 없던 무인체계가 필요에 따라 투입되었을 경우도 포함한다. 그리고 센서 네트워크에 비해 상대적으로 충분한 계산량, 배터리 용량을 보유한다. 또한 팀 내부 통신을 위해 애드혹 형태의 네트워크가 구성되며, 외부 통신은 리더 무인체계를 경유하여 수행된다. 즉, 리더 무인체계는 외부 네트워크와의 접점이 된다. 하지만 전장 환경의 특성상 외부와의 장거리 통신이 항상 보장되지는 않는다고 가정한다. 한편, 무인체계들은 작전에 투입되기 전에 정비, 무장, 유류 보충 또는 충전, 통신 및 인증 관련 정보 주입 등이 이루어지며, 작전이 종료되고 새로운 작전이 계획되면 이와 같은 절차는 반복된다. 즉, 모든 무인체계는 작전에 투입되기 전에 일차적으로 인증을 마쳤다고 할 수 있다. 따라서 본 논문에서는 내부공격자의 존재는 가정하지 않는다.

3.2 공격 모델

사전에 검증이 완료된 무인체계만이 작전에 투입되기 때문에 내부위협 보다는 적에 의한 외부위협이 상대적으로 크다고 할 수 있다. 또한 내부 네트워크의 신호 전송범위 내에 위치한 공격자는 내부 네트워크의 모든 송·수신 신호를 수집할 수 있다고 가정한다. 따라서 본 논문에서는 다음과 같은 외부 위협의 공격 시나리오를 가정한다.

첫째, 공격자는 메시지 재전송 공격(message replay attack)을 수행할 수 있다. 메시지 재전송 공격은 정당한 데이터의 전송이 악의적으로 반복되거

나 지연되어 전송되는 네트워크 공격의 한 유형이다. 이러한 공격을 이용하여 공격자는 인증요청자와 인증자 사이에서 무선으로 전달되는 인증 관련 메시지를 수집하여 재사용함으로써 불법적으로 인증을 획득하거나 인증요청을 승인할 수 있다. 둘째, 공격자는 위장 공격(impersonation attack)을 수행할 수 있다. 위장 공격은 인증절차에 불법적으로 개입하여 공격자가 정당한 인증자 또는 인증요청자인 것처럼 위장하는 것으로 정상적인 네트워크 운용을 방해할 수 있다. 셋째, 공격자는 메시지 변형 공격(message fabrication attack)을 할 수 있다. 공격자는 수신된 신호로부터 유의미한 데이터를 추출하여 이를 위·변조함으로써 불법적인 인증 요청 또는 인증 승인을 시도할 수 있으며 이를 통해 정상적인 인증 절차를 방해할 수 있다.

3.3 보안 요구사항

내부 통신 신호를 감청할 수 있는 적이 상존하는 전장 환경에서 무인체계들간의 안전한 인증을 위해 다음과 같은 조건들이 충족되어야 한다.

첫째, 내부 네트워크의 외부에 위치한 인증서버와의 접속 없이 인증이 가능하여야 한다. 왜냐하면 네트워크 환경이 열악할 수밖에 없는 전술 무선 네트워크 환경에서 인증서버가 위치한 외부와의 통신이 100% 보장될 수 없기 때문이다. 둘째, 인증 관련 메시지들이 외부로 유출되지 않아야 한다. 즉, 암호화되어야 한다. 이는 공격자가 해당 메시지를 위·변조하여 정상적인 네트워크 운용을 방해할 수 있기 때문이다. 셋째, 인증 요청을 위해 사용되었던 인증 관련 메시지들이 재사용될 수 없어야 한다. 즉, 인증 요청 메시지는 유효시간이 있어야 한다. 인증 요청 메시지를 수집한 공격자가 별도의 메시지 내용 변경 없이 일정한 시간 이후에 해당 메시지를 통해 인증을 요청할 수 있기 때문이다. 넷째, 인증요청자와 인증자 모두가 상호 인증이 가능해야 한다. 공격자는 인증자와 인증요청자 사이의 모든 신호를 수신할 수 있어 인증요청자 뿐 아니라 인증자로도 위장할 수 있기 때문이다.

IV. 제안하는 인증 프로토콜

본 장에서는 전장 환경에서 제안하는 인증기법의 절차를 상세히 설명한다. Table 1은 제안하는 인증

Table 1. Symbols used in paper

Symbol	Meaning
ID_i	ID of unmaned systems
$M_m(\ )$	Mapping function with m output values
$H_{SHA\text{-}3}(\ )$	SHA-3 hash function
SK	Secret key
TS	Time stamp
$E(m, key)$	Encrypt plain text m with key
$D(c, key)$	Decrypt cipher text c with key
ACMT	Auth. Code Material Table
ARM	Auth. Request Message
$s_{i,j}$	element in the i^{th} row and j^{th} column in the ACMT

기법을 설명하는데 사용되는 주요 기호를 나타낸다.

4.1 작전 투입전 입력 정보

모든 무인체계는 작전에 투입될 때마다 인증에 필요한 기본 정보를 주입한다. 즉, 작전별로 인증 관련 정보들이 갱신된다고 할 수 있다.

주입되는 정보는 크게 3가지이다. 첫 번째 주입되는 정보인 ACMT(Authentication Code Material Table)는 $n \times n$개의 랜덤값으로 구성된 데이터 테이블로 인증코드 생성을 위해 사용된다. 제안하는 인증절차에서 실제 사용되는 데이터는 ACMT의 특정 행 또는 열의 n개 데이터이다. Fig. 1은 ACMT의 구조를 나타낸다. $s_{i,j}$는 i번째 행의 j번째 열의 데이터를 의미하고, $ACMT_{i,:}$와 $ACMT_{:,j}$는 i번째 행의 데이터들과 j번째 열의 데이터들을 각

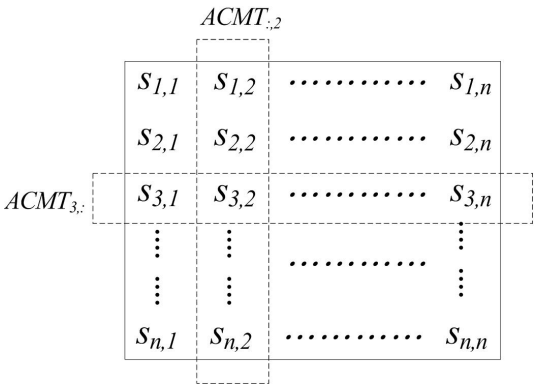

Fig. 1. ACMT structure

각 의미한다. 제안하는 프로토콜에서는 모든 무인체계가 동일한 ACMT를 보유하는데, 인증코드를 생성하기 위한 기초 자료를 모두가 동일하게 소유하는 것과 서로 다르게 소유하는 것은 운용하고자 하는 환경에서의 저장공간, 인증 처리의 효율성을 고려하여 선택하여야 한다. 제안하는 프로토콜은 저장공간의 효율성, 네트워크 멤버십의 동적 변화, 추가적인 무인체계 투입의 가능성 등을 고려하여 동일한 ACMT를 주입한다. 두 번째 주입되는 정보는 $m(\leq n)$개의 출력값을 갖는 매핑(mapping) 함수이다. 세 번째 정보는 무인체계간 데이터를 암·복호화하기 위한 비밀키이다.

최초 작전계획에 투입이 예정되어 있지 않았던 무인체계라 하더라도, 앞서 언급한 3가지 정보가 주입된다면 작전 중인 무인체계들과 인증이 가능하다. 즉, 융통성있게 무인체계를 운용할 수 있는 것이다.

4.2 멤버 무인체계의 인증 요청

멤버 무인체계(즉, 인증요청자)는 인증코드(AC, authentication code)를 생성하여 인증요청메시지(ARM, Authentication Request Message)를 구성하고, 비밀키로 암호화하여 전송한다. 인증을 요청하는 멤버 무인체계의 ID를 ID_i라 하고 인증코드 생성 및 검증을 위해 ACMT의 k번째 행의 데이터들이 사용된다고 하자. 이때 멤버 무인체계의 세부 인증절차는 다음과 같다.

4.2.1 인증코드(AC) 생성

ID_i는 $M_m(\cdot)$으로 자신의 ID를 사상하여 식(1)과 같이 사상 결과값 h를 계산한다.

$$h = M_m(ID_i) \tag{1}$$

한편, 식(2)와 같이 $h = M_m(ID_i \| s_{k,j})$를 만족하는 ACMT의 k번째 행의 원소들의 집합을 T라 하자.

$$T = \{s_{k,j} | h = M_m(ID_i \| s_{k,j}), j = 1, 2, ..., n\} \tag{2}$$

그리고 AC는 식(3)과 같이 계산된다. 즉, 집합 T가 공집합이 아닌 경우 원소들을 XOR 연산한 결과가 AC가 된다. 반면, T가 공집합인 경우에는 모든 $s_{k,j}$를 XOR 연산한 결과가 AC가 된다. 이는 공격자가 AC를 쉽게 추측하지 못하도록 하기 위함이다.

$$AC = \begin{cases} \bigoplus_{j=1}^{T_n(T)} T_j & , \quad T \neq \varnothing \\ \bigoplus_{j=1}^{n} s_{k,j} & , \quad otherwise \end{cases} \tag{3}$$

식(3)에서 T_i는 i번째 원소를 의미하고, $n(T)$는 집합 T의 원소의 개수를 나타낸다.

4.2.2 인증요청메시지(ARM) 구성 및 암호화

ID_i는 인증코드에 자신의 ID와 메시지 생성 시간 정보(TS_i) 등을 접합연산하여 SHA-3로 해시하고 자신의 ID와 TS_i, AC 생성을 위해 사용한 ACMT의 데이터의 위치정보(L_i)를 접합하여 인증요청메시지 ARM_i를 식(4)와 같이 구성한다.

$$ARM_i = H_{SHA-3}(AC_i \| ID_i \| TS_i) \| ID_i \| TS_i \| L_i \tag{4}$$

여기서 L은 2개의 정수값으로 표현되는데 $L=(0, k)$인 경우는 ACMT의 k번째 열의 데이터가 사용되었음을 의미하고, $L=(k, 0)$인 경우는 ACMT의 k번째 행의 데이터가 사용되었음을 의미한다. 그리고 ARM_i는 식(5)와 같이 사전에 분배된 비밀키로 암호화하여 리더 무인체계에게 전송된다.

$$E(ARM_i, SK) \tag{5}$$

4.3 리더 무인체계의 인증요청 검증

암호화된 ARM_i을 수신한 리더 무인체계(즉, 인증자)는 식(6)과 같이 사전에 분배된 비밀키로 복호화하여 해시값과 인증요청 무인체계의 ID, TS_i, 그리고 ACMT 위치정보 L_i 등의 데이터를 획득한다. 이때 획득한 TS_i가 유효하지 않을 경우 인증을 거절한다. TS_i가 유효할 경우, 획득한 ID_i와 L_i을 기초로 식(1)과 (2)를 이용하여 인증코드를 생성한다. 그리고 생성한 인증코드와 획득한 무인체계의 ID_i, TS_i를 접합하여 해시값을 계산한다. 이때 해시값이

인증을 요청한 무인체계로부터 수신한 해시값과 일치하면 인증에 성공한 것이고 일치하지 않으면 인증에 실패한 것이다.

$$D(E(ARM_i, SK), SK) \quad (6)$$

4.4 리더 무인체계의 인증 요청

멤버 무인체계의 인증요청이 검증되면 리더 무인체계는 멤버 무인체계에게 반대로 인증을 요청한다. 인증을 요청하는 리더 무인체계의 ID를 ID_h라 하자. 리더 무인체계의 인증코드 생성과정은 식(2)와 동일하다. 그리고 리더 무인체계의 인증요청메시지(ARM_h)는 식(4)를 통해 생성되며 비밀키를 이용하여 암호화되어 멤버 무인체계(ID_i)에게 전송된다.

4.5 멤버 무인체계의 인증요청 검증

멤버 무인체계(ID_i)가 리더 무인체계의 인증요청을 검증하는 과정은 4.3절에서 설명한 리더 무인체계가 멤버 무인체계의 인증요청을 검증하는 과정과 기본적으로 동일하다. Fig. 2는 제안하는 인증 프로토콜의 동작 절차를 종합적으로 나타낸다.

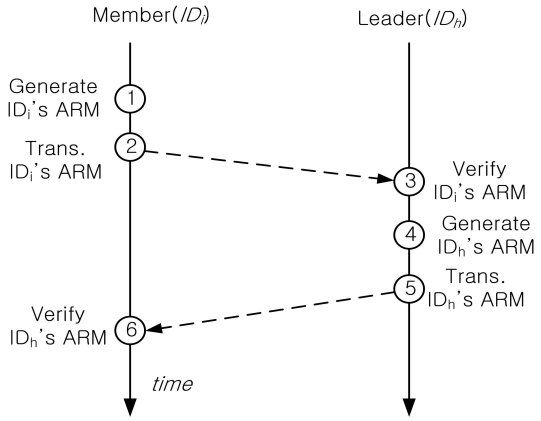

Fig. 2. Message flow diagram of the proposed authentication protocol

V. 성능 분석

본 장에서는 제안하는 인증 프로토콜의 성능을 안전성 및 효율성 측면에서 분석하고 데이터 충돌 발생 확률을 통해 적절한 파라미터 값 설정에 대해 살펴본다. 안전성은 앞서 2장에서 서술한 공격모델을 고려하여 메시지 재전송 공격, 위장 공격, 메시지 변형 공격 측면에서 분석한다. 효율성은 제안하는 프로토콜의 통신 오버헤드와 계산량 관점에서 분석한다. 한편, 공격자는 인증과정에서 발생하는 모든 신호를 수신할 수 있다고 가정한다.

5.1 안전성 분석

5.1.1 메시지 재전송 공격(message replay attack)

제안하는 인증 프로토콜에서 리더 무인체계와 멤버 무인체계 사이에 유통되는 모든 메시지는 비밀키로 암호화되기 때문에 비밀키가 유출되지 않는 한 복호화되지 않는다.

만약 비밀키가 공격자에게 유출되었을 경우 공격자는 식(4)와 같은 형태로 해당 메시지를 복호화할 수 있다. 즉, 공격자는 송신자의 ID, TS_i, L_i 등의 데이터를 수집할 수는 있다. 하지만 인증요청메시지에 TS_i가 포함되어 있어 해당 메시지를 그대로 재사용할 수는 없다. 일정 시간이 경과된 후에는 해당 TS_i가 유효하지 않기 때문이다.

그런데 [10]에서 노출된 시간정보의 보안취약 문제를 제기한 것과 같이 공격자가 TS_i를 변형하여 메시지 재전송 공격을 시도할 수 있다. 하지만 해시함수의 인자로 TS_i가 포함되어 있기 때문에 인증요청메시지의 수신자가 메시지 검증과정에서 해당 메시지에 오류가 있다는 것을 쉽게 식별할 수 있고 인증절차는 중단된다. 결과적으로 인증요청메시지를 재전송하는 공격은 전혀 효과가 없게 된다.

5.1.2 위장 공격(impersonation attack)

공격자는 암호화된 인증 관련 메시지를 모두 수신할 수 있기 때문에 해당 메시지를 복호화할 수 있다면 인증 절차 중에 개입하여 리더 무인체계 또는 멤버 무인체계로 위장하는 공격을 시도할 수 있다.

멤버 무인체계로부터 인증요청메시지를 받은 공격자는 리더 무인체계로 위장하기 위해 인증요청메시지의 검증 절차를 생략하고 자신의 인증요청메시지를 임의로 생성하여 멤버 무인체계에게 전달할 수 있다. 하지만 공격자는 ACMT를 보유하고 있지 않아 정상적인 인증요청메시지를 생성할 수 없다. 따라서 공격자의 인증요청메시지는 멤버 무인체계의 검증 절차를

통과할 수 없다. 즉, 공격자는 리더 무인체계로 위장할 수 없다. 공격자가 멤버 무인체계로 위장하는 경우도 같은 이유로 불가능하다. 결론적으로 ACMT를 보유하고 있지 않은 공격자의 위장 공격은 실패할 수밖에 없다.

5.1.3 메시지 변형 공격(message fabrication attack)

인증 과정 중 발생되는 모든 인증요청메시지는 비밀키로 암호화된다. 따라서 비밀키가 유출되지 않는 이상 인증요청메시지의 내용은 절대 복호화되지 않는다. 또한 식(4)에서 보는 바와 같이 인증코드, ID, 시간정보들이 접합되어 해시값과 함께 전달되므로 메시지의 무결성을 보장할 수 있다.

만약 비밀키가 유출되어 인증요청메시지가 복호화된다면 ID, 메시지 생성 시간정보, 인증코드 생성을 위해 사용되는 ACMT의 데이터 위치정보들이 노출된다. 하지만 공격자는 ACMT가 없기 때문에 올바른 인증코드를 생성할 수 없다. 따라서 공격자가 인위적으로 메시지 내용을 변경하더라도 수신자가 쉽게 변형 여부를 확인할 수 있다. 즉, 제안하는 프로토콜은 메시지 변형 공격에 안전하다.

5.2 효율성 분석

5.2.1 통신 오버헤드

제안하는 인증 프로토콜은 양방향 인증을 실현하기 위해 두 번의 단방향 인증처리를 하지 않고, Fig. 3에서 보는 바와 같이 인증요청과 인증승인을 한 개의 메시지로 처리하여 양방향 인증을 구현하였다. 즉, 양방향 인증을 위한 메시지의 수를 줄였다. 뿐만 아니라 제안하는 인증 프로토콜은 외부 네트워크에 위치한 인증서버에 접근할 필요가 없다. 채널 환경이 양호하지 않은 전술 무선 네트워크 환경을 고려했을 때 외부 인증서버와의 데이터 송·수신 실패율은 높을 수밖에 없다. 이는 인증 지연으로 이어져 인증 프로토콜의 비효율성을 초래한다.

결론적으로 제안하는 인증 프로토콜은 외부 인증서버로의 접근이 필요 없고, 인증승인과 인증요청을 하나의 메시지로 처리하여 양방향 인증을 구현하였기 때문에 통신 오버헤드, 인증에 소요되는 시간 측면에서 단방향 인증을 번갈아 가면 반복해서 수행하는 인증 프로토콜에 비해서 효율적이다.

5.2.2 계산량 분석

제안하는 인증 프로토콜의 계산량은 Fig. 3의 ① 번, ③번, ④번, ⑥번 처리과정에서 주로 발생한다. Table 2에서 보는 바와 같이 각 단계별로 인증요청 메시지의 생성 또는 검증을 위한 암·복호화, SHA-3 해시 연산이 필요하다. 특히, 인증코드 생성과 검증을 위해 각각 n번의 $M_m(\cdot)$ 사상 함수 연산을 해야 한다. 하지만 SHA-3 연산에 비해 $M_m(\cdot)$는 상대적으로 매우 간단하다. $M_m(\cdot)$는 입력값을 m으로 나누어 나머지를 구하는 연산만으로도 충분하기 때문이다. 이는 배터리와 계산량의 제약을 받는 IoT(Internet of Things) 장비에 적용되는 인증 프로토콜들과 유사한 수준의 계산량이다[12-14]. 또한 제안하는 프로토콜이 일반적인 센서와 같이 저전력, 저용량의 시스템이 아닌 전술 환경에서 이동이 가능한 무인체계를 대상으로 하고 있음을 고려할 때 계산량이 과도하게 요구되는 것은 아니다.

Table 2. Computation analysis in the proposed protocol

Category [1]	Enc.	Dec.	SHA-3	$M_m(\ )$
①	*1*	*0*	*1*	*n*
③	*0*	*1*	*1*	*n*
④	*1*	*0*	*1*	*n*
⑥	*0*	*1*	*1*	*n*

5.3 데이터 충돌 확률

제안하는 프로토콜에서는 식(1)의 h와 동일한 매핑값을 갖는 ACMT의 원소들이 존재하는 경우, 즉 데이터 충돌이 있는 경우, 이들의 조합을 통해 AC를 생성한다. 물론 h와 동일한 매핑값을 갖는 원소들이 없는 경우에도 모든 원소들의 조합으로 AC를 생성한다. 그런데 데이터 충돌이 발생하지 않을 확률이 높다면 동일한 AC가 발생할 확률이 높아진다. 또한 ACMT가 유출되었다고 가정했을 때 단순히 모든 원소들의 조합으로 AC가 생성된다면 공격자가 쉽게 AC를 유추할 수 있게 된다. 따라서 데이터 충돌이 발생할 확률이 높아야 안전하다고 할 수 있다.

데이터 충돌 확률은 ACMT의 크기와 맵핑 결과

1) Fig. 2에서의 데이터처리절차를 나타낸다.

값의 개수에 의해서 좌우된다. 즉, m과 n에 의해서 결정된다. 매핑 함수의 결과값이 균등분포(uniform distribution)라고 가정하자. h 값과 일치하는 데이터가 i개 있을 확률은 다음과 같다.

$$P_i = \binom{n}{i}(\frac{1}{m})^i(\frac{m-1}{m})^{n-i} \quad (7)$$

따라서 충돌이 발생하는 데이터가 존재할 확률(즉, 매핑 결과가 h와 일치할 데이터가 존재할 확률)은 다음과 같다.

$$\begin{aligned} P_c &= 1-P_0 \quad (8)\\ &= 1-(\frac{m-1}{m})^n \end{aligned}$$

그림 4는 n과 m의 비율($\alpha = m/n$) 에 따른 P_c를 나타낸다. 그림에서 알 수 있는 바와 같이 P_c는 n의 크기와는 상관관계가 크지 않고 α 값에 의해 크게 좌우된다. α가 0.1인 경우 P_c가 1을 나타내므로 확률적으로 항상 데이터 충돌을 발생시키기 위해서는 α가 0.1 이하가 되도록 m과 n의 값을 설정할 필요가 있다.

한편, 평균적으로는 ACMT의 n개의 데이터 중 충돌이 발생되는 데이터의 개수는 다음과 같다.

$$k = \sum_{i=1}^{n} iP_i \quad (9)$$

따라서 만약 ACMT가 유출되었다고 하더라도 공격자가 충돌 데이터쌍을 정확히 선택할 확률은 다음과 같다.

$$P_s = 1/\binom{n}{k} \quad (10)$$

식 (10)은 식 (7)-(9)에 의해 n과 m의 값의 선택에 따라 조정이 가능하다. 그림 5에서 보는 바와 같이 n이 커질수록 P_s는 당연히 작아지며, α가 커질수록 증가하고 그 값은 매우 작다. 예를 들어, $n=100$, $\alpha=0.1$인 경우, $P_s = 5.7\times10^{-14}$ 이다. 따라서 운용환경에 따라 적절하게 파라미터들을 선택한다면 ACMT가 유출되더라도 충돌 데이터쌍을 찾을 수 있는 확률이 매우 낮기 때문에 안전성을 유지할 수 있다.

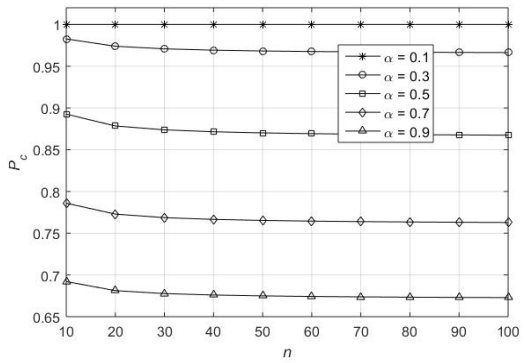

Fig. 3. The value of P_c according to α and n

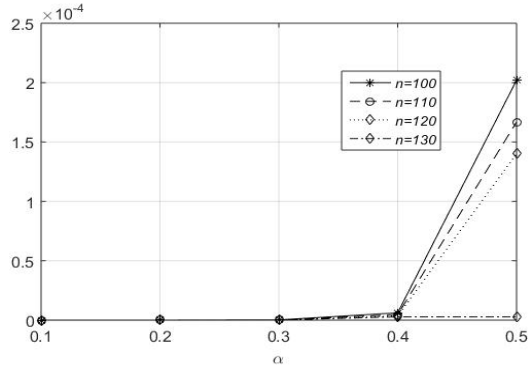

Fig. 4. The value of Ps according to α and n

그림 4와 그림 5를 통해 제안하는 프로토콜에서 α를 0.1 이하로 유지한다면 안전성을 보장할 수 있다는 것을 확인할 수 있다.

VI. 결론 및 향후연구

본 논문에서 원활한 장거리 통신이 보장되지 않는 전술 무선 네트워크에서 운용되는 무인체계를 고려한 해쉬 충돌 기반의 양방향 인증 프로토콜을 제안하였다. 제안하는 인증 프로토콜은 무인체계들이 동일하게 소유하고 있는 임의의 데이터들 중 해시충돌을 일으키는 데이터들의 조합을 인증코드로 사용하여 상호 교환함으로서 양방향 인증을 수행한다.

다양한 공격 모델을 대상으로 성능을 분석한 결과 제안하는 인증 프로토콜은 메시지 재전송 공격, 위장 공격, 메시지 변형 공격 등에 안전하다. 또한 장거리 통신이 요구되는 별도의 인증서버와의 통신이 불필요하고 하나의 메시지로 인증요청과 인증승인을 처리하

여 메시지 전송 횟수와 인증에 소요시간 측면에서 효율적이다. 또한 전장 환경에서 운용되는 무인체계의 계산능력, 배터리 용량 등을 고려했을 때 많은 계산량을 요구하지 않는다. 따라서 통신환경이 불안정한 전술 무선 네트워크 환경에서 적절한 파라미터들을 선택하여 운용한다면 제안하는 프로토콜이 효율적으로 적용될 수 있다.

한편, 작전 운용환경을 고려했을 때 실행 가능성과 실효성은 크지 않지만 제안하는 프로토콜은 아군 무인체계가 자신이 아닌 다른 무인체계로 위장할 수 있다. 제안하는 프로토콜이 범용적으로 사용되기 위해서는 내부 위협에 대한 대응책이 필요하다. 따라서 향후연구에는 제안하는 프로토콜의 활용 분야를 넓히기 위해서 내부 위협에 대한 대응방안을 추가하여 발전시킬 예정이다.

References

[1] W. Stallings and L. Brown, "Computer Security: principal and practice," 3rd Ed., pearson, 2014.

[2] L. Reyzin, N. Reyzin "Better than BiBa: short one-time signatures with fast signing and verifying," *Proceedings of the 7th Australian Conference on Information Security and Privacy*, London, UK, pp. 144-153, 2002.

[3] Josef Pieprzyk, Huaxiong Wang, and Chaoping Xing, "Multiple-time signature schemes against adaptive chosen message attacks," *International Workshop on Selected Areas in Cryptography*, Springer, pp. 88-100, 2003.

[4] J. Lee, S. Kim, Y. Cho, Y. Chung, Y. Park, "HORSIC: an efficient onetime signature scheme for wireless sensor networks," *Inform. Processing Letters,* vol. 112, pp. 783-787, 2012.

[5] L. Eschenuer, V. D. Gligor, "A key-management scheme for distributed sensor networks," *Proceedings of the 9th ACM conference on computer and communications security*, pp.41-47, Nov. 2002.

[6] W. Du, J. Deng, Y. S. Han, P. K. Varshney, "A key predistribution scheme for sensor networks using deployment knowledge," *IEEE Transactions on Dependable and Secure Computing,* vol. 3, no. 1, pp. 62-77, 2006.

[7] S. Zhu, S. Setia, and S. Jajodia, "LEAP+: Efficient security mechanisms for large-scale distributed sensor networks," *ACM Trans. Sen. Netw.*, vol. 2, pp. 500-528, 2006.

[8] J. Jang, T. Kwon, J. Song, "A time-based key management protocol for wireless sensor networks," *Proceedings of ISPEC*, LNCS 4464, pp. 314-328, 2007.

[9] S. Nesteruk, S. Bezzateev, "Location-Based Protocol for the Pairwise Authentication in the Networks without Infrastructure," *Proceeding of the 22nd FRUCT Association*, pp. 190-197, 2018.

[10] P. Vijayakumar, M. Azees, A. Kannan and L. Jegatha Deborah, "Dual Authentication and Key Management Techniques for Secure Data Transmission in Vehicular Ad Hoc Networks," *IEEE Transaction on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 1015-1028, April 2016.

[11] Jin Sook Bong, Yu Hwa Suh, Ui Jin Jang and Yongtae Shin, "RSU-independent Message Authentication Scheme using CRT-based Group Key in VANET," *Journal of KIISE*, Vol. 46, No. 3, pp. 277-284, 2019.

[12] Bamasag, Omaimah Omar, and Kamal

Youcef-Toumi, "Towards continuous authentica-tion in internet of things based on secret sharing scheme," *Proceedings of the WESS'15: Workshop on Embedded Systems Security*, pp. 1-8, 2015.

[13] Xiao, J. andChen, C., "Authentication and Access Control in the Internet of Things," *Proceedings of 32nd International Conference on Distributed Computing Systems Workshops*, pp. 588-592, 2012.

[14] Yavuz, A.A. "An efficient real-time broadcast authentication scheme for command and control messages," *IEEE Transactions on Information Forensic and Security*, vol. 9, no. 10, pp. 1733-174, 2014.

〈저자소개〉

이 종 관 (Jong-kwan Lee) 정회원
2000년 2월: 육군사관학교 전자공학과 졸업
2002년 2월: 한국과학기술원 전자공학과 석사
2014년 2월: 아주대학교 NCW(네트워크중심전)학과 박사
2017년~현재: 육군사관학교 컴퓨터과학과 조교수
〈관심분야〉 사이버전, 네트워크중심전, 인공지능 보안, 전술네트워크, 그룹키 관리