전술 무선 네트워크에서 무인전투체계를 위한 인증 프로토콜

이종관[1*] · 이민우[2]

[1]육군사관학교 · [2]아주대학교

Authentication Protocol for Unmanned Combat Systems in Tactical Wireless Networks

Jong-Kwan Lee[1*] · Minwoo Lee[2]

[1]Korea Military Academy · [2]Ajou University

E-mail : jklee64@kma.ac.kr / iminu@ajou.ac.kr

요 약

본 논문에서 장거리 통신이 항상 보장될 수 없는 전술 무선 네트워크 환경에서 무인전투체계들간의 안정한 상호 인증 프로토콜을 제안한다. 제안하는 프로토콜은 임의로 선택된 데이터의 해시 충돌을 이용하여 인증코드를 생성한다. 인증요청자는 이를 인증자의 공개키로 암호화여 전송한다. 인증요청자와 인증자가 정당한 인증코드를 상호 공유함으로써 인증을 수행한다. 다양한 공격 시나리오를 대상으로 제안하는 기법의 안전성을 분석한다.

ABSTRACT

In this paper, we propose a stable mutual authentication protocol between unmanned combat systems in tactical wireless networks where long distance communications are not always guaranteed due to a poor channel condition. The proposed protocol generates an authentication code using hash collision of arbitrarily selected random data. The authentication requester encrypts and transmits it to the authenticator. They performs authentication by sharing the valid authentication code. We analyze the safety of the proposed method for various attack scenarios.

키워드

Mutual Authentication, Hash Collision, Unmanned Combat Systems, Tactical Wireless Networks

Ⅰ. 서 론

위험도가 높거나 인간이 수행하기에 비효율적인 전투상황에서 무인전투체계가 많이 활용될 것이다. 현재는 무인전투체계가 인간 전투원의 보조적 역할에만 국한되어 있으나, 급격한 기술적 발전을 고려했을 때 무인전투체계의 역할은 인간의 중간 개입이 배제된 독립적인 작전 수행으로 확대될 것이다. 다시 말해 인간은 작전목표와 작전시 제한사항만을 제시하고 무인전투체계가 스스로 상황을 인지, 판단, 결심하여 작전을 효과적으로 수행하는 것이다. 또한 단일 무인전투체계가 수행하기에 난이도가 높은 상황에서는 다수의 무인체계가 군집 형태로 임무를 수행하게 될 것이다. 뿐만 아니라 작전임무의 목적과 상황의 변화에 따라 군집의 형태와 가입자가 빈번하게 변경될 수 있다.

한편 전장상황에서의 무선 네트워크는 적의 인위적인 전파 방해와 해킹 시도가 상존할 뿐 아니라 통신 주체가 물리적인 생존성 확보를 위해 통신환경이 열악한 지형(즉, LOS가 확보되지 않는 지역)으로 이동 또는 배치되는 경향이 있다. 따라서 안정적인 장거리 통신이 통상 보장되지 못한다.

따라서 장거리 통신이 보장되지 않는 상황에서 자율적으로 작전을 수행하는 군집 무인전투체계를 위한 안전한 인증 프로토콜이 필요하다.

II. 시스템 모델 및 가정사항

본 논문에서는 다음과 같은 사항들을 가정한다. 먼저, 미래 전장환경에서 무인전투체계들은 팀단위의 편제를 유지한 상태에서 작전을 수행한다고 가정한다. 즉, 팀 단위로 리더가 존재하며 리더는 새로 진입하는 무인전투체계에 대한 인증을 담당한다. 기존 리더의 임무수행이 불가한 경우에는 새로운 리더가 선출될 수 있다. 또한 무인체계들은 센서 네트워크의 센서체계와는 달리 충분한 통신 및 연산 능력을 보유한다고 가정한다. 그리고 모든 무인체계는 작전에 투입되기 전에 인증에 필요한 기본 정보들이 입력되며 자신의 개인키는 안전하게 관리된다.

한편, 팀단위로 활동하던 무인체계는 다양한 이유로 팀 소속이 변경되거나 다수의 팀이 한 개의 팀으로 통합 또는 하나의 팀이 다수의 팀으로 분할 될 수 있다.

III. 제안하는 인증 프로토콜

제안하는 인증 프로토콜에서 인증코드는 각 무인체계가 동일하게 보유하고 있는 임의의 데이터들을 해시하여 해시충돌이 발생하는 데이터들에 대한 적절한 연산 결과를 인증코드로 사용한다[1]. 인증코드는 적의 중간자 공격에 대비하기 위한 타임스탬프, 자신의 공개키, 해시할 데이터를 선택하는 기준 정보 등과 함께 수신자의 공개키로 암호화하여 인증자에게 전달된다. 인증자(즉, 리더 무인체계)는 자신의 개인키로 해당 메시지를 복호화하고 인증코드의 검증, 타임스탬프의 유효성을 확인하여 이상이 없는 경우 인증 결과를 팀 내부 무인체계들에게 전달한다.

그런데 인증요청자도 인증자의 정당성을 확인할 필요가 있다. 따라서 인증자도 앞서 서술한 방법과 동일한 과정을 통해 인증요청자에게 인증을 받는다. 상호 인증이 모두 정상적으로 종료된 이후 인증요청자는 새로 가입한 네트워크를 통해 정보를 송수신한다. 그림 1은 제안하는 인증 프로토콜의 동작 절차를 간략히 나타낸다.

IV. 안전성 분석

본 장에서는 제안하는 인증 프로토콜에 대해 다양한 공격 시나리오를 바탕으로 안전성을 평가한다. 데이터 송수신 범위에 위치한 공격자는 인증요청자와 인증자 사이의 모든 메시지를 수신할 수 있다. 하지만 수신자의 개인키가 없는 경우 해당 메시지를 복호화할 수는 없다.

공격자는 인증 관련 메시지를 중간에서 수신하여 자신이 정당한 인증요청자 또는 인증자인 것처럼 위장을 시도할 수 있다. 하지만 제안하는 인증

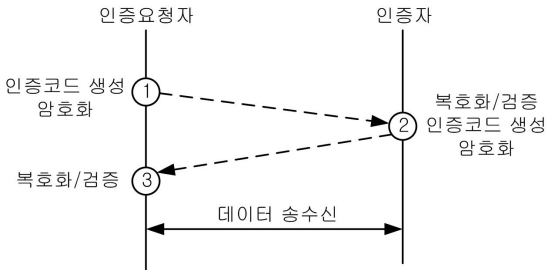

그림 1. 제안하는 인증 프로토콜의 동작 절차

프로토콜에서는 타임스탬프를 포함하고 있으므로 과거에 수신한 인증 관련 메시지를 재사용하여 인증 과정에 개입할 수 없다. 또한 아군 무인전투체계간의 공유된 임의의 데이터들을 공격자는 소유하고 있지 않으므로 정당한 인증코드를 생성하는 것이 불가능하다. 따라서 인증요청자 또는 인증자로 위장하는 것이 불가능하다.

제안하는 인증 프로토콜에서는 인증코드, 공개키, 타임스탬프 정보들의 해시값이 함께 전달되므로 정보의 무결성을 보장할 수 있다. 따라서 공격자가 메시지의 내용을 변경하기 위해 시도하는 경우 이를 쉽게 식별할 수 있다.

그리고 공격자가 인증코드를 추정하기 위해서는 개인키, 해시를 하기 위해 선택된 임의의 데이터들, 사용되는 해시 함수 등이 모두 필요하다. 하지만 이들 인증 정보들은 통상 작전수행 전, 후 또는 주기적으로 갱신되도록 운용하기 때문에 이들이 동시에 유출될 확률은 거의 없다. 따라서 공격자의 인증코드 추정 공격은 현실적으로 불가능하다.

V. 결론 및 향후연구

본 논문은 장거리 통신이 보장될 수 없는 전술무선 네트워크 환경에서 무인전투체계간의 상호인증 프로토콜을 제안하였다. 제안하는 프로토콜은 임의의 데이터들에 대한 해시충돌 결과를 활용하여 인증을 수행한다. 다양한 공격 시나리오를 대상으로 제안하는 기법의 안전성을 분석한 결과 제안하는 기법은 중간자 공격, 메시지 변경 공격, 인증코드 추정 공격에 대해 안전함을 확인하였다.

향후 제안하는 프로토콜에 대해 통신 오버헤드 및 계산량의 효율성 등을 시뮬레이션을 통해 추가 분석할 예정이다.

References

[1] J. K. Lee, “Two-Way Authentication Protocol between Unmanned Systems in Combat Field,” *The Journal of KIMST*, 2019.(submitted)