Private Blockchain 을 활용한 UAV 네트워크 보안성 향상 모델

윤지영, 유재민, 박경준
대구경북과학기술원

{hailey_yoon; ryujm95; kjp} @dgist.ac.kr

UAV Network Security Enhancement Model Using Private Blockchain

Jiyoung Yoon, Jaemin Yu, Kyung-Joon Park
Daegu Gyeongbuk Institute of Science & Technology (DGIST)

요 약

최근 레저, 촬영 등의 목적과 함께 드론봇 전투단이 군부대에서 출범되는 등 공공기관에서도 일상의 안전을 위해 드론이라 불리는 UAV (Unmanned Aerial Vehicle)가 활용되고 있다. 드론은 GCS (Ground Control Station)와 P2P (peer-to-peer) 네트워크로 연결되어 임무를 할당 받고 수행중인 임무를 보고하기 위한 상호 간의 신뢰성있는 통신이 필요하다. 하지만 기존의 UAV 네트워크는 다양한 네트워크 공격에 취약한 문제점이 있다. 따라서 본 논문에서, 우리는 분산 저장, 상호 간의 신원 증명 시스템을 통해 P2P 네트워크의 신뢰성을 향상시키는 private blockchain 을 활용하여 UAV 네트워크의 보안성을 향상시키는 시스템 모델을 제안한다.

Ⅰ. 서 론

드론이라 불리는 무인항공기(UAV: Unmanned Aerial Vehicle)는 레저, 촬영, 배송의 목적으로 활용될 뿐만 아니라 최근 드론봇 전투단이 군부대에 출범된 것과 같이 정찰, 감시, 방어 등의 역할을 목적으로 공공기관에서도 일상의 안전을 위해 UAV 가 활용되고 있다. 이는 CPS (Cyber Physical System)의 중요한 애플리케이션 중 하나로 대두되고 있다 [1,2]. GCS (Ground Control Station)는 셀룰러 시스템, Wi-Fi, Telemetry 등과 같은 무선 통신 방법을 통해 드론을 제어한다. UAV 네트워크는 신뢰성을 보장하여 드론의 상태, 임무, 위치, 고도 정보를 전송하는 중요한 역할을 한다. 하지만 UAV 네트워크는 다양한 네트워크 공격에 취약한 문제점을 가지고 있다.

일반적인 UAV 네트워크는 중앙 서버가 존재하지 않는 P2P (peer-to-peer) 형태의 네트워크로 구성되어 있다. 하지만 P2P 네트워크는 데이터의 위변조 여부 파악 불가, 데이터의 무결성 침해와 같은 보안적인 문제점이 존재한다 [3].

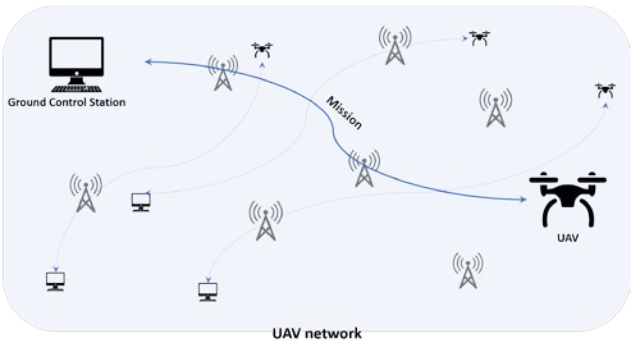
본 논문에서는 blockchain 기술을 통해 UAV 네트워크에서의 임무 정보에 대한 위변조 및 도청과 같은 네트워크 공격으로부터 안정적이고, UAV 와 GCS 로 이루어진 노드 사이의 신뢰성을 높이는 UAV 네트워크 보안성 향상 시스템 모델을 제안한다.

Ⅱ. 본 론

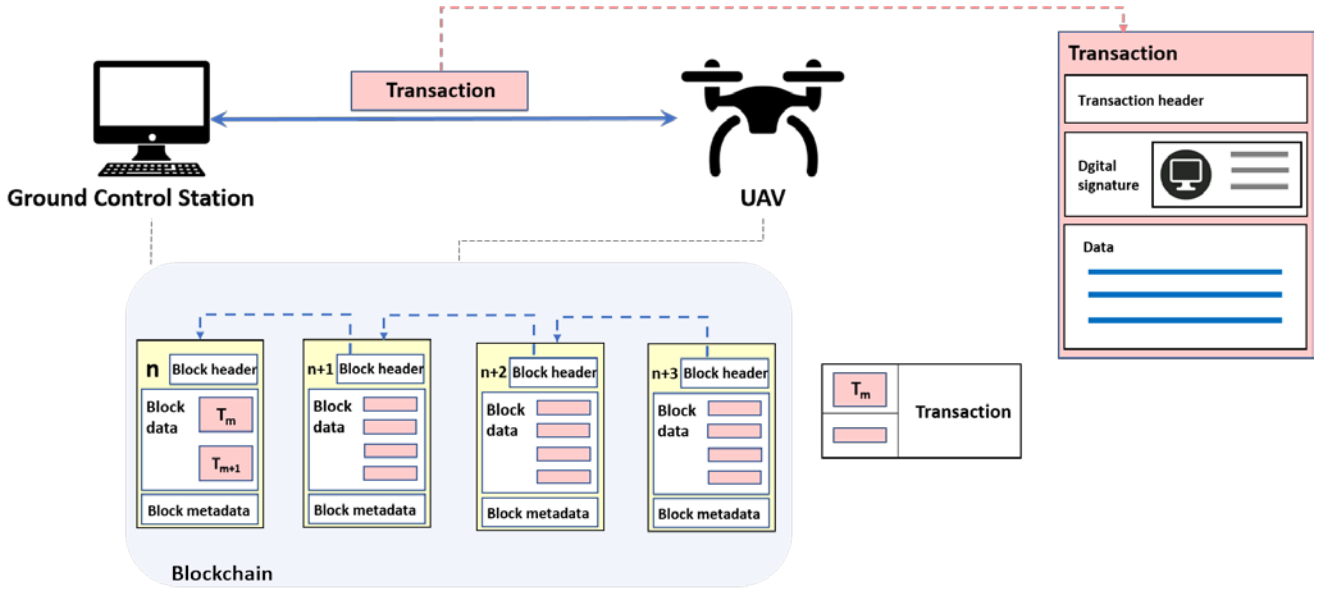
Blokchain 은 중앙 서버가 존재하지 않는 P2P 형식의 네트워크에서 노드간의 주고받는 중요한 정보를 블록에 저장할 수 있다. 이 블록들은 체인 형태로 연결되어 모든 노드들에 분산저장하여 신뢰성 및 데이터의 무결성을 검증한다. 따라서 그림 1 과 같은 P2P 형식의 UAV 네트워크 환경에서 드론과 GCS 가 주고받는 데이터들의 무결성 및 보안성을 향상시키기위해 private blockchain 을 활용한다.

Private blockchain 은 사전에 관리자로부터 데이터 접근 권한을 부여받아 신원이 증명된 노드들만이 네트워크에 참여할 수 있다. UAV 네트워크에서 신원 증명은 관리자 엔티티가 그림 3 과 같이 GCS 와 드론에게 디지털 인증에 필요한 고유의 private key, public key 를 할당하는 것을 말한다. Private blockchain 에서 노드들의 신뢰성 보장을 위해 작업 증명 알고리즘인 Proof of Authority(PoA)를 사용한다. PoA 는 신원이 보장된 노드 중 검증자 (validator)를 선정하여 블록의 유효성 검증을 한다. 블록들은 검증자에 의해 유효성 검증이 되면 네트워크에 분산 저장된다.

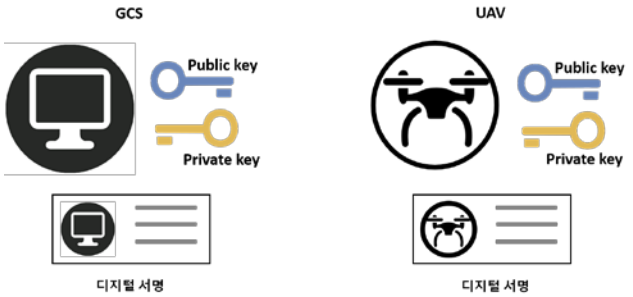
그림 2 는 우리가 제안한 private blockchain 을 활용한 UAV 네트워크 시스템 모델 개요를 보여준다. 우리는 GCS 가 UAV 에 새로운 임무를 할당할 때를 가정한다. UAV 와 GCS 노드의 신원 증명 과정은 다음과 같다.



<그림 1> UAV 네트워크 환경.



<그림 2> Private Blockchain 을 활용한 UAV 네트워크 시스템 모델 개요.



<그림 3> 제안된 모델의 신원 증명 시스템.

- GCS 는 UAV 가 수행할 임무 정보를 작성하고 고유의 private key 를 이용하여 디지털 서명을 생성해 함께 첨부하여 트랜잭션을 만든다.
- 트랜잭션을 UAV 로 전송하고 이를 수신한 UAV 는 GCS 의 public key 를 이용해 해당하는 GCS 가 맞는지 확인한다.
- 트랜잭션의 발신자 신원이 증명되면 UAV 는 트랜잭션에 저장된 임무를 수행한다.

Private key 는 공개되지 않는 고유의 값이므로 악의적인 공격자가 이를 이용한 디지털 서명을 만들 수 없다. 디지털 서명이 없는 메시지는 트랜잭션이 아니므로 드론이 받아들일 수 없고, 이로 인해 공격자가 GCS 로 위장하거나, 악의적으로 드론이 수행하고 있는 임무를 변경 및 중단시킬 수 없다.

다음으로는 임무의 분산 저장 과정을 설명한다.

- 위 과정에서 신원 증명이 완료된 트랜잭션을 블록의 block data 에 저장한다.
- 블록은 block data, block header 로 block hash 값을 구한다. 이때 블록은 검증자로부터 블록단위로 유효성 검증을 받으면 블록이 생성된다.
- N+1 번째 블록의 헤더에는 N 번째 block hash 값이 포함된 체인 형태로 블록이 연결되어 노드들에 분산 저장된다.

분산 저장을 통해 공격자는 임무를 삭제 또는 위변조시키기 어려우므로 UAV 의 임무 정보는 무결성을 보장받는다.

Ⅲ. 결 론

본 논문에서는 다양한 네트워크 공격에 취약하던 기존의 UAV 네트워크 문제점을 private blockchain 의 분산 저장 시스템과 신원 증명 시스템을 활용하여 공격자가 임무 정보의 기록을 수정할 수 없게 하여 데이터의 무결성을 보장하였고, 신뢰도가 보장된 GCS 만이 UAV 에게 임무를 부여하게 할 수 있게 하여 드론의 임무 수행에 대한 신뢰도를 향상한 모델을 제안하였다.

ACKNOWLEDGMENT

본 연구는 과학기술정보통신부에서 지원하는 DGIST 기관고유사업에 의해 수행되었습니다(19-ST-02).

참 고 문 헌

[1] K.-J. Park, R. Zheng, and X. Liu, "Cyber-physical systems: Milestones and research challenges," Computer Communications, vol. 36, issue 1, pp. 1-7, December 2012.

[2] K.-J. Park, J. Kim, H. Lim, and Y. Eun, "Robust path diversity for network quality of service in cyber-physical systems," IEEE Transactions on Industrial Informatics, vol. 10, no. 4, pp. 2204-2215, November 2014.

[3] Engle, Marling, and Javed I. Khan. "Vulnerabilities of P2P systems and a critical look at their solutions." Kent State University, Tech. Rep (2006).