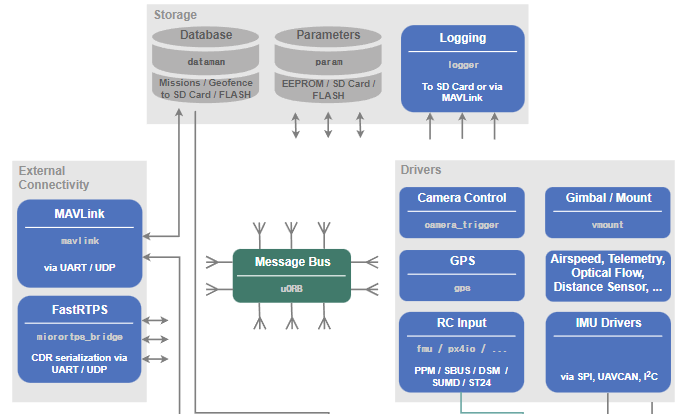
|  |
| --- |
| **PX4 Autopilot 로그 데이터 무결성 검증 방안**  **요 약**  최근 드론이 군사, 건설, 스포츠, 물류 등 다양한 분야에서 활용되며 UAV(Unmaned Aerial Vehicle) 시장이 빠르게 성장하고 있다. 그러나 시장의 빠른 확산세와 함께 드론의 취약점을 이용한 공격 및 데이터 변조에 대한 위협도 함께 커지고 있다. 이에 본 논문은 PX4 Autopilot을 대상으로 설정하여 ULog 데이터의 해시값을 merkle tree 구조로 저장하여 데이터 위변조 가능성 분석을 효율적으로 수행하는 방안을 제시한다. merkle root와 이전 블록 해시값을 비롯한 정보들을 블록의 해시값으로 저장하여 각 파일 간 연쇄적인 데이터 검증 구조를 구축하였다. |

**1. 서론**

최근 빠른 속도로 사물인터넷이 확산되고 있으며, 대표적인 사물인터넷 기기로 UAV(Unmaned Aerial Vehicle)이 주목받고 있다. 민간 UAV시장은 2021년 기준 263억달러 규모에서, 2026년에는 413억달러까지 매년 9.6%의 급격한 성장세를 보일 것으로 예측된다.[1] 이러한 UAV의 성장은 다양한 분야에 UAV 활용을 촉진 시키고 있지만, 보안 안전성을 검증하지 않은 UAV의 보급에 대한 위험성 또한 대두되고 있다. 이는 군사, 건설, 스포츠, 물류 등 다양한 분야에서 활용되고 있는 UAV의 특성을 고려하였을 때, UAV의 취약점을 악용한 공격 및 데이터 변조는 각종 사고를 유발할 수 있으며, 인간의 생명을 위협할 수 있다. 따라서 기존에 활용되고 있는 UAV에 대한 위변조 가능성 분석과 대응 방안 수립이 시급한 실정이다. 이에 본 논문에서는 오픈 소스 드론 시장의 높은 점유율을 보유하고 있으며,[2] Linux foundation의 관리를 받는 오픈 소스 드론 플랫폼 Dronecode platform의 공식 flight code인 PX4 오토파일럿을 대상으로 데이터 위변조 방지에 대한 연구를 진행하였다. PX4 오토 파일럿에서 기록되는 로그 데이터를 해시화하여 merkle tree와 root를 만들어 각 로그 파일의 데이터 무결성을 검증하는 라이브러리를 개발했으며, 해당 라이브러리는 이전 로그 파일들의 정보와 merkle root를 해시화 해 블록 해시를 만들고 이들을 블록 구조로 연결하여 각 블록과 merkle root의 무결성을 검증한다.

**2. 관련 연구**

**2.1 PX4 Autopilot architecture**

****

**[그림 1] PX4 autopilot architecture**

[그림 1]은 PX4에서 비행 데이터가 저장되는 방식을 나타낸 구조도이다. GPS, Airspeed 등의 센서 데이터는 드라이버 소프트웨어를 통해 처리되어, 이를 기반으로 드론의 상태를 예측하는 Estimator로 보내는 동시에 uORB를 통해 Logger 모듈에도 전송된다. Logger 모듈은 uORB의 topic을 보고 받은 데이터의 종류를 구분해 로깅한다. Estimator나 Controller에서 처리된 비행 데이터들 역시 uORB를 통해 Logger 모듈로 전달된다. 설정 데이터들은 SD card와 Flash 두 가지 방식으로 모두 저장될 수 있다. 이 논문에서는 Logger 모듈을 통해 SD card에 저장되는 데이터들을 중심으로 위변조 방지 방안을 다루었다. 본 논문에서 다룰 Logger 모듈은 /msg 디렉토리에 저장되어 있는 데이터 타입을 정의하는 토픽들에 대한 정보를 SDcard(/fs/microSD) 폴더 하위에 저장한다. 토픽은 PX4가 실행될 때 기본적으로 logger가 자동으로 실행되고, 실행 시간에 맞는 yyyy-mm-dd 형식의 이름을 가진 폴더 하위에 hh-mm–ss.ulg 형식으로 파일이 저장된다. 또한 사용자가 logger on 명령어를 전달하면 로거 세션이 따로 실행되고[3], logger off 명령을 받으면 sess<[i]> 폴더 아래에 저장된다. 한 번 logger가 실행되고 종료될 때까지의 정보들은 같은 세션 폴더에 저장된다.

**2.2 ULog**

ULog는 PX4에서 데이터를 로깅하는 파일 형식으로, 메시지 유형을 포함하는 self-describing 포맷을 가지고 있다. ULog는 센서 등의 디바이스 입력, 고도를 포함한 드론의 내부 상태, 그리고 로그 메시지를 기록하며, 해당 데이터들은 바이너리 형식으로 저장된다. 파일은 Header, Definition, Data 세 섹션으로 구성된다. [4] Header 섹션에는 파일 형식 버전과 타임스탬프가 기록되고, Definition 섹션에는 버전 정보와 메시지 형식, 초기 파라미터 값이 포함된다. Data 섹션에는 메시지의 id, name 그리고 기록한 데이터가 포함된다.

**2.3 해시 함수**

해시 함수는 임의의 길이의 문자열을 고정 길이의 문자열로 매핑한다. 문자열 슬라이싱, 치환, 전치를 이용해 해시값이라 부르는 결과를 만들어 낸다. 입력값의 작은 변화로도 완전히 다른 결괏값을 만들어야 하며, 입력값으로 결괏값을 예측하거나, 같은 결괏값을 만드는 서로 다른 입력값을 유추할 수 있으면 안 된다. 이러한 특성을 이용하여 데이터의 무결성을 검증을 위해 사용할 수 있다. 해시 함수는 메시지의 크기와 관계없이 고정된 해시값을 생성하며, 계산 속도가 빠르다. 대표적인 해시 알고리즘으로는 SHA, MD5가 있다.

**2.4. Merkle Tree**

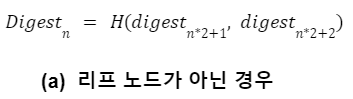
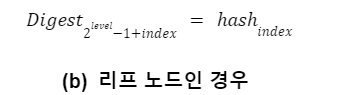
merkle tree는 주로 블록체인에서 블록 하나에 포함된 거래 정보를 트리 형태로 표현하기 위해 사용되는 데이터 구조이다.[5] 블록체인 구조를 적용한 암호화폐 거래에서는 거래 정보를 해시화하고 해시값을 짝지어 다시 해시화하여 상위 해시값을 만드는 단계를 거친다. 이 트리의 최상위의 해시값을 ‘merkle tree root’라고 한다. 본 논문에서는 해당 구조를 이용해 비행 데이터의 정보를 저장하는 방안을 제안하였다.

**3. 제안하는 방안**

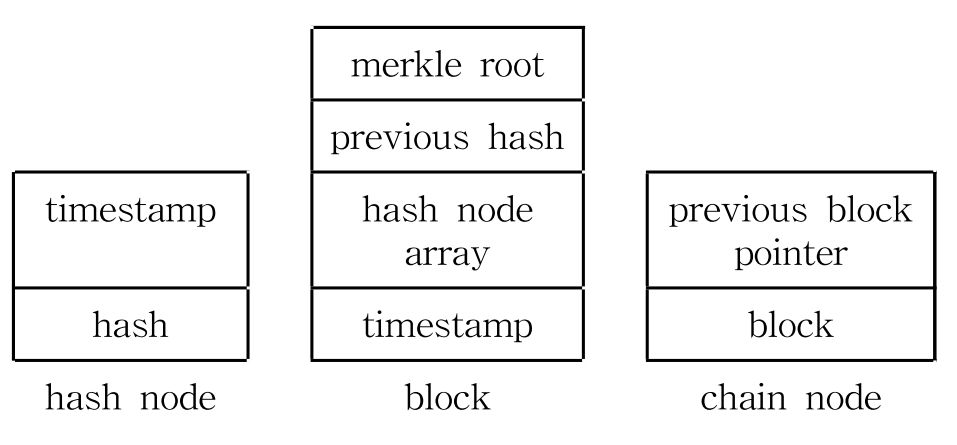
비행 중에 수집된 각 종류의 데이터들은 Logger 모듈을 통해 외장 SD카드 내에 저장될 수 있다. 본 논문에서는 px4 autopilot의 아키텍처를 기반으로 Logger 모듈에서 기록되는 로그 데이터의 위변조 방지 방안을 제시한다. 사용 환경은 pixhawk 4 mini[7]와 px4 fmu v5 펌웨어를 기반으로 하였다.

**3.1. 데이터 구조**

로그 데이터의 무결성을 검증하기 위해, 체인을 생성 및 관리하는 라이브러리를 개발하였다. 데이터를 구성하는 가장 작은 단위는 hash node이며, 새로운 데이터를 저장할 때 이를 해시화한 값과 timestamp를 해당 구조체에 저장한다. 이후 hash node를 block 객체에 추가 메서드를 통해 저장한다. 사전에 설정한 블록을 구성하는 노드의 수만큼 hash node가 들어오면, 해당 노드들을 리프 노드로 가지고 있는 머클 트리를 구성한다. 각 노드들은 배열로 구현되는 이진 트리를 구성하며 트리의 한 노드는 자식 노드들의 해시값을 짝지어 해시화한 값을 digest로 갖는다. 배열 내의 index가 n인 노드는 n\*2+1, n\*2+2 노드를 자식 노드로 갖는다. 따라서 index가 0인 노드가 merkle root가 되며 block 객체에 저장된다. 각 노드의 해시를 생성하는 수식은 [그림 2]와 같다. block 객체에는 이전 블록의 해시값, hash node를 저장하는 배열, 블록의 노드 중 가장 마지막 노드의 timestamp를 저장한다. 이 데이터들을 해시화한 값이 해당 block의 hash가 된다. 트리 생성이 완료된 후 block 객체는 chain 객체의 linked list에 추가된다. chain node 클래스는 block 객체를 체인 구조로 관리하는 역할을 한다. chain 클래스는 chain node의 포인터 형태인 genesis, leaf를 가지고 있으며, leaf 노드에서 시작해 각 노드가 previous block pointer를 가리켜 genesis 블록에서 끝나는 linked list를 이룬다.



**[그림 2] 다이제스트 생성 수식**

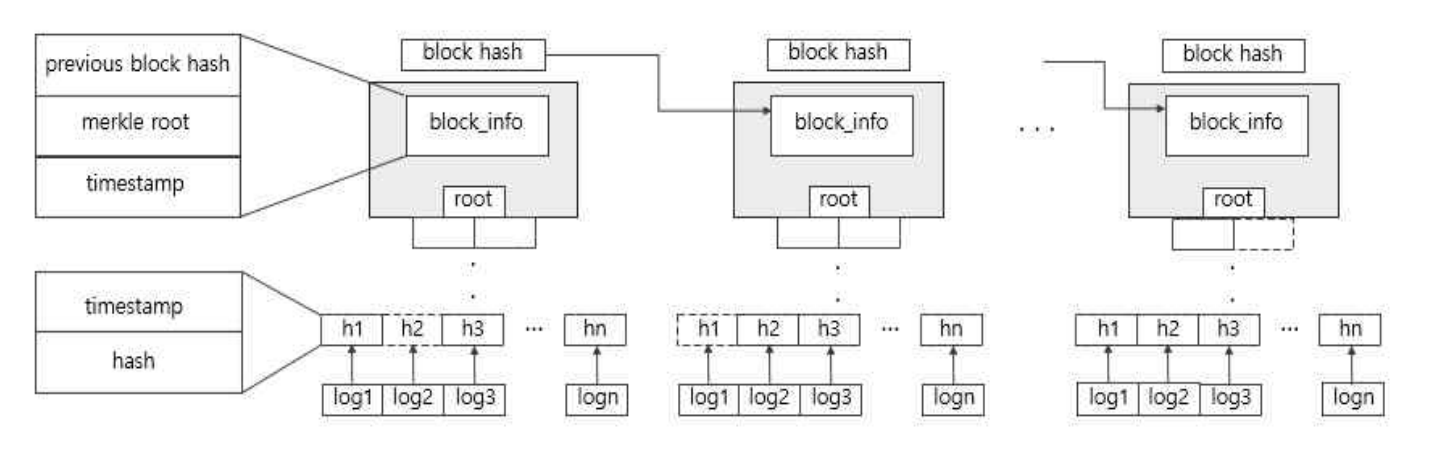


**[그림 3] 데이터 구조**

**3.2 검증 방식**

**3.2.1 block hash 비교 검증**

merkle root 값의 위변조 가능성은 블록 간 block hash 값을 비교하여 수행한다. 무결성 검증을 수행할 블록의 다음 블록부터, 해당 블록에 저장되어 있는 previous block hash 값과 이전 블록의 block hash 값을 비교한다. 이 값이 일치할 경우, 이전 블록의 무결성 검증을 수행하는과정을 반복하다, 기원 블록에 도달하게 되어 SD카드에 저장된 모든 ULog 파일들의 merkle root의 무결성을 보장할 수 있다. 반대로 previous block hash 값과 이전 블록의 block hash가 불일치하는 경우, 이전 merkle root 데이터가 위변조 되었거나 혹은 정상적인 경로로 생성되지 않은 파일이 추가되었다고 판단한다. 이 경우에는 merkle root를 비롯한 block\_info 데이터의 진위 여부를 판단할 수 없으니 후술할 ULog 파일 데이터의 무결성 검증결과의 신뢰도도 보장할 수 없게 된다.

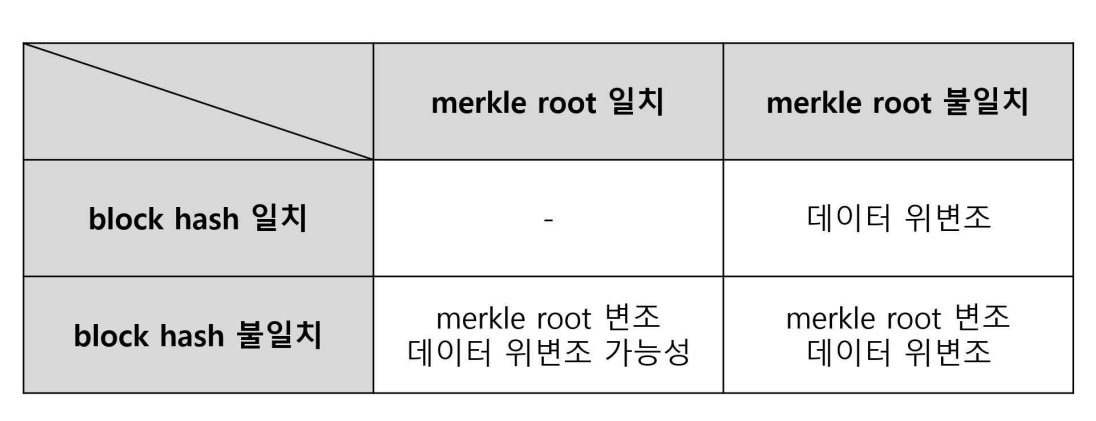


**[그림 4] 체인 구조**

**3.2.2 ULog 파일 내부 데이터 무결성 검증**

ULog 파일 내부 데이터의 무결성 검증은 merkle root값과 파일 내부 데이터의 해시값을 비교하여 수행한다. 무결성 검증을 수행할 파일의 데이터들을 해시화 한 후, 이를 리프 노드로 하는 merkle tree를 생성한다. 이 merkle tree의 merkle root가 block에 저장되어 있는 merkle root 값과 다르게 나올 경우, 해당 ULog 파일의 내부 데이터가 위변조되었다고 판단할 수 있다. 특정 데이터 혹은 데이터 구간의 위변조 여부도 확인할 수 있다. timestamp를 통해 해당 데이터의 트리 내의 인덱스를 확인한 후 [그림 2]의 수식을 적용해 merkle treeq 에서 해당 데이터의 해시값을 저장했던 노드의 위치를 찾는다. 속도를 보다 높이기 위해서 기존에 존재하는 Merkle tree에 Segment tree 개념을 적용시켜 해시화 하는 방안을 제안한다. 두 해시값을 짝을 지어 해시화하는 것을 Segment tree 생성 과정에서의 덧셈으로 본다. tree를 구성하는 노드들은 자신의 해시값을 구성하는 데 사용되었던 하위 노드들을 포함하게 된다. 구성하는 데 사용되었던 하위 노드들을 포함하게 된다. 위변조 검증을 위해 데이터를 해시화하여 대응되는 Merkle tree 상의 노드에 적용하는 것을 update 과정에 대입하게 되면, Segment tree에서 구간합을 구하는 과정과 유사하게 위변조 검증 대상이 아니었던 데이터들을 사용하려면 기존에 저장되어 있던 merkle tree에서 동일한 위치의 있는 노드의 digest 값을 이용하면 된다. 검증 대상 데이터의 변화에 영향을 받는 노드들만 골라 해시화를 수행한다. 이 방안을 사용할 때는 트리에 저장된 상위 레벨 노드를 활용해 merkle root 값을 구하기 때문에 전체 데이터를 해시화하지 않고도 빠른 속도로 특정 데이터의 위변조 여부를 확인할 수 있다.

**[표 1] 상황별 위변조 상태표**

****

**4. 결론 및 향후 연구**

본 논문은 PX4 오토 파일럿의 데이터 위변조 검증을 위해 PX4의 로그 데이터를 블록화 하고, 이전 블록의 해시값을 저장하여 체인구조를 형성함으로써 신뢰성을 향상시킬 수 있는 방안을 고안하였으며 이를 라이브러리 형태로 개발하였다. 라이브러리를 사용하여 외부 파일에 데이터의 해시값 및 merkle tree, 블록에 대한 정보를 저장하며 위변조 여부를 검증한다. 또한 각 블럭을 체인 구조로 연결하여 인근 데이터의 무결성을 검증할 수 있다. 이는 UAV에 잘못된 데이터가 사용되는 것을 방지하여 데이터의 신뢰성을 높일 수 있게 한다. 향후 PX4 Autopilot 리소스를 활용할 때 위변조 탐색을 시간과 메모리 공간의 측면에서 보다 효율적으로 수행할 방안을 찾고, 데이터의 무결성 검증을 포함한 PX4 오토파일럿 포렌식 도구를 제시할 계획이다.

**5. 참고문헌**

[1] Lukas Schroth, Hendrik Bödecker. DRONE MARKET SIZE 2021-2026(pp.26-33). Drone Market Report 2021-2026:Drone Industry Insights. 2021

[2] David Benowitz, The Rise of Open-Source Drones, Drone Analyst, Drone rone Analyst. 2021. <https://droneanalyst.com/2021/05/30/rise-of-open-source-drones>

[3] PX4 autopilot. software overview. <https://px4.io/software/software-overview/>

[4] PX4 autopilot. 로깅. <https://docs.px4.io/v1.12/ko/dev_log/logging.html>

[[](https://docs.px4.io/v1.12/ko/dev_log/logging.html[)5] PX4 autopilot. ULog 파일 형식. <https://docs.px4.io/master/ko/dev_log/ulog_file_format.html>

[6] 한국정보통신기술협회 정보통신용어사전. 머클 트리, -, merkle tree. <http://terms.tta.or.kr/dictionary/dictionaryView.do?word_seq=171397-1>

[7] PX4 autopilot. Pixhawk 4 Mini. https://docs.px4.io/v1.12/en/flight\_controller/pixhawk4\_mini.html