위치정보를 활용한 전력 IoT 단말장치의 인증서 유효성 검증 방안 연구

김민용, 장승진, 김수현, 이준영*

한전KDN(주) 전력ICT기술원 전력보안기술부

{kmyong_0902, sara_0309, suhyeon2_12, ljy.953386}@kdn.com

A Study on a Certificate Validation Method for Electric Power IoT Devices Using Location Information

MinYong Kim, SeongJin Chang, SuHyeon Kim, JunYoung Lee*

Power ICT Technology Institute, Power Security Technology Department, KEPCO-KDN

요 약

본 연구는 전력 IoT 단말장치의 물리적 위치 변경 및 인증서 복제 공격에 대응하기 위한 새로운 인증서 검증 기술을 제안한다. 기존의 PKI 기반 X.509 인증 체계는 주체 식별정보만을 검증하며, 단말장치의 실제 물리적 위치를 확인하지 못한다는 한계를 가진다. 본 연구에서는 단말장치에 내장된 GPS 모듈을 통해 획득한 위치정보(위도, 경도, 고도 정보)를 해시 알고리즘으로 처리하여 고유한 위치 해시값을 생성하고, 이를 인증서 확장필드에 포함시켜 위치 기반 인증 검증 기술을 도출한다. 또한, 단말장치의 임의 이동이나 인증서 복제 공격을 실시간으로 탐지하여 TLS 통신을 자동 차단함으로써 전력 IoT 인프라의 물리적·논리적 보안성을 동시에 강화한 모델을 설계 및 제시하고자 한다.

Ⅰ. 서론

전력 산업의 디지털 전환이 가속화되면서, 현장에 설치된 단말장치(RTU, PMU, 스마트 미터 등)는 데이터 수집 및 제어를 위해 지속적으로 네트워크에 연결되어 통신하고 있다. 이러한 단말장치는 보안성 강화를 위해 PKI(Public Key Infrastructure) 기반의 X.509 인증서를 활용하여 TLS(Transport Layer Security) 기반 보안 통신을 도입하는 추세로 변화하고 있다.

그러나 기존 X.509 인증서는 주체명, 공개키, 유효기간 등의 논리적 정보만을 포함할 뿐, 장치의 물리적 위치를 검증하지 않는다. 이로 인해 공격자가 인증서를 복제하여 다른 장치에 이식하거나, 장치 자체를 무단 이동시키더라도 TLS 세션이 정상적으로 수립되는 문제가 발생한다. 이러한 취약점은 고정형 전력설비의 특성상 물리적 위치 변경이 거의 없다는 점을 악용할 수 있는 심각한 위협이다. RADIUS·Diameter 등의 인증·인가 프로토콜을 통해 인가되지 않은 기기의 접속을 차단하거나 인증서의 중복 사용을 제한하려는 시도가 있으나, 이들 방식은 별도의 인증 장비 및 중앙 인프라의 도입을 전제로 하므로 인프라 의존성 증가와 관리 부담을 초래한다.[1] 또한 물리적 위치 검증을 본질적으로 제공하지 못하므로 인증서 자체만으로 취약점을 해결하기에는 한계가 있다.

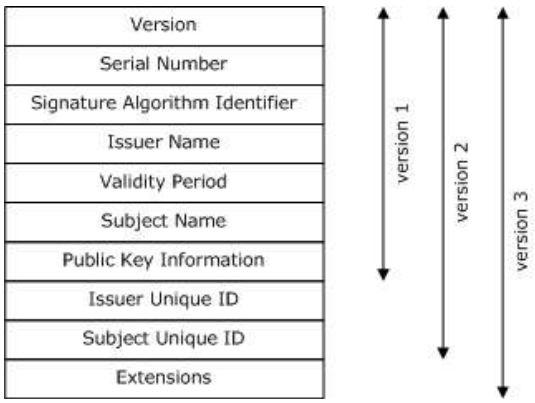
따라서 본 연구에서는 GPS 정보를 이용하여 단말장치의 실제 위치정보를 기반으로 인증서의 유효성을 검증하는 새로운 방식의 보안 기술 모델을 설계 및 제시하고자 한다.

Ⅱ. 본론

2.1 X.509 공개키 인증서 구조

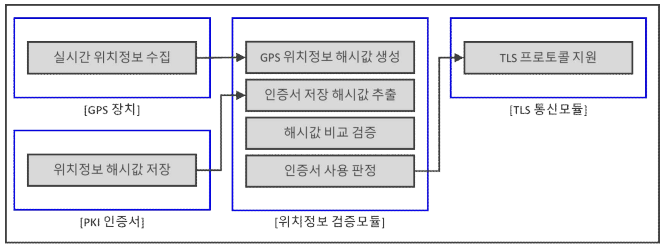
전력 IoT 단말장치에서 사용되는 인증서는 X.509 표준 형식 구조를 기반으로 한다. X.509 인증서는 주체명(Subject Name), 발행자명(Issuer Name), 공개키(Public Key), 유효기간(Validity), 서명(Signature) 등의 필드를 포함하며, 인증서 검증은 인증기관(CA, Certification Authority)에서 인증서의 유효기간 및 서명 검증, 인증 경로 확인, 인증서 폐기 목록(CRL) 또는 OCSP 상태 검증 절차로 이루어진다.

그러나 기존 구조는 장치의 물리적 위치와 인증서의 중복 사용 여부를 검증하지 못하므로, 동일한 인증서가 다른 장소나 설비에서 사용되더라도 인증서만으로 완전한 검증이 제한된다. 본 연구에서는 이러한 취약점을 해결하기 위해 X.509 인증서의 확장 필드(Extensions)에 위치정보 해시를 추가하여, 인증서 유효성을 검증하는 보안 모델을 제시한다.



[그림 1] X.509 표준 형식 구조

2.2 전력 IoT 단말장치의 위치정보 기반 인증서 유효성 검증 모델



[그림 2] 위치정보 기반 인증서 유효성 검증 모델

본 연구에서 제시하는 위치정보 기반 인증서 유효성 검증 모델은 전력 IoT 단말장치 내부에서 동작하는 GPS 장치, 위치정보 검증모듈, PKI 인증서, TLS 통신모듈의 네 가지 주요 구성요소로 이루어진다. 이 아키텍처는 GPS 장치를 통해 단말의 물리적 위치를 측정하고, 위치정보 검증모듈에서 이를 해시화하여 인증서 검증 과정에 반영함으로써, 단말장치의 실제 위치와 논리적 인증 정보를 함께 검증할 수 있도록 설계되었다.

GPS 장치는 단말장치의 물리적 위치를 실시간으로 측정하기 위한 핵심 구성요소로, 위도(latitude), 경도(longitude), 고도(altitude) 정보를 수집한다. 수집된 좌표값은 국제표준 좌표계인 WGS84(World Geodetic System)에 기반하며, 소수점 단위의 정밀한 수치 형태로 표현된다.

위치정보 검증모듈은 GPS 장치에서 수집된 좌표 데이터를 결합한 후, SHA 해시 알고리즘을 적용하여 고정 길이의 위치정보 해시값을 생성한다. 생성된 해시값은 인증서 확장필드에 포함된 해시값과 비교되어 단말장치의 위치 변경 여부를 판별한다. 이때 인증서에 포함된 해시값은 단말의 위도, 경도, 고도 정보를 기반으로 사전에 생성된 값이다.

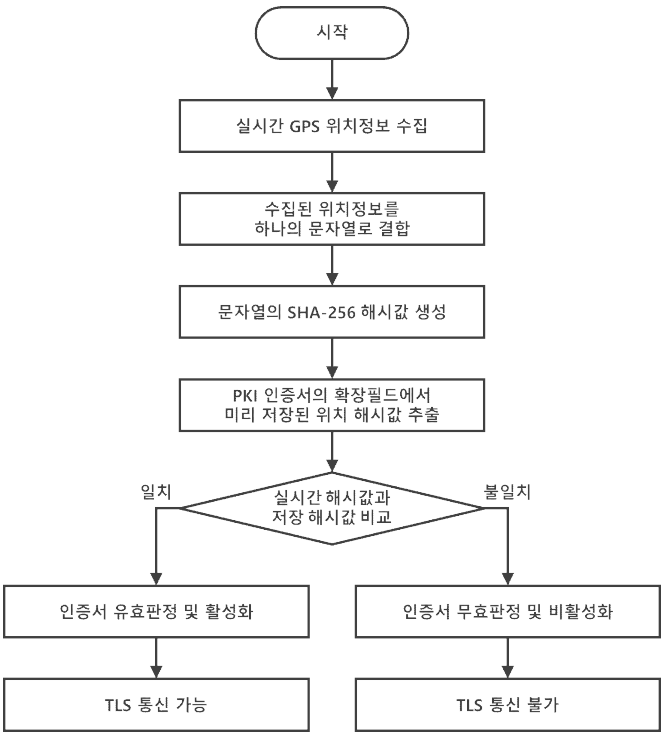
PKI 인증서는 X.509 표준 형식을 사용하며, 확장필드에 단말장치 설치 시점의 위치정보 해시값을 포함한다. 이 확장필드는 CA에 의해 서명되어 무결성이 보장되며, 외부에서 임의로 변경할 수 없다.

넷째, TLS 통신모듈은 검증모듈의 결과에 따라 TLS 세션의 수립 여부를 제어한다. 해시값 비교 결과가 일치하는 경우 인증서를 유효 상태로 설정하고 세션 수립을 허용하며, 불일치하는 경우 인증서를 무효 상태로 전환하여 TLS 핸드셰이크 과정을 중단한다.

이와 같은 구조는 기존 PKI·TLS 체계와 호환성을 유지하기 용이하며, 하드웨어 수준의 GPS 모듈과 소프트웨어 기반 인증 절차가 결합되어, 물리적 보안과 네트워크 보안이 통합된 보호 구조를 구현할 수 있다

2.3. 인증서 유효성 검증 및 TLS 통신 사용 여부 판정 절차

위치정보 해시는 단말장치 설치 시점의 위치정보를 표준화된 형식으로 변환 및 생성되며, 인증서 발급 시 확장필드에 삽입된다. 이후 인증서 검증 시점에 위치정보 해시를 활용하여 TLS 통신의 유효성을 판정한다.



[그림 3] 위치정보 기반 TLS 통신 사용 여부 판정 절차

첫째, 좌표 데이터 결합 단계에서는 GPS 모듈로부터 수집된 위도, 경도, 고도 값을 쉼표(,)로 구분한 문자열 형태로 결합한다. 예를 들어, 수집된 위치정보가 위도 37.5665, 경도 126.9780, 고도 32.4m인 경우, 결합 문자열은 37.5665,126.9780,32.4로 표현된다.

둘째, 해시 변환 단계에서는 결합된 문자열에 대해 SHA-256 해시 알고리즘을 적용하여 256비트 길이의 고정된 해시값을 생성한다. 이 해시값은 단말장치의 고유 물리적 위치를 표현하는 비가역적 데이터로서, 동일한 장소에서만 동일한 해시 결과가 생성된다.

셋째, 인증서 확장필드 삽입 단계에서는 생성된 해시값을 X.509 인증서의 확장필드에 포함한다. 확장필드는 ASN.1 문법에 따라 정의되며, 해시 알고리즘 식별자와 해시값을 함께 표현하는 SEQUENCE 구조(Location HashSyntax)로 구성된다. 정의된 ASN.1 구조는 DER(Distinguished Encoding Rules) 형식으로 인코딩되어 인증서 본문에 삽입되며, 이때 확장 OID는 자체 정의한 고유 식별자를 사용한다. 이후 CA는 해당 인증서에 전자서명을 적용하여 확장필드를 포함한 전체 인증서의 무결성과 진위성을 보장한다.

```
LocationHashSyntax ::= SEQUENCE {
    hashAlg     OBJECT IDENTIFIER,          -- 예: SHA-256 OID
    hashValue   OCTET STRING (SIZE(32))     -- SHA-256 결과 32바이트
}
```

```
LocationHashSyntax ::= SEQUENCE {
    hashAlg     OBJECT IDENTIFIER : 2.16.840.1.101.3.4.2.1,
    hashValue   OCTET STRING :
        5A54628007820470737C68F35124E789A8B39E1692A4FB779EF74DD7BF258A48
}
```

[표 1] 위치정보 해시 확장필드의 ASN.1 구조 정의 및 데이터 예시

마지막으로, 인증서 배포 및 제안 아키텍처 적용 단계에서는 CA가 발급한 인증서를 단말장치에 적용하고, 단말장치는 TLS 통신 과정에서 GPS 장치에서 수집된 실시간 위치정보로 해시값을 생성하여 인증서에 저장된 위치정보 해시와 비교한다. 두 값이 일치하면 해당 인증서가 지정된 물리적 위치에 설치된 것으로 판단되어 통신이 허용되고, 불일치 시 TLS Handshake 과정에서 세션 수립이 거부된다.

이 절차는 위치정보를 인증 요소로 활용함으로써, 기존의 논리적 인증 구조에 물리적 신뢰요소를 결합한 새로운 보안 메커니즘을 제공한다. 또한 인증서의 확장필드를 활용하기 때문에, X.509 표준과의 완전한 호환성을 유지하면서 별도의 포맷 변경없이 구현이 가능하다.

Ⅲ. 결론

본 연구에서는 전력 IoT 단말장치의 물리적 위치정보를 활용하여 인증서의 유효성을 검증하는 기술을 제안하였다. GPS 모듈로부터 획득한 위도·경도·고도 정보를 해시 처리하여 X.509 인증서의 확장필드에 포함함으로써, 단말장치의 위치 변경과 인증서 복제 공격을 실시간으로 탐지할 수 있는 기술을 도출하였다.

향후 연구에서는 ASN.1 기반 구조 정의를 통해 위치정보 해시를 X.509 인증서의 확장필드에 삽입(포함)하기 위한 구문 구조를 설계하고, DER 인코딩을 적용하여 인증서의 발급 및 검증 절차를 구현하고자 한다. 이를 통해 위치정보 기반 인증서 검증 기술의 실질적 구현 가능성과 표준 호환성을 검증할 계획이다.

참 고 문 헌

[1] 최재덕, 서정택, “스마트그리드 보호를 위한 AMI 망 분리 및 인증 프레임워크”, 한국정보보호학회, 2012.6