https://doi.org/10.33778/kcsa.2024.24.1.011

무선 환경에서 데이터의 신뢰성을 보장하는 효율적인 BACnet/SC 개선 방안 연구★

김 서 연*, 임 성 식**, 김 동 우**, 한 수 진***, 이 기 찬***, 오 수 현****

요 약

최근 ICT 기술을 활용하여 에너지를 효율적으로 관리하고, 실시간으로 다수의 IoT 센서의 데이터를 수집하여 빌딩 자동화 시스템을 통해 운영 및 제어가 가능한 스마트빌딩이 주목받고 있다. 그러나 센서 데이터 관리가 개방형 환경을 통해 이루어짐에 따라 기존 빌딩 자동화 프로토콜의 보안 취약점으로 인해 스마트빌딩의 안전성이 위협받고 있다. 따라서 본 논문에서는 범용적으로 사용되는 BACnet의 주요 데이터 링크 기술을 분석하고, 무선 환경에서 데이터의 신뢰성을 보장할 수 있는 OWE 기반의 효율적인 BACnet/SC를 제안한다. 제안하는 프로토콜은 OWE를 적용하여 개방형 네트워크에서도 안전한 통신이 가능하게 하며 TLS 환경에서의 BACnet/SC와 동일한 수준의 보안성을 제공한다. 결과적으로 2회의 연결 과정 감소 및 평균 소요 시간이 40% 단축되어 기존에 비해 효율적인 통신이 가능하다.

A Study on Efficient BACnet/SC to ensure Data Reliability in Wireless Environments

Seo-yeon Kim*, Sung-sik Im**, Dong-woo Kim**,
Su-jin Han***, Ki-chan Lee***, Soo-hyun Oh****

ABSTRACT

Recently, smart buildings that can efficiently manage energy using ICT technology and operate and control through the building automation system by collecting data from a large number of IoT sensors in real time are attracting attention. However, as data management is carried out through an open environment, the safety of smart buildings is threatened by the security vulnerability of the existing building automation protocol. Therefore, in this paper, we analyze the major data link technology of BACnet, which is used universally, and propose OWE-based efficient BACnet/SC that can ensure the reliability of data in a wireless environment. The proposed protocol enables safe communication even in an open network by applying OWE and provides the same level of security as BACnet/SC in a TLS environment. As a result, it reduces the connection process twice and reduces the average time required by 40%, enabling more efficient communication than before.

Key words : Smart Building, IoT, BACnet/SC, OWE

접수일(2023년 12월 21일), 게재확정일(2024년 01월 30일)

★ 본 과제(결과물)는 교육부와 한국연구재단의 재원으로 지원을 받아 수행된 3단계 산학연협력 선도대학 육성사업(LINC 3.0)의 연구결과입니다.

* 호서대학교 정보보호학과 석사과정(주저자)
** 호서대학교 정보보호학과 석사과정(공동저자)
*** 호서대학교 컴퓨터공학부 학부생(공동저자)
**** 호서대학교 컴퓨터공학부 교수(교신저자)

1. 서 론

최근 건물과 시설이 지능화됨에 따라 전력, 공조(HVAC, Heating, Ventilation, Air-Condition), 조명 등의 다양한 분야에서 ICT 기술을 활용하여 에너지를 효율적으로 관리하는 스마트빌딩이 확대되고 있다.

스마트빌딩은 빌딩 자동화 시스템을 통해 실시간으로 다수의 IoT 센서 데이터를 수집 및 분석하여 이를 통해 자동화된 운영과 제어가 가능한 빌딩을 말하며, 빌딩 에너지 관리 시스템 등과 결합하여 다양한 서비스를 제공한다. 이러한 시스템은 빌딩 자동화 프로토콜을 통해 실시간으로 센서 데이터를 수집한다. 그러나 수집된 데이터의 관리가 점차 유선 매체가 아닌 무선 매체를 통한 클라우드와 같은 개방형 환경으로 변화하면서, 센서 데이터 관리의 중요성이 증가하고 있다. 이와 동시에 충분히 고려되지 않았던 빌딩 자동화 프로토콜의 보안 취약점으로 인한 스마트빌딩의 보안 위협 또한 증가하였다.

이에 따라 데이터 수집 과정에서의 신뢰성이 보장되지 않을 경우, 유효하지 않은 데이터로 인한 비정상적인 시스템 작동과 더불어 전체적인 빌딩의 안전성에 직접적인 위협을 가할 수 있다. 범용적으로 사용되는 BACnet은 초기에 보안 기능이 내장되어 있지 않아 이를 추가로 정의하였으나, 외부 연결을 고려하지 않았던 기존 빌딩 시스템의 설계로 인해 해당 기능에 대한 구현이 보편화되지 않았다. 이후 BACnet/SC가 새로 정의되었지만 다소 많은 연결 과정과 자원이 한정적인 IoT 기기에 TLS 기반의 적지 않은 부담을 필요로 하고 있어 간소화가 필요하다. 따라서 본 논문에서는 무선 환경에서 수집되는 데이터의 신뢰성을 보장하도록 OWE를 적용한 효율적인 BACnet/SC를 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 OWE와 AEAD 및 TLS 1.3에 대해 정리한다. 3장에서는 BACnet의 개념 및 주요 데이터 링크 기술을 분석하고, 4장에서는 무선 환경에서 OWE를 적용한 BACnet/SC를 제안한다. 5장에서는 제안하는 프로토콜의 안전성을 분석하고 기존 BACnet/SC와 비교하여 성능을 분석한다. 마지막으로, 6장에서 결론을 맺는다.

2. 관련연구

2.1 OWE

Wi-Fi Alliance의 OWE(Opportunistic Wireless Encryption)는 Enhanced Open으로도 알려져 있으며, WPA2-Open의 보안 취약점을 개선하여 개방형 무선 네트워크에서도 안전한 통신이 가능한 프로토콜이다. 단말과 AP는 OWE 연결을 위해 802.11 Association 단계에서 서로의 임시 ECC 공개키를 전송한 뒤, 4-way Handshake 및 암호화 통신을 수행한다.

OWE의 장점은 별도의 인증이나 패스워드 없이도 상호 간 키를 나누어가질 수 있어 간편하고, ECDHE(Elliptic Curve Diffie-Hellman Ephemeral) 키 교환 방식을 통해 전방향 안전성을 제공한다는 점이다.

2.2 AEAD

AE(Authenticated Encryption)는 암호화와 MAC 연산을 통해 데이터의 기밀성과 무결성 및 인증을 동시에 제공하는 방식으로, AEAD(Authenticated Encrypted with Associated Data)는 AE 방식의 MAC 연산에 AAD(Additional Associated Data)를 추가하여 신뢰성을 강화한 방식이다. AAD는 수신 측에서 동일한 AAD를 생성하는 경우에만 검증할 수 있으므로 기밀성을 요구하지 않는 데이터를 포함하여 인증을 제공한다. 즉 평문의 경우 암호화와 MAC 연산을 모두 수행하지만, AAD에 대해서는 암호화를 수행하지 않는다.

RFC 5116에 정의된 AEAD 알고리즘은 AES 기반의 GCM 및 CBC 방식이 있으며, 암호화와 MAC 연산 순서에 따라 <표 1>과 같이 구분한다.

<표 1> 수행 순서에 따른 AEAD 방식

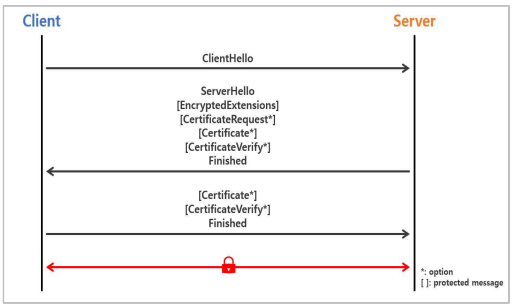
방식	설명
MAC-then-Encrypt	평문에 대해 MAC 연산 수행 후 평문과 MAC에 대한 암호화 수행
Encrypt-and-MAC	평문에 대해 암호화와 MAC 연산을 별도로 수행
Encrypt-then-MAC	평문에 대해 암호화 수행 후 암호문에 대한 MAC 수행

AEAD 암호화는 TLS 1.3에서 해당 방식을 기본 암호 알고리즘으로 사용하며 주목받게 되었다. 기존의 TLS는 MAC-then-Encrypt 방식을 사용하여 MAC 연산 이후 암호화를 수행하였으나, 이 경우 복호화가 먼저 수행되어도 MAC 연산이 수행되기 전에는 데이터를 완전히 신뢰할 수 없다는 한계가 존재한다. 이에 따라 TLS 1.3에서는 Encrypt-then-MAC 방식을 사용하여 암호화 수행 후 MAC 연산을 수행함으로써 이전 방식에 비해 효율적이고 높은 보안성을 제공할 수 있다.

2.3 TLS 1.3

TLS(Transport Layer Security)는 안전하지 않은 채널을 통해 통신하는 클라이언트와 서버 간의 신뢰성 있는 연결을 설정할 수 있도록 하는 전송 계층 프로토콜이다. 기존 TLS 1.2는 취약한 블록 암호 모드 사용 등의 보안 문제가 있었으나, TLS 1.3은 Hello 메시지 이후의 모든 Handshake 및 Application 메시지를 해당 세션의 키로 암호화하여 전송한다. 또한 DHE 기반의 키 교환으로 모든 경우에 대한 전방향 안전성을 제공하며, 인증을 위해 AAD를 MAC 연산에 포함하여 보안성을 강화한 AEAD Cipher를 기본 암호 알고리즘으로 사용하여 기존의 Cipher Suite를 간소화하였다.

초기 연결 시 클라이언트와 서버는 (그림 1)과 같이 1-RTT Handshake 과정을 수행하여 안전한 채널에서 통신을 수행할 수 있다. 이후 세션 재개 시 클라이언트는 서버로부터 발급받은 NewSessionTicket을 통해 PSK(Pre Shared Key) 기반의 Handshake를 수행하고, 필요에 따라 0-RTT Handshake를 수행하여 연결 속도를 향상할 수 있다.

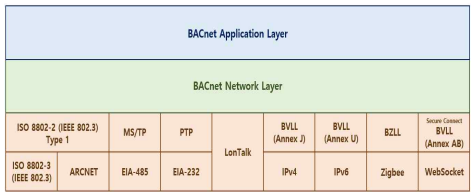


(그림 1) TLS 1.3의 1-RTT Handshake 과정

3. BACnet 프로토콜 분석

BACnet(Building Automation and Control network)은 기존의 빌딩 자동화 시스템 환경에서의 상호 운용성을 제공하기 위해 등장한 데이터 통신 프로토콜로 대표적인 빌딩 자동화 개방형 프로토콜이다.

BACnet은 기본적으로 모든 데이터를 객체(Object)와 해당 객체를 구성하는 속성(Property)으로 표현하여 서로 다른 데이터 링크 간 통신이 가능하다. 다수의 데이터 링크를 지원하는 BACnet의 범용적인 기술은 BACnet MS/TP와 BACnet/IP가 있으며, 본 논문에서는 BACnet/IP와 BACnet/SC를 중점적으로 분석한다.



(그림 2) BACnet 프로토콜의 스택 구조

3.1 BACnet/IP

BACnet/IP는 표준 Annex J에 정의된 BACnet의 네트워크 구성 중 하나로 IPv4를 사용한다. 일반적으로 BACnet 네트워크는 하나 이상의 IP 서브넷으로 구성되어 브로드캐스트 통신을 수행한다. 이를 위해 BACnet/IP가 아닌 장치와 통신하기 위해 BVLL (BACnet Virtual Link Layer)을 추가로 정의하였다.

BACnet은 다양한 데이터 링크의 지원이 가능함에 따라 공통적인 주소 체계가 존재하지 않아 BACnet 네트워크 계층의 경우, 장치의 IP 주소와 UDP 포트로 구성된 6바이트의 VMAC(Virtual MAC) 주소를 사용하여 네트워크의 유연성을 확장한다. 이러한 BACnet 네트워크 계층과 특정 하위 시스템 간의 연결은 BVLC(BACnet Virtual Link Control) 기능을 통해 이루어지며, BBMD(BACnet Broadcast Management Device) 및 BACnet 라우터를 통해 브로드캐스트 통신을 제어하고 다른 네트워크와 통신을 수행한다. BACnet 라우터 및 BBMD는 주로 빌딩 컨트롤러 또는 기타 제어 장치에 내장되어 하나의 장치로 사용된다.

BACnet은 별도의 연결 과정이 존재하지 않으므로 네트워크에 새로 참여하고자 하는 장치는 주기적으로 Who-Is/I-Am 메시지를 통한 Device Discovery 작업을 수행하고, 컨트롤러의 경우 I-Am-Router-To-Network 메시지를 전송하여 자신의 역할을 네트워크에 알린다. 해당 과정을 통해 네트워크 구성과 통신하고자 하는 장치의 주소를 파악하여 통신을 수행한다.

또한, BACnet/IP를 포함한 기존의 BACnet은 폐쇄적인 환경에서 외부 연결 없이 통신을 수행하였기에 별도의 보안 기능이 정의되어 있지 않았다. 이후 보안 메커니즘이 새로 추가되었지만, DES 기반의 취약한 암호 알고리즘 및 56비트의 짧은 키 길이 사용으로 인해 AES 암호 알고리즘을 사용하도록 개정되었다. 그러나 이후에도 해당 메커니즘에 대한 구현이 이루어지지 않아 BACnet/SC가 새롭게 등장하였다.

3.2 BACnet/SC

BACnet/SC(BACnet Secure Connect)는 TCP 환경에서 TLS 1.3 기반의 Secure WebSocket을 통해 안전한 통신을 수행하여 데이터의 기밀성, 무결성 및 인증 기능을 제공할 수 있도록 정의된 새로운 데이터 링크 프로토콜이다. 기존의 BACnet/IP와 BACnet/SC의 보안 기능은 <표 2>와 같이 비교된다.

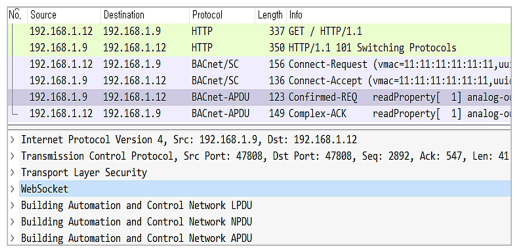
<표 2> BACnet/IP와 BACnet/SC 보안 기능

구분	BACnet/IP	BACnet/SC
전송 프로토콜	UDP	TCP
데이터 기밀성	미수행	TLS 1.3
데이터 무결성	미수행	TLS 1.3
기기 인증	미수행	TLS 1.3

BACnet/SC의 BVLL은 기존과 같이 VMAC 주소를 사용하고, BACnet 네트워크 계층과 WebSocket 기반의 하위 시스템 간 인터페이스를 제공한다. 일반적인 BACnet의 네트워크 구성과 달리 BACnet/SC는 Hub Function 및 BACnet/SC 노드로 구성된 Hub & Spoke 구조를 따르며, 동일한 Hub Function에 연결되는 두 개 이상의 BACnet/SC 노드의 집합이 있을 때 해당 네트워크를 BACnet/SC 네트워크라고 한다.

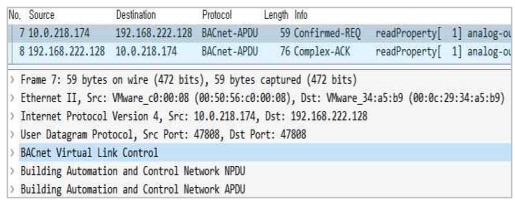
단일 네트워크의 중심에 위치하여 유니캐스트 메시지 및 브로드캐스트 메시지 배포를 담당하는 Hub Function은 BACnet/IP의 BBMD와 같은 기능을 수행한다. Hub Function은 BACnet/SC 노드의 연결 요청을 수락하여 장치를 네트워크에 참여시키고, 다른 Hub Function과 연결을 맺어 서로 다른 네트워크상의 장치가 원활히 통신할 수 있도록 돕는다. BACnet/SC 노드의 경우, 기본적으로 Hub Connection 기능을 내장하고 있으며 해당 기능을 통해 Hub Function과 연결 설정을 수행하여 BACnet/SC 네트워크 참여가 가능하다.

BACnet/SC 연결은 Secure WebSocket 기반의 연결을 통해 수행되며, BACnet/SC 노드의 요청에 대해 Hub Function이 수락하는 과정으로 간단히 이루어진다. Secure WebSocket은 단일 TCP 연결을 통해 양방향 트래픽 기능을 제공하는 WebSocket을 HTTPS(HTTP over TLS) 상에서 사용하는 방식으로, (그림 3)과 같이 BACnet/SC 노드와 Hub Function의 BACnet/SC 연결을 위해 사용한다.



(그림 3) BACnet/SC 연결 과정

연결 설정을 마친 장치와 컨트롤러는 수행하는 작업에 따라 필요한 데이터를 BACnet-APDU로 전송한다. TLS 기반의 Secure WebSocket으로 캡슐화되어 데이터의 신뢰성이 보장되는 BACnet/SC와 달리 기존의 BACnet/IP는 (그림 4)와 같이 별도의 암호화 없이 데이터를 평문으로 전송하므로 데이터의 신뢰성이 보장되지 않는다.



(그림 4) 기존 BACnet/IP의 데이터 전송

4. 무선 환경에서 데이터의 신뢰성을 보장하는 효율적인 BACnet/SC

본 논문에서는 무선 환경에서 장치와 컨트롤러 간 수집되는 데이터의 신뢰성을 보장할 수 있는 효율적인 BACnet/SC 프로토콜을 제안한다. 제안하는 프로토콜은 기존의 BACnet/SC에 비해 간소화된 연결 과정을 수행하면서도 동일한 수준의 보안을 제공한다.

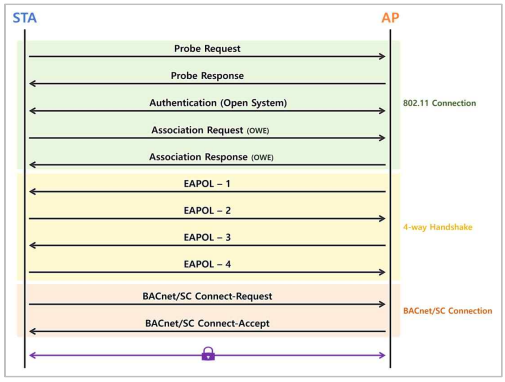
4.1 제안하는 프로토콜의 전체 연결 과정

제안하는 프로토콜은 <표 3>과 같은 보안 기능을 제공하며, 상대적으로 가볍고 빠른 통신을 위해 BACnet/SC와 달리 UDP를 전송 프로토콜로 사용한다. UDP 페이로드의 경우 AEAD 암호화를 수행하여 데이터의 기밀성과 무결성을 동시에 보장한다.

<표 3> 제안하는 프로토콜의 보안 기능

보안 기능	방식
기기 인증	화이트리스트 기반
키 교환	OWE 프로토콜 적용
암·복호화	AEAD 암호화

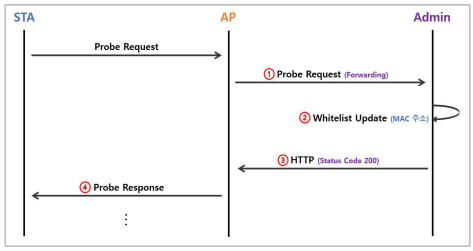
전체 연결 과정은 (그림 5)와 같으며, 초기 연결 시 관리자를 통해 인증된 단말과 AP는 무선 환경에서의 4-way Handshake 및 BACnet/SC 연결 이후 곧바로 암호화 통신이 가능하다. 802.11 연결의 경우, 무선 환경을 고려하여 빌딩 네트워크의 비인가적 접근을 제한하기 위해 Beacon 프레임의 사용을 제한한다.



(그림 5) 제안하는 프로토콜의 전체 연결 과정

4.2 제안하는 프로토콜의 기기 인증 과정

(그림 5)에 따라 802.11 연결로 시작되는 제안하는 프로토콜은 통신을 수행하는 단말에 대해 정당한 사용자임을 증명하기 위해 사전에 (그림 6)과 같은 기기 인증 절차가 필요하다. 이때, Beacon 프레임의 사용을 제한하므로 AP의 SSID를 제대로 알지 못하는 기기는 올바른 Probe Request를 전송할 수 없어 기기 인증 절차를 정상적으로 수행하지 못하므로 통신이 거부된다.



(그림 6) 제안하는 프로토콜의 기기 인증 과정

기기 인증 절차는 빌딩 자동화 시스템의 관리자가 상주하고 있다는 가정하에 다음과 같이 기기의 MAC 주소를 통해 화이트리스트 기반 방식으로 수행된다.

① 컨트롤러는 SSID를 알고 있는 장치로부터 올바른 Probe Request를 수신한 경우, 이를 관리자에게 포워딩한다. 이때 컨트롤러는 Probe Response를 전송하지 않은 상태로 대기해야 한다.

② 관리자는 패킷을 수신하여 정당한 기기라고 판단한 경우, 장치의 MAC 주소를 확인 및 저장하여 화이트리스트 목록에 추가한다.

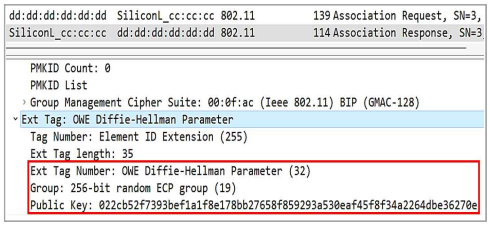
③ 이후 관리자는 컨트롤러에 HTTP 통신을 통해 Status Code 200을 전송하여 승낙을 알린다.

④ 컨트롤러는 Probe Response를 전송하여 장치와 802.11 연결을 이어서 진행한다.

4.3 제안하는 프로토콜의 키 설정 과정

관리자를 통해 정상적으로 기기 인증 절차를 수행한 장치는 네트워크에 참여하기 위해 컨트롤러와 802.11 연결 및 4-way Handshake 과정을 수행한다. 이때, 컨트롤러는 OWE 기반 키 설정을 위해 802.11 Probe Response 전송 시 RSN IE 내의 AKM 필드를 통해 OWE의 사용을 알려야 한다.

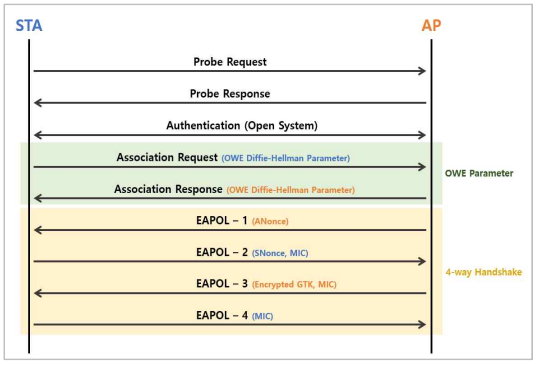
802.11 Probe Response를 전송한 후, 컨트롤러와 이를 수신한 장치는 ECDHE 키 교환을 수행하기 위해 해당 세션에서 사용할 임시 ECC 키 쌍을 생성하고, 802.11 Association 과정에서 OWE Diffie-Hellman Parameter 태그를 통해 (그림 7)과 같이 자신의 임시 ECC 공개키를 전송한다. 이후 수신한 상대의 공개키와 자신의 개인키에 대해 스칼라 연산을 수행하여 공유 비밀 값을 생성한다.



(그림 7) OWE Diffie-Hellman 파라미터

상호 간 같게 생성된 공유 비밀 값은 4-way Handshake 과정에서 세션 키 파생을 위해 사용되며, 해당 세션 키를 사용하여 암호화 작업을 수행함으로써 안전한 채널을 통해 데이터를 전송할 수 있다.

최종적으로 장치와 컨트롤러는 BACnet 통신을 수행하기 위해 각각 BACnet/SC 노드 및 Hub Function으로써 BACnet/SC 연결을 설정하고, (그림 8)과 같이 BACnet 기반의 안전한 통신을 수행한다. 본 논문에서 제안하는 프로토콜은 기존 BACnet/SC와 달리 TCP 환경에서 작동하지 않으므로 TLS 기반의 세션 설정 및 Secure WebSocket 연결은 수행하지 않는다.

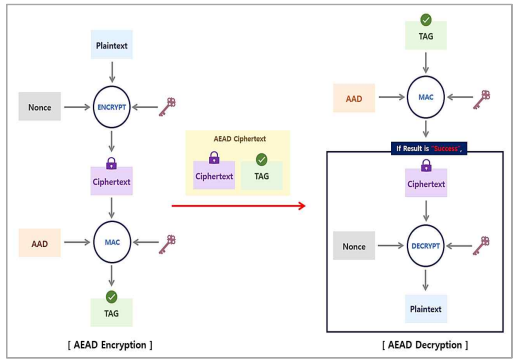


(그림 8) 제안하는 프로토콜의 키 설정 과정

4.4 제안하는 프로토콜의 데이터 송수신 과정

본 논문에서 제안하는 프로토콜은 UDP를 통해 전송되는 데이터에 대해 AEAD 암호화를 수행하며, 상대적으로 적은 연산량과 높은 효율성으로 인해 가장 많이 사용되는 AES-GCM을 AEAD 알고리즘으로 사용한다. 해당 방식의 알고리즘은 Encrypt-then-MAC 방식을 따르기 때문에 AEAD 방식 중 가장 높은 보안성을 제공할 수 있다.

제안하는 프로토콜의 데이터 송수신 시 수행하는 전체적인 AEAD 암복호화 과정은 (그림 9)와 같으며, 각 과정에서 사용되는 입출력 파라미터 및 관련 설명은 <표 4>와 같다.



(그림 9) 제안하는 프로토콜의 암복호화 과정

암호화 과정의 경우 평문과 암호화 키, Nonce를 입력으로 받아 AES 암호화를 수행하고, 출력된 암호문과 MAC 키 및 AAD를 사용하여 MAC 연산을 수행하여 AES 암호문과 인증 태그로 결합된 AEAD 암호문을 생성 및 전송한다.

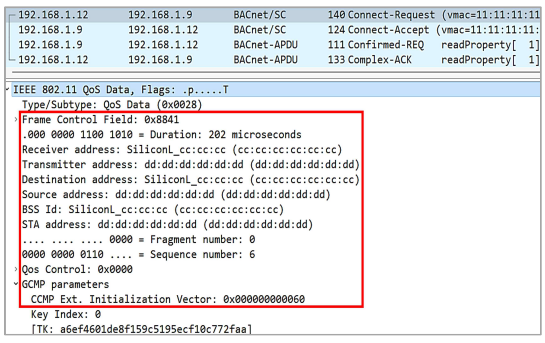
AEAD 암호문에 대한 복호화 과정은 생성한 AAD 및 MAC 키, AEAD 암호문의 AES 암호문을 입력으로 받아 MAC 연산을 수행한다. 이때, AAD를 동일하게 생성하고 데이터 변조가 발생하지 않은 경우에 한해 AES 복호화를 수행한다. AES 복호화는 AES 암호문과 암호화 키, Nonce를 사용하여 수행하며 최종적으로 평문을 반환한다. 본 논문에서는 RFC 5116에 정의된 AEAD_AES_GCM_128 알고리즘에 따라 Nonce의 길이는 12바이트, 키 길이는 16바이트를 사용한다.

<표 4> AEAD 암복호화 과정의 입출력 파라미터

파라미터	입출력 구분	설명
평문	암호화 입력, 복호화 출력	AES 암호화 입력값 또는 복호화 수행 시 얻어지는 평문
키	암복호화 입력	AES와 MAC 연산에 사용되는 키
Nonce	암복호화 입력	임의성을 위해 사용하는 Initial Vector
AAD	암복호화 입력	인증을 강화하기 위해 추가하는 연관 데이터
AES 암호문	암호화 출력, 복호화 입력	AES 암호화 출력값 또는 복호화 수행 시 필요한 입력값
인증 태그	암호화 출력, 복호화 입력	AES 암호문의 MAC

AEAD 암호화를 통해 전송되는 데이터는 <표 4>의 파라미터에 대해 다음과 같이 정의한다.

- 평문: 임의 길이의 전송하고자 하는 데이터로 UDP 페이로드에 해당한다.
- 키: 16바이트의 세션 키 TK를 사용한다.
- Nonce: 수신자의 6바이트 MAC 주소 및 (그림 10)의 GCMP 파라미터 내 6바이트 IV(Initial Vector) 값을 결합하여 총 12바이트의 값을 사용한다.
- AAD: 802.11 QoS Data 프레임 내 일부 정보들을 조합하여 (그림 10)과 같이 총 24바이트의 값을 사용한다. AAD는 2바이트의 Frame Control 필드와 12바이트의 송수신자 MAC 주소 필드, 6바이트의 BSSID 필드, 2바이트의 시퀀스 넘버 필드 및 2바이트의 QoS Control 필드 값을 결합하여 사용한다.



(그림 10) 802.11 QoS Data 프레임

5. 제안하는 프로토콜의 안전성 분석 및 성능 비교

본 논문에서는 제안하는 프로토콜에 대한 보안 요구사항을 정의하여 안전성을 분석하고, 제안하는 프로토콜과 기존의 BACnet/SC를 무선 환경에서 구현하여 성능을 비교한다.

5.1 제안하는 프로토콜의 안전성 분석

제안하는 프로토콜 및 기존 BACnet/SC의 보안 요구사항은 <표 5>와 같이 정의한다. 보안 영역은 식별 및 인증, 데이터 보호, 암호 관리의 항목으로 분류하였으며, 각 보안 영역에 대한 보안 요구사항과 기존 BACnet/SC 및 제안하는 프로토콜이 해당 요구사항을 만족시키는 방식을 정의한다.

대다수의 보안 요구사항을 TLS 1.3을 통해 충족시키는 기존 BACnet/SC와 달리, 제안하는 프로토콜은 화이트리스트 기반의 인증을 통하여 기기 인증 여부 및 통제를 수행할 수 있다. 제안하는 프로토콜은 기본적으로 UDP 환경에서 통신하도록 설계하였으며, 4-way Handshake 과정을 통해 파생한 공유 비밀키 기반의 암호화를 수행하여 안전하게 데이터를 보호할 수 있다. 전송되는 데이터의 경우, 기존 BACnet/SC와 동일한 수준의 보안을 제공하기 위해 AEAD 암호화를 수행한다. AEAD 알고리즘은 AES-GCM 기반의 안전한 암호 알고리즘을 통해 데이터의 기밀성 및 무결성을 보장함으로써 높은 수준의 보안성을 제공할 수 있다. 또한 데이터 송수신 과정에서 사용되는 암복호화 키의 경우, ECDHE 방식의 안전한 키 설정 과정을 수행하여 전방향 안전성을 제공한다.

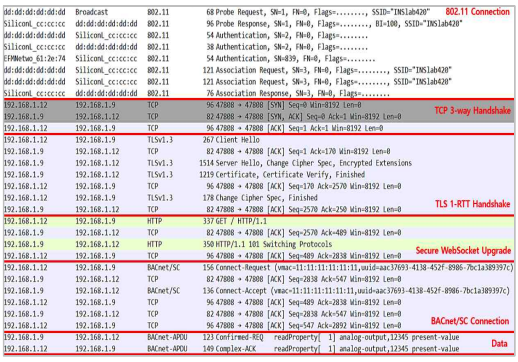
5.2 제안하는 프로토콜의 성능 비교

본 논문에서는 무선 환경에서 데이터의 신뢰성을 보장할 수 있는 프로토콜을 제안한다. 기존 BACnet/SC는 제안하는 프로토콜과 성능 비교를 수행하기 위해 802.11 환경에서 구현한다. 제안하는 프로토콜은 기존 BACnet/SC와 같게 보안 요구사항을 만족하며, 데이터 송수신까지 존재하는 5회의 연결 설정 횟수를 3회로 간소화하여 통신을 수행할 수 있다.

<표 5> 제안하는 프로토콜의 보안 요구사항 분석

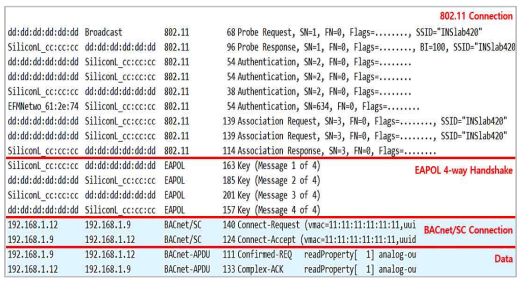
보안 영역	보안 요구사항	BACnet/SC	제안하는 프로토콜
식별 및 인증	AP의 기기 인증 수행 및 통제	TLS 1.3 기반 인증서	화이트리스트 기반 인증
데이터 보호	설치된 AP와 기기 간 안전한 데이터 전송	TLS 1.3 기반 TCP 계층 암호화	공유 비밀키를 통한 UDP 계층 암호화
	전송 데이터의 암호화를 통한 기밀성 및 무결성 보장	AEAD 암호화	AEAD 암호화
	안전한 암호 알고리즘 사용	AES-GCM	AES-GCM
암호 관리	안전성이 검증된 방식을 통한 기기별 고유 암호키 생성 및 관리	ECDHE	ECDHE

비교되는 두 프로토콜은 무선 환경에서 802.11 연결을 수행하여 작동을 시작한다. 기존 BACnet/SC의 경우, (그림 11)과 같이 다소 많은 연결 절차를 거쳐야만 데이터 송수신 과정을 수행할 수 있다. 802.11 연결 수행 이후에는 TCP 환경에서의 통신을 위해 3-way Handshake를 수행하며, 장치와 컨트롤러는 데이터 송수신 시 ACK 메시지에 기반하여 신뢰성 있는 통신을 수행할 수 있다. 기존 BACnet/SC는 TLS 1.3의 사용을 요구하므로 1-RTT Handshake를 수행하여 안전한 보안 채널을 통해 통신을 수행하며, 데이터의 신뢰성을 보장하기 위해 TLS 세션 설정 이후의 모든 데이터에 AEAD 암호화를 수행하여 전송 데이터를 안전하게 보호한다. 또한 HTTP 기반의 WebSocket 통신을 HTTPS를 통해 Secure WebSocket으로 업그레이드한 뒤, BACnet 통신을 위해 BACnet/SC 연결을 설정하여 모든 연결 과정을 마무리한다. 이후 장치와 컨트롤러는 ReadProperty 서비스를 통해 실시간으로 장치의 센서 데이터를 수집하며, 제안하는 프로토콜 또한 동일한 방식으로 데이터를 수집한다.



(그림 11) 기존 BACnet/SC의 전체 연결 과정

본 논문에서 제안하는 프로토콜은 사전에 관리자를 통한 기기의 인증 절차를 수행한 뒤, (그림 12)와 같이 802.11 연결을 시작으로 작동한다. 장치와 컨트롤러는 802.11 Association 과정에서 OWE 파라미터를 사용하여 서로의 임시 ECC 공개키를 주고받아 키 교환을 수행한다. 스칼라 연산을 통해 생성된 공유 비밀 값은 4-way Handshake 수행 시 해당 세션의 공유 비밀키 생성에 사용되며, 제안하는 프로토콜은 TCP 상에서 3-way Handshake를 수행하는 기존과 달리 UDP 상에서 곧바로 BACnet/SC 연결을 설정하여 전체 연결 설정을 마무리한다. 연결 설정 이후에 전송되는 데이터는 신뢰성 보장을 위해 AEAD 방식의 암호화를 수행하여 안전한 데이터 통신이 가능하게 한다.



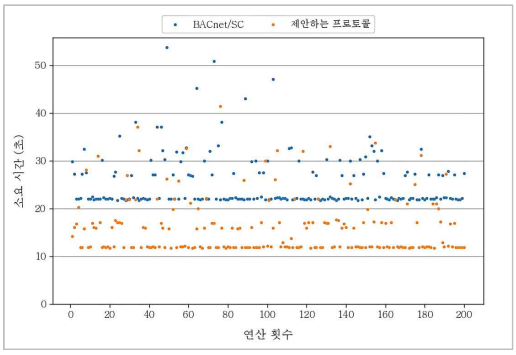
(그림 12) 제안하는 프로토콜의 전체 연결 과정

기존 BACnet/SC는 <표 6>과 같이 802.11 연결을 시작으로 데이터 송수신까지 총 5회의 연결 설정을 거쳐 BACnet-APDU를 통한 통신을 수행한다. 제안하는 프로토콜 또한 802.11 환경에서 연결 설정을 수행하지만, 키 설정을 위해 4-way Handshake 과정을 추가로 수행하였음에도 연결 과정이 2회 감소하여 총 3회의 간소화된 연결 설정을 거쳐 통신한다.

<표 6> 제안하는 프로토콜의 연결 설정 과정 비교

연결 설정 과정	BACnet/SC	제안하는 프로토콜
802.11 연결	○	○
EAPOL Handshake	-	○
TCP Handshake	○	-
TLS Handshake	○	-
WebSocket 연결	○	-
BACnet/SC 연결	○	○

또한, 구현한 기존 BACnet/SC와 제안하는 프로토콜의 성능 비교를 위해 802.11 Probe 과정을 시작으로 데이터 송수신까지의 과정을 200회 반복 수행한 소요 시간은 (그림 13)의 분포 그래프에 나타내었다. 해당 그래프에서 좌측은 전체 과정에 대한 소요 시간(초)으로 구분하고 하단은 연산 횟수로 구분한다. 기존의 BACnet/SC의 경우, 평균적으로 약 25초의 시간이 소요되었으나 제안하는 프로토콜은 평균적으로 약 15초의 시간이 소요되어, 최종적으로 약 10초의 평균 소요 시간 차이가 존재하여 40%의 성능 차이가 존재함을 확인하였다.



(그림 13) 제안하는 프로토콜의 소요 시간 비교

6. 결 론

실시간으로 다수의 IoT 센서 데이터를 수집하여 빌딩의 자동화된 운영을 수행하는 스마트빌딩은 수집되는 데이터의 신뢰성이 보장되지 않을 경우, 전체적인 빌딩의 안전성이 저하되는 문제가 발생한다. 대표적인 빌딩 자동화 프로토콜인 BACnet은 상호 운용성을 위해 다수의 데이터 링크 기술을 지원하지만, 보안 메커니즘에 대한 구현 부재의 한계가 존재한다. 이에 따라 BACnet/SC가 새로 정의되었으나 복잡한 연결 과정과 함께 성능이 제한된 IoT 기기의 경우 적지 않은 부담이 존재한다. 따라서 본 논문에서는 무선 환경에서 데이터의 신뢰성을 보장할 수 있는 OWE를 적용한 BACnet/SC 프로토콜을 제안하였다. 제안하는 프로토콜은 기존의 BACnet/SC와 동일하게 보안 요구사항을 만족하며, 성능상 2회의 연결 과정 감소와 40%의 소요 시간 단축이 가능하다. 이를 통해 무선 환경에서 안전하고 효율적인 통신을 수행함으로써 스마트빌딩의 보안성을 강화할 수 있을 것으로 기대한다.

참고문헌

[1] “Standard 135-2020 - BACnet – A Data Communication Protocol for Building Automation and Control Networks”, ASHRAE, 2020.

[2] D. Harkins, Ed., “Opportunistic Wireless Encryption,” RFC 8110, Internet Engineering Task Force (IETF), 2017.

[3] D. McGrew, “An Interface and Algorithms for Authenticated Encryption,” RFC 5116, Network Working Group, 2008.

[4] E. Rescorla, “The Transport Layer Security (TLS) Protocol Version 1.3,” RFC 8446, Internet Engineering Task Force(IETF), 2018.

[5] I. Fette, “The WebSocket Protocol,” RFC 6455, Internet Engineering Task Force(IETF), 2011.

[6] “IEEE Standard for Information technology -Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications”, IEEE SA, 2020.

[7] “스마트시티 보안모델 PART 2: 스마트 안전 서비스”, 한국인터넷진흥원, 2021.

〔저자소개〕

김 서 연 (Seo-yeon Kim)
2023년 2월 호서대학교 컴퓨터공학부 학사
2023년 3월 ~ 현재 호서대학교 정보보호학과 석사과정
email : komtti@naver.com

임 성 식 (Sung-sik Im)
2023년 2월 호서대학교 컴퓨터공학부 학사
2023년 3월 ~ 현재 호서대학교 정보보호학과 석사과정
email : sungsik9797@gmail.com

김 동 우 (Dong-woo Kim)
2023년 2월 호서대학교 컴퓨터공학부 학사
2023년 3월 ~ 현재 호서대학교 정보보호학과 석사과정
email : penetrick0@gmail.com

한 수 진 (Su-jin Han)
2021년 3월 ~ 현재 호서대학교 컴퓨터공학부 학부과정
email : tnwls5875@naver.com

이 기 찬 (Ki-chan Lee)
2019년 3월 ~ 현재 호서대학교 컴퓨터공학부 학부과정
email : ohkatan2@gmail.com

오 수 현 (Soo-hyun Oh)
1998년 2월 성균관대학교 정보공학과 학사
2000년 2월 성균관대학교 전기전자 및 컴퓨터공학과 석사(공학석사)
2003년 8월 성균관대학교 전기전자 및 컴퓨터공학과 박사(공학박사)
2004년 3월~현재 호서대학교 컴퓨터공학부 교수
email : shoh@hoseo.edu