Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.29, NO.5, Oct. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.5.1063

ISA 100.11a 및 WirelessHART 기반 보안위협 식별 및 보안요구사항 도출 연구

정 재 한,[1†] 권 성 문,[1] 손 태 식[1,2‡]
[1]아주대학교 컴퓨터공학과, [2]아주대학교 사이버보안학과

Security Threats Analysis and Security Requirement for Industrial Wireless Protocols : ISA 100.11a and WirelessHART

Jae-Han Jeong,[1†] Sung-Moon Kwon,[1] Tae-Shik Shon[1,2‡]
[1]Department of Computer Engineering, Ajou University
[2]Department of Cyber Security, Ajou University

요 약

최근 산업에서는 산업 자동화를 구축하여 효율적인 시스템 관리를 위해 WISN(Wireless Industrial Sensor Network)를 도입하고 있다. 무선센서를 도입하는 WISN는 도입하여 많은 엔지니어링 비용을 절감하고 공정 프로세서의 최적화를 이루어내면서 무선으로의 통신의 사용이 증가하고 있다. 산업용 무선 센서 네트워크에 대한 실증 연구는 활발하게 진행되고 있지만, 이에 대한 보안 연구는 적으며 그만큼 위협에 노출되어 있다. 뿐만 아니라 무선 통신 프로토콜의 표준 자체의 문제점이 있을 경우 표준에 따라 인증된 기기 또한 문제점을 포함한 보안 위협이 따를 수 있다. 각 프로토콜의 표준에서는 보안키를 분배하기 위한 절차가 제시되어 있지 않거나 혹은 기기가 네트워크에 진입할 때 Global Data Link 키를 사용하여 보안에 취약한 문제점이 있었다. 본 논문에서는 표준에 기반하여 ISA 100.11a와 WirelessHART 프로토콜 스택에 따른 보안 기능과 위협에 대해 분석 표준 자체의 문제점을 제시하고 그에 따른 보안 요구 사항에 대해 제시한다.

ABSTRACT

In recent years, industrial automation has been established and WISN (Wireless Industrial Sensor Network) has been introduced for efficient system management. By introducing WISN, many engineering costs have been reduced and process processors have been optimized. And communication flow using wireless is increasing. An empirical study on industrial wireless sensor networks is actively conducted, but there are few security studies on them and they are exposed to such threats. If there is a problem with the standard of the wireless communication protocol itself, the device that is certified according to the standard may also be subject to security threats including problems. We analyze security functions and threats of ISA 100.11a and WirelessHART protocol stack based on standards. Procedures for distributing the security key are not provided or it is vulnerable using the Global Data Link key when the device enters the network. This paper presents the problems of the standard itself and presents the security requirements accordingly.

Keywords: ISA 100, WirelessHART, Security, WISN, Threat Analysis

Received(07. 03. 2019), Modified(09. 04. 2019), Accepted(09. 24. 2019)

† 주저자, qnpfr7179@ajou.ac.kr
‡ 교신저자, tsshon@ajou.ac.kr(Corresponding author)

I. 서 론

유선 케이블로 구성되어 오던 기존 산업제어 시스템에서 산업 자동화를 구축하여 더욱 효율적인 운용 및 시스템의 관리를 위해 무선 센서 네트워크를 활용하는 WISN을 도입하는 연구들이 활발히 진행되고 있다. WISN의 도입을 통해 효율적인 정보의 관리와 산업 공정 프로세서의 통찰력을 높일 수 있으며 이를 통해 엔지니어링 비용을 절감할 수 있다. 또한 기존 유선 케이블의 설치 및 관리의 비용문제를 해소하며, 상대적으로 관리하기 용이한 무선 센서를 사용하여 산업 제어 시스템 통신에서 무선의 사용이 증가하고 있다.

산업용 무선 센서 네트워크를 위한 실증 연구가 활발히 진행되고 있으며, 2014 년 3월 AT&T, 시스코, General Electric, IBM 및 인텔에 의해 설립된 IIC(Industrial Internet Consortium)는 산업 분야에서 무선 네트워크를 접목하는 다양한 연구 프로젝트를 진행하고 있다. 그 중 하나인 2016년 4월부터 진행된 Smart Factories 프로젝트는 오스트리아의 B&R Industrial Automation 社[1]가 주도한 프로젝트로 제조 및 생산 분야에서 지능형 기계 및 장치 프로세스를 적용하였다. 이러한 프로세스는 기계 (Machines), 자산(Assets), 시스템 및 사물(Things)간의 실시간 상호작용을 통해 완벽한 통제를 목적으로 한다. IIC를 통한 또 다른 연구로는 2017년 02월부터 진행된 Communication & Control Testbed for Microgrid Applications, Cisco프로젝트이다[2]. 해당 연구는 IIoT(Industrial IoT)를 통해 전력을 보다 정확하고 안정 적으로 생성시켜 효율적으로 활용하는 것을 목적으로 하며, Cisco 社와 RTI(Real-time Innovations), National Instruments 그리고 Wipro 社가 공동으로 추진한 프로젝트이다. 이는 자동화된 시스템을 기반으로 한 IIoT 노드를 제공하여, 지능형 분석 기능과 분산된 위치 처리 및 제어 어플리케이션 결합을 통해 전력의 효율적이고 안정적인 생성을 보장한다. IIoT 센서를 적용한 스마트 마이크로 그리드를 통해 National Instruments 社의 Industrial IoT Lab에 적용하여 개관식을 하였고 추가적인 실제 적용을 진행 중이다.

위와 같이 산업에 무선 통신을 사용하기 위한 실증 연구들이 활발하게 진행되고 있지만, 그에 반해 산업용 무선 통신에 대한 보안 관련 연구는 적으며 그만큼 위협에 노출되어 있다. 실제로 ISA (International Society of Automation) 100을 포함한 WISN 규격에서 새로운 네트워크 장비가 기존의 네트워크에 진입하기 위해 정보를 얻는 Provisioning단계가 있다. Provisioning 절차는 대개 제품의 생산단계에 정보를 주입하는 factory pre-provisioned 정보에 의존하고 있다. 이러한 사전보안 단계의 취약점으로, 2015년 Zillner가 공개한 technical report[3]에 따르면 Zigbee Pro를 사용하는 규격중 하나인 Zigbee Light Link(ZLL)의 마스터 키가 유출 된 경우가 있었다. 이러한 취약점으로 인해, 기반 시설에서 사고가 일어날 경우 가스 유출과 같은 직접적인 피해 및 산업의 생산과 공급에서의 막대한 금전적 손해가 일어날 수 있으므로 각별한 주의가 필요하다. 하지만 대부분의 경우 산업용 무선통신 적용 시 실제 제어 시스템 자체에 적용 가능성 및 안정성 연구만 진행하고 있을 뿐 사이버 보안에 대한 연구는 부족하다. 이에 따라 본 논문에서는 산업용 무선통신 프로토콜로 많이 연구 및 사용되고 있는 규격인 ISA 100.11a와 WirelessHART 프로토콜의 표준을 중심으로 보안 취약성에 대해 분석하고, 위협에 따른 보안 요구사항을 제시하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 산업용 무선 센서 네트워크 보안에 대한 관련연구를 소개하고, 3장에서는 ISA 100.11a와 WirelessHART의 규격 및 분석한 보안기능을 기술한다. 4장에서는 각 프로토콜이 표준을 따랐을 때 발생할 수 있는 보안 위협에 대해 기술하고, 5장에서는 위협에 따른 보안 요구사항에 대해 제시한다. 마지막으로 6장에서는 결론과 향후 연구에 방향에 대해 제시한다.

II. 관련연구

산업 자동화 기술과 함께 무선 기술의 이용에 대한 실증 연구가 증가함에 따라 다양한 무선 통신 표준의 프로토콜 분석 및 성능 평가 연구가 많이 진행되고 있다. Nixon et al.[4]은 실제 산업에서 많이 사용되고 있는 WirelessHART와 ISA 100.11a의 통신 스택에 대한 전체 비교 분석을 하고 있으며, 제공하는 기능에 대한 주요 차이점에 대해 제시하고 있다. 그에 따라 스택에 따른 보안 기능에 대해 간략하게 분석하고 있지만 프로토콜 자체의 비교 연구에 그치고 있으며 보안 기능에 대한 설명은 표로 간단하게

제시하고 있다. WirelessHART와 ZigBee프로토콜의 분석을 한 Lennvall et al.[5]는 프로토콜 분석에 더불어 각 프로토콜에서 암호화를 위해 사용하는 키와 보안에 대해 비교분석하고 있지만 키를 사용한 보안 분석에서 그치고 있다. 보안 문제에 집중하여 분석 및 보안 대책을 제시하고 있는 Zhang et al.[6]은 ISA 100.11a-2009 기반 자체 센서 노드 플랫폼을 개발하여, 자체 플랫폼에 대한 통신비용 및 스토리지 기능과 같은 ISA 100.11a 기반 네트워크의 보안 성능을 테스트하였다. 이 외에도 ISA 100.11a에 정의 된 보안 프로토콜에 대한 요약을 하여 위협과 대책에 대해 제안하고 있다. Cristina Alcaraz와 Javier Lopez[7]은 Zigbee Pro와 WirelessHART 그리고 ISA100 Wireless 프로토콜의 기밀성, 무결성 및 가용성 관점에서 위협 및 취약점을 분석하여 그에 따른 대책을 제시하고 있다.

위의 기존 연구에서는 표준에서 제공하는 보안기능들의 정리를 통해 어떠한 공격들이 방지되는지 정리해 놓거나 특정 상황에 대한 보안 공격의 분석들을 수행했다. 하지만 해당 표준에 따라 규격이 인증된 기기라 하더라도 표준 상에 문제점을 포함하고 있을 시 보안 위협이 따를 수 있으며 이러한 표준 자체의 문제점을 분석하는 연구는 적다. 따라서 본 논문에서는 실제 표준에서 제공한 보안기능에 따른 보안위협뿐만 아니라, 표준에서 보안 기능을 권고 하고 있지만 실제 정의되지 않은 기능들이나 잘못 설계된 부분에 의해 실제 인증된 제품의 경우 발생할 수 있는 보안 위협을 분석한다. IEC(International Electrotechnical Commision) 표준으로 채택되어 많이 사용되고 있는 두 산업용 무선통신 프로토콜인 ISA 100.11a와 WirelessHART의 표준의 구조와 보안 기능에 대해 분석하고 그에 따른 보안 요구 사항에 대해 제시한다.

III. 산업용 무선 통신 프로토콜 보안 기능 분석

본 장에서는 ISA 100.11a와 WirelessHART 프로토콜의 규격의 각 계층에 따른 보안 기능에 대해 분석한다.

3.1 ISA 100.11a 프로토콜

3.1.1 프로토콜 스택 분석

Fig.1.처럼 ISA 100.11a 프로토콜은 TCP/IP(Transmission Control Protocol/ Internet Protocol) 스택과 유사하며, 각 계층에서는 검증된 프로토콜들을 선택하여 사용하고 있다[8]. 실제 사용 계층으로는 Physical 계층, Data link 계층, Network 계층, Transport 계층과 Application 계층을 사용하고 있다. Physical 계층과 Data link 계층은 IEEE 802.15.4 (Institute of Electrical and Electronics Engineers Standard for Local and metropolitan area networks– Part 15.4: Low-Rate Wireless Personal Area Networks)를 사용한다[9]. 여기에 추가적으로 Data Link 계층에서는 주파수를 규칙에 따라 바꾸는 주파수 호핑(hopping)을 위해 ISA 100.11a만의 상위 계층이 추가되어 있다. 그리고 Network 계층에서는 6LoWPAN(IPv6 over Low-Power Wireless Personal Area Networks, IETF(Internet Engineering Task Force) RFC(Request for Comments) 4944)을 사용하고 있으며, Transport계층에서는 UDP(User Datagram Protocol, IETF RFC 768)를 사용하고 있다[10]. 마지막 Application 계층에서는 ISA 100.11a 프로토콜 응용 계층이 사용된다. ISA 100.11a은 IEEE 802.15.4, 6LoWPAN 그리고 UDP와 같은 널리 사용되고 있는 공식 표준을 사용해서 상호 운용성이 뛰어나다.

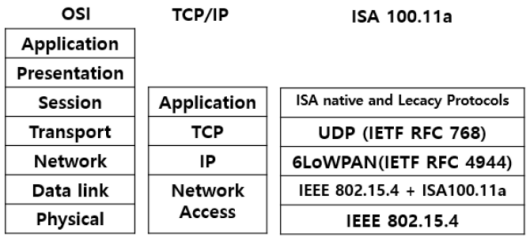

Fig. 1. ISA 100.11a Protocol Stack Comparison

3.1.2 하위계층 보안 기능 분석

ISA 100.11a는 Fig.2.와 같은 구조와 보안 기

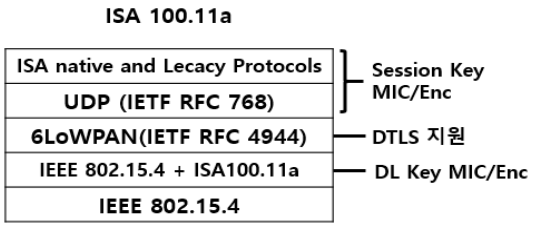

Fig. 2. ISA 100.11a Stack

능을 가지고 있다. IEEE 802.15.4 보안 기능을 Data Link계층과 Transport계층, 두 계층에서 중복하여 사용하고 있다. Data Link계층에서는 Data Link 키를 이용하여 hop-by-hop 보안을 제공하고 있고, Transport 계층에서는 세션 키를 사용하여 end-to-end 보안을 제공한다.

보안을 위해 Data Link계층과 Transport계층의 헤더에는 보안 헤더를 포함하고 있으며, 각 계층에서 4바이트의 TAI(International Atomic Time)를 nonce로 사용하여 재전송 공격을 방지할 수 있다. 이는 nonce 충돌을 피하기 위해 47.5일 이전에 키 교환을 해야 한다.

Network계층에서 6LoWPAN은 IPv6를 사용하기 때문에, IPsec(Internet Protocol Security)을 사용하여 IP패킷을 암호화하고 인증하는 보안통신이 가능하다. Transport계층에서 UDP를 사용하고 있기 때문에 DTLS(Datagram Transport Layer Security)를 사용할 수 있다. 이를 통해 패킷의 암호화, 무결성 그리고 인증을 보장할 수 있지만, 이러한 부분은 표준에서 명시하지는 않으며 기본적으로 IEEE 802.15.4에서 제공하는 보안 기능을 사용한다.

3.1.3 응용계층 보안 기능 분석

Fig.3.은 ISA 100.11a 통신에서 보안 통신을 생성하기 위한 프로세스 단계를 나타내고 있다. ISA 100.11a 표준에서 요구하는 보안 기능을 분석한다.

ISA 100.11a 프로토콜은 기기 간에 보안 통신을 위한 기능은 모두 Security Manager에서 수행한다. 새로운 기기가 ISA 100.11a 무선 네트워크로 진입하기 위한 보안정보(trust-related information)를 취득하기 위한 단계를 Provisioning단계라고 한다. Provisioning단계에서 취득한 보안 정보를 통해 기존 무선 네트워크로

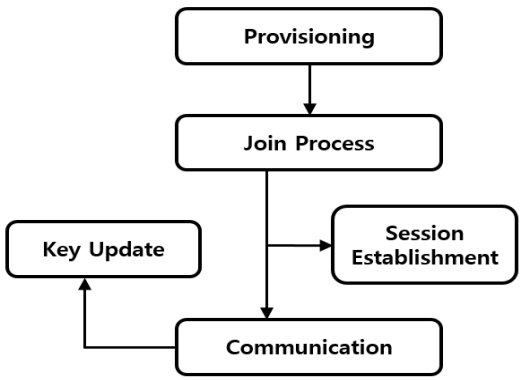

Fig. 3. ISA 100.11a Secure Communication Creation Process

진입하는 Join Process, 두 기기간의 추가적인 세션이 필요한 경우 추가적인 세션과 세션 키를 생성하는 Session Establishment단계가 있다. Security Manager에 정의된 보안 정책에 따라 각 기기의 암호화와 복호화에 사용되는 키가 만료된 경우 Key Update절차를 수행한다.

3.1.4 응용계층 단계별 보안 분석

Provisioning 단계란 새로운 기기가 ISA 100.11a 무선 네트워크로 진입하기 위한 보안정보를 취득하기 위한 단계이며, 정보를 가지지 않은 기기를 사전준비 하는 과정이다.

ISA 100.11a 네트워크에서 Join 키를 생성하는 방안으로는 공장에서 각 센서 기기를 생성할 때 특정한 Join 키를 삽입하는 방법인 사전주입(provisioning) 방식과 적외선 통신이나 NFC(Near Field Communication) 등을 사용하는 OOB(Out of Band) 방법이 있다. OOB의 경우 어떠한 기술을 사용하여 키를 분배할지 명확하게 다루고 있지 않다. Pre-installed방식은 각 센서 기기에 Join 키를 미리 삽입해놓는 것으로, 디바이스를 공장에서 생성하는 과정에서 Join Process에 필요한 정보를 입력 및 유저에게 제공시 배포하는 방법이다. OOB에 비해 실용적인 방법이지만 보안성 관점에서는 취약하다. Zillner[1]가 공개한 보안사고 같이 사전주입 방식은 한번 설정해놓은 값을 변경하기 쉽지 않고 같은 값을 계속 사용하기 때문에 반복해서 사전준비를 수행하는 경우 유추하기 쉬운 취약성을 가지고 있다.

Join Process단계는 크게 Symmetric/ Asymmetric 기법으로 나눌 수 있다. Symmetric 기법은 같은 키를 공유하여 암호화등을 진행하는 것이고, Asymmetric기법은 공개 키 암호 방식과 같은 방법으로 CA(Certificate Authority)가 요구된다. 또한 Asymmetric기법은 한정적인 자원을 요구하는 센서 디바이스에서는 큰 용량을 차지하는 길이가 긴 키를 사용하기에는 적합하지 않다는 단점이 있다. Join Process단계는 기기(sensor node)의 진입요청으로 시작하는데, Security Manager는 전송받은 진입요청에 대한 보안 진입 응답을 보내기 전에 신뢰할 만한 기기인지 인증을 수행한다. 기기인증은 표준(IEC 62734-2014)에서 Whitelist나 Blacklist로 확인하라고 간단히 언급되어 있으며 상세한 기술은 되어 있지 않다. 따라서 해당 인증에 대한 구현과 인증 절차의 보완이 필요하다.

Join Process를 위해 G/W와 통신을 할 때 마스터 키를 사용하여 AES128-CCM*로 암호화 통신을 한다. 마스터 키를 생성하기 위한 수행과정은 Join 키 또는 세션 키로 보안이 이루어진다. 하지만 센서 노드와 G/W의 직접적인 통신이 아닌 중간에 중계하는 기기(Advertising router DMO)가 더 추가되는 경우 Data Link 키가 없기 때문에 Global Data Link 키를 사용해야 한다. 이때, Global Data Link 키는 공개된 정보이기 때문에 보안적인 측면에서 문제가 될 수 있다.

Session Establishment단계는 두 기기간의 새로운 보안 통신을 위해 새로운 세션 키를 발급 받기 위한 단계이다. 두 기기간의 통신을 하기 위한 세션 키는 Security Manager에서 생성되어 두 기기에게 분배된다. 반면, Key Update는 각 키의 정책에 따른 기존 키의 갱신 주기가 되었을 경우 새로운 키를 발급받기 위해 사용되나 Session Establishment와 동일한 메소드를 사용한다. 두 기기간의 새로운 보안 통신을 생성하기 위해 세션 키를 발급 받고 ACL(Access Control List)을 확인한 후 세션 키를 생성하는데, 표준에서는 올바른 세션에 대한 요청인지를 확인하는 ACL에 대한 정의를 하고 있지 않다. ACL의 정의와 개발이 필요하다.

Policy는 개인 프로그램들과 디바이스들이 만들 수 있는 보안 옵션들을 제한하며 Policy단계를 위한 정보나 구조체는 정의되어 있으나, 어떻게 사용하는지 그리고 어떻게 관리하는지에 대한 규칙이나 정의는 없다. 실제 사용할 경우 관리자가 설정하고자 하는 정책에 따라 Policy를 관리하는 방 안이 필요하며, 키 업데이트 주기나 키 유효기간 등의 정책 수립이 필요하다.

3.2 WirelessHART 규격 분석 및 보안 기능 식별

3.2.1 프로토콜 스택 분석

Fig.4.은 WirelessHART 프로토콜 스택 구조를 나타낸다[11]. WirelessHART 또한 ISA 100.11a 프로토콜과 같이 IEEE 802.15.4 Data Link 계층을 사용하며 2011년 기준의 IEEE 802.15.4 표준에 기반 하여 설계 되어있다. 그러나 이외 계층은 WirelessHART 독자적인 계층을 사용한다. Network 계층으로는 Mesh Network, Transport계층으로는 TCP와 유사한 계층을 사용하였지만, 이는 어떠한 표준에 기반 한 것이 아니기 때문에 ISA 100.11a와 달리 WirelessHART는 기타 통신 프로토콜과의 상호 운용성은 전혀 존재하지 않는다.

Data Link 데이터 구조에서 IEEE 802.15.4계층의 첫 바이트는 Frame Control로, WirelessHART는 0x41을 사용하는 특징이 있으며, MIC과 CRC를 포함한다. 보안기능으로는 IEEE 802.15.4의 암호화 및 인증 기능을 사용한다. 0x41 이후의 필드는 일반적인 IEEE 802.15.4 표준을 준수하기 때문에 추가적인 설명은 하지 않는다.

추가적으로 ISA 100.11a와 WirelessHART의 Network 계층의 차이점은 WirelessHART는 Broadcasting을 지원한다는 점이다. 주로 게이트웨이에서 동일한 데이터를 전체 기기에게 전송하는 것과 같이 전체 기기를 관리하는데 사용된다.

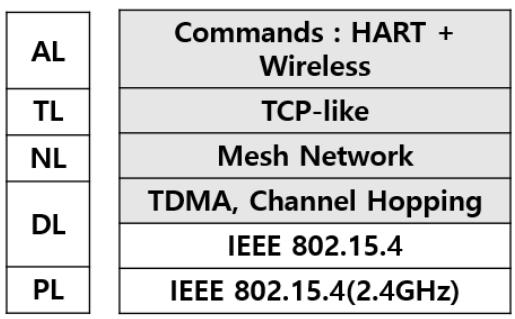

Fig. 4. WirelessHART Protocol Stack

3.2.2 하위 계층 보안 기능 분석

IEEE 802.15.4에서 제공하고 있는 cipher suite를 선택적으로 사용하는 ISA 100.11a과 달리 WirelessHART는 각 계층 별 사용 보안 옵션이 정해져있다. Data Link 계층에서는 암호화 없이 MIC 32bit만을 사용하며, Network 계층에서는 AES-CCM* 128bit, MIC 32bit를 사용한다. 또한 각 기기 당 하나의 세션 및 이에 해당하는 네트워크 키를 사용한다. 이외 WirelessHART만의 특이점으로 각 계층 별 nonce사용이 있다. WirelessHART의 경우 Data Link 계층과 Network계층의 nonce가 다르게 구성된다. Data Link계층의 경우 5바이트의 현재 슬롯 번호와 EUI-64 또는 6바이트의 0 및 2바이트의 nickname으로 이루어져 있으며, WirelessHART의 경우 10ms의 고정 슬롯 시간을 사용하고 있기 때문에 최대 7.28일의 시간을 담을 수 있는 시간 값을 사용하여 nonce를 구성하고 있다. Network계층의 경우 5바이트의 시간 값 대신 메시지 유형에 대한 1바이트(join response인 경우 1, 나머지는 0)와 4바이트의 nonce counter를 사용하고 있다. 이 nonce counter는 해당 기기가 join을 수행하는 순간부터 메시지를 전송할 때마다 1씩 증가하는 카운터로, 기타 네트워크 명령 등으로는 초기화 되지 않는 특성이 있다.

3.2.3 응용 계층 보안 기능 분석

WirelessHART의 경우 ISA 100.11a과 달리 Provisioning에 대한 절차가 명시되어 있지 않다. 또한 다중 세션을 지원하지 않으며 기기 간의 하나의 세션과 해당 세션에 해당하는 하나의 네트워크 키만을 사용하기 때문에 보안 기능은 크게 Joining단계와 Key change로 볼 수 있다. 이외의 특이점으로는 표준 IEC 62591-2016에서 추가된 기능으로 Joining단계 이후 즉시 데이터 리포팅 및 제어 등의 동작을 수행하지 않고, 대기상태인 Quarantine 모드가 있는 점이다. Quarantine 모드의 기기는 게이트웨이와 데이터 리포팅, 제어와 관련 하여는 수행할 수 없으며 오직 Network manager와만 통신할 수 있다. Network manager로부터 네트워크 관련 세팅 이후 또는 설정되어진 일정 시간 이후에 Operation 모드가 되며 게이트웨이와 통신을 수행할 수 있다.

3.2.4 응용 계층 단계별 보안 분석

WirelessHART의 표준에는 Provisioning단계에 대한 절차가 명시되어 있지 않다. 단, Joining 단계에서 Provisioning 단계의 절차를 포함하고 있으며 사전준비하는 과정에서 사용할 수 있는 함수들은 정의를 해두고 있다. Provisioning은 Maintenance tool을 통해 수행하는 것으로 정의하고 있으며, Maintenance tool은 WirelessHART 기기 자체에 내장된 Maintenance port나 사용자가 지니고 다니는 무선장치 정도로 정의되어 있다. Provisioning 절차 동안 Maintenance tool로부터 네트워크에 진입하는 기기가 취득해야 하는 정보는 Join 키, 네트워크 ID이다. Maintenance tool은 Provisioning 이후에도 연결되어 Joining단계의 상태를 체크할 수도 있다.

Joining 단계에서는 ISA 100.11a과 달리 WirelessHART는 별도의 마스터 키를 생성 및 관리하지 않는다. 오직 Join 키를 통해 암호화하여 세션 키를 할당할 뿐이며 Joining 단계의 정상 동작을 2중으로 점검하기 위한 확인 과정도 존재하지 않아 비교적 간단히 수행된다. 우선 사전준비하는 과정을 통해 Join 키와 네트워크 ID를 취득한 상태에서 시작한다. 주변 네트워크를 모니터링하여 네트워크 ID와 동일한 네트워크의 Advertisement 신호를 수신한다. 수신한 Advertisement 신호 중 신호 세기가 적당한 곳으로 시간 동기화 및 Joining을 요청하며 Network manager는 해당 메시지를 전송받아 Join 키 및 EUI-64 주소 등 을 통해 해당 기기의 인증을 수행한다.

기기의 인증을 통한 방법으로는 Whitelist, Blacklist 등이 있으나 기기 인증을 위한 상세 방법은 해당 표준에서 다루지 않는다. 단, 기기가 이미 해당 네트워크에 통신 중인 active 기기 목록에 있는지는 검사해야 한다. 정상적으로 인증되었으며 active 기기 목록에 없는 경우 네트워크에서 사용될 주소인 nickname을 할당하며 Data Link 계층의 무결성을 위한 그룹 키인 Network 키와 Network Manager와 통신하기 위한 세션 키를 발급 및 Join 키로 암호화하여 전송한다. 이후 주변의 기기와도 통신을 수행할 수 있도록 라우팅 정보를 공유하

여 Joining단계를 위한 네트워크에 진입하는 기기와 Network Manager 간의 링크에서 일반 네트워크 링크로 전이한다. 여기까지 수행되면 기기는 Quarantine 단계에 들어가며, Network Manager의 설정에 따라 즉시 게이트웨이와의 세션을 할당하여 operation 모드로 들어가거나, 일정 시간 또는 관리자의 설정에 따라 관리되게 된다. 특히 이러한 Quarantine 단계가 있는 주요한 이유는 gateway가 많은 세션을 유지하며 통신을 하는 중에 추가적인 세션을 할당하는 경우 gateway의 timetable 업데이트에 따른 다수의 내부 트랜잭션이 발생한다. 또한 gateway는 joining 기기와의 통신을 수행해야하기 때문에 gateway의 순간적인 성능이 저하될 수 있다. 따라서 현재 통신 중인 기기 및 게이트웨이의 상황에 따라 새로운 네트워크 진입을 수행할지에 대한 판단이 필요할 수 있으며 이를 위해 중간에 버퍼 역할을 수행하는 것이 Quarantine 단계이다.

WirelessHART는 broadcasting을 함에 따라 Key Change 단계에서 키 교환 과정이 두 가지로 나뉜다. Data Link의 무결성을 위해 같은 네트워크에서 공통으로 사용되는 Network 키는 broadcast 세션 키를 통해 broadcasting된다. 이를 전송 받은 모든 기기는 해당 네트워크 키를 이용하여 ACK를 수행하나 해당 키는 즉시 사용되거나 특정 시간 이후 사용 될 수 있다. 이외 Join 키, 세션 키는 unicast를 통해 해당 키에 대한 업데이트를 수행하지만, 분배되는 키를 암호화하기 위한 키는 정의되어 있지 않다. 이러한 키 교환은 스케줄링이 요구되며, 특히 Network 키에 대한 변경은 네트워크에서 사용되는 전체 Network 키를 바꾸기 때문에 네트워크를 순간적으로 마비시킬 수 있어서 운영 관점에서 문제가 되지 않도록 확실한 키 스케줄링이 필요하다.

Security Manager단계에서 사용되는 데이터

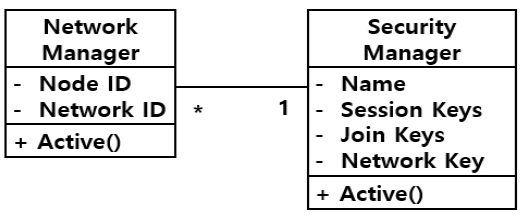

Fig. 5. WirelessHART Network manager, Security manager

및 해당 역할이 상세히 기술된 ISA 100.11a와 달리 WirelessHART에서의 Security Manager의 역할은 명백하게 정의되어 있지 않다. Fig. 5.는 표준에서 설명하는 Security Manager를 표현한 것이다. Network Manager가 가지는 값들과 Security Manager가 가져야하는 값 등, 암호학적으로 필요한 값들과 키를 생성하는 역할을 수행하는 것으로 기술되어 있다. 이에 대한 Security Manager의 상세 기능과 통신 방법은 표준 외 항목으로 두고 있다.

IV. 산업용 무선통신 프로토콜 보안 위협 식별

본 절에서는 3장에서 설명한 프로토콜의 규격과 이에 대한 보안기능에 기반 한 위협에 대해 분석한다.

4.1 ISA 100.11a 단계별 보안 위협 식별

4.1.1 Provisioning 단계

Provisioning단계에서 대칭키 기반의 보안성을 보장하는 기법을 정의하지 않았다. Join 키를 분배하기 위해 다양한 데이터 교환을 위한 사전준비 과정에 대한 기법을 제시하고 있으나 공개키 및 인증서를 사용하지 않는 경우 OOB 통신, Open-Key(0x004F 0050 0045 004E 0000 0000 00000000)를 사용하여 암호화하여 전송하는 OTA만을 제안하고 있어 대칭키를 사용하는 경우 적절한 보안을 제공하지 못하고 있다.

Fig. 6.은 데이터 교환을 위한 사전준비 기능에 대한 다양한 경우에 따른 센서 노드의 상태 전이를 나타내고 있다. 빨간색으로 표시한 루트로 사전준비 과정을 위한 기능을 진행하는 경우 보안 취약성이 확인되었다. 타겟 네트워크에 진입하기 위한조건으로 Join 키가 발급되어 있지 않은 경우에는 제조 과정에서 사전주입 된 K_open을 OTA 방법으로 Provisioning 네트워크 단계에 진입하여 Join 키를 발급받게 된다. Join 키를 발급받는 과정에서 공격자에 의해 도청되었을 경우 마스터 키 뿐만 아니라 세션 키, 사전준비에 관한 정보와 네트워크 관한 정보가 탈취될 가능성이 있다. 다른 상태 전이의 경우 인증서 및 비 대칭키 기반은 CA 구축이 추가적으로 필요하고 센서 기기가 비 대칭키 연산을 하기 때문에

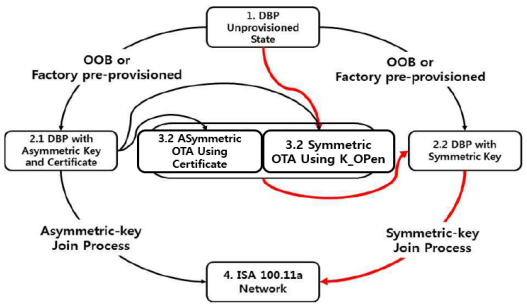

Fig. 6. Provisioning Function Simplified State Transition Diagram

연산량이 많아서 무선 산업 센서 네트워크에 적합하지 않다. 또한 OOB 방법은 본 연구에서는 무선 산업 센서 네트워크를 제외한 추가적인 보안 장치나 회선을 고려하지 않기에 사용하기 쉽지 않다. 공장 사전주입 방법에서는 Zigbee ZLL(zigbee light link)과 연관되어 마스터 키와 보안을 외부에 의존해야 하며 결과적으로 보안을 외부에 전적으로 맡기게 되므로 추가적인 보안 고려사항이 발생한다. 따라서 CA 구축이 되어 있지 않으며 OOB, 공장 사전주입을 사용하지 않는 경우 Fig.6.의 빨간색으로 표시한 루트인 (Fig.6.의 1.상태에서 3.2로의 상태, 3.2상태에서 2.2로의 상태 그리고 2.2상태에서 4상태로의 루트) 사전중비 기능을 진행하게 되나 이 경우 Open-Key(0x004F0050 0045 004E 0000 0000 0000 0000)를 사용하게 되므로 공격자가 패킷을 도청 시 모든 보안 정보가 탈취 가능하다.

4.1.2 Join Process 단계

Join process 과정은 네트워크에 진입하기 위해서 타겟 네트워크에 관한 정보를 전송받는다. Join process를 수행하는 센서 노드에 관한 인증 기능이 정의되어 있지 않아, Join 키를 탈취한 공격자가 다른 센서 노드와 같이 네트워크에 진입할 가능성이 있다. 표준에서는 이러한 인증 기능을 옵션으로 사용하기를 권고하고 있으며, 이는 Provisioning 된 기기의 EUI-64(Extended Unique Identifier-64)를 Whitelist로 작성하고 활용함으로써 수행가능하다. 그러나 표준에서 명확히 특정 기능을 사용하라고 명시하고 있지는 않다. 그리고 Join Process는 아직 암호화키를 발급 받기 이전이기 때문에 센서 노드, 라우터 간 hop-by-hop 통신을 위한 Data Link 키가 발급되지 않아 Global Data Link 키를 사용하는 것을 확인함으로서 보안 취약성이 확인되었다.

Join Process의 첫 단계인 진입요청 메시지의 필드에서 마지막 인자로 메시지의 무결성을 위해 MIC 값을 포함하고 있다. 표준에서는 진입요청 메시지 필드의 element 1~4 인자를 통해 MIC 값을 생성하도록 하고 있으나 element 4가 MIC값 자체이다. 이는 MIC 스스로를 인자로 포함하여 올바르지 않은 생성 인자이다. 이 부분은 ISA 100.11a-2011 표준에도 똑같은 오류를 포함하고 있으나 ISA 100.11a의 가장 초기 표준인 ISA 100.11a-2009 표준에서는 4개가 아닌 5개의 인자로 정상적인 MIC 값 생성을 지시하고 있음을 확인하였다. 추후 무선 산업 기기의 보안을 검증할시 암호화 및 인증 코드에 사용되는 인자에 대한 검증도 명확히 수행될 필요가 있다.

4.1.3 Session Establishment/Key Update 단계

Session Establishment와 Key Update 단계 시 새로운 세션 및 키의 발급을 요청하는 대상을 검증하는 것은 보안상 중요한 이슈이다. IEC 62734-2014에서는 ACL을 통해 검증하기를 권고하고 있다. 그러나ACL에 대한 어떠한 상세 내용도 없어, ACL에 대한 정의와 활용 방안에 대해 상세 보안 설계가 필요하다.

Security Policy는 각 키 마다 설정되는 데이터로 Session Establishment 단계 및 Key Update단계 시 각 보안키에 해당하는 Policy 객체를 전달한다. 이러한 Policy 자체는 정의가 잘 되어 있으나, 보안 관리자 입장에서 이러한 Policy를 관리하기 위해 Policy를 저장하고 제어하기 위한 수단은 표준에서 언급하지 않고 있어 이에 대한 상세 보안 설계가 필요하다.

4.2 WirelessHART 단계별 보안 위협 식별

4.2.1 Provisioning 단계

Provisioning단계에서 Join 키가 최상위 보안키임에도 불구하고 이를 분배하기 위한 사전준비 절차가 제시되어 있지 않다. ISA 100.11a 표준의 경우 공개키 또는 공장 사전주입과 OOB에 의존하는 사

전준비 기법을 제시하고 있다. 그러나 WirelessHART는 이러한 기법조차 제시하지 않고 있다. 더욱이 ISA 100.11a은 Join 키로부터 마스터 키를 생성하여 보안 절차에 Join 키가 차지하는 비중이 적은 반면, WirelessHART는 마스터 키를 별도로 사용하지 않고 Join 키를 사용하여 모든 키 분배를 하기 때문에 Join 키가 보안에 주는 영향이 매우 크다. 따라서 Join 키의 분배를 위한 안전한 절차 및 방안이 필요하다.

4.2.2 Joining 단계

Joining단계에서 Blacklist, Whitelist 개념은 정의하고 있지만 이에 대한 사용을 옵션으로 두고 있으며, Join을 수행하려는 기기에 대한 인증 또한 선택사항으로 제시하고 있다. 이러한 문제점 때문에 실제 WirelessHART기기에서 실제 접근 제어가 구현되지 않고 사용되는 경우가 많으며, 따라서 비인가 기기가 네트워크에 참여하는 보안 문제점이 발생할 수 있다. Join단계의 요청 메시지 중 Data Link키가 존재하지 않아 Global Data Link 키를 사용하고 있기 때문에 취약할 수 있다.

Data Link계층에서는 비 암호화 및 MIC 32, Network 계층에서는 AES-128, MIC 32를 고정적으로 사용하고 있다. Data Link 계층에서는 암호화를 수행하고 있지 않기 때문에 Data Link 계층의 명령인 disconnection 명령을 캡처한 경우 nonce의 주기인 최대 7.28일 간의 재전송 공격에 대한 발생 가능성이 존재하며, 이는 47.5일의 ISA 100.11a와 비교하여 다소 짧은 주기이다.

4.2.3 Key Change 단계

Key Change단계에서는 절차가 Network 키 및 broadcast 키 와 같은 그룹 키와 Join, 세션 키와 같은 단일 키로 나뉜다. Broadcast 키의 경우 broadcast 세션 키를 이용하여 분배한다고 명시되어 있으나 단일 키의 경우 어떤 키로 암호화하여 분배하는지에 대한 언급이 없어 이에 대한 명시가 필요하다. 또한 그룹 키의 경우 키 교환 시 네트워크의 마비가 오는 문제점을 언급하여 키 스케쥴링이 필요하다는 내용은 있으나 이를 위한 데이터 정의 및 방안은 기술되어 있지 않아, 키 스케쥴링에 대한 데이터 구조 및 방안에 대한 기술이 필요하다. 이외 broadcaset 키를 사용하는 경우 Bayou, Lyes, et al.[12]이 제안한 공격에도 취약할 수 있다.

V. 안전한 무선통신 사용을 위한 보안 요구 사항

5.1 ISA 100.11a 보안 요구 사항

5.1.1 Provisioning 단계

Provisioning 단계에서 OOB, 공장 사전주입, CA 기반 비 대칭키 암호화 기법을 제외하면 안전한 Provisioning 기법이 존재하지 않는 것이 주요 문제이다. OOB는 기타 회선을 만들어야 하는 것을 의미하며, 이는 USB와 같은 장비를 포함한다. 그러나 기타 보안 라인을 관리하는 것이 주요 옵션이 되기 힘들며, 물리적 장비의 경우 네트워크가 다수의 기기를 포함하거나, 위험 지역에 설치된 무선기기의 경우 효율적인 관리가 힘들다. 공장 사전주입 방법의 경우 제품 생산자에게도 보안이 중요시 되며 보안이 지켜졌다 하더라도, Zigbee의 마스터키 유출 사건과 같이 대규모 네트워크 관리가 필요한 경우가 발생할 수 있어 공장 사전주입 이외의 기법은 필수적이다. CA 기반의 비 대칭키 암호화 기법은 별도의 CA 시스템 구축을 요구하며 오버헤드로 인해 저 전력 통신에 어느 정도 적합하지 않은 옵션이라 볼 수 있다. 결과적으로 데이터 교환을 위한 사전준비 단계와 보안 유출에 따른 보안 관리에 대비하여 안전한 기타 회선 또는 CA 기반 비 대칭키 암호화 기법 구현이 요구되며, 이 두 경우가 사용 불가능하다면 이외의 사전준비를 위한 방안이 요구된다. 하나의 예로는 기기 자체가 임베디드 기기에서 활용도가 높은 ECDH(Elliptic-Curve Diffie-Hellman) 키를 생성하여 사전준비 기능의 수행을 보장하고, 기기의 EUI-64 주소를 Whitelist로 관리하여 허용된 기기를 받거나 사전준비를 유도하는 Advertising 기기의 물리적 신호 세기를 제한하고 물리적 접근제한을 통해 허용된 기기의 접속만을 허용하는 방법 등이 있을 수 있다.

5.1.2 Join Process 단계

Join Process단계의 인증은 표준에서 Whitelist, Blacklist, 관리자의 콘솔에 알람을 통한 인증 등 방안을 제시하지만 특정 기능으로 제한을

Table 1. Security threats and Security Requirements for ISA100 Protocol and WirelessHART Protocol

ISA 100		
	Security Threats	Security Requirements
Provisioning	- No procedure based on symmetric key	- Use ECDH, CA or OOB
Join	- No join device authentication process - Using Join Request Global Key - Incorrect MIC Value Generation Factor	- Use EUI-64 for whitelist or use secondary Authentication system - Using temporary ECDH key - Check the parameters used by the device or sensor node
Key Update	- ACL undefined and no policy management plan	- Using for management and authentication with ACL throught information in the Policy object
WirelessHART		
Provisioning	- No Procedure for provisioning	- Use ECDH, CA or OOB
Joining	- Join device authentication procedure is optional - Using Join Request Global Key	- Implementation and using of the whitelist or blacklist - Using temporary ECDH key
Key Change	- No key management plan	- Need to define key management scheme

두고 있지는 않다. 기기 생산 이후 기기를 네트워크에 배치하기 전에 EUI-64 주소를 Whitelist에 등록하는 절차를 수행하거나, 응용 프로그램을 개발하여 관리자의 2차 인증 시스템을 사용하여야 한다.

또한 Join 과정 중에는 사전에 분배된 암호화키가 없어 Global Data Link 키를 사용하여 hop-by-hop 통신을 하게 된다. 이 경우 위변조에 취약할 수 있는 문제가 있으며, 이를 해결하기 위해서는 임시로 ECDH 키를 Join 하려는 기기와 Join Process를 담당하는 기기 간에 서로 발급받아 통신을 수행하는 방법이 이상적이나 기기 자체에 추가적인 개발이 필요한 사항이다. 이외에는 Join Process를 담당하는 기기 자체를 Security Manager 기기로 제한하고 Security Manager와 one-hop 통신을 수행하여 Join 키를 활용하는 방안이 있으나, 네트워크 확장성이 떨어지는 문제가 있다. 네트워크의 규모에 따라 적합 한 보안 절차를 구성해야 할 것이다.

MIC 값 생성 인자는 현재 표준에서 부정확한 부분으로, 향후 표준의 개정이 된 후 해당 내용을 준수하거나, 통신상에 문제가 발생하지 않도록 ISA 100.11a-2011 또는 이후의 버전으로 일관된 파라미터를 사용하는 기기를 사용하여야 한다. 두 방법이 혼용되는 경우 MIC 값을 생성하는 Security Manager가 이 부분을 처리할 수 있어야 한다. 이와 같은 표준상의 부정확함으로 인한 문제 외에도 각 암호화 알고리즘의 파라미터가 표준을 잘 따르는지 확인되어야 할 것이다.

시중에 상용중인 기기는 AES-CCM* 128로 단일화되어 있어 국내 암호화 알고리즘의 사용은 제품 제조사와 사전에 협의가 필요한 사항이다.

5.1.3 Session Establishment/Key Update 단계

Session Establishment, Key Update단계에서 요구하는 기기에 대한 인증과 각 키에 대한 정보를 담고 있는 Policy 객체에 대한 관리가 주요 이슈사항이다. ACL에 대한 인증은 Join Process에서의 기기 인증과 같이 정의해놓은 방법은 없다. 다만 Policy 객체 에서 EUI-64, IPv6, Port 번호 정보가 공유되기 때문에 Policy 객체를 ACL로 관리하여 인증이 가능하다. 이 방법은 Policy 객체를 관리하기 위한 수단도 되며 키 관리 주기 변경 등과 같은 관리가 필요한 상황에서도 유효히 사용 될 수 있는 DB로 활용 될 수 있을 것이다. 이와 같이 ACL에 대한 정의와 Policy를 관리하기 위한 데이터 구성과 방안이 요구된다.

5.2 WirelessHART 보안 요구 사항

5.2.1 Provisioning 단계

Provisioning단계에서 주요 내용은 ISA 100.11a와 같다. 특히 WirelessHART는 ISA 100.11a과 달리 마스터 키를 생성하는 절차도 존재하지 않으며 Join 키를 키 분배에 바로 사용하기 때문에 Provisioning의 보안은 더욱더 강조된다. 또한 표준에서 Provisioning을 위한 Maintenance tool에 대한 내용은 있으나 이와 같은 handheld 기기 및 maintenance port는 대규모 관리 및 원격에서 관리가 불가능하여 IIoT 네트워크가 확장성을 제한하는 문제점이 있어 원격에서 수행 가능한 보안 Provisioning 절차가 요구된다.

5.2.2 Joining 단계

Join단계를 수행하려는 기기에 대한 인증에 대해 Whitelist, Blacklist에 대한 개념을 제시하고는 있으나 사용자에게 옵션사항으로 두고 있다. 그러나 비인가 기기의 경우 broadcast 취약성까지 연결될 수 있어 Whitelist, Blacklist를 통한 기기의 인증은 필수적이다.

앞서 기술한 ISA100과 같이 Join 요청 메시지 중 Data Link키가 없어 Global Data Link 키를 사용하고 있으며, ECDH사용이나 Security Manager와 one-hop통신과 같은 적절한 방안이 필요하다.

AES-CCM* 128, MIC-32 단일 보안모드 사용 및 Data Link 계층은 암호화 비수행하는 문제에 대해서는 Data Link 계층의 명령 중에서도 disconnection 등 주요 통신 유형이 포함되기 때문에 특정 명령은 암호화를 수행하는 것이 보안상 필요할 것으로 분석된다.

5.2.3 Key Change 단계

Key Change단계에서 WirelessHART는 ISA 100.11a과 같은 Policy 구조체가 정의되어 있지 않다. 각 보안 키에 대한 만료 및 갱신을 통한 보안 관리를 위해 ISA 100.11a과 같은 Policy 구조체 및 관리 방안이 정의되어야 한다. 또한 WirelessHART의 경우 최대 표현 시간이 7.28일이기 때문에 nonce 충돌을 피하기 위해 최대 키 갱신 주기는 7.28일이어야 한다. 이외 키 갱신 시 키 분배를 위해 어떤 키로 암호화를 수행할지에 대한 명확한 정의가 필요하다.

VI. 결 론

본 논문에서는 IEC 표준으로 채택되어 많이 사용되고 있는 두 산업용 무선통신 프로토콜 표준인 ISA 100.11a와 WirelessHART의 보안 기능과 보안 위협 분석을 하였다. 표준 상에 문제점이 있을 시 표준에 따라 규격이 인증된 기기라 하더라도 해당 문제점을 포함하고 있기 때문에 이에 따른 보안 위협이 있을 수 있다. 그렇기에 표준 자체의 문제점을 분석하는 것은 중요하다. 특히 잘못된 설계 외에도 보안상으로 중요하지만 옵션 사항으로 두거나, 표준 상의 out-of-scope으로 두어 사용자에게 맡기는 부분 또한 기기의 인증 과정에서 중요하게 분석되지 않을 수 있기 때문에 보안 기능에 대한 면밀한 분석이 필요하다. 본 논문에서는 이러한 관점에서 ISA 100.11a와 WirelessHART 최신 표준의 분석을 통해 표준에서 보완되어야 할 보안사항과 표준에서 정의하고 있지 않아 명확하게 해야 하는 부분 등 다양한 관점에서 표준을 상세 분석하였다. 그 결과 Table 1.과 같이 각 프로토콜 스택의 보안 기능과 위협사항에 대해 도출하였다. 응용 계층의 각 동작 단계에 따라 ISA 100.11a 프로토콜에서는 총 5가지의 보안 위협과 그에 따른 보안 요구사항에 대해 제시하였으며, WirelessHART 프로토콜의 경우 총 4가지의 보안 위협과 그에 따른 보안 요구사항을 제시하였다. 향후 연구에서는 Provisioning 단계에서 사전주입 방식이나 OOB보다 더 보안이 강화된 인증을 키 교환 방법에 대해 연구를 진행할 것이다.

References

[1] B&R Industrial Automation, "Smart Factory:Industry 4.0", 2016

[2] Dr.Manjari Asawa, Brett Murphy and Sujan Bose, "Synchronized and Business-Ready Microgrid:An Industrial Internet Consortium Results White Papaer", 2017

[3] Zillner, "Tobias: White paper: ZigBee

Exploited - The good, the bad and the ugly. Technical report", Cognosec, pp. 1-6, August 2015.

〔4〕 Nixon, Mark, and T. X. Round Rock, "A Comparison of WirelessHART and ISA100. 11a." Whitepaper, Emerson Process Management (2012), pp. 1-36, July 2012.

〔5〕 Lennvall, Tomas, Stefan Svensson, and Fredrik Hekland, "A comparison of WirelessHART and ZigBee for industrial applications." 2008 IEEE International Workshop on Factory Communication Systems. IEEE, pp. 85-88, May 2008.

〔6〕 Zhang, Xuan et al., "Research and implementation of security mechanism in ISA100. 11a networks." 2009 9th International Conference on Electronic Measurement & Instruments. IEEE, pp. 4-716, August 2009.

〔7〕 Alcaraz, Cristina, and Javier Lopez, "A security analysis for wireless sensor mesh networks in highly critical systems.", IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews) 40.4, pp 419-428, April 2010

〔8〕 ANSI/ISA-100, "ANSI/ISA-100.11a-2011 Wireless systems for industrial automation: Process control and related applications", pp. 1-792, 2011

〔9〕 Montenegro, Gabriel et al, "Transmission of IPv6 packets over IEEE 802.15. 4 networks.", No. RFC 4944, September 2007.

〔10〕 Wang Gengyun, "Comparison and Evaluation of Industrial Wireless Sensor Network Standards ISA100. 11a and WirelessHART.", Master of Science Thesis, Chalmers University of Technology, 2011

〔11〕 HART Communication Foundation, "IEC-62591:Industrial networks - Wireless communication network and communication profiles - WirelessHART™", pp. 1-1043, 2016

〔12〕 Bayou and Lyes et al. "Security analysis of WirelessHART communication scheme.", International Symposium on Foundations and Practice of Security. Springer, pp. 223-238, 2016.

〈저자소개〉

정 재 한(JaeHan Jeong) 학생회원
2017년: 아주대학교 정보컴퓨터공학과 졸업(학사)
2017년~2019년: 아주대학교 컴퓨터공학과 졸업(석사)
〈관심분야〉 침입탐지시스템, 딥러닝, IoT 보안

권 성 문 (Sungmoon Kwon) 학생회원
2013년: 아주대학교 정보컴퓨터공학부 졸업(학사)
2013년~현재: 아주대학교 대학원 컴퓨터공학과 석박사통합과정
〈관심분야〉 스마트그리드 보안, 딥러닝, Anomaly Detection

손 태 식 (Taeshik Shon) 종신회원
2000년: 아주대학교 정보및컴퓨터공학부 졸업(학사)
2002년: 아주대학교 정보통신전문대학원 졸업(석사)
2005년: 고려대학교 정보보호대학원 졸업(박사)
2004년~2005년: University of Minnesota 방문연구원
2005년~2011년: 삼성전자 통신· DMC 연구소 책임연구원
2017년~2018년: Illinois Institute of Technology 방문교수
2011년~현재: 아주대학교 정보통신대학 사이버보안학과 교수
〈관심분야〉 ICS/SCADA, DFIR, Anomaly Detection