JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지 Vol. 24, No. 6: 802~808, Jun. 2020

IoT Sensor가 연결된 국방정보통신망의 사이버보안 연구

한현진[1] · 박대우[2*]

Cybersecurity of The Defense Information System network connected IoT Sensors

Hyun-Jin Han[1] · Dea-Woo Park[2*]

[1]Graduate Student, Department of Convergence Engineering, Hoseo Graduate School of Venture, 06724 Korea
[2*]Professor, Department of Convergence Engineering, Hoseo Graduate School of Venture at Hoseo University, Seoul, 06724 Korea

요 약

IoT(Internet of Things)는 센서 기술의 발전과 고속의 통신 인프라를 바탕으로 네트워크에 연결되는 단말의 수가 사람의 수보다 더 많아지고 있고 그 증가도 매우 빠르다. 기존 유선부터 무선네트워크까지 연결되는 IoT의 수가 증가하면서 동시에 사이버 위협도 증가하고 있다. 국방분야도 작전, 군수, 기지방어, 정보화 등 다양한 분야에서 IoT의 필요성은 증가하고 있다. PC/서버의 정보보호체계와는 다르게 정보보호가 취약한 IoT Sensor가 네트워크에 증가함에 따라 사이버 위협도 증가하고 있어 국방정보통신망(이하 국방망)을 보호하기 위한 플랫폼 연구가 필요하다. 본 연구에서는 유·무선 IoT를 국방망에 연결하는 사례를 알아보고 국방망과 접점을 최소화한 보안성이 강화된 IoT 통합 독립 네트워크의 효율적인 연동 설계 방안을 제시하였다.

ABSTRACT

The IoT(Internet of Things) is based on the development of sensor technology and high-speed communication infrastructure, and the number of IoT connected to the network is increasing more than the number of people, and the increase is also very fast. In the field of defense, IoT is being deployed in various fields such as operations, military, base defense, and informatization, and the need is also increasing. Unlike the existing PC/server information protection system, cyber threats are also increasing as IoT sensors, which are vulnerable to information protection, are increasing in the network, so it is necessary to study the platform to protect the defense information and communication network. we investigated the case of connecting wired and wireless IoT to the defense network, and presented an efficient interlocking design method of the IoT integrated independent network with enhanced security by minimizing the contact point with the defense network.

키워드 : 사물인터넷, 국방정보통신망, IoT 네트워크, 사이버보안, 스마트비행단

Keywords : IoT(Internet of things), Defense Information System Network, IoT Network, Cybersecurity, Smart-Wing

Received 27 May 2020, **Revised** 1 June 2020, **Accepted** 2 June 2020

*** Corresponding Author** Dea-Woo Park(E-mail: prof_pdw@naver.com, Tel:+82-2-2059-2352)
Professor, Department of Convergence Engineering, Hoseo Graduate School of Venture at Hoseo University, Seoul, 06724 Korea

Open Access http://doi.org/10.6109/jkiice.2020.24.6.802 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

4차 산업혁명 시대는 ICBMA(IoT, Cloud, Big data, Mobile, Artificial intelligence)의 혁신기술을 통한 모든 사물이 연결되는 초연결사회(Hyper-Connected), 인공지능으로 무장한 초지능사회(Hyper-Intelligence), 고속의 통신 속도를 보장하는 초고속 사회인 하이퍼월드(Hyper-World)가 될 것이다[1].

가트너(Gartner)에 의하면 2017년 이미 80억대의 기기가 인터넷에 연결됐다고 분석하고, 2020년 이후 204억대 이상까지 증가할 것으로 보고 있으며 앞으로도 다양한 분야에서 사물들이 연결을 통해 IoT(Internet of Things)는 지속해서 성장할 것으로 예상하고 있다[2].

이러한 초연결·초지능·초고속 사회에서는 단 한 번의 사이버 공격으로도 국가안보에 치명적인 위협이 될 수 있다. 이러한 환경에서의 사이버 공격은 시간과 장소에 무관하게 적용될 것이며 우리 사회가 인터넷 환경에 최적화될수록 피해 확산 속도는 빠르고 추적을 통한 공격자의 공격 거점을 찾아내기는 더 어렵다.

조직의 사이버안보 수준은 가장 취약한 부분에서의 사이버 공격 대응(준비) 능력에 따라 결정된다. 국방 분야에서 운용하는 국방정보통신망(이하 국방망)은 사이버 위협에 대응하기 위해 가장 취약한 부분인 인터넷과 분리하여 운영하고 있으나. 2016. 9월 국방망에 대한 사이버 공격은 [그림 1]과 같이 인터넷 백신 서버의 2개 LAN 카드를 통해 국방망과 인터넷망의 접점을 식별한 후 인터넷을 거쳐 국방망에 침투해 서버와 PC에 악성코드를 유포했고 자료를 탈취했다[3].

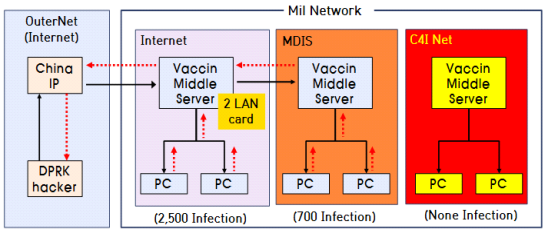

Fig. 1 Cyber-attack Type of Defense Information System at 2016.9

사전에 미식별된 국방망과 인터넷망의 LAN 카드 접점은 대응 정보보호체계 미흡과 사용자 관리 감독 부실로 조직 전체에 상당히 큰 피해를 주었다. 이후 악성코드 제거, 백신 업데이트, 망혼용 방지조치 등 침해 대응 방안을 수립하고 구축하는데 많은 시간과 노력이 소요되었다.

4차 산업혁명 기술의 발달로 온도, 이미지(영상), 습도, 압력, 속도/가속도, 가스, 초음파, 성분, 유량, 자기, 전류 등 다양한 산업 분야에서 [그림 2]와 같이 IoT Sensor 종류가 지속해서 증가하고 있다.

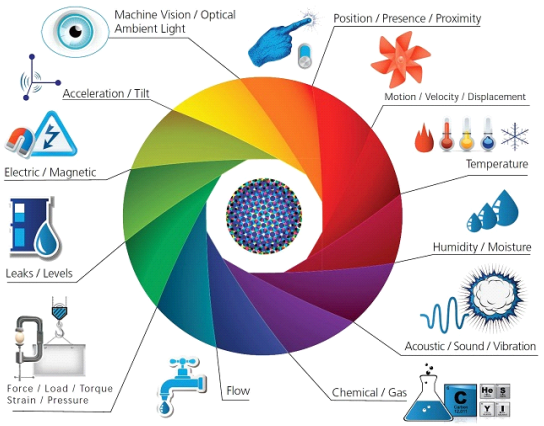

Fig. 2 Types of IoT(Source : Postscapes)

IoT 환경은 센서가 수집한 정보를 서버로 전달하고 서버가 센서를 제어할 수 있는 수준의 연결형 IoT, 서버에 인지기능을 추가하여 수집된 정보를 분석, 진단, 예측하여 사용자에게 지능적인 서비스를 제공하는 지능형 IoT, 더 발전하여 서버뿐만 아니라 센서에서도 인지기능이 탑재되는 형태의 자율형 IoT 환경으로 발전하고 있다[4].

4차 산업혁명 핵심기술인 IoT는 다양한 분야에서의 활용도 증가와 함께 국방 분야에서도 IoT Sensor 구축이 증가하고 있고 보안이 중요한 이슈가 되고 있다. 다양한 IoT Sensor를 인터넷에 연결 시, 사이버 공격을 통해 내부 센서 정보가 외부로 유출될 수 있다. 따라서, 기지 내 IoT Sensor를 국방망에 연결해 운영하였다.

하지만, 국방망은 유선 네트워크를 기반으로 PC/서버(Personal Computers/Servers) 중심의 다양한 정보보호 장비를 구축하여 사이버보안체계를 발전시키고 있다. 다양한 유·무선 IoT Sensor를 국방망에 연결하는 것은 또 다른 취약한 위협이 되는 상황으로 자리하고 있다. 결과적으로 기지의 각 IoT Sensor들은 사이버 공격의 주요 표적이 될 수 있다.

따라서 국방 분야에서도 IoT, Cloud, Big data,

Mobile, AI 등 4차 산업혁명 기술들을 응용한 무기체계에는 Sensor가 필수적으로 포함되므로 IoT Sensor를 네트워크에 연결 시 사이버보안에 관한 연구가 필요하다.

본 연구에서는 IoT Sensor의 유/무선보안 취약점을 분석하고 국방망과 연결된 접점을 최소화한 보안성이 강화된 IoT 통합 독립 네트워크 플랫폼을 제시한다.

Ⅱ. IoT의 사이버 공격 위협 및 취약점

IoT Sensor 네트워크에 대한 사이버 공격 위협 및 취약점을 분석이 필요하다. IoT Sensor를 활용한 공군의 지능형 스마트비행단 추진내용을 통해 국방망과의 연동 접점 최소화로 사이버 위협에 대응하는 사례를 알아보고, IoT Sensor가 가지고 있는 보안 취약점 분석을 통해 사이버 공격으로부터 보안성을 강화하기 위한 보안 요구사항을 알아본다.

2.1. 공군 지능형 스마트비행단의 IoT 운영

국방부는 2017년부터 『지능형 스마트비행단』 시범구축 1단계 사업을 통해 「정보통신체계 및 장비 기술 표준화와 상호운용성 확보」를 위해 '기술표준서'를 제작하고, 2018년부터 2단계 사업으로 「정보공유 및 상황통제 능력 신장」을 위해 정보통신체계 및 장비의 연동능력을 갖추어 네트워크 구조를 최적화하고, 기지 내 CCTV와 C4I를 연동해 지휘통제실에서 모든 상황을 시각적으로 통제할 수 있는 '지휘 결심 가시화 체계'를 구축했다. 또한 '다목적 전술 통제 LTE 체계'를 구축해 이동 중 지휘 통제 능력을 보강하고, 상용 모바일기기의 촬영 및 녹음을 방지하는 보안체계를 설치했다.

향후 3단계 사업은 [그림 3]과 같이 「4차 산업혁명 기술 기반 지능형 스마트비행단 완성」을 위해 인공지능과 빅데이터 기술 기반 '지휘결심지원체계'를 구현하고 스마트 관제탑을 통해 효과적인 항공기 관제를 지원하며 드론을 활용한 기지 경계 및 조류퇴치 등 기지작전을 지원하는 체계 등 다양한 IoT를 통합하고 통제되는 체계를 구축한다[5].

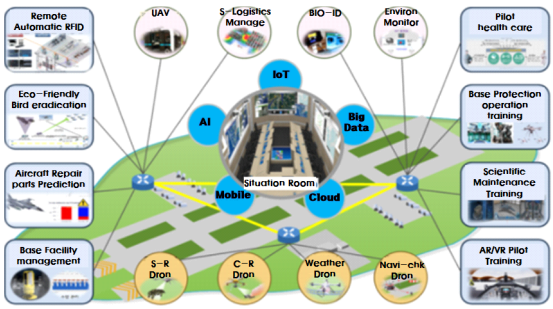

Fig. 3 Concept of Intelligent Smart Wing(Source : cndnews)

2.2. IoT Sensor의 보안 취약성 분석

IoT Sensor들이 물리적인 환경과 연동되는 과정에서의 보안 취약성 및 IoT 다비이스 자체의 보안 결함에 따른 무력화, 오용, 작동 정지, 기기 손상 등 다양한 증상이 발생 할 수 있다.

이러한 IoT의 취약점은 해당 IoT 기기와 직간접적으로 연동되는 타 IoT 기기와 전체 네트워크 작동에도 영향을 미치게 된다. IoT Sensor 제품에 대한 다양한 보안 취약점이 보고되고 있으며, 실질적으로 IoT 제품이 해킹을 당한 사례 또한 다수 보고되고 있다.

2016년 10월 깃허브(GitHub), 페이팔(PayPal), 스포티파이(Spotify), 트위터(twitter) 등 주요 웹 서비스 중단을 일으켰던 연쇄적인 DDoS(Distributed Denial of Service) 공격이 DNS 서버를 대상으로 발생했는데 해당 공격은 전 세계의 수많은 취약한 IoT 기기로 인해 가능했다[6].

IoT Sensor는 영상, 신호 등 형태별 운용, 소형화, 다량 운용, 저렴한 생산단가 등에 따라 여러 보안 취약요소가 존재한다. 만약, 유·무선 통신 모듈이 평문으로 인터페이스가 구성되면 중요 수집데이터를 평문 상태에서 전송하게 될 것이고 이는 보안상 문제를 초래한다. 또한, 네트워크에 암호화를 지원하더라도 IoT 기기 간 통신을 위한 최신 업데이트를 적시에 지원받기 어려운 문제도 발생한다. IoT 기기 암호화 소프트웨어 버전의 차이로 통신에 문제가 발생 할 수 있다[7].

IoT Sensor에 직접 제어정보를 수정하기 위해 원격접속을 사용하고 있으나 보안상에 문제가 발생 할 수 있다. 이런 경우 적은 기기를 정상 작동하지 않게 하거나, 기기 자체를 무력화시킬 수 있다. 또한, 중요 데이터를 평문으로 저장하게 될 때 인가되지 않은 자가 데이터에 접근하여 정보를 탈취/조작하게 될 수 있다. 따라서 해킹 방지를 위해 IoT의 중요한 데이터는 반드시 암호화하여 보관하여야 한다[8].

무선 센서 네트워크(Wireless Sensor Networks, WSNs)

는 원하는 지역에 다량의 Sensor들을 배치하고 정보를 수집하여 중앙시스템(서버)에 전송하는 것으로 미리 정해진 위치에 계획적으로 배치되기보다는 무작위로 정해지는 경우가 많다. 이러한 Sensor들의 정확한 위치정보를 획득하기 위해 거리 정확도를 측정하는 연구도 다양하게 진행되고 있다[9].

다양한 IoT Sensor의 많은 수량 운영으로 인해 분실이나 적에 의한 탈취 가능성도 있다. Sensor 분실의 경우는 기기 내부에 포함된 정보 유출로도 이어질 수 있다. Sensor의 네트워크 접속 불가 또는 미연결 Sensor 확인을 위한 상황 인지(Context-Awareness)는 전체 네트워크의 성능을 관리하는 중요한 요소이다.

IoT Sensor를 대상으로 한 서비스 거부(Denial of Service) 공격이 발생할 수 있다. 악의를 가진 공격자가 대량의 연결요청을 지속해서 전송하는 것으로 서비스 거부 공격을 일으킬 수 있으며, 이러한 공격에 따라 기기 자체의 전력 소모와 결과적으로 정상적인 서비스가 이루어지지 않도록 할 수 있다[10].

따라서 IoT 보안기기의 보안을 위해서는 올바른 기기에서 보내진 자료인지 식별 및 인증하는 절차가 있어야 한다. 각 IoT에 대한 상황 인지 기반으로 운용하여 기기 오작동 시 신속하게 대응할 수 있어야 한다. 또한, 반드시 인가된 응용체계로만 접속이 허용되도록 통제해야 한다. 특히 무선 IoT 접속은 응용체계 하위 레벨에 설치된 보안장치를 거치도록 설정이 필요하다. 표 1과 같이 단말·네트워크·애플리케이션에서의 보안 요구사항 확보가 필요하다.

Table. 1 Security requirements of IoT

Title		Requirement of security
Normal	Terminal	Confidentiality, Integrity, Authority setting, Certification, Access control,
	Network	Confidentiality, Integrity, Authority setting, Certification,
	Application	Confidentiality, Integrity, Authority setting, Privacy, Security check, Vaccine
Special	Special field requirements such as mobile payments	

특히 국방망에 연결된 IoT Sensor의 보안 취약점은 조직 전체에 치명적인 영향이 발생함으로 네트워크에서 인증과 무결성을 보장하기 위한 대책에 관한 연구가 필요하다.

Ⅲ. IoT Sensor 연동 네트워크 분석

기존 네트워크에 IoT Sensor 네트워크를 연동하는 방법에 관해 설명하고 방안별 분석을 통해 효율적인 IoT 네트워크와 연동방안을 설계한다.

3.1. IoT와 기존 네트워크 직접 연결 분석

기지 내 대표적인 IoT인 CCTV는 다수의 단말기로부터 영상정보를 수집하고 기지 내부에서 활용하거나 원격지로 정보를 제공하기 위해 국방망에 직접 연결되어 있다. IoT Sensor에서 생산된 영상정보는 국방망에서 실시간 수집, 시현되고 저장된다. 또한, 원격지 기지에서 수집된 정보를 수신하는 경우에도 네트워크를 통해 전송받는다. [그림 4]는 기존 네트워크에 연결된 유·무선 IoT Sensor 네트워크를 보여 준다.

기존 네트워크에 유·무선 IoT 센서 네트워크가 직접 연결되어 있어 기지 내 및 외부 기지에서도 수집된 정보를 활용하게 된다.

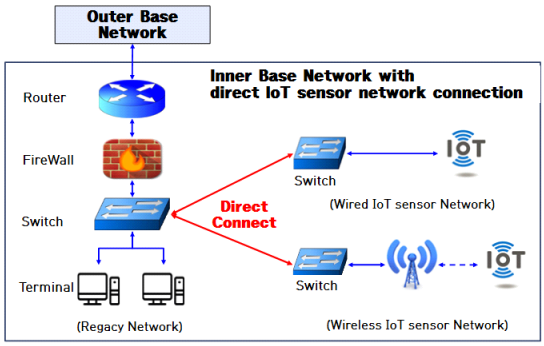

Fig. 4 Integrated IoT Sensor and Legacy network

하지만 앞에서 언급한 것처럼 국방망은 PC/서버를 기반으로 네트워크 최적화 및 정보보호체계를 구축해 왔으며 IoT Sensor 네트워크의 직접 연결을 통한 접점의 증가와 기기의 취약점은 새로운 취약요소로 식별되었다.

3.2. VPN을 통한 IoT Sensor 연결 분석

IoT가 직접 연결된 국방망을 보호하기 위해 VPN (Virtual Private Network) 장비를 추가하여 안전한 가상통로를 생성해 IoT 네트워크를 통합 운영한다.

하지만 VPN 운영하는 방식은 몇 가지 제한사항이 있다. 첫째로 VPN의 해킹 가능성이다. 미 NSA의 알렉스

할더맨(Alex Halderman)과 나디아헤닝어(Nadia Heninger)는 VPN에서 사용되는 디피헬만 알고리즘을 공격하여 HTTPS, SSH, VPN 트래픽을 해독할 수 있는 능력을 개발했음을 발표[11]하기도 했다. 둘째로 국방망과 IoT 네트워크가 동일 대역의 IP 네트워크를 운영하게 되고 취약한 IoT Sensor는 VPN을 통해 국방망에 직접 접속하게 된다. VPN은 원거리 네트워크에서 기밀성은 보장하지만, IoT Sensor가 가지고 있는 취약점을 해결해 주지는 못한다. 또한, 다양한 분야별 IoT 네트워크를 구축함에 따라 국방망과의 접점은 계속해서 증가하게 된다. 셋째로는 비용의 증가이다. IoT 네트워크는 분야별로 소요에 따라 구축하기 때문에 [그림 5]와 같이 다수 IoT 네트워크별 VPN 구축 비용이 지속 발생하게 된다. 또한, 기지 내부 네트워크는 유선 구간의 물리적 침해위협이 적기 때문에 내부구간에 VPN 운용을 통한 데이터 암호화는 큰 의미가 없다.

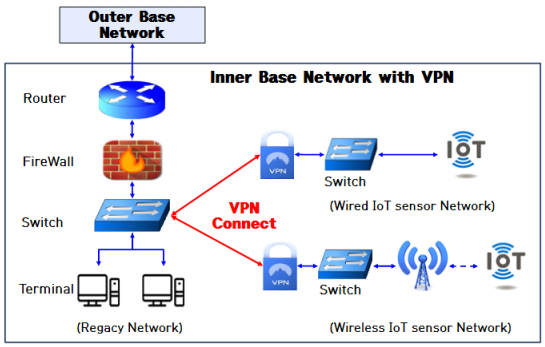

Fig. 5 Integrated IoT Sensor and Legacy network with VPN

Ⅳ. IoT 통합 네트워크 플랫폼 구축

IoT Sensor를 국방망과 분리하여 모든 IoT를 통합한 독립 네트워크를 구축하는 것은 보안성 강화를 위해 중요한 요소이다. 보안을 강화하고 수집된 정보를 활용 할 수 있게 기지 내 모든 IoT를 통합한 네트워크 플랫폼 구축을 제안한다. [그림 6]은 먼저 다양한 분야에서의 유무선 IoT 통합 독립 네트워크를 구성하고 네트워크에 연결된 Sensor에 필요한 보안 요구사항을 구축하고 원격지 통제부서에서도 수집된 정보를 활용할 수 있도록 연동 접점을 단일화한다.

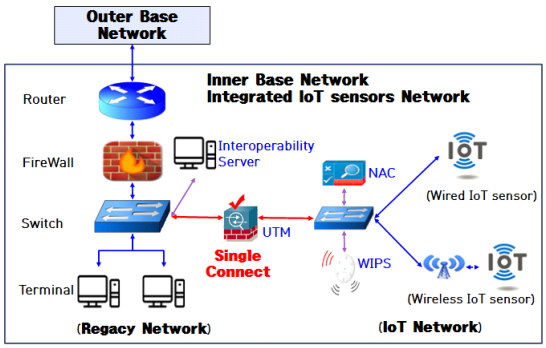

Fig. 6 IoT Sensor Integrated network and only one connection with Legacy network

4.1. IoT Sensor 통합 독립 네트워크 설계

IoT Sensor는 유·무선망 분리를 채택하여 국방망·인터넷과 물리적으로 분리된 지역 내 모든 IoT Sensor를 통합하는 독립망 구축을 우선 제안하다.

현재에도 IoT Sensor는 국방망이나 Sensor별 소규모로 독립망에서 운영하고 있다. 또한, 다양한 분야에서 추가적인 IoT 도입이 증가하고 있어 독립된 네트워크 장비를 연결한 기지 내 IoT 통합 독립망 구축이 무엇보다 선행되어야 한다. 통합 독립망 구축이 늦어질수록 기존에 국방망 또는 소규모 독립망에 구축된 IoT Sensor들을 통합 독립망으로 이전시키는 시간과 비용은 더 증가하게 된다.

IoT Sensor를 통합하는 독립망 구축은 계획수립, 예산확보, 장비도입, 망 구축, 정보보호체계 확보, 망 관리 유지보수 등 노력과 비용이 소요되더라도 다음 몇 가지 장점이 있다. 먼저 네트워크에 연결된 모든 IoT Sensor를 모니터링 할 수 있다. 둘째 IoT Sensor들의 체계적인 IP 관리가 가능하다. IoT Sensor 구축은 다양한 분야에서 대규모 구축보다는 소규모 비용으로 진행되는 만큼 지역별로 통합 독립 네트워크가 구축되어 있으면 네트워크에 Sensor 분야별로 IP를 부여하고 NAC를 통해 인증·통제할 수 있다. 셋째 독립망에 정보보호체계 확보를 통해 네트워크별로 구축되어야 하는 정보보호체계 구축 비용을 절감할 수 있다. IoT Sensor의 보안 요구사항을 Sensor가 구축되는 시기마다 확보하지 않고 통합해서 체계적인 정보보호체계를 확보해 나갈 수 있다. 이를 통해 독립망의 보안 안정성 및 정보보호체계 확보 비용을 절감할 수 있다.

4.2. IoT 네트워크 사이버보안 설계

통합 단독 네트워크에 참여하는 IoT Sensor 및 노드들의 IP주소 체계 부여는 유선체계, 무선 AP 대역, 연동 서버 대역, 정보보호체계 대역을 구분하여 설정한다. 구분된 IP 대역을 통해 사이버 위협에 대한 인식 및 대응 방안을 빠르게 식별할 수 있다.

분야별로 구축된 유·무선 IoT 통합 독립 네트워크의 보안 요구사항을 확보하기 위해 네트워크접근통제장비(Network Access Control: NAC), 상호연동서버, 통합위협관리장비(UTM), 무선침입차단시스템(Wireless Intrusion Protection System: WIPS) 등의 정보보호 조치가 필요하다.

네트워크접근통제장비를 통해 네트워크에 물리적으로 비인가 접근하는 유·무선 단말을 차단하다. 상호연동서버를 통해 IoT 네트워크를 통해 국방망과 교환되는 수집정보를 제어한다. 통합위협관리는 사전 인가된 단말에서만 내부 접속을 허용하고 접속 대상 서버에는 운용하는 포트로만 데이터가 송·수신될 수 있도록 허용한다. 무선 IoT Sensor는 보안을 강화하여 네트워크를 구성하는 것이 필요하다. Sensor는 사전 등록 후 고정 IP를 할당받아 운용한다. 무선 접속장치(Access Point: AP)는 WPA2-CCMP(AES) 이상 보안성을 가진 방식으로 암호화하고 AP 접속을 위해 무선침입차단시스템을 운영한다. 이를 통해 사전 등록된 인가 단말만 허용하는 방식으로 무선환경을 통제하고 관리자가 모니터링 할 수 있도록 한다.

4.3. 국방망과 IoT 네트워크 연동 설계

수집된 IoT Sensor 정보를 기지 내에서 사용하는 경우 외에 원격지까지 정보를 제공하고 기지별 데이터를 종합하여 Bigdata 및 AI 분석을 위해 IoT 통합망을 구축하는 것은 비용이 대폭 증가하게 된다. 이를 위해 기존 국방망과 IoT 통합 독립망을 단일접점으로 구성한다.

상호연동서버, UTM 또는 방화벽을 구축하여 네트워크가 허용되지 않은 정보가 IoT Sensor 네트워크 외부로 유통되지 않도록 차단한다. 인가된 단말과 허용된 포트만 데이터를 송·수신 할 수 있도록 최소화한다.

IoT Sensor 네트워크를 국방망과 연결하는 방법으로는 직접 연결, VPN 이용하는 방법 및 모든 IoT를 통합하여 독립 네트워크를 구성하고 연동 접점을 단일화하는 플랫폼을 제안하였으며 각 방안별 장단점 비교는 표 2와 같다.

Table. 2 Security Comparison of IoT Sensor networks.
X Inadequate, △ Middle, ○ Equipped

Title	Direct Connect	VPN	Offer platform
Confidentiality	×	○	○
Integrity	×	△	○
Availability	○	○	○
Access control	△	△	○
Certification	△	△	○
Maintenance cost	×	×	○

기존 방식은 국방망과 IoT별 다접점 연결 구조와 Sensor 기기 취약요소에 따라 보안의 3요소 중 기밀성과 무결성에서 취약하고, 제안 방식은 단일 연동 접점과 연동 서버를 통해 보완된 것으로 분석하였다. 접근통제, 인증은 모든 방식에서 NAC를 운영하나, 제안 방식에서 단일접점에 연동 서버, UTM, WIPS를 통해 강화되었다. 망 구축 및 유지비용은 기존 방식에서는 신규 구축되는 IoT Sensor 별 독립망 인프라 및 사이버 방호체계 확보에 따른 비용이 중복 및 증가하는데, 제안 방식은 통합 독립망을 구축하고 IoT를 추가하는 것으로 비용이 절감되는 것으로 분석하였다.

제안하는 IoT Sensor 통합 독립망 플랫폼은 NAC, UTM 등 정보보호체계를 구축하여 보안성을 강화하고 국방망과 연동 접점을 단일화하여 IoT Sensor 환경을 만들 수 있다.

Ⅴ. 결 론

본 논문에서는 IoT Sensor에 대한 공격 위협과 취약점을 분석하였다. 그 결과 IoT Sensor와 연결된 무선망과 유선망에서 보안성 강화방안을 제시하였다. 보안이 강화된 IoT 환경을 위해 IoT 통합 독립 네트워크를 구축한다. 이를 기반으로 원거리 기지에서 IoT Sensor의 수집정보를 공유하고 분석하기 위해 국방망과 접점을 단일화하고 접점에 대한 보안이 강화된 연동 플랫폼을 제시하였다.

향후 연구로는 IoT 보안성 강화방안과 자율형 IoT 증가에 대비한 AI를 통한 상호 신뢰가 확보된 사이버보안에 관한 연구가 필요할 것으로 보인다.

REFERENCES

[1] U. S. Choi, *The rulers of future after 4th Industrial Revolution*, Business Books Press, 2019.

[2] J. S. Kim, *How to connect all things of Hyper-connect society*, Wikimedia Press, 2019.

[3] J. J. Lee, Hacker penetrates internal network through Defense Data Center [Internet]. Available: https://www.yna.co.kr/view/AKR20161207026700014.

[4] S. L. Yu, K. M. Lee, Y. S. Yun, and J. M. Hong, "An Autonomous IoT Programming Paradigm Supporting Neuromorphic Models and Machine Learning Models," *Journal of the Korean Institute of Information Scientists and Engineers*, vol. 47, no. 3, pp. 310-318, Mar. 2020.

[5] S. H. Kim, Intelligence Smart Wing construction phase 2 [Internet]. Available: http://m.cndnews.co.rk/226712.

[6] K. Sheridan, New IoT Botnet Discovered 120K IP Cameras At Risk of Attack [Internet]. Available: https://www.darkrading.com/attacks-breach es/new-iot-botnet-discovered-120k-ip-cameras-at-risk-of-attack/d/d-id/1328839.

[7] D. H. Lee and N. J. Park, "Institutional improvements for security of IoT Devices," *Korea Institute of Information Security And Cryptology*, vol. 27, no. 3, pp. 607-615, Jun. 2017.

[8] D. H. Lee and N. J. Park, "IoT Secure Identification and Security management," *Korea Institute of Communication Sciences*, vol. 33, no. 12, pp. 28-34, Nov. 2016.

[9] H. J. Han and T. W. Kwan, "A Method to Improve Location Estimation of Sensor Node," *Korea Institute of Communication Sciences*, vol 34, no. 12, pp. 1491-1497, Dec. 2009.

[10] D. H. Lee, S. W. Yun, and Y. P. Lee, "Security for IoT Service," *Korea Institute of Communication Sciences*, vol. 30, no. 8, pp. 53-59, Jul. 2013.

[11] vpn-Mentor, Can I VPN Hacking [Internet]. Available: https://ko.vpnmentor.com/blog/vpn.

한현진(Hyun-Jin Han)

호서대학교 벤처대학원 박사과정
국방대학교 전산정보학과 석사
※ 관심분야 : 센서네트워크, IoT, 사이버보안, 블록체인

박대우(Dea-Woo Park)

호서대학교 벤처대학원 교수
※ 관심분야 : Hacking, 포렌식, CERT/CC, 침해사고 대응, 국가사이버보안, 정보보안, 이동통신보안