IoBT 네트워크 환경에서 작전 영역의 보안 대응 체계 연구

강해영*, 이제민**, 김유경*, 고명현*, 이경호*
*고려대학교 정보보호대학원 정보보호학과
**고려대학교 정보보호연구원
haeyee@korea.ac.kr, jeminjustinlee@korea.ac.kr, rladb1125@korea.ac.kr,
mhgo@korea.ac.kr, kevinlee@korea.ac.kr

Evaluating the Operational Capabilities and Security of the IoBT Network Architecture

Hae-Young Kang*, Jemin Justin Lee**, Yu-Kyung Kim*, Myong-Hyun Go*,
Kyungho Lee*
*Institue of Cyber Security & Privacy, Korea University
**Center for Information Security Technology

요 약

IoBT시장은 2023년까지 317억 달러로 성장할 것으로 예측되며, 센서 및 웨어러블 디바이스와 같은 IoBT 장비의 수가 급격히 늘어나고 있다. IoBT 장비들로부터 수집된 생체 정보와 같은 민감한 데이터를 효율적이고 안전하게 처리하기 위해 많은 노력이 필요하다. 하지만 초경량화, 저전력화된 IoBT 장비들은 보안적인 측면에서 취약한 상황이다. 본 논문은 Fog computing을 적용하여 전장과 지휘관 사이에서 결심 및 통제에 필요한 시각화 자료를 신속하게 제공하고 IoBT 장비의 보안 사항과 공격에 따른 완화 기법을 수행할 수 있는 새로운 네트워크 아키텍처를 제공하고자 한다.

1. 서론

최근 방대하게 늘어나고 있는 Wireless Sensor는 사회 전역으로 스며들어 여러 분야에서 IoT를 접목한 영역이 복잡해지고 있다. 또한 각 분야의 IoT 환경이 완벽하게 적용되지 않아 취약점들이 발생하고 있다. 이에 따라 IoT를 각 분야의 요구사항에 맞추어 적용하기 위한 연구가 진행되고 있다 [1][2]. 군 영역에서도 통신장비와 네트워크 기술에서의 보안적 요소, 병력 및 장비 관리, 전장에서 향상된 시야 확보 등을 위해서 IoBT(Internet of Battlefield Things)에 관심이 집중되고 있다 [3].

최근 미군은 Alliance for Internet of Battlefield Things Research on Evolving Intelligent Goal-driven Networks(IoBT REIGN)에게 2500만 달러(한화 약 282억 원)를 전장 분석 분야에 투자했다 [4]. 2016년 NATO는 IST-147 연구과제 그룹을 편성하여 안전한 IoBT 환경을 구축하기 위해 IoBT 장비 도입 과정에 검증과 검토과정이 필요하다고 제안했다 [5]. CCDCOE는 향후 near-peer adversary에 대응하기 위해서 IoBT를 인공지능(AI, Artificial Intelligence) 및 지휘 통제(C2, Command and Control)와 함께 활용해서 임무를 수행해야 할 것이라고 언급했다 [6].

APT(Advanced Persistent Threat) 그룹 등장과 함께 육상, 해상, 공중, 우주 영역뿐만 아니라 사이버공간까지 군 영역으로 포함하였다. 사이버 공간에서 공격하는 APT 그룹이 늘어남에 따라 정보공유의 중요성이 대두되고 있다 [6][7]. 정보공유를 기반으로 한 의사결정을 하기 위해서는, IoBT 체계의 각기 다른 센서 및 장비들이 자율성을 기반으로 AI 및 C2를 함께 사용해야 효율적인 의사결정을 할 수 있다 [8].

본 논문은 IoBT 환경의 취약점에 대응하기 위해 Fog computing을 적용한 새로운 네트워크 아키텍처를 제시한다. 그리고 CTI(Cyber Threat Intelligence) 기반으로 APT 그룹의 전술, 기술, 절차(TTPs, Tactic, Technique, Procedures)를 분석하는 MITRE의 ATT&CK(v.8.2)을 활용하여 Fog computing을 활용한 대응방안을 제시한다. 2장은 IoBT의 보안 및 네트워크에 관련한 선행 연구를 분석하고, 3장은 IoBT 환경에 Fog computing을 접목시켜 TTP를 분석한 결과에 대해 설명한다. 4장은 결론 및 추후 연구에서 진행할 부분을 설명하고자 한다.

2. 선행 연구

IoT에서 발생하는 취약점을 제거하고 보안 요구사항을 갖추기 위한 연구는 각 분야에서 활발히 진행되고 있다. Park & Lee [1]는 스마트시티의 방대한 양의 데이터 보안시스템에 대한 이상 탐지 접근 방식을 IIoT(Industrial Internet of Things) 분야로 확장하는 연구를 진행하였다. Min et al. [2]은 IoT 장비의 취약점을 악용한 비정상적인 활동과 거래문제를 해결하기 위해 RNN(Recurrent Neural Network) 및 LSTM(Long Short-term Memory)과 같은 시계열 알고리즘을 사용하여 이상행위를 방지하는 SafeZone을 제안했다.

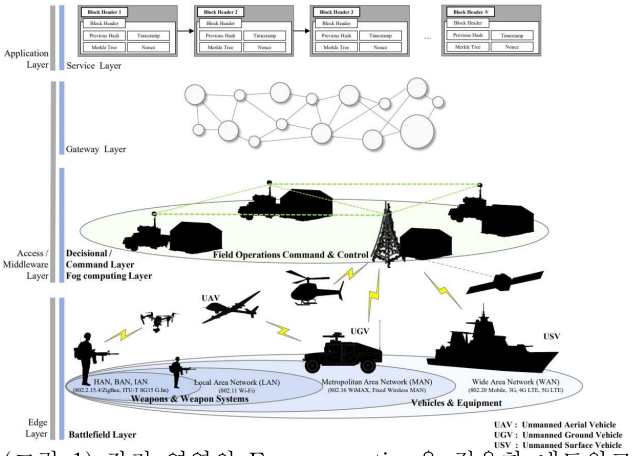
센서 및 장비가 급격히 늘어남에 따라 기존대비 데이터량이 폭증하는 상황으로 인해, 프로빙, 스누핑, 핑거프린팅 등 공격기술로 인한 Cellular, WiFi, Bluetooth와 같은 사이버물리(Cyberphysical) 자산들의 취약점이 드러나고 있다 [8]. 그러므로 네트워크 기반시설을 보호할 수 있는 데이터 필터, 엣지 디바이스 규제와 같은 대응책이 필요하다.

이를 위해 군 영역에서는 IoBT가 새롭게 도입되었으며, 추가적으로 IoBT는 의사결정 및 MDO(Multi-Domain Operations)에 중요한 역할을 할 것이다 [8][9]. 급격히 늘어나는 무인기기(UxVs, Unmanned Air, Ground, Sea, and Space Vehicles) 기반인 군의 임무 수행 중 사이버 레질리언스를 개선하기 위해 IoBT가 중요한 역할을 할 것이라고 많은 연구를 통해 그 중요성이 강조되고 있다 [9].

Doku et al. [10]에 따르면 IoBT 네트워크는 장비들의 낮은 리소스로 인한 패킷 손실률이 높아서, 이를 보완하기 위해 블록체인 및 NDN(Named Data Newtork)을 활용하여 문제점을 해결하고자 했다. 이 연구에서는 노드의 성격상(드론, 전차 등) 네트워크를 군집화할 수 있는데 이를 기반으로 IoBT 환경에서 사용하는 노드 중 30개를 무작위로 선택해서 군집화했을 때와 하지 않았을 때로 구분하여 패킷 손실률을 비교 분석했다. Azmoodeh et al. [11]은 멀웨어 분류 알고리즘을 분석하기 위해 Intel Core i7 2.67GHz 및 8GB RAM을 활용해서 MATLAB R2015a를 기반으로 비교분석을 했다. 이 연구는 정크코드 삽입 공격에 대응할 수 있는 IoBT 멀웨어 탐지 방식 중 고유공간 학습 접근법을 활용해서 멀웨어 정확도를 98.37%, 정밀도를 98.59%로 탐지할 수 있는 새로운 탐지 기법을 제시했다. Tosh et al. [12]은 IoBT 장비의 대규모 및 분산된 특성으로 인한 여러 보안 문제를 해결하기 위해 블록체인을 적용한 3계층 IoBT 아키텍처를 제안했다. 이 연구는 IoBT 네트워크를 전장 계층, 네트워크 계층, 서비스 계층으로 구분하여 각 계층별 역할을 나누고 관련된 연구과제에 대해 논의했다.

Tuli et al. [13]은 블록체인을 적용한 IoT 환경은 다수의 IoT 장비가 동시에 인터넷을 통해 데이터를 전송할 때, 네트워크 혼잡이 발생할 수 있다고 지적함에 따라 Fog computing을 IoT에 접목하는 방안을 연구했다. 이 연구에서 Fog computing을 활용하여 서로 다른 IoT 장비를 지원하며 서비스 지연 및 네트워크의 정체를 줄이고 QoS를 증가시킬 수 있다는 점을 강조했다. Bonomi et al. [14]은 Fog computing을 말단 장비와 클라우드 컴퓨팅 데이터 센터 사이에서 계산, 저장, 네트워킹 서비스를 제공하는 플랫폼으로 정의했으며, 수집된 데이터 중 로컬에서 사용할 데이터를 필터링하여 시각화를 다루는 개념으로 제안했다.

현재 IoBT 장비들의 수집 데이터는 무선통신, 영상 및 음성 등의 정보이지만, 향후 미래에는 생체신호 모니터, 광범위한 영상 및 음성, 생체 인증 정보 등을 수집하게 되면서 접속 가능한 기기의 수가 기하급수적으로 늘어나는 문제를 기존의 클라우드 형태의 네트워크에서는 지원하기에는 한계점들이 존재한다 [14]. 이러한 한계점을 Fog computing은 장비와 사람 사이에서 데이터 필터링, 압축, 시각화 표현을 통해 수용 가능한 형태로 변환하는 작업을 수행한다. 그리하여 전장에서 무수히 많이 생성되는 서로 다른 형태의 정보를 일관된 형태와 시각화한 자료를 제공하게 되고 지휘관이 방향성을 잃지 않고 신속한 결심 및 통제할 수 있도록 보장한다.



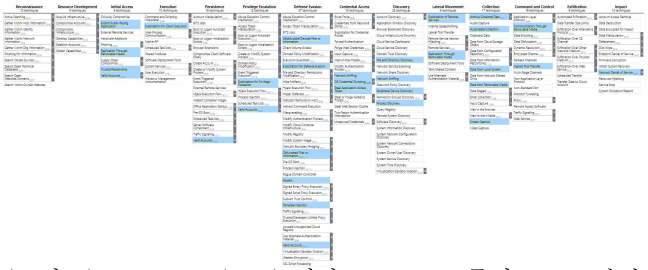
(그림 1) 작전 영역의 Fog computing을 적용한 네트워크 아키텍처

3. 분석 및 평가

군은 '국방개혁 2.0' 아래 스마트한 군사력 운용을 위한 무기체계 지능화와 스마트 병영환경을 조성하고 있어 군 영역 중 사이버공간이 확장되고 있다. AI, 빅데이터 등을 활용한 사이버공간에서의 우위 확보에 노력하고 있지만, IoT 장비와 최첨단 무기체계가 도입됨에 따라 보안 위협이 증대되고 있다.

또한 IoBT를 한국 전장에 적용시키기 위해 제한된 환경을 극복해야 한다. 산악지형이 많은 한국 전장 지형에서는 LoS(Line of Sight)를 확보해야 정상적인 네트워크를 구축할 수 있다. 그러나 LoS를 확보하기 어려운 초경량화 및 저전력화된 IoBT 장비로는 원활한 네트워크를 구축하기 어렵다. 이를 보완하기 위해 현장에 본 논문은 비교적 많은 리소스와 통신능력을 보유하고 있는 중계소, 차량통신소 등이 위치한 전장에 Fog computing 개념을 도입하는 것을 제안한다. 다양한 센서들의 전송량, 상호 운용성을 개선할 수 있고, 전송 출력의 감소로 인한 장시간의 작전능력을 확보할 수 있다.

본 연구에서는 블록체인과 Fog computing을 IoBT에 적용하여 (그림 1)과 같은 네트워크 아키텍처를 제시한다. Battlefield 계층은 UxVx, 생체 신호, 무기체계 및 각종 장비의 데이터를 전송하게 된다. Computing, 암호화 등의 보안 작업은 초경량화, 저전력화된 Battlefield 계층의 IoBT 센서 및 장비에는 다소 제한적이다. 그러므로 Fog computing 계층에서 이러한 보안 작업을 수행하고, IoBT 장비의 리소스 절약 및 보안적 이점을 확보할 수 있다. Fog computing 계층은 인접한 중계소, 차량통신소 등의 위치에서 데이터를 처리하며, 이기종 간에 상호 운용성을 보장하고, 보안기능을 담당한다. 블록체인 합의를 담당하는 지휘소 등의 노드와 Battlefield 계층의 IoBT 장비 사이에서 Fog computing 계층은 수집된 데이터를 계산하고 결심 및 통제에 용이한 형태로 가공하여 지휘관에게 시각화자료를 제공한다. Gateway 계층에서는 블록체인 합의에 참여하는 노드로 데이터를 전송한다. Fog computing 계층에서 데이터가 가공되어 다수의 연결로 인한 네트워크 트래픽 과부하 등의 문제를 해소할 수 있다. Service 계층은 블록체인 합의 메커니즘을 사용하여 데이터를 블록체인 트랜잭션에 추가하게 된다. 이를 통해 IoBT 장비의 부담을 Fog computing을 통해 분담하고 서비스 응답속도와 무결성을 확보할 수 있어 적대적인 전장 환경에서 작전역량을 발휘할 수 있다.



(그림 2) ATT&CK(v8.2) 기반 APT28 그룹의 IoBT 관련 TTPs

<표 1> IoBT 계층 별 TTP 분석

ATT&CK TTP (Mitigation)	Edge Layer	Battlefield Layer	Fog computing Layer
Exfiltration Over Other Network Medium T1011 (M1028)	-	-	○
Vaild Accounts T1078 (M1013)	○	○	○
Endpoint Denial of Service T1499 (M1037)	○	○	○
Man in the Middle T1557 (M1041, M1035)	-	-	○

○ : Applicable, - : Non-applicable

MITRE의 ATT&CK(v8.2)을 기반으로 IoT 환경을 공격한 APT 그룹을 분석한 결과 (그림 2)와 같이 APT28 그룹의 TTP를 분석했다. 이에 대응하기 위해 개발자 지침(M1013)과 같은 완화기법으로 대응할 수 있다. 분석한 TTP를 <표 1>과 같이 기존 IoT 계층과 본 논문에서 제안한 네트워크 아키텍처 계층별로 분석하였다. 적은 리소스를 지닌 Edge 계층의 IoBT 장비에서는 Exfiltraion Over Other Network Medium (T1011) 등의 공격이 예상되는 반면 완화 기법인 User Account Management (M1028) 등을 수행하는데 제한사항이 발생하는 것을 확인했다. 하지만 Battlefield 계층에 Fog computing 계층을 도입하여서 그 완화 기법을 수행하도록 분석한 결과 보안적 측면에서 Fog computing 메커니즘으로 해결할 수 있었다.

4. 결론 및 추후 연구

본 논문은 작전 영역에서 IoBT 환경의 보안 취약점을 분석했으며, 이를 해결하기 위하여 Fog computing을 적용한 새로운 네트워크 아키텍처를 제시했다. 그리고 MITRE의 ATT&CK(v.8.2)을 통해 IoBT 환경에 대한 APT28 그룹의 TTP를 계층별로 분석하여, Fog computing 계층을 적용했을 때 적용가능한 완화기술을 제시했다.

추후 연구에서는 IoBT를 구성하는 각 계층(Battlefield, Fog computing, Gateway, Service)별

자산들을 보호하기 위한 위험관리를 실시하고, MITRE의 ATT&CK(v.8.2)을 기반으로 적대적 캠페인 및 플레이북을 분석하여 계층별 적용 가능한 지휘관의 의사결정 프레임워크를 만들고자 한다.

5. Acknowledgements

본 연구는 방위사업청과 국방과학연구소의 지원으로 수행되었습니다 (UD190016ED).

참고문헌

[1] Park, S., & Lee, K. (2021). Improved Mitigation of Cyber Threats in IIoT for Smart Cities: A New-Era Approach and Scheme. *Sensors, 21*(6), 1976.

[2] Min, M., Lee, J. J., Park, H., & Lee, K. (2021). Detecting Anomalous Transactions via an IoT Based Application: A Machine Learning Approach for Horse Racing Betting. *Sensors, 21*(6), 2039.

[3] Islam, A., Masuduzzaman, M., Akter, A., & Shin, S. Y. (2020, October). MR-Block: A Blockchain-Assisted Secure Content Sharing Scheme for Multi-User Mixed-Reality Applications in Internet of Military Things. In *2020 International Conference on Information and Communication Technology Convergence (ICTC)* (pp. 407-411). IEEE.

[4] Cameron, L. (2018). Internet of things meets the military and battlefield: connecting gear and biometric wearables for an IoMT and IoBT. Retrieved from URL https://publications. computer. org/cloud-computing/2018/03/22/internet-ofmilitary-battlefield-things-iomt-iobt.

[5] Pradhan, M., & Noll, J. (2020). Security, Privacy, and Dependability Evaluation in Verification and Validation Life Cycles for Military IoT Systems. *IEEE Communications Magazine, 58*(8), 14-20.

[6] Gady, F. S., & Stronell, A. (2020). Cyber Capabilities and Multi-Domain Operations in Future High-Intensity Warfare in 2030. *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*, 151.

[7] Howard, R., & Olson, R. (2020). Implementing Intrusion Kill Chain Strategies. *The Cyber Defense Review, 5*(3), 59-76.

[8] Abdelzaher, T., Ayanian, N., Basar, T., Diggavi, S., Diesner, J., Ganesan, D., ... & Veeravalli, V. (2018, July). Will distributed computing revolutionize peace? the emergence of battlefield iot. In *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)* (pp. 1129-1138). IEEE.

[9] Russell, S., Abdelzaher, T., & Suri, N. (2019, November). Multi-domain effects and the internet of battlefield things. In *MILCOM 2019-2019 IEEE Military Communications Conference (MILCOM)* (pp. 724-730). IEEE.

[10] Doku, R., Rawat, D. B., Garuba, M., & Njilla, L. (2020, January). Fusion of Named Data Networking and Blockchain for Resilient Internet-of-Battlefield-Things. In *2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC)* (pp. 1-6). IEEE.

[11] Azmoodeh, A., Dehghantanha, A., & Choo, K. K. R. (2018). Robust malware detection for internet of (battlefield) things devices using deep eigenspace learning. *IEEE transactions on sustainable computing, 4*(1), 88-95.

[12] Tosh, D. K., Shetty, S., Foytik, P., Njilla, L., & Kamhoua, C. A. (2018, October). Blockchain-empowered secure internet of battlefield things (iobt) architecture. In *MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM)* (pp. 593-598). IEEE.

[13] FogBus: A Blockchain-based Lightweight Framework for Edge and Fog Computing
Tuli, S., Mahmud, R., Tuli, S., & Buyya, R. (2019). FogBus: A blockchain-based lightweight framework for edge and fog computing. *Journal of Systems and Software, 154*, 22-36.

[14] Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012, August). Fog computing and its role in the internet of things. In *Proceedings of the first edition of the MCC workshop on Mobile cloud computing* (pp. 13-16).