
# BRIEFING NOTES

#BN-34-Emerging technology and military application-Feb2021

## CHALLENGES IN DEVELOPING INTERNET OF BATTLEFIELD THINGS (IOBT)

Authors: Mehdi Taheri[1] and Kash Khorasani[2]
1 Graduate student, Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada
2 Professor, Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada

## SUMMARY

- Internet of Battlefield Things (IoBT) technology is capable of connecting warfighters to a network of sensors and wearable smart devices in highly dynamic and unpredictable combat zones.
- By leveraging IoBT, armed forced can decrease collateral damage caused by military attacks to civilians, improve chances of success in missions, and reduce the human cost of military operations.
- However, since IoBT devices depend on networked communications, they trigger the emergence of a new frontier for cyber defence mitigation and protection solutions against malicious adversarial attacks.


## CONTEXT

- The Internet of Battlefield Things (IoBT) is capable of connecting a network of sensors, wearable devices, and Internet-of-Things (IoT) systems to utilize cloud and edge computing to guide and protect combat forces and improve their operational effectiveness [1].
- Since IoBT devices and systems require a communication network for transmitting information, they are prone to cyberattacks by malicious adversaries. Consequently, one needs to monitor, detect, and identify cyberattacks and their counter-measures to defend IoBT systems. Moreover, protecting data privacy in IoBT systems is of paramount importance since these systems are involved in transmitting sensitive information.
- Rapid growth in the number of IoT and IoBT devices and systems is creating novel vulnerabilities that can be exploited by adversaries. In [1], cyberattacks in IoBT are categorized into three clusters, namely (a) multiple entry-points and single device hacking, (b) attacks on unmanned aerial vehicles (UAVs), and (c) collateral damage from cyberattacks such as attacks on the power grids. Moreover, common types of cyber defence mechanisms are identified as comply to connect (C2C), blockchain-based methodologies, and artificial cyber hunters [1].
- In addition to cyber security, IoBT technology has raised concerns regarding potential liabilities and ethics in these devices and systems. An important concern relates to “what decisions must remain with humans?”, for instance the decision for firing a weapon [2]. In order to increase safety in decision making and weapon use, “smarter” IoBT devices and systems should be utilized in the foreseeable future that can reduce the unintended loss of life [2].
- The decision-making process is hierarchical in military armed forces. Therefore, the speed of response is limited by the chain of commands and actions can be delayed as a consequence of it. Adoption of IoBT can result in an increased autonomy of subordinate units by shortening the decision-making process loop [2]. Consequently, by utilizing IoBT,

commanders only specify goals of a mission and leave the details to subordinate units who are equipped with more relevant and detailed local information.

- The IoBT technology can enhance automation in the decision-making process by warfighters in highly dynamic and unpredictable adversarial environments while enabling them to fully carry out commander's commands safely and in a resilient manner [2].
- As opposed to IoT systems, IoBT devices and systems cannot use public communication infrastructures such as cellular networks. Therefore, IoBT systems in battlefield environments require a dedicated device-to-device (D2D) communication capabilities for transmitting information to nearby devices and systems. Consequently, factors such as the number of things, their location and proximity, and transmission capabilities and power of devices affect the information sharing capabilities of the network. Moreover, cyberattacks such as jamming communication channels, physical attacks on devices, and failures due to attack on the power supplies can have a major impact on information exchange among the IoBT devices [3].
- Consequently, given that information flow in IoBT devices and systems to make timely and accurate decisions is crucial, these systems are required to satisfy and guarantee certain levels of reliability, security, and availability [3].
- Connectivity of the network for exchanging information and achieving desired transmission of data is essential in IoBT systems. However, due to cyberattacks, faults and failures in physical components, and limited available resources one cannot achieve perfect connectivity in the network [3]. Hence, one requires development of resilient IoBT systems and reconfigurable communication networks to successfully achieve the overall mission goals and requirements.

## CONSIDERATIONS AND RECOMMENDATIONS

- There are a number of requirements in developing communication networks for IoBT systems that should be considered. First, in order to increase autonomy of units, the communication infrastructure should not rely on a central operational C&C center. Second, accuracy and correctness of exchanged information should be guaranteed and ensured. Finally, the IoBT system should satisfy high levels of resiliency against cyber and physical adversarial attacks.
- The IoBT systems are comprised of highly heterogeneous devices, network standards, and infrastructures, and hence they are highly vulnerable to security and privacy challenges once various devices transmit information to one another. In [4], a blockchain-empowered auditable methodology has been proposed for IoBT systems to address crucial security and privacy challenges. Moreover, architectural components of the proposed blockchain-empowered methodology, including the battlefield-sensing layer, network layer, and consensus and service layer architectures have been studied.

- In the battlefield-sensing layer, information about the battlefield environment and device information will be collected by sensors and disseminated to rest of the network. Next, dynamic topology among military nodes and devices will be considered by the network layer. Finally, in the consensus and service layer roles of individuals and operational protocols are defined [4].
- The proposed immutable ledger or blockchain-based communication method proposed in [4] is capable of providing trustful data communication among heterogeneous devices as well as addressing the security and privacy concerns. The blockchain communication is resilient to corruption and manipulation of data. Hence, the blockchain technology can be utilized and integrated into IoBT systems to improve and enhance trust in transmitted information and security of communications in network-centric military operations [4].
- In network-centric military operations, actions and commands can be executed in real-time while they can be audited by the blockchain technology of the ledger system [4].
- In development of IoBT systems, one should consider the rapidly changing and unpredictable environment, and hence operational missions in the battlefield, which implies that IoBT devices and systems require a flexible and adaptive communication network. In order to reduce complexity of utilizing IoBT devices and systems in the battlefield, network adaptation and management should be carried out autonomously [5]. Moreover, given that units are under extreme cognitive and physical stress in the battlefield environment, volume of generated information and their complexity should be made manageable and reduced as much as possible [5].
- Consequently, in addition to the battlefield, the cyberspace and adversarial cyberattacks should be considered in developing the IoBT systems. The cyberspace in IoBT itself can be considered as a battlefield for defenders and attackers, which requires formal, resilient, and robust defence mechanisms and methodologies [5].

## REFERENCES


[1] Zhu, Lin and Majumdar, Suryadipta and Ekenna, Chinwe, “An invisible warfare with the internet of battlefield things: A literature review,” *Human Behavior and Emerging Technologies*, November 2020.

[2] T. Abdelzaher *et al*., "Will Distributed Computing Revolutionize Peace? The Emergence of Battlefield IoT," *2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*, Vienna, pp. 1129-1138, 2018.

[3] M. J. Farooq and Q. Zhu, "Secure and reconfigurable network design for critical information dissemination in the Internet of battlefield things (IoBT)," *15th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt)*, Paris, 2017, pp. 1-8, 2017.

[4] D. K. Tosh, S. Shetty, P. Foytik, L. Njilla and C. A. Kamhoua, "Blockchain-Empowered Secure Internet -of- Battlefield Things (IoBT) Architecture," *MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM)*, Los Angeles, CA, 2018, pp. 593-598.

[5] A. Kott, A. Swami and B. J. West, "The Internet of Battle Things," in *Computer*, vol. 49, no. 12, pp. 70-75, Dec. 2016.