Security-Policy
NET Nexus of Emerging Technologies

BRIEFING NOTES

# BN-65-Emerging technology and military application-Aug2021

THE PROBLEM OF SECURITY AND ROBUSTNESS IN 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

- The Internet of Things (IoT) offers a novel opportunity for large-scale utilization of smart devices that will be connected ubiquitously. Consequently, data will be extensively distributed among various devices that allow a high degree of situational awareness. Since real-time situation awareness on the battlefield is a prerequisite for development of coordinated decision-making in a modern army, IoT is capable of providing a promising foundation for the advancement of modern warfare and the so-called Internet of Battlefield Things (IoBT).
- Due to the wireless nature of the IoBT, malicious adversaries are capable of exerting damage to particular channels and data packets, that could lead to interruption and eventually the disruption of communication links in these systems. Thus, the robustness of the IoBT network against the enemy's malicious cyber-attacks is a vital factor in providing the connectivity among warfighters and command and control centers on the battlefield.
- In order to ensure the robustness of IoBT against malicious adversarial cyber-attacks, the application of the directionality of network has been recommended for modeling the wireless communication characteristics of the IoBT network, which is a quantitative indicator of the network connectivity. Moreover, the optimality of the model is evaluated by establishing an optimization model to simulate the adversary's optimal cyber-attack strategy.

CONTEXT

- While Internet of the Things (IoT) devices execute tasks within fields such as health, agriculture, and transportation through a network of inter-connected devices, they can similarly contribute to the enhancement of combat capabilities in the battlefields. Incorporating IoT into military operations and defensive applications is known as the Internet-of-Battlefield-Things (IoBT) [1].

- The Internet of Battlefield Things (IoBT) is defined as the application of IoT technology for the purpose of establishing interconnection between combat equipment and other battlefield resources. Furthermore, for the IoBT network to perform at its maximum capacity, it is necessary that through connectivity of the network real-time data collection and dissemination are provided [2].

- A distinctive quality of IoBT networks that cannot be taken for granted is the directionality of communication which has not been taken into consideration by previous studies of robustness of the network infrastructure. In this context, the role of nodes and edges in the network in providing robustness is significant [2].

- In other words, in the process of generating the operational command, the command and control node/center receives data from nearby nodes and sends it to the fire strike nodes, i.e., warfighters. Therefore, in systems that rely on directional connections, the data can be distributed between the nodes along the sending or receiving directions. Moreover, edges have certain directions that make network connectivity resistant to edge removal attacks through predicting the worst possible attack patterns [2].

- The utilization of directed network model illustrates that the growth in the proportion of unidirectional edges in IoBT networks results in a drop-in robustness which indicates that as with the occurrence of a cyber-attack the number of nodes maintaining mutual access will be reduced [2].

- Although IoBT provides armed forces numerous advantages, it also creates the downside of cyber security challenges with the potential threat that a malicious adversary might through unsecure gate penetrate and compromise the classified information through its vulnerabilities. Hence, US Department of Defense (DoD) has devised Comply to Connect (C2C) to secure network endpoints, to identify and validate the connection of new devices to the network, to evaluate their compliance with DoD security policies, to conduct ongoing monitoring, and to automatically address the device issues [3].

- In cyber warfare, as the number of devices on a network increases, adversaries are provided with greater opportunities to compromise the system. Given that in many cases the security measures of the communication network at different nodes is the same, once a device is compromised, the entire system would be at risk and the entry points would be multiple. Consequently, data might be disclosed or corrupted, sending false information from a seemingly trustworthy source [4].

- In the context of IoBT and as far as the sensitive nature of cyber warfare are concerned, possible threats and damages could extend to put civilians at risk. In case of a cyber-attack on the military infrastructure, the electrical grid will be aimed to shut down the military bases that in turn imposes collateral damage, such as the collapse of hospital systems, heating and cooling systems, and disrupting the supply chains for basic goods for the civilians [4].

- IoT often has to deal with fundamental privacy and security risks which are not completely dissolved. However, in IoBT systems, such potential risks gain more urgency as IoBT devices are more prone to be the target of malicious attacks and malware infections by cyber-criminals who are mostly state-sponsored and professionals [1].

- Malware detection methods have been classified into static and dynamic analyses. In the latter, the program is executed in a controlled environment such as a sandbox, aiming to gather data on behavioural characteristics to distinguish between the malware or the benign injections. A framework developed based on the Deepsign has been proposed to automatically recognize malware through a signature generation method which generates a dataset based on behaviour logs of the API calls, registry entries, web searches, and port accesses in a sandbox. The above framework that converts logs into binary vectors has demonstrated to have an accuracy of 98.6% [1].

CONSIDERATIONS AND RECOMMENDATIONS

- To tackle the problem of network robustness in traditional infrastructure, the network dis-integration model in complex network theory has been proposed for the purpose of modeling and analysis. In this context, nodes or edges should be removed from the network, either randomly or intentionally, to simulate failures or malicious attacks. Hence, the key nodes or edges in the network will be captured and identified accurately [2].

- In recent studies, machine learning and deep learning techniques have been incorporated into the process of malware detection to increase accuracy and robustness for the prevention and detection of malware intrusions. In this regard, four criteria have been introduced, namely: 1) True Positive (TP): this indicates that a malware is correctly identified as a malicious application 2) True Negative (TN): this indicates that a benign is detected as a non-malicious application correctly 3) False Positive (FP): this indicates that a benign is falsely detected as a malicious application, and finally 4) False Negative (FN): this indicates that a malware is not detected and labeled as a non-malicious application [1].

- The Comply to Connect (C2C) identifies and verifies new devices that are connected to the network to ensure that they comply with security policies of DoD. C2C provides commanders with the ability to make informed risk decisions and to assess potential threats [4].

- Due to the heterogeneous nature of IoBT systems, data exchanges among battlefield entities often lack reliability, security, and privacy. In order to enhance the credibility of real-time executions, the distributed ledger system can be employed to audit and track network-centric operations. This system relies on the architectural components of IoBT. The “battlefield sensing layer” in an IoBT system is responsible for gathering and distributing data, and providing entities with the ability to cooperate for achieving common gaols. The “network layer” generates a dynamic topology between nodes that serve blockchain-related operations. Finally, the “consensus and service layer” defines individual roles and mechanisms to secure consistency [4].

- Moreover, artificial cyber hunters have been considered as a solution to the security challenges of IoBT. These mobile agents autonomously petrol the network to detect and destroy malware. Due to the evolving nature of cyber-attacks, these agents should be adaptive. Although such a capability has not been accomplished yet, it remains the focus of future research to tackle the problem of cyber-attacks in the highly complex, dynamic, and competitive future battlefields [4].

REFERENCES

[1] Azmoodeh, Amin and Dehghantanha, Ali and Choo, Kim-Kwang Raymond, "Robust malware detection for internet of (battlefield) things devices using deep eigenspace learning," IEEE transactions on sustainable computing, vol. 4, pp. 88-95, 2018.

[2] Feng Yuan, Li Menglin, Zeng Chengyi, and Liu Hongfu (2020) "Robustness of Internet of Battlefield Things (IoBT): A Directed Network Perspective", Entropy 22, 1116.

[3] https://nationalinterest.org/blog/buzz/how-secure-internet-battlefield-things-cyber-attacks-64731

[4] Zhu Lin, Majumdar Suryadipta, Ekenna Chinwe "An Invisible Warfare with the Internet of Battlefield Things: A Literature Review," Hum Behav & Emerg Tech, 2020.