BRIEFING NOTES

BN-66-Emerging technology and military application-Aug2021

PUBLIC POLICY FRAMEWORK FOR INTERNET-OF-BATTLEFIELD-THINGS (IOBT)- PART 2

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) is a transformative technology which will change the modern warfare. This technology will assist human war fighters and commanders to make correct decisions in the highly dynamic battlefield environments.
- IoBT systems will provide commanders with real-time information on the battlefield. Moreover, these systems can protect critical infrastructure, assets, and communication networks against malicious adversaries.
- To protect communication networks and develop a cyber defense mechanism against malicious adversaries, one needs to develop autonomous intelligent software agents and deploy them in our system to detect, identify, and destroy the adversarial software and malwares.

CONTEXT

- The Command & Control (C2) has been defined as "the exercise of authority and direction by a properly designated commander over assigned forces in the accomplishment of the mission" by the U.S. Department of Defense (DoD) [1]. The C2 includes objectives of a commander and required resources to successfully carry out a mission, however, it does not indicate how the objectives and commands should be communicated in the battle zone. Hence, if one considers communication in C2, one has command, control, and communication (C3). Moreover, it is necessary to include situation awareness and intelligence in C3, which results in command, control, communication, and intelligence (C3I) [1].
- The Internet of Battlefield Things (IoBT) utilizes integration of both networking and artificial intelligence (AI) and accomplishes pervasive sensing and automation. The performance of C3I highly depends on information technology and requires efficient decision making and control [1]. Many military operations and air-superiority can be conducted and achieved as a result of developments in C3I, which is considered as "the brain of modern warfare" [1]. Pervasive sensing and automation capabilities of IoBT can effectively change and improve C3I. Consequently, autonomous vehicles and assets can utilize a wide range of sensors and actuators to carry out missions in the highly dynamic environment of battlefield and gather information to enable and improve informed decision-making processes and protocols [1].
- Given the development of Internet of Things (IoT) and IoBT whose sensors generate a large amount of data and provide control over complex industrial and military processes, the boundaries of modern and network-centric warfare extend beyond the state-sponsored operations into asymmetric warfare [1].

- In the cyber domain of the battlefield, cyber robots and intelligent agents will reside in computer networks to protect communications, filter and transmit information. Moreover, there will be intelligent agents that protect our infrastructure, electronic devices, and will provide humans, physical robots, and autonomous assets and advices by analyzing the battlefield situation [2].
- Although the use of IoBT and AI makes individual and collective behaviour of war fighters more intelligent and efficient, it also makes the management of the battlefield more challenging [2]. Intelligent "things" and robots/autonomous assets will think and act different from human war fighters. This implies that they are harder to control and manage [2]. Moreover, intelligent things should understand and predict their human team-mates' actions to have an efficient and effective collective behaviour [2].
- IoBT devices are manufactured by different companies with various, designs, purposes, and standards. Moreover, behaviours and characteristics of these devices should be updated and learned autonomously in the battlefield environment [2]. Hence, developing IoBT devices that work in cooperation with humans and other intelligent devices is challenging due to the heterogeneousity of these systems. Both human war fighters and IoBT devices require reasonably sized, essential in nature, and relevant information to operate effectively, unless, the information would result in harmful actions in these systems [2].
- Considering that in a conflict situation the adversaries are technically sophisticated and enemies will use software cyber agents to attack our infrastructure and IoBT systems, one needs to develop AI-based, intelligent, and autonomous cyber agents to respond and fight back [2]. The friendly cyber agents will detect and identify occurrence of attacks and malicious behaviours in the system. Moreover, these protective cyber agents need to have an adaptive nature to be updated in response to the evolving adversarial malware.
- For instance, in [3], a deep learning-based methodology was proposed which utilizes Eigenspace and deep convolutional neural networks to detect and classify malware applications in IoBT.
- In the battlefield environment, communications may be disrupted and jammed among IoBT devices. Hence, utilizing a centralized cyber defence scheme cannot be practical in real-world conditions. Moreover, one cannot rely on the human war fighters under battlefield conditions to carry out cyber defense tasks [2]. Hence, the cyber defense should be accomplished by distributed or decentralized intelligent agents throughout the network. Since adversaries can discover vulnerabilities of these cyber defense agents, they are required to be stealthy and reduce the probability of their identification by adversaries.
- Transport layer security (TLS) and datagram TLS have been widely used as security standards for Internet of Things (IoT), which provide authentication, integrity, and confidentiality of these systems [4]. Moreover, IEEE 1888.3 standard provides and determines security requirements for the control network protocol [4]. In addition to

conventional security standards, recently, Blockchain which is a distributed ledger technology has been utilized that does not require a centralized and a third-party authority [4]. The Blockchain technology can potentially be used in IoBT systems which require a distributed security standard and measure.

- The North Atlantic Treaty Organization (NATO) Research Task Group IST-152 has proposed the development of autonomous intelligent cyber-defense agents (AICA) that are capable of protecting IoBT systems and infrastructure in the case of battles and conflicts against sophisticated adversaries [5]. The agent should have certain properties such as planning capabilities, analyzing, and being autonomous. Moreover, agents should be able to work in cooperation with other friendly agents against adversarial software and malwares [5].

CONSIDERATIONS AND RECOMMENDATIONS

- Two crucial requirements in developing the IoBT technology are to have a reliable communication network and to address the problem of heterogeneousity in these systems.
- In order to have a reliable communication network, one needs to take appropriate security measures and develop communication and network infrastructures that cannot be easily compromised by malicious adversaries, and hence, ensure the availability of the communication network.
- Moreover, a secure and reliable communication network should guarantee the integrity of data and provide a high level of confidentiality. Towards this end, one needs to employ encryption methods and hash function-based methodologies to protect the privacy and integrity of data.
- However, due to the low computational power of IoBT devices and the importance of having a real-time stream of data and communication, one should consider utilizing cryptographic methods with low computational complexities.
- In addition to cryptographic methods, one needs to develop intelligent agents by using AI that can detect and identify cyber-attacks that are carried out by adversarial IoBT and defend our IoBT network, infrastructure, and assets.
- Moreover, since human war fighters cannot keep up with and comprehend the fast dynamics of the future battlefield environments, one requires a fleet of autonomous robots/assets and intelligent cyber agents to carry out offensive missions against adversarial IoBT devices.
- In order to address the problem of cooperation among various heterogeneous IoBT devices in the network, one needs to develop a synchronization unit and a layer in our system architecture which can synchronize heterogeneous devices by interpreting their sensor and actuation information into a common appropriate data and signal.

REFERENCES

[1] Russell, Stephen and Abdelzaher, Tarek, “The internet of battlefield things: the next generation of command, control, communications and intelligence (C3I) decision-making," MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM), pp. 737-742.

[2] Kott, Alexander and Stump, Ethan, “Intelligent autonomous things on the battlefield," Artificial intelligence for the internet of everything, 2019, pp. 47-65.

[3] 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.

[4] Salman, Tara and Jain, Raj, “A survey of protocols and standards for internet of things," arXiv preprint arXiv:1903.11549, 2019.

[5] Kott, Alexander and Theron, Paul and Drasar, Martin and Dushku, Edlira and LeBlanc, Benoit and Losiewicz, Paul and Guarino, Alessandro and Mancini, Luigi and Panico, Agostino and Pihelgas, Mauno and others, “Autonomous Intelligent Cyber-defense Agent (AICA) Reference Architecture. Release 2.0," arXiv preprint arXiv:1803.10664, 2018.