Short Communication
Volume 15:10, 2022

Journal of Computer Science & Systems Biology

ISSN: 0974-7230

Open Access

A Strategy to Evaluating Cybersecurity Risk in Internet of Things-Enabled Transport Networks

John Hausman*

Department of Information Science, University of Western Australia, 35 Stirling Hwy, Crawley WA 6009, Australia

Introduction

A critical transportation infrastructure integrated with a wireless sensor network based on the Internet of Things functions as a cyber-physical system. However, due to inherent cyber vulnerabilities of IoT devices and a lack of control barriers that could protect it, the new form of IoT enabled transportation infrastructure is vulnerable to cyber-physical attacks in the sensing area. Traditional risk assessment processes treat the physical and cyber spaces as separate environments, resulting in stakeholders (i.e., operators, civil and security engineers) failing to assess IoT enabled transportation infrastructure for cyber-physical attacks. This paper proposes a new risk assessment approach for cyber-physical attacks on IoT-based wireless sensor networks.

Until recently, critical infrastructure was thought to exist in a separate cyber or physical environment. However, critical infrastructure's increasing reliance on advanced technologies (e.g., the Internet of Things (IoT)) has enabled the integration of the physical world with computational facilities and the operation of critical infrastructure as a cyber-physical system. A significant number of IoT applications have recently been introduced in the domain of critical transportation infrastructure, providing reliable services with less human intervention. These services include, but are not limited to, an early warning system against hazards (e.g., scour) and a smart management system in the life cycle assessment of a bridge.

Description

The approach is based on the identification and proposal of novel cyber-physical characteristics, such as threat source (e.g., motives), vulnerability (e.g., lack of authentication mechanisms), and physical impact types (e.g., casualties). The level and importance of these characteristics are used to calculate cyber-physical risk [1-3]. To evaluate the results of an IoT enabled bridge subjected to cyber-physical attack scenarios, Monte Carlo simulations and sensitivity analysis are used. According to the findings, 76.6% of simulated cases are high-risk, and control barriers operating in physical and cyber space can reduce cyber-physical risk by 71.8%. Furthermore, cyber-physical risk differs when the significance of the characteristics considered during risk assessment is overlooked.

Advances in IoT technology have revealed the potential for several applications in the field of structural health monitoring and damage assessment (e.g., monitoring through image processing). These Internet of Things applications improve the ability to automate processes, allowing civil engineering professionals to make informed decisions about the structural health of their systems. Such IoT applications would be impossible to realise without the use of an IoT-based wireless sensors network (WSN) as a key technology that enables connectivity with the physical environment within their layered architecture. The fundamental three-layer IoT architecture consists of the sensing, network, and application layers, each defined by its functions and devices. IoT devices (e.g., sensors, gateways) located in physical space (e.g., the deck of a bridge) as part of the sensing layer, detect, collect, and process data collaboratively [4,5]. The network layer enables wireless data transmission by leveraging recent advances in wireless network protocols (e.g., ZigBee, Bluetooth). Through the application layer, this data is sent to the end-user for data analytics and processing.

Conclusion

Quantitative scores are used to evaluate the level and significance of cyber-physical characteristics. To demonstrate the application and utility of the approach, an illustrative, yet realistic, case study of an IoT enabled bridge being subjected to a cyber-physical attack (i.e., energy depletion attack) against its IoT based WSN is used. The cyber-physical attack is divided into four scenarios based on the use of various control barriers that can prevent and detect cyber-physical attacks. Control barriers can operate separately or concurrently in cyberspace (e.g., intrusion detection systems) and physical space (e.g., motion detectors) (i.e., integrated control barriers).

Acknowledgement

None.

Conflict of Interest

Authors declare no conflict of interest.

References

1. Mostafaie, Taha, Farzin Modarres Khiyabani and Nima Jafari Navimipour. "A systematic study on meta-heuristic approaches for solving the graph coloring problem." *Comput Oper Res* 120 (2020): 104850.
2. Lowe, Matthew, Ruwen Qin and Xinwei Mao. "A review on machine learning, artificial intelligence and smart technology in water treatment and monitoring." *Water* 14 (2022): 1384.
3. Chen, Jianyong, Sad Jarall, Hans Havtun and Björn Palm. "A review on versatile ejector applications in refrigeration systems." *Renew Sustain Energy Rev* 49 (2015): 67-90.
4. Anagnostopoulou, Alexandra, Charis Styliadis, Panagiotis Kartsidis and Evangelia Romanopoulou, et al. "Computerized physical and cognitive training improves the functional architecture of the brain in adults with Down syndrome: A network science EEG study." *Netw Neurosci* 5 (2021): 274-294.
5. Rodríguez-Abreo, Omar, Juvenal Rodríguez-Reséndiz, L. A. Montoya-Santiyanes and José Manuel Álvarez-Alvarado. "Non-linear regression models with vibration amplitude optimization algorithms in a microturbine." *Sensors* 22 (2021): 130.

***Address for Correspondence:** John Hausman, Department of Information Science, University of Western Australia, 35 Stirling Hwy, Crawley WA 6009, Australia, E-mail: jhausman@wc.edu*

Received: 07 October, 2022, Manuscript No. jcsb-22-84877; **Editor assigned:** 08 October, 2022, Pre QC No. P-84877; **Reviewed:** 21 October, 2022, QC No. Q-84877; **Revised:** 26 October, 2022, Manuscript No. R-84877; **Published:** 03 November, 2022, DOI: 10.37421/0974-7230.2022.15.439

How to cite this article: Hausman, John. "A Strategy to Evaluating Cybersecurity Risk in Internet of Things-Enabled Transport Networks." J Comput Sci Syst Biol 15 (2022):439.