Proceedings of the 8th International Conference on Civil Structural and Transportation Engineering (ICCSTE'23)
Canada – June 04-06, 2023
Paper No. 172
DOI: 10.11159/iccste23.172

A Vulnerability Assessment Approach for Internet of Things Enabled Transportation Networks Subjected To Cyber-Physical Attacks

Konstantinos Ntafloukas[1], Liliana Pasquale[2], Beatriz Martinez-Pastor[1], Daniel P. McCrum[1]
[1] School of Civil Engineering, University College of Dublin
D07 R2WY, Dublin, Ireland
konstantinos.ntafloukas@ucdconnect.ie
[2] School of Computer Science, University College of Dublin
D07 R2WY, Dublin, Ireland

Abstract **-** Transportation networks play a vital role in society's well-being. While in the past, transportation networks were considered fragile only against threats in physical space (e.g., natural hazards), this is no longer the case. Previous events (e.g., Denial of Services attack against the Swedish Transport Administration) have highlighted the susceptibility of transportation domain to cyber-attacks. The integration of Internet of Things based wireless sensor networks in the sensing layer of a critical transportation infrastructure, increase the vulnerability of transportation networks to cyber-physical attacks. Current vulnerability assessment studies that treat transportation networks in the form of a graph (i.e., nodes, edges), overlook the security issues. In this paper, a new vulnerability assessment approach for transportation network subjected to cyber-physical attack, is proposed. The novelty of the approach relies on the consideration of vulnerabilities states, both in physical and cyber space, using a Bayesian network attack graph. A new probability indicator, that considers different attacker characteristics (e.g., skills) and control barriers (e.g., cameras) is proposed to drive the assignment of probability scores to vulnerability states. Following the probability-based ranking table, we measure the vulnerability of transportation network as a drop of network efficiency, after the removal of the highest probability-based ranked nodes. A transportation network case study is used to demonstrate the application of the approach. Monte Carlo simulations are performed as a method to evaluate the results, that indicate that transportation networks are probabilistically more susceptible to cyber-physical attacks, when IoT enabled transportation infrastructure is based on deficient control barriers. The approach is of interest to stakeholders (i.e., operators, civil and security engineers) who attempt to incorporate the cyber domain in vulnerability assessment procedures of their system.

Keywords**:** Transportation network; Vulnerability; Cyber-physical attacks; Internet of Things; Bayesian network attack graph; Efficiency; Monte Carlo

1. Introduction

Transportation networks are fundamental to the efficient and safe functioning of modern societies and rely on the stable operation of critical transportation infrastructure (e.g., bridge, road etc) as integral parts of public transportation network. Therefore studies related to vulnerabilities of the transportation network is of major importance [1]. However, studies mainly focus on threats derived from physical space, such as man-made attacks (e.g., bombing) or natural hazards (e.g., earthquake) [2], treating cyber space as an isolated environment. Both research studies [3], [4] and previous events, such as the two-days Denial of Services attack (DoS) against the Swedish Transport Administration that led to major delays [5], have highlighted the susceptibility of transportation domain to cyber-attacks that impact the physical space (i.e., cyber-physical attack). The consistent operation of critical transportation infrastructure (e.g., bridges) in physical space relies more and more on advanced technologies (e.g., Internet of Things (IoT)) and subsequent in cyber space. Indeed, transportation infrastructure is embedded with IoT devices in the form wireless sensor network (i.e., IoT based wireless sensor network (WSN)), to provide data in real time for wireless engineering services such as early warning systems against hazards (e.g., foundation scour), or wireless structural health monitoring [6]. Therefore, the successful transition from traditional transportation network to a cyber-physical transportation network, depends on the operation of sensing layer as an integral layer of IoT architecture system [7]. Specifically sensing layer, includes the IoT devices (e.g., sensors) deployed in the sensing area of the transportation infrastructure (e.g., deck of a bridge), that detect, collect, and process data to the end-user.

Despite the benefits of IoT enabled transportation infrastructure, it suffers from the inherent security deficiencies of IoT devices (e.g., lack of authentication mechanisms) in the sensing layer. Those can be exploited by attackers, who target to breach the confidentiality, integrity and availability of data. Studies related to security issues in transportation networks have raised security awareness due to security issues of transportation systems such as smart traffic lights [8]. However, there is

a lack of research focusing on vulnerability assessment of transportation network to cyber-physical attacks against IoT enabled transportation infrastructure.

To bridge this gap, a new vulnerability assessment approach for transportation network subjected to cyber-physical attacks at the sensing layer, is proposed in this paper. Transportation network in this approach is represented in the form of a graph with a set of nodes being the target of the cyber-physical attack, that are connected through edges. The approach is based on a Bayesian network (BN) attack graph [9], that enables the modeling of vulnerabilities states in a probabilistic manner, combining cyber and physical space for the first time. Assignment of probability scores to vulnerability states, is accomplished based on a proposed probability indicator (PI). The PI assists stakeholders towards the detailed assignment of probability score, considering the attacker, under certain profile characteristics (e.g., motives), and the control barriers that protect the vulnerability state (e.g., protection of physical area through cameras). Following the probabilistic analysis, a probability-based ranking table is developed, that describes the most vulnerable nodes to the considered cyber-physical attack. Vulnerability of transportation network is then measured as a drop of efficiency, after the removal of the highest probability-based ranked nodes. We demonstrate the application of the approach by measuring the vulnerability of an illustrative transportation network, as a case study. Monte Carlo simulations are performed, as a method to evaluate the results, indicating that transportation networks relying on IoT enabled transportation infrastructure that lacks control barriers, are probabilistically more susceptible to cyber-physical attacks.

2. Related work

A review of related work within the area of vulnerability assessment of transportation networks is presented in this section. The unforeseen nature of attacks against transportation networks, necessitates the use of static analysis. A static analysis requires the removal of nodes, following a centrality measure-based ranking (e.g., descending order of node degree) and the evaluation of changes in certain transportation indexes (e.g., connectivity), as a vulnerability measure. For example, Zhang et al. [10] proposed the removal of nodes following a ranking of descending node degree in the Shanghai metro to measure the vulnerability as a drop of network connectivity. Cai et al. [11] considered the travel time and passenger flow, in a topological vulnerability analysis, to measure the vulnerability of the Beijing metro network as drop of network efficiency. Although these studies succeed in assessing vulnerability of transportation network, availing of topological attributes in physical space, they are impractical when security issues should be considered. In contrast, this work studies the susceptibility of transportation network due to security issues of IoT enabled transportation infrastructure in cyber space.

Within the domain of security of transportation network, Ghena et al. [12], managed to raise security awareness due to the increasing number of cyber vulnerabilities in transportation systems (e.g., traffic lights). In order to analyze the security of traffic infrastructure, a case study was used in cooperation with a road agency in Michigan, USA, highlighting the number of existing vulnerabilities in traffic systems. Similarly, Laszka et al. [13] studied the vulnerability of a transportation network to traffic signal tampering attacks. The proposed approach is based on an attacker model, relying on certain characteristics (e.g., goal of the attacker), a traffic model and an algorithm responsible for computing optimal attacks. Vulnerability is then measured as drop of total travel time of the network, considering the worst-case attack and the default travel time. Comert et al. [14], developed a belief-network-based attack modelling at signalized traffic networks under connected vehicle and intelligent signals frameworks. Vulnerability scores for signal controllers' equipment (e.g., sensor), as part of the Bayesian network, were based on metrics (i.e., low) resulting in the quantification of impact (e.g., delays).

Although related work succeeds in raising awareness for the susceptibility of transportation networks to different type of threats, they have certain deficiencies. Firstly, cyber space is treated as an isolated environment, focusing on certain topological attributes from physical space. Studies related to security issues, overlook the security issues of IoT enabled transportation infrastructure and rely on limited attacker characteristics [13]. In contrast, this approach considers the security issues of IoT enabled transportation infrastructure for the first and detailed attacker profiles.

3. Overview of vulnerability assessment approach

The proposed vulnerability assessment approach, targets to assist stakeholders (i.e., operators, civil and security engineers), who act as assessors, towards the vulnerability assessment of an IoT enabled transportation network subjected to

cyber-physical attacks at the sensing layer. In this novel approach the transportation network is in the form of a graph G(N, E) with a set of N nodes (i.e., n_i) that represent the IoT enabled transportation infrastructure, as potential targets of a cyber-physical attack, and edges (i.e., e_i) that represent the distance between the nodes.

As shown in Figure 2, the approach includes five activities. The first activity (i.e., *Selection of a sensing area cyber-physical attack scenario*) describes the selection of a cyber-physical attack scenario. The activity is facilitated by using public available catalogues of common attack patterns (e.g., CAPEC [15]]) and current theoretical or experimental studies. The second activity (i.e., *Division of cyber-physical attack scenario into vulnerability states in physical and cyber space*), is based on the BN attack graph that details the vulnerability states, in both physical and cyber space, that should be exploited by the attacker, to accomplish the selected cyber-physical attack scenario (i.e., First activity). The third activity (*i.e., Development of conditional probability table (CPT) for every node i*) necessitates the development of CPT, as part of the Bayesian network. The fourth activity (i.e., *Calculation of probability indicator (PI)*), describes the calculation of the proposed PI, that will enable assessors to assign a probability score to every vulnerability state. The ratio considers both a detailed attacker profile and the physical and cyber control barriers that protect every vulnerability state. In the fifth activity (i.e., *Removal of nodes based on probability-based rank and vulnerability assessment as drop of efficiency*), we measure vulnerability of transportation network as loss of efficiency, after the removal of the highest probability based ranked nodes [16]. The fourth and fifth activities are further described in section 3.1 and section 3.2.

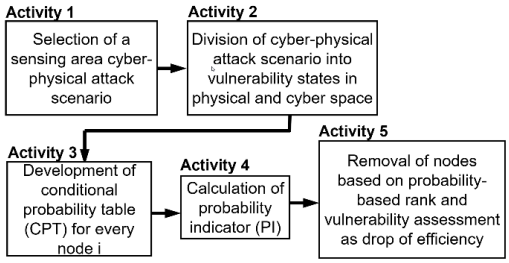

Fig. 1: Process diagram of proposed vulnerability assessment approach

3.1. Calculation of probability indicator

Traditionally, it is common practice for expert(s) who have bespoke knowledge of the system, to determine the probability scores. To enable a more detailed assessment, we propose the integration of PI that acts as a ratio, as shown in Equation 1. The numerator of PI, is equal to the weighted average of the level of attacker who targets to exploit the vulnerability state and has been detailed in our previous work [3]. In summary, it builds on the level (i.e., X_i) and the importance index (i.e., W_i) of the following characteristics namely, *Knowledge* (i.e., X_{KN}, W_{KN}) (i.e., describes cyber skills, attack methods etc) , *Resources* (i.e., X_{RE}, W_{RE}) (i.e., describes budget, manpower etc), *Psychology* (i.e., X_{PS}, W_{PS}) (i.e., describes the motives), *Terrorism experience* (i.e., X_{Te}, W_{Te}) (i.e., describes the ability of attacker to remain undetected in public areas and the ability of gaining access to sensitive critical information infrastructure). These characteristics enable the assessment of classified attacker profiles that act against critical infrastructure such as Basic-users, Cybercriminals, Nation-States, Hostile organizations [17]. The denominator of PI is equal to the level of control barriers (i.e., X_{cb}), that protect the vulnerability state from being exploited in the physical and cyber space. Physical control barriers describe traditional protection measures (e.g., perimeter protection) that have been applied in the past, or advanced protection measures (e.g., smart video-surveillance) that have been designed for cyber-physical system protection. We divide physical control barriers to those based on; i) *technological operation* such as CCTV systems, motion detectors, line crossing, smart video-surveillance and ii) *non-technological or human operation* such as perimeter protection, continual inspection from trained personnel [18]. Cyber control barriers protect vulnerabilities of IoT devices and are related to the level of encryption (i.e., prevent an attacker from violating data confidentiality and control IoT devices), authentication, access control, energy resources, proper patch management and audit mechanisms. Further details can be found in [19].

$$PI = \frac{\text{Weighted average attacker level}}{\text{Control barrier level}} = \frac{\frac{W_{KN} \times X_{KN} + W_{RE} \times X_{RE} + W_{PS} \times X_{PS} + W_{Te} \times X_{Te}}{W_{KN} + W_{RE} + W_{PS} + W_{Te}}}{X_{CB}} \quad (1)$$

A rating scale (i.e., Very Low (00.01-0.20) etc.) similar to our previous work [3], is applied to assign values to X_i, W_i and enable the calculation of PI, as shown in Table 1.

Table 1. Rating scale per level Xi, and importance index Wi

Rating scale level/Level Xi	Rating scale level/Importance index Wi
Low /1	Very Low / 0.01–0.20, Low / 0.21–0.40
Medium / 1-2	Medium / 0.41–0.60, High / 0.61–0.80
High / 2-3	Very High / 0.81–1.0

Based on the calculation of PI for very vulnerability state, the probability scores should range within the values shown in Table 2. It is evident that a greater attacker level with a lower control barrier level will result in higher values of PI.

Table 2. Range of PI and probability scores

Range of PI	Range of probability scores
$0 \leq PI \leq 0.33$	$0 \leq P(i) \leq 0.25$
$0.33 \leq PI \leq 1$	$0.25 \leq P(i) \leq 0.50$
$PI = 1$	$P(i) = 0.50$
$1 \leq PI \leq 2$	$0.50 \leq P(i) \leq 0.75$
$2 \leq PI \leq 3$	$0.75 \leq P(i) \leq 1.0$

The assigned probability scores facilitate the numerical use of BN attack graph that enable the update of posterior probabilities. Application of the chain rule of probability theory allows to factorize joint probabilities, for a set of v vertexes, from X_1 to X_V, as shown in Equation 2. $Pa(X_i)$ is the collection of all parent vertexes of the vertex Xi.

$$P(X_1, X_2, \ldots, Xv) = \prod_{i=1}^{n} P(Xi \mid Pa(Xi)) \times Xi \times Xv \quad (2)$$

3.2. Calculation of transportation network efficiency

The efficiency of a transportation network in the form of a graph (i.e., E(G)) considers the distance between node pairs and is mathematically computed as shown in Equation 2 [16] .

$$E(G) = \frac{1}{N \times (N-1)} \times \sum_{i \neq j \in G} \frac{1}{d_{ij}} \quad (3)$$

where, N represents the number of nodes in the network graph and d_{ij} represents the shortest distance between node pairs. E(G) varies in the range [0 -1], with values closer to 1 representing more efficient transportation networks. After the removal of the highest probability based ranked nodes, vulnerability is measured as loss if efficiency, as in Equation 4. E(G) and E'(G) represent the initial efficiency and the efficiency of the transportation network after the removal of a node.

$$V(G) = \frac{E(G) - E'(G)}{E(G)} \quad (4)$$

4. Case study of a transportation network vulnerability assessment approach

An illustrative case study of a cyber-physical transportation network, as shown in Figure 2, subjected to cyber-physical attacks, is presented to demonstrate the application of the proposed vulnerability assessment approach. The topology of the is in the form of an undirected graph G with a set of eight nodes (i.e., N=8) that represent the IoT enabled transportation

infrastructure, and a set of fourteen weighted edges (i.e., E=14) that represent the geodesic distances (i.e., d_{ij}) between the interconnected nodes N. For the purposes of this case study, we consider that the ZigBee devices form the IoT based WSN of every node, as a widely used IoT technology for monitoring purposes in civil engineering infrastructures [20]. A main security issue of ZigBee technology relies on the key management, that enables the sniffing of security key and the conduction of DoS attack, that will be considered in this case study as the first activity (i.e., see Figure 1, *Selection of a sensing area cyber-physical attack scenario*). The specific exploitation has been experimentally tested with success [21]. Network key acts as a security mechanism in order to enable the secure communication within the devices of the ZigBee network (i.e., IoT based WSN) and relies on two security levels namely, *High security level*, in which network key is transmitted encrypted over-the-air and thus attack is impractical, and *Standard security level,* in which network key is transmitted unencrypted over-the-air and thus attacker can legitimately communicate with other devices and flood them with bogus messages resulting in a DoS attack and disruption of IoT enabled transportation infrastructure. Following the second activity (i.e., *Division of cyber-physical attack scenario into vulnerability states in physical and cyber space*), the attacker i) should infiltrate into the physical sensing area of critical transportation infrastructure, where the ZigBee enabled network is located, by overcoming the physical control barriers (i.e., see Section 3.1) that are based on non-technological or human operation (i.e., State A, V_A) and technological operation (i.e., State B, V_B) ii) should capture the over-the-air traffic and parse the network key by using packet sniffers, by overcoming the cyber control barriers, that rely on either the *Standard* or *High security level* (i.e., State C, V_C) and iii) conduct a DoS attack, overcoming the cyber control barriers that rely on the energy resources level and audit mechanisms (i.e., State D, V_D). Third activity (i.e., *Development of conditional probability table (CPT) for every node i*), is then performed, to develop the CPT for every node i of transportation network. In figure 2, the BN attack graph and CPT for node 6, where V_A, V_B, V_C, V_D should be exploited (i.e., True as T, False as F), are illustrated.

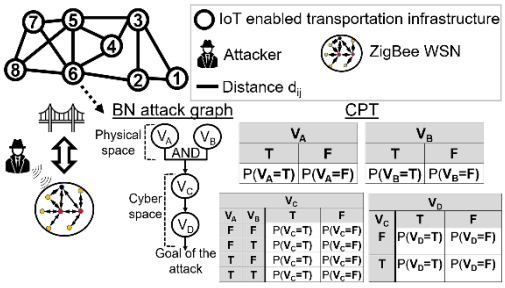

Fig. 2: Transportation network case study and development of CPT through BN attack graph, for node 6

Fourth activity (i.e., *Calculation of probability indicator (PI)*), enables the assignment of probability score (i.e., see Table 2). Nation-states, are considered as common attackers against critical infrastructure [17], and corresponding levels of profile characteristics can be assigned, as shown in Table 3. Nation-State is generally characterized as an attacker with high level of access to sensitive information or resources, strong motives (e.g., political) and cyber skills. For State A and State B (i.e., physical space), State C and State D (i.e., cyberspace), the level of profile characteristics of *Terrorism experience* (i.e., X_{Te}) and *Psychology* (i.e., X_{PS}) are High level (i.e., 2-3) in the rating scale (i.e., see Table 1). As shown in Table 3, *Terrorism experience* is of very high importance (i.e., W_{Te} varies to 0.81-1.0). *Psychology* is of high importance (i.e., W_{PS} varies to 0.61-0.80) towards the successful exploitation of every state. For State C and State D, the associated level of *Knowledge* (i.e., X_{KN}) and *Resources* (i.e., X_{RE}) are High level (i.e., 2-3). The possession of cyber skills (i.e., *Knowledge*) through the exploitation of vulnerability State C and D is of very high importance (i.e., W_{KN} varies to 0.81-1.0). The possession of budget is of very low importance (i.e., W_{RE} varies to 0.01-0.20) as it only requires access to packet sniffers.

Table 3. Case study attacker characteristics level per vulnerability state

Vulnerability state	**Characteristic / Level**
A-B-C-D	Terrorism experience / (X_{Te}=2-3, W_{Te}=0.81-1.0), Psychology / (X_{PS}=2-3, W_{PS}=0.61-0.80)
C-D	Knowledge / (X_{KN}=2-3, W_{KN}=0.81-1.0), Resources / (X_{RE}=2-3, W_{RE}=0.01-0.20)

The level of control barriers (i.e., X_{CB}) with respect to every vulnerability state in physical or cyber space, is described in Table 4 and should be assigned by stakeholders who have bespoke knowledge of their system. For example, Node 6, is protected by physical control barriers that relies on; i) advanced non-technological or human operation barriers, including perimeter protection, continual inspection from trained personnel and, ii) advanced technological operation barriers including smart video-surveillance and motion detectors. Therefore, X_{CB} for the vulnerability States A and B vary to a high level (i.e., 2-3). Additionally, Node 6, is protected by cyber control barriers that rely on; i) high levels of security (i.e., network key is transmitted encrypted over-the-air) and ii) critical audit mechanisms that ensure the inspection and maintenance level of energy resources. Therefore, X_{CB} for the vulnerability States C and D are High level (i.e., 2-3). Similarly, different control barriers have been considered for every individual node of transportation network case study. Details for node 6, 4, 1 and 8 have been provided in Table 4, as an example.

Table 4: Description and level of control barriers per vulnerability state for node 6,4,1 and 8

Number of Node	Vulnerability state	Control barriers / Level (X_{CB})
6	A, B	Continual inspection from trained personnel and perimeter protection/ (High, 2-3), Smart video-surveillance / (High, 2-3)
	C, D	High security level / (High, 2-3), Continual audit mechanisms (High, 2-3)
4	A, B	Continual inspection from trained personnel and perimeter protection/ (High, 2-3), Lack of technological operation barriers - **State B does not exist**
	C, D	High security level / (High, 2-3), Poor audit mechanisms / (Low, 1)
1,8	A, B	Rare inspection from trained personnel / (Low, 1), line crossing (Low, 1)
	C, D	Standard security level / (Low, 1), Poor audit mechanisms / (Low, 1)

Based on Tables 3,4, we calculate the PI for every vulnerability state (e.g., PI_A as for probability indicator for vulnerability state A, etc) in order to assign a detailed probability score (i.e., see Table 2). Monte Carlo simulations are performed in order to calculate the probability scores for every vulnerability state of every node i and with the use of Equation 1, we calculate the total probability score. Table 5 presents the results of the overall process and the total probability score for every Node *i* in a descending probability-based ranking. The ranking probabilistically indicates the nodes that are most vulnerable to the considered cyber-physical attack. Table 5 demonstrates that the existence of higher-level control barriers, both in physical and cyber space, results in a low probability of successful exploitation (i.e., P(6)=0.06), while deficient control barriers in physical and cyber space results in a high probability of successful exploitation (i.e., P(8)=0.60).

Table 5: Probability based ranking of successful attack in a descending order for every Node i

Node	Probability of successful attack for Node i, P(i)
8	P(8) = 0.60
1	P(1) = 0.57
7	P(7) = 0.27
3	P(3) = 0.22
4	P(4) = 0.22
2	P(2) = 0.21
5	P(5) = 0.12
6	P(6) = 0.06

To perform the fifth activity (i.e., *Removal of nodes based on probability-based rank and vulnerability assessment as drop of efficiency*), we remove the nodes based on a probability-based rank and assess the vulnerability of transportation network

as drop of efficiency using Equation 3, 4, as presented in Table 6. To calculate initial efficiency and efficiency after the removal of a selected node, the shortest path distance (i.e., d_{ij}) between all set of nodes is applied, considering that every edge has a weight equal to one. For example the shortest path distance between node 1 and node 5 is equal to two, as node 3 acts as a bridge between them (i.e., $d_{15}=2$). Results indicate that the case study transportation network is more vulnerable to the example sensing layer attack, when node 6 is successfully attacked (i.e., drop of network efficiency by 30.6%) although it has been ranked as the probabilistically less vulnerable node (i.e., P(6)=0.06, see Table 5). In contrast the case study transportation network is less vulnerable to the example sensing layer attack, when Node 1 is successfully attacked (i.e., drop of network efficiency by 20.1%), although it has been probabilistically ranked as the second most vulnerable node (i.e., P(1)=0.57, see Table 5). This aligns with the notion of cyber-physical attack, that can result in unforeseen degradation of serviceability level of victimized cyber-physical system [22].

Table 6: Case study vulnerability assessment as drop of efficiency for every Node i

Initial efficiency E(G)	Efficiency E'(i) after node removal	Vulnerability assessment as drop of efficiency (%)
0.369	E'(8)= 0.283	V(8)=23.3%
	E'(1)= 0.295	V(1)=20.1%
	E'(7)= 0.283	V(7)=23.4%
	E'(3)= 0.265	V(3)=28.2%
	E'(4)= 0.279	V(4)=24.2%
	E'(2)= 0.283	V(2)=23.3%
	E'(5)= 0.256	V(5)=30.6%
	E'(6)= 0.256	V(6)=30.6%

5. Conclusion

Transportation networks are gradually transforming to cyber-physical systems due to the merging of IoT enabled devices. IoT devices improve the operation of transport networks but also increase their susceptibility to cyber-physical attacks. Existing studies in vulnerability assessment of transportation network overlook the security issues of IoT enabled transportation infrastructure. To address this gap, a novel vulnerability risk assessment approach is proposed. The approach is based on a BN network attack graph, that enables to integrate both physical and cyber space for the first time. To enable accurate assessment of vulnerability states, the ratio PI that considers a detailed attacker profile and control barriers from cyber and physical space is proposed. The probabilistic based ranking table, enable to identify the most vulnerable nodes and measure the vulnerability of transportation as drop of efficiency after their removal. A case study of a transportation network subjected to a cyber-physical attack was applied to demonstrate the usefulness of the approach. Results from Monte Carlo simulations indicate that IoT enabled transportation that lacks control barriers in physical and cyber space are probabilistically more vulnerable, resulting in drop of transportation network efficiency. Overall, the proposed transportation vulnerability assessment approach subjected to cyber-physical attacks can constitute a valuable method for stakeholders who target to integrate the cyber domain in the assessment process of transportation network.

Acknowledgements

This work is financially supported by a University College of Dublin Advanced PhD Scholarship Scheme.

References

[1] B. Martinez-Pastor, M. Nogal, A. O'Connor, and R. Teixeira, "Identifying critical and vulnerable links: A new approach using the Fisher information matrix," *International Journal of Critical Infrastructure Protection,* vol. 39, p. 100570, 2022.

[2] M. Chen, S. Mangalathu, and J.-S. Jeon, "Bridge fragilities to network fragilities in seismic scenarios: An integrated approach," *Engineering Structures,* vol. 237, p. 112212, 2021.

[3] K. Ntafloukas, D. P. McCrum, and L. Pasquale, "A Cyber-Physical Risk Assessment Approach for Internet of Things Enabled Transportation Infrastructure," *Applied Sciences,* vol. 12, no. 18, p. 9241, 2022.

[4] K. Ntafloukas, D. P. McCrum, and L. Pasquale, "A risk assessment approach for IoT enabled transportation infrastructure subjected to cyber-physical attacks," in *32nd European Safety and Reliability Conference*, Ireland, 28th August – 1st September 2022 2022, doi: doi:10.3850/978-981-18-5183-4_S23-01-053-cd. [Online]. Available: https://www.rpsonline.com.sg/proceedings/esrel2022/html/S23-01-053.xml

[5] ENISA, "Security measures in the Railway Transport Sector," in "Railway Cybersecurity," European Union Agency for Cybersecurity, November 13, 2020 2020. [Online]. Available: https://www.enisa.europa.eu/publications/railway-cybersecurity

[6] M. Mishra, P. B. Lourenço, and G. V. Ramana, "Structural health monitoring of civil engineering structures by using the internet of things: A review," *Journal of Building Engineering,* p. 103954, 2022.

[7] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of things (IoT) security: Current status, challenges and prospective measures," in *2015 10th international conference for internet technology and secured transactions (ICITST)*, 2015: IEEE, pp. 336-341.

[8] Z. Li, D. Jin, C. Hannon, M. Shahidehpour, and J. Wang, "Assessing and mitigating cybersecurity risks of traffic light systems in smart cities," *IET Cyber-Physical Systems: Theory & Applications,* vol. 1, no. 1, pp. 60-69, 2016.

[9] Y. Liu and H. Man, "Network vulnerability assessment using Bayesian networks," in *Data mining, intrusion detection, information assurance, and data networks security 2005*, 2005, vol. 5812: SPIE, pp. 61-71.

[10] D.-m. Zhang, F. Du, H. Huang, F. Zhang, B. M. Ayyub, and M. Beer, "Resiliency assessment of urban rail transit networks: Shanghai metro as an example," *Safety Science,* vol. 106, pp. 230-243, 2018.

[11] H. Cai, J. Zhu, C. Yang, W. Fan, and T. Xu, "Vulnerability analysis of metro network incorporating flow impact and capacity constraint after a disaster," *Journal of Urban Planning and Development,* vol. 143, no. 2, p. 04016031, 2017.

[12] B. Ghena, W. Beyer, A. Hillaker, J. Pevarnek, and J. A. Halderman, "Green lights forever: Analyzing the security of traffic infrastructure," in *8th USENIX workshop on offensive technologies (WOOT 14)*, 2014.

[13] A. Laszka, B. Potteiger, Y. Vorobeychik, S. Amin, and X. Koutsoukos, "Vulnerability of transportation networks to traffic-signal tampering," in *2016 ACM/IEEE 7th International Conference on Cyber-Physical Systems (ICCPS)*, 2016: IEEE, pp. 1-10.

[14] G. Comert, J. Pollard, D. M. Nicol, K. Palani, and B. Vignesh, "Modeling cyber attacks at intelligent traffic signals," *Transportation research record,* vol. 2672, no. 1, pp. 76-89, 2018.

[15] CAPEC. "Common Attack Pattern Enumeration and Classification." https://capec.mitre.org/ (accessed February 9th, 2023).

[16] V. Latora and M. Marchiori, "Efficient behavior of small-world networks," *Phys. Rev. Lett.,* vol. 87, no. 19, p. 198701, 2001.

[17] M. Rocchetto and N. O. Tippenhauer, "On attacker models and profiles for cyber-physical systems," in *European Symposium on Research in Computer Security*, 2016: Springer, pp. 427-449.

[18] V. Novotný, P. Sysel, J. Přinosil, J. Mekyska, K. Slavíček, and I. Lattenberg, "Critical Infrastructure Monitoring System," in *2021 IEEE 17th International Colloquium on Signal Processing & Its Applications (CSPA)*, 2021: IEEE, pp. 165-170.

[19] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations," *IEEE Communications Surveys & Tutorials,* vol. 21, no. 3, pp. 2702-2733, 2019.

[20] A. I. Ali, S. Z. Partal, S. Kepke, and H. P. Partal, "ZigBee and LoRa based wireless sensors for smart environment and IoT applications," in *2019 1st Global Power, Energy and Communication Conference (GPECOM)*, 2019: IEEE, pp. 19-23.

[21] O. Olawumi, K. Haataja, M. Asikainen, N. Vidgren, and P. Toivanen, "Three practical attacks against ZigBee security: Attack scenario definitions, practical experiments, countermeasures, and lessons learned," in *2014 14th International Conference on Hybrid Intelligent Systems*, 2014: IEEE, pp. 199-206.

[22] C. Foglietta, C. Palazzo, R. Santini, and S. Panzieri, "Assessing cyber risk using the CISIApro simulator," in *International Conference on Critical Infrastructure Protection*, 2015: Springer, pp. 315-331.