

Ranking Resilience Events in IoT Industrial Networks

Maryam Nooraei Abadeh
Department of Computer
Engineering, Abadan Branch,
Islamic Azad University, Abadan,
Iran
Email: mnooraei@iauabadan.ac.ir

Mansoorreh Mirzaie
Faculty of Electrical and Computer
Engineering, Golpayegan University
of Technology, Golpayegan, Iran
Email: mirzaie@gut.ac.ir

Abstract— Maintaining critical data and process availability is an important challenge of Industry 4.0. Given the variety of smart nodes, data and the maximum access latency that can be tolerated by consumers in modern IoT-based industry, we propose a method for analyzing the resiliency of an IoT network. Due to the complexity of the structure of a system, different components in the system can affect the system's resiliency. Therefore, a fundamental problem is to propose an insightful centrality measure to quantify the value of resilience contribution of a node in each system effectively. This paper aims to identify the most critical vertices of the network with respect to the latency constraint resiliency metric. Using important centrality metrics, we identify critical nodes in industrial IoT networks to analyze the degree of resiliency in the IoT environments. The results show that when nodes with the highest value of Closeness Centrality (CC) were disrupted RL would have the lowest value that indicates the nodes with the high values for CC are most critical in an IoT network.

Keywords: *resiliency, centrality metrics, industrial IoT network*

I. INTRODUCTION

Industry 4.0 known as the industrial revolution that by incorporating new information and communication samples, such as the Internet of Things (IoT) is introduced [1]. Two of Industry 4.0's technical enablers are (i) the smart communication infrastructure that will sustain varieties in devices, users and connection methods and (ii) the data processing schemes based on communication infrastructure that will allow efficient delivery of data within future factories. Usually, industrial IoT networks are used for condition control, production processes and predictive maintenance, among others. These industrial applications place strict end-to-end latency provisions on data transmission between hundreds or thousands of network nodes in order to preserve reliability and to monitor performance [2], e.g., end-to-end latencies of 1-100 ms.

The capacity of the hard framework or physical system to deal with serious disruptions is often associated with infrastructure resilience; however, soft infrastructure, i.e. structures and businesses that are vital to social and economic continuity, is often vulnerable to disasters and needs to be well prepared to withstand them. Increasing the resilience of soft infrastructures is not a simple matter for preparing scenarios of

how to response to crisis; the emergency plans are ineffective without creating an organizational culture that aims at achieving resilience. It is also crucial to assess the current resilience and examine the effectiveness of strategies that help a resilient organization. There are several recommendations and methodologies available to date to better clarify organizational stability and strategies for risk reduction. There is, however, minimal research that assesses the stability of soft infrastructure networks in quantitative terms. Using a resilience quantification approach based on an industrial IoT network structure, this paper aims to fill this gap. How to identify essential components in a network is the first stage in analyzing resilience. In this step, the industrial IoT network structure is considered as a directed graph, therefor to obtain resiliency values under disruptive events, the network analysis techniques are applied. The resilience metrics allow system engineers to estimate the existing resilience of the system and act as a benchmark for measuring and demonstrating the added value of the efficacy of resilience strategies.

To analyze resiliency, it is important to consider the structural perspective of a system. Centrality metrics play a basic role in evolving dynamical processes in some networks, such as epidemic spreading and synchronization. There are several metrics for quantifying network structures that we selected four important metrics including degree centrality (DC), betweenness centrality (BC), closeness centrality (CC) and, Eigen Vector centrality (EC).

We implement this approach with 95 real devices and its performance would be analyzed on the FIT IoT-LAB testbed. To investigate the changes of Resiliency of Latency (RL), we implement five scenarios in the IoT-LAB testbed. For each scenario, we assumed that a node with the highest value of each four structural metrics is disrupted and the RL value is computed. The main contributions of this paper are (1) identifying critical nodes in industrial IoT networks to analyze the degree of resiliency in the IoT environment, (2) measuring the resiliency of industrial IoT networks in terms of performance before and after disrupting the critical activities.

The remainder of this paper is organized as follows: In Section 2, we discuss related work. In Section 3, the proposed approach scheme is provided. Section 4 discusses the resiliency in industrial IoT networks. Quantitative experiments are presented in Section 5, and finally, conclusions are provided in Section 6.

II. RELATED WORK

Resilience may be described as a system's ability to perform its function in an acceptable way, which does not tolerate disruptions and regains its performance after an unwanted system failure [3], [4].

As another example, the authors in [5] define network resilience as the capacity, within a certain minimum time span, to provide at least one operational backup path when at least one node fails on the basic path. Traffic resilience can be calculated functionally over the time taken by the network to restore its regular service following interruption [6]. Another strategy uses failure tolerance mechanisms to recover broken systems without missing data based on data replication and synchronization [7].

Also, some resilient routing protocols are proposed in IoT networks [6], [8], [9] and being categorized into various types on the basis of the pathfinding methodology. Another main aspect is the number of failed nodes or links [10] that the network should tolerate as it maintains its performance. Some studies focus on challenges in building a resilient IoT for the Cyber-Physical Systems, e.g., [11], [12], [13].

Supply chain resiliency is another key research area discussed to define the mechanism of its improvement by employing IoT, e.g., [14], [15], [16].

IoT Industrial system resiliency and vulnerability analyses have always been a matter of interest for research regarding the security issues of IoT networks. A detailed cyber security analysis was conducted in [17] for the smart grids system. In this work, a cyber-security framework is proposed which is based on the network traffic management regarding the security issues, automation and power switch management.

A novel approach to identify the vulnerabilities in industrial systems is proposed in [18]. This approach scan and analyses the network traffic and also fuzzing based classification. Furthermore, it could generate the three types of test cases after assessing the network traffic protocol such as protocol data and content.

A comprehensive study, with a focus on the existing security issues, for industrial control systems and industrial IoT devices is done in [19]. The authors discovered that middleware IoT devices may be used for launching attacks on ICS networks. Hence, for increasing security, it is necessary to monitor the linked IT and IoT devices.

In [20], the evolution in IoT based industrial control systems presented and some privacy challenges were discussed. The authors proposed a strong blockchain encryption method. This method is named the Privacy-preserving Energy Transactions (PETra) solution to deal with the security of the system and evaluating the privacy concerns of the modern ICS networks.

In [21], some characteristics of cyber security for industrial IoT systems were presented. The authors found that the ICS nodes attract various types of threats according to their performance and functions. These attacks are usually carried out from inside organizational networks on the ICS nodes. In

comparison with the traditional IT nodes, the number of IoT nodes is more frequent and widely used in various industries and have the risk of collateral damage linked with it.

The authors in [22] analyzed the estimated vulnerability frequency. Furthermore, they investigated the impact of IoT networks from CVSS metric. Their method uses Bayesian belief network (BBN). Some predictions using the environmental metrics had been done to analyzing vulnerability by combining it with integrity, confidentiality and privilege availability. Therefore, the vulnerability frequency score is anticipated by using some structural metrics such as access vector, access complexity and authentication criteria. In this method, the BBN technique is used to predict these additional values.

III. PROPOSED METHOD

This section described the steps of the proposed resiliency ranking method in industrial IoT. The architecture is shown in Figure. 1. For an extracted graph of an IoT industry, various centrality measures are calculated and resiliency is analyzed for each scenario, when a node with the highest value of each structural metric is disrupted. The steps are described in various parts in this section.

A. Industrial IoT network

In this paper, we consider $G = (N, E)$ as a general directed graph with nodes set N and edges set $E \subseteq N \times N$. We assume that $N = \{1, 2, \dots, n\}$ with a total number of $|N|=n$ nodes. Let an ordered pair of nodes $(i, j) \in E$ denote a directed edge from i to j . Networks of industrial IoT devices are considered such as sensor motes, actuators and controller devices. The range value r_u of a node u has changed considering the specifications of the relevant protocol and the limitations of the technical implementation. Nodes $u, v \in N$ are communicating with each other if $r_u, r_v \geq c(u, v)$, where $c(u, v)$ is the Euclidean distance between u and v .

The locations of the nodes are known in industrial applications. Furthermore, traffic flows are deterministic and interaction patterns are developed. The shortest paths in the network had been computed and $n \times n$ matrix D had been created, where $D_{u,v}$ is the length of the shortest path between nodes u and v (the offline shortest path approximation between two nodes is regarded as a major factor in graph theory. This problem can be solved in a polynomial way, using Dijkstra's algorithm).

B. IoT network structural metrics definition

Soft infrastructure networks as non-physical systems need a methodology that is directed towards reliable social systems. The four most important centrality measures considered in the proposed approach are degree, eigenvector, closeness and betweenness. We propose to use structural centrality as a ranking measure to find critical nodes in an IoT industrial network.

For an IoT network, structural-based metrics inspired by [23] are considered as a control on the data structure and dependencies between nodes and the events that occur in each node. Analyzing these metrics to detect the potential IoT design

anti-patterns is one of the great interests, and this study also serves as an interesting baseline for analyzing the critical nodes in IoT environments.

The degree Centrality (DC), as the most typical indicator, assigns a significance score depending on the number of links kept by each node.

EigenVector Centrality (EC) is based on the idea that a relationship with more interconnected nodes causes the own centrality to a greater value than a relationship with a less well-interconnected activity.

Closeness Centrality (CC) can be defined as the inverse shortest-path average length between node x and any other nodes in a process chain.

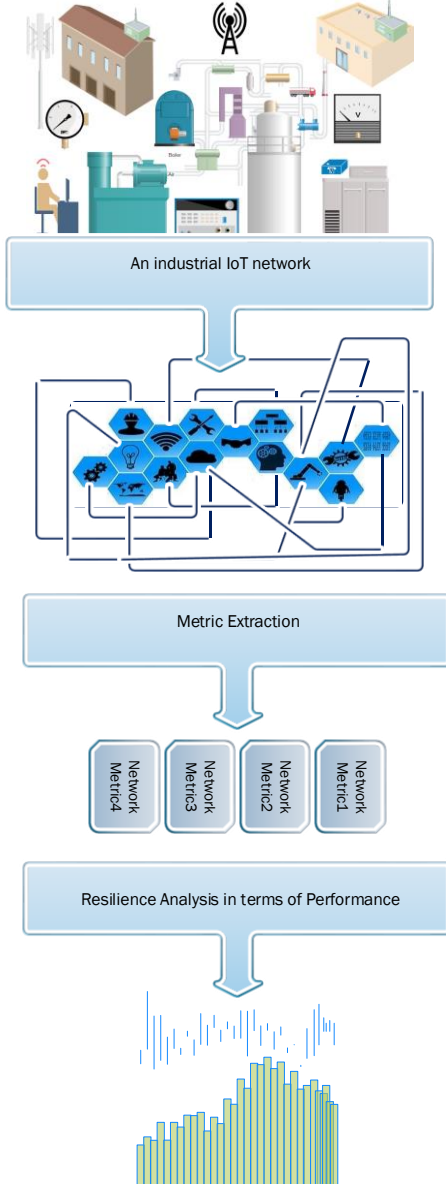


Figure 1. The architecture of the proposed approach

Betweenness Centrality (BC) can be defined as the proportion of the shortest paths between two nodes containing a particular node. On the other hand, this centrality metric

calculates the number of times a node sits on the shortest path to other nodes.

The latency constraint can be defined as the data transmission latency from a node u to another node v is defined by $L_{u,v}$. The access latency is defined as the amount of time it takes for the data to hit user u , after u 's request the data follow a multi-hop propagation between u and p . $\bar{L}$ is defined as the average access latency across all users as the mean value of all the latencies $L_{u,v}$. More specifically, $\bar{L}$ can be computed as the following equation:

$$\bar{L} = \frac{\sum_{u \in S} L_{u,v}}{m} \quad (1)$$

Industrial applications are typically time-critical, so in this work, latency constraint is considered as the main resilience metric to compare the quality of the degraded network with the as-planned network quality during the disruption period.

We measure the ratio of the transmission latency of the network before a disruption, and after a disruption. Therefore, this value varies from 0 to 1. The maximum accessible resilience is 1 and the minimum is close to 0. The information latency time is completely depending on the type of an IoT network, and also the type of operation that has to be executed.

$$R_L = \frac{\bar{L}_{before-shock}}{\bar{L}_{after-shock}} \quad (2)$$

In this paper, we define the resilience of an IoT network by adding hypothetical disturbances to the network. The resilience value is 1 in normal operating conditions. On the other hand, this value indicates that the network is functioning in the expected manner. A network will deteriorate the functionality depending on how resilient is, which will make the resilience metric approach 0. Therefore, most resilient networks provide resilience values of 1 or near to it.

The capacity of the link or severing the link completely makes disruption affect the network resiliency in terms of performance. Reducing the number of links may cause the workload increasing in the remaining links. As a consequence, the time it takes for the necessary information flow to be transmitted or retrieved rises.

IV. EVALUATION

To analyse the changes of RL, we implement five scenarios in the IoT-LAB testbed which named $s_1, s_2, \dots, s_5$. For each scenario, we assumed that a node with the highest value of each four structural metrics is disrupted and RL is computed (Table 1). The rows indicate four important selected structural metrics of networks, which the disrupting node is selected based on the highest value for these metrics. The column indicates RL value for five executed scenarios in the dataset. The result shows that when nodes with the highest value of CC were disrupted RL would have the lowest value that indicates nodes with the high value for CC are most critical in an IoT network.

TABLE1. THE NETWORK RESILIENCY CHANGES FOR VARIOUS SCENARIO

	RL_{s1}	RL_{s2}	RL_{s3}	RL_{s4}	RL_{s5}
DC	0.857143	0.9	0.833333	0.857143	0.878049
BC	0.8	0.857143	0.9375	0.96	0.947368
EC	0.75	0.947368	0.882353	0.827586	0.972973
CC	0.666667	0.75	0.652174	0.774194	0.837209

Furthermore, we interested in understanding the other possible changes of L based on removing Top n nodes with respect to their CC values. So, we define the latency assessment problem (LAP) as follows:

$$V^* = \operatorname{argmax} \Delta L(v')_{v' \in V, |v'| \leq k} \quad (3)$$

$$\Delta L(v) = L(V \setminus v') - L(V) \quad (4)$$

This problem aims to identify the most critical vertices of the network with respect to the latency constraint metric. On the other hand, we analyze the changes of the latency time when the most structural nodes encounter with an unwanted disruption.

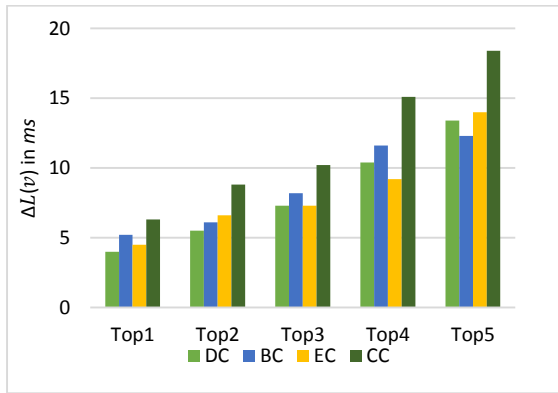
Figure 2. Critical node identification using $\Delta L(v)$

Figure 2 shows the evaluation results of $\Delta L(v)$ based on four centrality metrics when removing Top n important nodes. The charts show the disrupting n top-rank nodes at once (in the horizontal axis) and the changes of latency time (in the vertical axis). It is attempted to find how this accumulative disruption affects the efficiency of the IoT industrial network. As observed in the figure, when some nodes with the highest CC values are disrupted, latency gives more values, in comparison with the other metrics. In other words, the nodes with the highest value of CC have the largest number of important direct links; thus, the impact of a disruption is maximized when these activities are affected. These prove that nodes with a high value of CC are the most critical nodes.

V. CONCLUSION AND FUTURE DIRECTIONS

In this paper, using their structural analysis, we proposed a new method to analyze resiliency in an industrial IoT network.

We consider a way of defining a small number of nodes in an IoT industrial network where given a set of data, the set of user nodes and the maximum connection latency that users can analyze the resiliency of the network. Using the IoT-LAB testbed, we apply the technique and determine its performance. As seen in the figure, when certain nodes with the highest CC values are interrupted, in comparison with other metrics, latency values have a larger increase. In other words, the nodes with the highest value of CC have the largest number of important direct links; thus, the impact of a disruption is maximized when these activities are affected. This shows that the most important nodes are nodes with a higher CC score. When incoming traffic reaches outgoing bandwidth, the next step is to consider account decreased bandwidth in the network, that could lead to congestive failure.

REFERENCES

- [1] S. H. Houmb, V. N. Franqueira, and E. A. Engum, "Quantifying security risk level from CVSS estimates of frequency and impact," *Journal of Systems and Software*, vol. 83, no. 9, pp. 1622-1634, 2010.
- [2] E. Manavalan and K. Jayakrishna, "A review of Internet of Things (IoT) embedded sustainable supply chain for industry 4.0 requirements," *Computers & Industrial Engineering*, vol. 127, pp. 925-953, 2019.
- [3] Y. Haimes, "On the Definition of Resilient Systems," *Risk analysis: an official publication of the Society for Risk Analysis*, vol. 29, pp. 498-501, 05/01 2009.
- [4] P. Uday and K. Marais, "Designing resilient systems - of - systems: A survey of metrics, methods, and challenges," *Systems Engineering*, vol. 18, no. 5, pp. 491-510, 2015.
- [5] J. P. Sterbenz, "Smart city and IoT resilience, survivability, and disruption tolerance: Challenges, modelling, and a survey of research opportunities," in *2017 9th International Workshop on Resilient Networks Design and Modeling (RNDM)*, 2017, pp. 1-6: IEEE.
- [6] Y. Wang, "System resilience quantification for probabilistic design of internet-of-things architecture," in *International Design Engineering Technical Conferences and Computers and Information in Engineering Conference*, 2016, vol. 50084, p. V01BT02A011: American Society of Mechanical Engineers.
- [7] G. Alonso, C. Hagen, D. Agrawal, A. El Abbadi, and C. Mohan, "Enhancing the fault tolerance of workflow management systems," *IEEE Concurrency*, vol. 8, no. 3, pp. 74-81, 2000.
- [8] Y. Tsado, D. Lund, and K. Gamage, "Resilient wireless communication networking for Smart grid BAN," in *2014 IEEE International Energy Conference (ENERGYCON)*, 2014, pp. 846-851: IEEE.
- [9] F. Xing and W. Wang, "Analyzing resilience to node misbehaviors in wireless multi-hop networks," in *2007 IEEE Wireless Communications and Networking Conference*, 2007, pp. 3489-3494: IEEE.
- [10] H. Q. Al-Shammari, A. Q. Lawey, T. E. El-Gorashi, and J. M. Elmirghani, "Resilient Service embedding in IoT networks," *IEEE Access*, vol. 8, pp. 123571-123584, 2020.
- [11] D. Ratasich, F. Khalid, F. Geissler, R. Grosu, M. Shafique, and E. Bartocci, "A roadmap toward the resilient internet of things for cyber-physical systems," *IEEE Access*, vol. 7, pp. 13260-13283, 2019.
- [12] H. Xu, W. Yu, D. Griffith, and N. Golmie, "A survey on industrial Internet of Things: A cyber-physical systems perspective," *IEEE Access*, vol. 6, pp. 78238-78259, 2018.
- [13] J. Rajamäki, "Industry-university collaboration on IoT cyber security education: Academic course," Resilience of Internet of Things and cyber-physical systems," in *2018 IEEE Global*

- Engineering Education Conference (EDUCON)*, 2018, pp. 1969-1977: IEEE.
- [14] Y. Cui, "Improving supply chain resilience with employment of IOT," in *International Conference on Multidisciplinary Social Networks Research*, 2015, pp. 404-414: Springer.
- [15] T. De Vass, H. Shee, and S. J. Miah, "Internet of Things for improving supply chain performance: A Qualitative study of Australian retailers," *ACIS2018 Proceedings*, 2018.
- [16] M. Al-Talib, W. Y. Melhem, A. I. Anosike, J. A. G. Reyes, and S. P. Nadeem, "Achieving resilience in the supply chain by applying IoT technology," *Procedia CIRP*, vol. 91, pp. 752-757, 2020.
- [17] D. Wei, Y. Lu, M. Jafari, P. Skare, and K. Rohde, "An integrated security system of protecting smart grid against cyber attacks," in *2010 Innovative Smart Grid Technologies (ISGT)*, 2010, pp. 1-7: IEEE.
- [18] S. Kim, W. Jo, and T. Shon, "A novel vulnerability analysis approach to generate fuzzing test case in industrial control systems," in *2016 IEEE Information Technology, Networking, Electronic and Automation Control Conference*, 2016, pp. 566-570: IEEE.
- [19] K. Kobara, "Cyber physical security for industrial control systems and IoT," *IEICE TRANSACTIONS on Information and Systems*, vol. 99, no. 4, pp. 787-795, 2016.
- [20] A. Laszka, A. Dubey, M. Walker, and D. Schmidt, "Providing privacy, safety, and security in IoT-based transactive energy systems using distributed ledgers," in *Proceedings of the Seventh International Conference on the Internet of Things*, 2017, pp. 1-8.
- [21] Y. Ge, X. Zhang, and B. Han, "Complex IoT control system modeling from perspectives of environment perception and information security," *Mobile Networks and Applications*, vol. 22, no. 4, pp. 683-691, 2017.
- [22] P. Johnson, R. Lagerström, M. Ekstedt, and U. Franke, "Can the common vulnerability scoring system be trusted? a bayesian analysis," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 6, pp. 1002-1015, 2016.
- [23] S. M. Srinivasan, N. Kilicay-Ergin, R. S. Sangwan, and C. J. Neil, "Ranking critical activities in process architectures," *Procedia Computer Science*, vol. 140, pp. 46-55, 2018.