Heliyon 10 (2024) e27104

Contents lists available at ScienceDirect

Heliyon

journal homepage: www.cell.com/heliyon

Research article

The security of IOT from the perspective of the observability of complex networks

Xu Wu [a,*], Zhengjun Jing [a], Xinwei Wang [b]

[a] School of Computer Engineering, Jiangsu University of Technology, Changzhou, China
[b] College of Automation and College of Artificial Intelligence, Nanjing University of Posts and Telecommunications, Nanjing, China

ARTICLE INFO

Keywords:
IOT
Security
Complex networks
Structural observability

ABSTRACT

The Internet of Things (IOT) is based on the computer Internet, using RFID, wireless data communication and other technologies to construct a network covering everything in the world. It contains numerous entities such as sensors, processors, transmitters and actuators, meanwhile the interactions of which are complicated. These characteristics of IOT are consistent with those of the complex network. Motivated by this, this paper comprehends the security issue of IOT from the sight of the observability of complex network and regards the ability of reconstruction as a security threat to IOT network. We try to identify the minimum vertices whose data could reconstruct the whole data of network, in other words, we need to implement additional protective measures on these vertices to enhance the security of IOT network. By analyzing the topology of IOT network, an identification strategy is adopted and the corresponding algorithm is proposed to identify the minimum protection vertices.

1. Introduction

Now, we live in an era where the Internet of Things is all around us, from mobile terminals like smartphones and wearable devices [1], smart home facilities like temperature controller [2], automatism curtain, and robot vacuum cleaner, industrial systems [3,4] like supply chain management and safety production management, intelligent transportation like vehicle networking [5] and intelligent traffic scheduling. One-sentence understanding of the Internet of Things is connecting all things to the Internet through sensing equipment to realize information exchange, intelligent identification and management. This requires giving each object the intelligence and connectivity to collect, process and transmit data [6]. No matter the smart dust advocating the interconnection of various sensor devices [7,8], the RFID IOT advocating the unique identification of all items [9], or the data ubiquitous aggregation IOT advocating the precise marking on each piece of data [10], all deal with immense amounts of data, along with the close association of industry, military, energy, transportation, logistics and all crucially important fields, the security issues of IOT are of great value and deserve much attention [11–13].

It is requested that the hardware, software and data in IOT are protected and free from accidental or malicious damage, tampering and theft. However due to the vulnerability of Internet, the complexity of network environment, the openness of wireless channels, the lack of monitoring unmanned equipment and so on, the security requirements are difficult to meet. The types of potential attacks include the physical attack, the data eavesdropping and analysis, the unauthorized access [14], the replay attack [15], the Dos attack

* Corresponding author.
E-mail address: xwu@jsut.edu.cn (X. Wu).

https://doi.org/10.1016/j.heliyon.2024.e27104
Received 1 December 2023; Received in revised form 5 January 2024; Accepted 23 February 2024
Available online 24 February 2024

and the malicious code attack [16]. Specifically, in the perception layer, the sensing devices are numerous in quantity and variety, and their own security protection is weak, simultaneously most of which are deployed at the unmonitored locations, the attackers are relatively easy to access to them [17]. In the transport layer, the malware has a large number of entries in wireless network and sensor network environment, so it needs to apply the IPsec, firewall, tunnel services, digital signatures and certificates to enhance the security [18]. In the application layer, the loopholes will affect the system itself, the support software, the network service software, the network router and the firewall [19].

As mentioned before, there are numerous entities such as sensors, processors, transmitters and actuators in IOT and the interactions of which are complicated. These characteristics are consistent with those of complex networks, so it is possible to study the IOT from the perspective of complex network. A large number of research results on complex network has been obtained in different fields such as the Internet, the communication network [20], the traffic network [21], the power grid [22], the social network [23], etc., which are all closely related to our lives. And the research interest involves the synchronization, state estimation, topology identification [24], fault diagnosis [25], virus spreading [26], multi-agents [27], Big Data [28], network game [29] and so on. In a manner of speaking, it covers almost all of aspects of the network. So, the theoretical framework and methods for complex networks provide a new idea in analyzing the IoT network [30].

The controllability and observability are fundamental issues in most complex networks [31–35], and the observability of network concerns the ability to reconstruct the whole states using the partial measured outputs. For a IOT network, if someone could place some sensors onto the partial processors, transmitters or steal the data of partial sensors, it is possible to reconstruct more data or even the whole data of the IOT network. Inspired by this, the concept of network observability is applied to study the security issue of IOT networks in this work. We introduce the IOT network onto a directed graph and try to identify the minimum vertices for implementing additional protective measures to enhance the security of IOT network, by analyzing its topology, an identification strategy that maximizing the number of pm-rSCCs (the definition sees Section 3) which contain unmatched vertices in a maximum matching is adopted. Then the corresponding algorithm is proposed and demonstrated by simulations.

The rest of the paper is organized as follows. Section 2 describes the main problem studied in this work. In Section 3, an identification strategy is adopted and the corresponding algorithm is proposed. In Section 4, a numerical example is given to validate the theoretical results. Finally, Section 5 concludes the paper and discusses the further research interests.

2. Problem statement

As mentioned above, it could study the IOT network from the perspective of the complex network. For an existing IOT, we could introduce it onto a directed graph $G = (V,E)$, where the entities in IOT are regarded as the vertices and the interactions between these entities are regarded as the links in the IOT network. Concretely, $V = \{1, \cdots, n\}$ is the vertex set and $E = \{(j,i) \mid \text{vertex } i \text{ transmits information to vertex } j\}$ is the edge set. In Fig. 1(a), there are four vertices in a simple IOT network.

According to the observability concept of complex network, it could reconstruct the whole information of the network only by information of partial vertices. So, it only needs to place sensors onto the partial vertices or steal the data of partial vertices in the sensor network, then the data of the whole IOT network could be obtained by reconstruction, and just few vertices are needed for reconstruction in the large-scale real networks in general. Inspired by this, we try to identify the minimum vertices for reconstructing the IOT network in this paper, and then we could implement additional protective measures on these vertices to enhance the security of IOT network. Here, we also called these vertices as the protection vertices.

Here we recall some graph-theoretic concepts.

Definition 1. For a directed graph, a maximum matching is a largest subset of edges which do not share common starting vertices or ending vertices.

The maximum matching M of $G = (V,E)$ could be determined by its bipartite representation $B(V^+, V^-, E')$ where V^+ and V^- denote the starting and ending vertices sets respectively, and $E' = \{(j^+, i^-) \mid (j,i) \in E\}$. In a maximum matching, a vertex is matched if it is an ending vertex of an edge in the matching and the others are unmatched vertices (see Fig. 1(b), vertices 1, 2, 3 are matched vertices). A maximum matching is called a perfect matching if every vertex is matched.

Definition 2. For a directed graph, a Strongly Connected Component (SCC) is a subgraph where there is a directed path from each vertex to every other vertex.

Further, a SCC is a root SCC (rSCC) if it has no incoming edges to its vertices from other vertices.

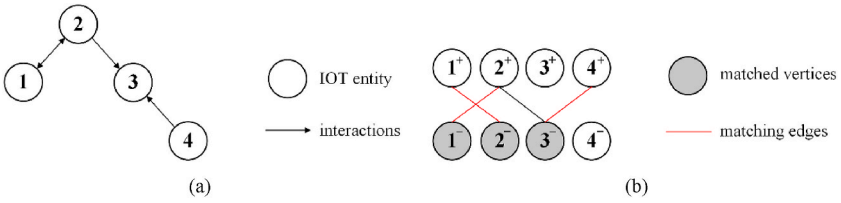

Fig. 1. A simple example of IOT network. (a) The vertices are marked in white circles and the interactions are marked by black arrows; (b) The bipartite representation and its maximum matching where the matched vertices are marked by grey and the matching edges are marked by red.

3. Main results

In this section, the strategy of identifying the minimum protection vertices is discussed, then the corresponding algorithm is proposed and analyzed.

3.1. Identification strategy

According to the Minimum Inputs Theorem [36] and the duality between the controllability and the observability, it should set sensors to measure the unmatched vertices to guarantee the network is observable. Here, these vertices are called sensor vertices (According to the security considerations in this paper, the sensor vertices are also the protection vertices). If the maximum matching of this rSCC is perfect, there exist no sensor vertices, whereas by definition, a rSCC is overall inaccessible, so we also need to measure it and a random vertex of which to be measured is enough. Here we called a rSCC which has perfect matching as a pm-rSCC (see Fig. 1, vertices 1, 2 and edges $(1,2)$, $(2,1)$ form a pm-rSCC). In this paper, we concentrate on the identification of the minimum protection vertices with the pm-rSCC existing in the IOT network.

With a goal of minimizing the number of protection vertices, the number of additional measured vertices should be minimized. While there exists an unmatched vertex in a pm-rSCC, there is no need to additionally set a sensor for this pm-rSCC. Consequently, the identification strategy in this paper is maximizing the number of pm-rSCCs which contain unmatched vertices in a maximum matching. For example, in Fig. 2, in the first kind of maximum matching, there exist no unmatched vertices in the pm-rSCC formed by vertices 1, 2 and edges $(1,2)$, $(2,1)$, so we need to choose the vertex 1 or 2 as an additional protection vertex, the number of protection vertices is 3. While in the second kind of maximum matching, vertex 1 is unmatched, so we just choose the unmatched vertices as the protection vertices, the number of protection vertices is 2.

Remark 1. For a directed graph, its maximum matching is not unique in the vast majority of cases. Therefore, we could choose an appropriate maximum matching to conform with the adopted identification strategy.

3.2. Algorithm design and analysis

According to the identification strategy mentioned in Section 3.1, we try to force the vertices in pm-rSCCs as the unmatched vertices, as long as one vertex in a pm-rSCC could be an unmatched vertex in a maximum matching, the number of protection vertices will decrease by one, hence an Algorithm is proposed. Some initial preparations are as follows: Compute an initial maximum matching M of $G = (V,E)$, and obtain the pm-rSCCs by applying twice depth-first searches, denoted by $\eta_1, \ldots, \eta_\beta$ where $S = \{1, \ldots, \beta\}$.

Algorithm
Identify the set of minimum protection vertices of an IOT network.

Input: M, $B(V^+, V^-, E^{'})$, $\eta_1, \ldots, \eta_\beta$
Output: Set of protection vertices $V^{protection}$
1: $V^{temp} = \{\}$;
2: for all $\lambda \in \eta_1 \cup \cdots \cup \eta_\beta - V^{temp}$
3: Compute a maximum matching M^{λ} with $B(V^+, V^-, E^{'} - \{(\nu,\lambda) : \nu \in V\})$, obtaining the unmatched vertices set V^{λ};

(*continued on next page*)

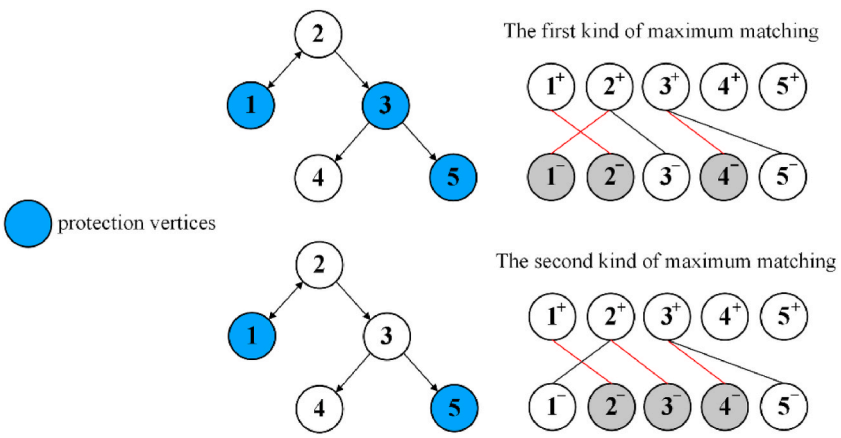

Fig. 2. An illustration of the adopted identification strategy. In the first kind of maximum matching, vertices 1, 3, 5 are protection vertices. In the second kind of maximum matching, vertices 1, 5 are protection vertices. The second kind of maximum matching conforms with the adopted identification strategy.

Algorithm (*continued*)

4: if $|M| == |M^{\lambda}|$ where $\lambda \in \eta_s$
5: $V^{temp} = V^{temp} \cup \eta_s$;
6: $S = S - \{s\}$;
7: $E^{'} = E^{'} - \{(\nu, \lambda) : \nu \in V\}$;
8: $V^{protection} = V^{\lambda}$;
9: else $V^{temp} = V^{temp} \cup \lambda$;
10: end if
11: end for
12: for all $s \in S$
13: Randomly choose a vertex λ from η_s and $V^{protection} = V^{protection} \cup \lambda$;
14: end

Now, we will explain the process of obtaining the minimum protection vertices of the IOT network with an illustrative example shown in Fig. 3. In this simple IOT network, there exist 3 p.m.-rSCCs which contain vertices 1 and 4, vertices 2 and 3, vertices 7 and 8 respectively. In the initial situation (see Fig. 3(a)), the matching edges are marked by red and the unmatched vertices are vertices 5 and 9. Here there are no pm-rSCCs which contain unmatched vertices, so randomly choose a vertex from each pm-rSCC, specifically, vertices 1, 2, 7 are chosen as the additional sensor vertices, here $V^{protection} = \{1,2,5,7,9\}$. Now it's time to execute the Algorithm, the initial data is $|M| = 7$, $V^{temp} = \{\}$, $S = \{1,2,3\}$. Select $\lambda = 1$ from η_1 and remove the edge $(4,1)$ in $B(V^{+}, V^{-}, E^{'})$, now the maximum matching $|M^1| = 7 = = |M|$, so $V^{temp} = \{1,4\}$, $S = \{2,3\}$, the edge $(2,1)$ is definitely removed, $V^1 = \{1,9\}$, if we stop at this moment and choose vertices 2, 7 as the additional sensor vertices, $V^{protection} = \{1,2,7,9\}$ (see Fig. 3(b)). Now execute the next loop, select $\lambda = 2$ from η_2 and remove the edge $(3,2)$ in $B(V^{+}, V^{-}, E^{'})$, now the maximum matching $|M^2| = 6 \neq |M|$, $V^{temp} = \{1,2,4\}$ (see Fig. 3(c)), so execute the next loop, select $\lambda = 3$ from η_2 and remove the edge $(2,3)$ in $B(V^{+}, V^{-}, E^{'})$, now the maximum matching $|M^3| = 6 \neq |M|$, $V^{temp} = \{1,2,3,4\}$ (see Fig. 3(d)). So continue the next loop, select $\lambda = 7$ from η_3 and remove the edge $(8,7)$ in $B(V^{+}, V^{-}, E^{'})$, now the maximum matching $|M^7| = 7 = = |M|$, so $V^{temp} = \{1,2,3,4,7,8\}$, $S = \{2\}$, the edge $(8,7)$ is definitely removed, $V^7 = \{1,7\}$, and at this moment the steps (1)–(11) have been completed, $V^{protection} = \{1,7\}$, and then choose the vertex 2 from η_2, the final $V^{protection} = \{1,2,7\}$ (steps (12)–(14)), which is shown in Fig. 3(e). Through the Algorithm, the number of protection vertices decrease from 5 to 3, as well as the minimum number of protection vertices.

Remark 2. The main process of the Algorithm is calculating multi maximum matchings, whose time complexity is $\sum_{s=1}^{\beta} |\eta_s| O(\sqrt{|V|}\,|E|)$. And the time complexity of the other processes is constant complexity.

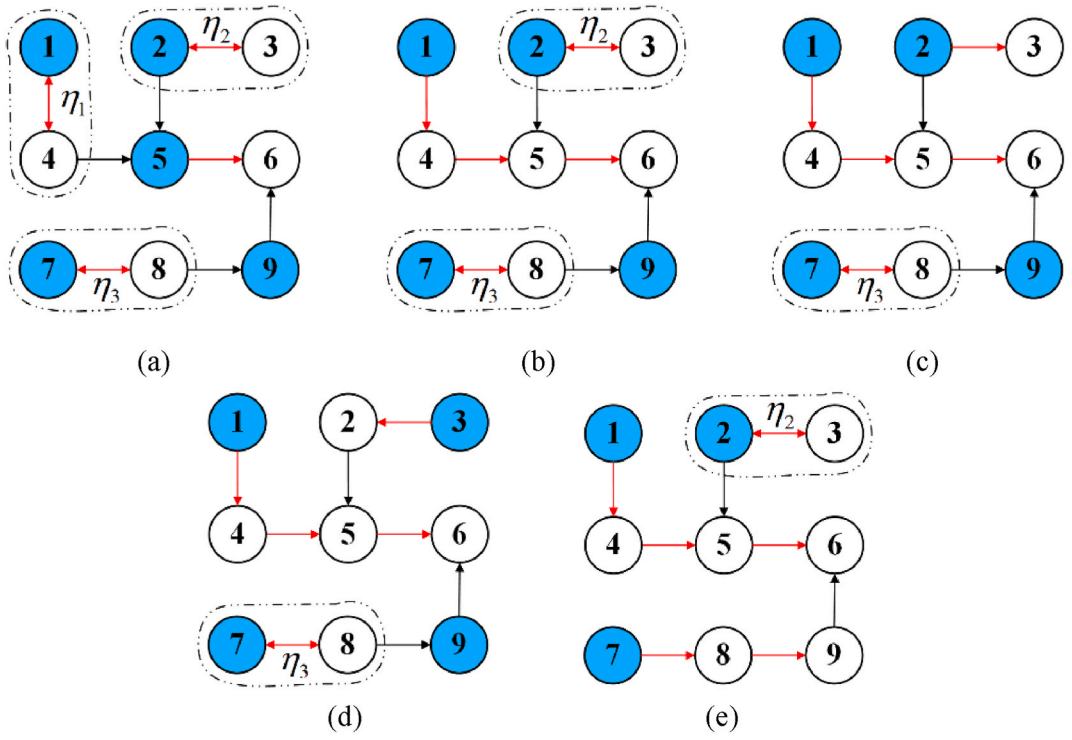

Fig. 3. An illustration of obtaining the minimum protection vertices. (a) The initial situation; (b)–(e) The execution of the Algorithm.

4. Simulations

Here, the IOT network for simulation still uses the example in Fig. 3. Simultaneously, in order to verify the reconstruction of the protection vertices, each vertex is given the following discrete dynamic:

$$\mathbf{x}_{i,k+1} = \mathbf{A}\mathbf{x}_{i,k} \tag{1}$$

where $\mathbf{A} = \begin{bmatrix} 0 & 0 & 0 \\ 2.1 & 0 & 0 \\ -1.6 & 0 & 0 \end{bmatrix}$ is the system matrix of the vertex, each vertex state is denoted as $\mathbf{x}_{i,k} = (x_{i1,k}, x_{i2,k}, x_{i3,k})^T \in R^3, i = 1,\ldots,9$. And then the IOT network could be formulated as follows:

$$\mathbf{x}_{i,k+1} = \mathbf{A}\mathbf{x}_{i,k} + \sum_{j=1}^{9} d_{ij}\mathbf{\Gamma}\mathbf{x}_{j,k} \tag{2}$$

where $\mathbf{\Gamma} = \mathbf{I}_3$ is the inner connecting matrix, $\mathbf{D} = (d_{ij})_{9\times 9}$ denotes the network topology.

From the previous results, vertices 1, 2 and 7 are protection vertices, so the output could be formulated as follows:

$$\mathbf{y}_{i,k} = \mathbf{C}_i\mathbf{x}_{i,k} \tag{3}$$

where $\mathbf{C}_i$ denotes the output matrix, and $\mathbf{C}_i = \mathbf{I}_3$ for $i = 1,2,7$, $\mathbf{C}_i = \mathbf{O}$ for else, $\mathbf{O}$ is a zero matrix of suitable dimension. Then equations (2) and (3) could be rewritten as follows:

$$\begin{aligned} \mathbf{X}_{k+1} &= \mathbf{A}^*\mathbf{X}_k \\ \mathbf{Y}_k &= \mathbf{C}^*\mathbf{X}_k \end{aligned} \tag{4}$$

where $\mathbf{X}_k = (\mathbf{x}_{1,k}{}^T, \ldots, \mathbf{x}_{9,k}{}^T)^T$, $\mathbf{A}^* = \mathbf{I}_9 \otimes \mathbf{A} + \mathbf{D} \otimes \mathbf{\Gamma}$, $\mathbf{C}^* = \begin{bmatrix} \mathbf{I}_3 & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} \\ \mathbf{O} & \mathbf{I}_3 & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} \\ \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{I}_3 & \mathbf{O} & \mathbf{O} \end{bmatrix}$.

Then an observer for this network is built as follows:

$$\begin{aligned} \hat{\mathbf{X}}_{k+1} &= \mathbf{A}^*\hat{\mathbf{X}}_k - \mathbf{L}(\hat{\mathbf{Y}}_k - \mathbf{Y}_k) \\ \hat{\mathbf{Y}}_k &= \mathbf{C}^*\hat{\mathbf{X}}_k \end{aligned} \tag{5}$$

where $\hat{\mathbf{X}}_k$ and $\hat{\mathbf{Y}}_k$ denote the states and outputs of the observer respectively, $\mathbf{L}$ is the observer gain. Then the observation errors could be obtained:

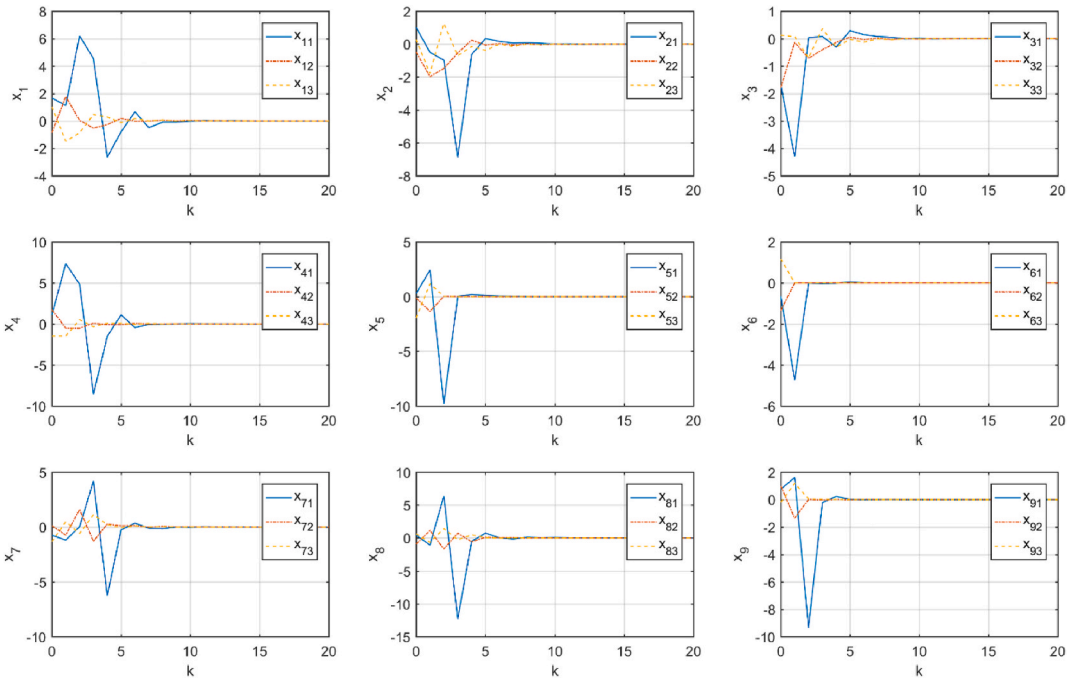

Fig. 4. The observation errors in each vertex.

$$\mathbf{E}_{k+1} = \widehat{\mathbf{X}}_{k+1} - \mathbf{X}_k = (\mathbf{A}^* - \mathbf{L}\mathbf{C}^*)\mathbf{E}_k \tag{6}$$

Define a Lyapunov function as follows:

$$V_k = \mathbf{E}_k^T \mathbf{P} \mathbf{E}_k \tag{7}$$

Differentiating V_k gives

$$\begin{aligned} \Delta V_k &= V_{k+1} - V_k \\ &= \mathbf{E}_{k+1}^T \mathbf{P} \mathbf{E}_{k+1} - \mathbf{E}_k^T \mathbf{P} \mathbf{E}_k \\ &= \mathbf{E}_k^T (\mathbf{A}^* - \mathbf{L}\mathbf{C}^*)^T \mathbf{P} (\mathbf{A}^* - \mathbf{L}\mathbf{C}^*) \mathbf{E}_k - \mathbf{E}_k^T \mathbf{P} \mathbf{E}_k \\ &= \mathbf{E}_k^T \left(\mathbf{A}^{*T} \mathbf{P} \mathbf{A}^* - \mathbf{A}^{*T} \mathbf{P} \mathbf{L} \mathbf{C}^* - \mathbf{C}^{*T} \mathbf{L}^T \mathbf{P} \mathbf{A}^* + \mathbf{C}^{*T} \mathbf{L}^T \mathbf{P} \mathbf{L} \mathbf{C}^* - \mathbf{P} \right) \mathbf{E}_k \end{aligned} \tag{8}$$

According to the Lyapunov stability theory, system (6) is asymptotically stable if $\Delta V_k < 0$, that is

$$\mathbf{A}^{*T} \mathbf{P} \mathbf{A}^* - \mathbf{A}^{*T} \mathbf{P} \mathbf{L} \mathbf{C}^* - \mathbf{C}^{*T} \mathbf{L}^T \mathbf{P} \mathbf{A}^* + \mathbf{C}^{*T} \mathbf{L}^T \mathbf{P} \mathbf{L} \mathbf{C}^* - \mathbf{P} < 0 \tag{9}$$

Then the observer gain $\mathbf{L}$ could be obtained by solving the inequation (9), here $\mathbf{L} \in R^{27\times 9}$, due to its large size, the concrete value is omitted.

Shown in Fig. 4, it is apparent that all observation errors converge to zero finally, implying it just needs the data of 3 vertices that the data of the whole IOT network could be reconstructed. Consequently, it is necessary to implement additional protective measures on these vertices to enhance the security of the whole IOT network.

5. Conclusion

In this paper, from the perspective of the observability of complex networks, we study the security of IOT network. The observability of complex networks is converted into the ability to reconstruct the whole data of the IOT network from the data of partial vertices. By analyzing the topology of IOT network, an identification strategy that maximizing the number of pm-rSCCs which contain unmatched vertices in a maximum matching is adopted. Then a corresponding algorithm is proposed and demonstrated by simulations that the algorithm proposed is effective.

The structure of IOT is quite complicated in practice, and in this work, the structure is simplified. The actual IOT networks may possess the multilayer structure, community structure and so on. Hence it faces more challenges to investigate the more complicated IOT network.

Data availability

No data was used for the research described in the article.

CRediT authorship contribution statement

Xu Wu: Writing – review & editing, Writing – original draft, Funding acquisition, Formal analysis. **Zhengjun Jing:** Supervision, Conceptualization. **Xinwei Wang:** Visualization, Software.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This work is supported by the Natural Science Foundation of the Jiangsu Higher Education Institutions of China (grant No. 21KJB120001).

References

[1] S. Wang, Sports training monitoring of energy-saving IoT wearable devices based on energy harvesting, Sustain. Energy. Techn. 45 (2021) 101168.
[2] V. Chang, C. Martin, An industrial IoT sensor system for high-temperature measurement, Comput. Electr. Eng. 95 (2021) 107439.
[3] E. Sisinni, A. Saifullah, S. Han, et al., Industrial internet of things: challenges, opportunities, and directions, IEEE Trans. Ind. Inf. 14 (11) (2018) 4724–4734.
[4] P. Radanliev, D.D. Roure, R. Nicolescu, et al., Digital twins: artificial intelligence and the IoT cyber-physical systems in Industry 4.0, Int. J. Intell. Robot. 6 (1) (2022) 171–185.
[5] E. Husni, G.A. Prayoga, J.D. Tamba, et al., Microclimate investigation of vehicular traffic on the urban heat island through IoT-Based device, Heliyon 8 (11) (2022) e11739.
[6] S. Amendola, et al., RFID technology for IoT-based personal healthcare in smart spaces, IEEE Internet Things 1 (2) (2014) 144–152.
[7] J. Liu, G. Faulkner, B. Choubey, et al., A tunable passband logarithmic photodetector for IoT smart dusts, IEEE Sensor. J. 18 (13) (2018) 5321–5328.
[8] J. Park, K.H. Park, A Network Traffic Reduction Method for a Smart Dust IoT System by Sensor Clustering[C]//Advances in Security, Networks, and Internet of Things: Proceedings from SAM'20, ICWN'20, ICOMP'20, and ESCS'20, Springer International Publishing, 2021, pp. 693–697.

[9] K. Fan, W. Jiang, H. Li, et al., Lightweight RFID protocol for medical privacy protection in IoT[J], IEEE Trans. Ind. Inf. 14 (4) (2018) 1656–1665.
[10] Y. Shen, T. Zhang, Y. Wang, et al., Microthings: a generic iot architecture for flexible data aggregation and scalable service cooperation, IEEE Commun. Mag. 55 (9) (2017) 86–93.
[11] K. Hughes-Lartey, M. Li, F.E. Botchey, et al., Human factor, a critical weak point in the information security of an organization's Internet of Things, Heliyon 7 (3) (2021) e06522.
[12] L. Xiao, X. Wan, X. Lu, et al., IoT security techniques based on machine learning: how do IoT devices use AI to enhance security? IEEE Signal Process. Mag. 35 (5) (2018) 41–49.
[13] A. Riahi, Y. Challal, E. Natalizio, et al., A Systemic Approach for IoT security[C]//2013 IEEE International Conference on Distributed Computing in Sensor Systems, IEEE, 2013, pp. 351–355.
[14] C. Hahn, J. Kim, H. Kwon, et al., Efficient iot management with resilience to unauthorized access to cloud storage, IEEE T Cloud. Comput. 10 (2) (2020) 1008–1020.
[15] F. Farha, H. Ning, S. Yang, et al., Timestamp scheme to mitigate replay attacks in secure ZigBee networks, IEEE Trans. Mobile Comput. 21 (1) (2020) 342–351.
[16] D. Wei, X. Qiu, Status-based Detection of Malicious Code in Internet of Things (IoT) devices[C]//2018 IEEE Conference on Communications and Network Security (CNS), IEEE, 2018, pp. 1–7.
[17] H.A. Khattak, M.A. Shah, S. Khan, et al., Perception layer security in internet of things, Future Generat. Comput. Syst. 100 (2019) 144–164.
[18] P. Li, J. Su, X. Wang, iTLS: lightweight transport-layer security protocol for IoT with minimal latency and perfect forward secrecy, IEEE Internet Things 7 (8) (2020) 6828–6841.
[19] P.K. Donta, S.N. Srirama, T. Amgoth, et al., Survey on recent advances in IoT application layer protocols and machine learning scope for research directions, Digit Commun. Netw. 8 (5) (2022) 727–744.
[20] X. Han, Q. Huangpeng, Q. Gao, et al., Study of data center communication network topologies using complex network propagation model, Front. Physiol. 11 (2023) 1174099.
[21] J.J. Wu, Z.Y. Gao, H. Sun, Optimal traffic networks topology: a complex networks perspective[J], Physica A 387 (4) (2008) 1025–1032.
[22] D. Zhou, F. Hu, S. Wang, et al., Power network robustness analysis based on electrical engineering and complex network theory, Physica A 564 (2021) 125540.
[23] D. Wanduku, A novel complex social network rumor stochastic model: convergence in distribution to a final rumor size, Heliyon 9 (4) (2023) e15125.
[24] S. Zhu, J. Zhou, G. Chen, et al., A new method for topology identification of complex dynamical networks, IEEE Trans. Cybern. 51 (4) (2019) 2224–2231.
[25] T. Huang, Q. Zhang, X. Tang, et al., A novel fault diagnosis method based on CNN and LSTM and its application in fault diagnosis for complex systems, Artif. Intell. Rev. (2022) 1–27.
[26] H.J. Li, W. Xu, S. Song, et al., The dynamics of epidemic spreading on signed networks, Chaos, Solit. Fractals 151 (2021) 111294.
[27] W. Lu, X. Liu, T. Chen, Adaptive algorithms for synchronization, consensus of multi-agents and anti-synchronization of direct complex networks, Neurocomputing 414 (2020) 365–370.
[28] S. Barja-Martinez, M. Aragüés-Peñalba, Í. Munné-Collado, et al., Artificial intelligence techniques for enabling Big Data services in distribution networks: a review, Renew. Sust. Energ. Rev. 150 (2021) 111459.
[29] R. Fan, Y. Wang, F. Chen, et al., How do government policies affect the diffusion of green innovation among peer enterprises?-An evolutionary-game model in complex networks, J. Clean. Prod. 364 (2022) 132711.
[30] X. Wu, J. Wang, P. Li, et al., Internet of things as complex networks, IEEE Network 35 (3) (2021) 238–245.
[31] D. Leitold, Á. Vathy-Fogarassy, J. Abonyi, Controllability and observability in complex networks–the effect of connection types, Sci. Rep. 7 (1) (2017) 151.
[32] F.L. Iudice, F. Sorrentino, F. Garofalo, On node controllability and observability in complex dynamical networks, IEEE Control Systems Letters 3 (4) (2019) 847–852.
[33] S. Pang, Z. Tian, W. Ma, Structural controllability and observability of complex network with output feedback, Physica A 620 (2023) 128790.
[34] R.M. D'Souza, M. di Bernardo, Y.-Y. Liu, Controlling complex networks with complex nodes, Nat. Rev. Phys. 5 (4) (2023) 250–262.
[35] C.W. Hays, A. Soderlund, S. Phillips, et al., Ubiquitous Controllability of Single Input Linear Time-Invariant Systems[C]//2023 American Control Conference, ACC). IEEE, 2023, pp. 4161–4166.
[36] Y.-Y. Liu, J.J. Slotine, A.-L. Barabási, Controllability of complex networks, Nature 473 (7346) (2011) 167–173.