

Spectral graph theoretic analysis of large-scale network topologies with applications to secure data transmission

Jyoti L. Bangare [†]

Nilofer Kittad ^{*}

Ashwini Rajurkar [§]

Department of Computer Engineering

MKSSS's Cummins College of Engineering for Women

Savitribai Phule Pune University

Pune 411052

Maharashtra

India

Abstract

As the topology of the network grows, nodes fail and links become unavailable, and there are more malicious attacks, the communication networks must be able to transmit data securely and reliably. This study introduces a spectral graph theoretic approach to study the network topology and provides security-aware routing. Communication networks are modeled as weighted graphs, and the spectral properties are used to measure connectivity, find structurally important nodes, discover vulnerable links, and determine the robustness of networks. The proposed solution is to utilize the spectral information and path reliability, communication cost, and security risk along with the transmission delay to choose the robust transmission paths. Multiple network sizes, topology structures and under normal and attack conditions are considered in experimental evaluation. Results show that proposed routing framework can obtain better packet delivery, path reliability, secure transmission, and network resilience than shortest path, reliability-based routing, and traditional security-aware routing methods. The results highlight the potential of spectral graph analysis to give global information about a network in the context of adaptive routing decision-making, as well as the scalability of the method for enhancing secure data transmission in large-scale, dynamic and complex communication networks.

Subject Classification: 68M12.

Keywords: Network topology, Algebraic connectivity, Network resilience, Security-aware routing, Vulnerability analysis, Large-scale networks.

[†] E-mail: jyoti.bangare@cumminscollege.in

^{*} E-mail: nilofer.attar@cumminscollege.in (Corresponding Author)

[§] E-mail: ashwini.rajurkar@cumminscollege.in

1. Introduction

As communication infrastructure, wireless systems, Internet of Things (IoT) environments, cloud platforms, and distributed computing have become increasingly large and complex, the diverse network topologies have increased in size and complexity, as well [1]. Mechanisms that allow to assess connectivity, identify structurally important nodes, detect vulnerable links and select reliable communication paths are required for efficient and secure transmission of information over these networks. First, local parameters, such as node degree, hop count, bandwidth, delay, and link quality, are usually used in conventional network analysis techniques [2]. While helpful, such measures may not be sufficient to capture a network's structural properties that affect its robustness and security across the world. A powerful mathematical tool to describe the structure of a network is spectral graph theory, which is based on the eigenvalues and eigenvectors of the matrices that are associated with the graph [3]. Communication network can be modeled by a graph in which nodes will be devices, routers, sensors, or servers, and links between nodes will be communication links. Quantitative descriptions of network connectivity are given by the adjacency matrix, the degree matrix and the graph Laplacian [4]. Algebraic connectivity, spectral radius, and spectral gap can provide insight into important nodes, connectivity holes, network partitions, and vulnerabilities in the network that could impact secure data transmission [5].

This work introduces a spectral graph theoretic method to analyse large scale network topologies and make a better secure data transmission. The proposed framework combines with spectral network characterization, critical-node identification, vulnerability assessment and security-aware route selection. Eigenvalue-based indicators are used to measure the robustness of a network and determine communication links that will continue to connect the network in the event of node failures or link failures, as well as malicious attack. The framework also takes into account the reliability of the transmission and the cost of a path when calculating the route, as well as the security risk. The study proposes a mathematical model of the spectral characteristics and experimental evaluation of secure routing performance and analyzes the relationship between them.

2. Mathematical Modeling of Large-Scale Network Topologies

The model of a large scale communication network is an undirected weighted graph ($G = (V, E, W)$) with nodes ($V = \{v_1, v_2, \dots, v_n\}$) and communication links (E) and weights on them (W). Each node can be a router, sensor, gateway, server or a communication device. The arrows ($e_{ij} \in E$) represent communication links that are available between the nodes (v_i) and (v_j). A link weight can be a measure of the transmission cost, latency, bandwidth, reliability or security risk [6]. An adjacency matrix ($A = [a_{ij}]$), is a matrix used to represent the network structure:

$$a_{ij} = \{w_{ij}, 0, \text{if } (v_i, v_j) \in E, \text{otherwise.}\}$$

The degree matrix (D) is a diagonal matrix whose entries are defined as shown below.

$$D_{\{ii\}} = \sum_{\substack{j=1 \\ \{ij\}}}^{\{n\}a} E$$

Using these matrices, the graph Laplacian is formulated as

$$L = D - A.$$

The eigenvalues of (L) are arranged as

$$0 = \lambda_1 \leq \lambda_2 \leq \dots \leq \lambda_n.$$

The algebraic connectivity (λ_2) is the second lowest (smallest non zero) eigenvalue of a network and it is a significant measure of network robustness. A large (λ_2) value often reflects high connectivity and high resistance to network partition while a low value means low structural connectivity. In a heterogeneous network, the normalized Laplacian is given by

$$L_N = I - D^{-\frac{1}{2}} A D^{-\frac{1}{2}}.$$

The spectral gap can further be represented as

$$\Delta_\lambda = \lambda_3 - \lambda_2,$$

Adding more of the information from structural separation and network communities. These spectral parameters allow the global characterization of network topology, in addition to the local ones that are traditionally used. The mathematical model integrates the eigenvalues of the system with the reliability of the links, the cost of the transmission, and the parameter of the risk of attack to the network, so it can be used to find out the most important points of the network and choose the most secure routes for communication. Therefore, the spectral representation can be used for further vulnerability analysis and routing optimization for secure data transmission in the large-scale network.

3. Proposed Spectral Graph-Based Secure Transmission Framework

The proposed Secure Transmission Scheme based on the Spectral Graph is a graph spectral-based scheme with security awareness routing to enhance reliable data transmission in large-scale communication networks. This framework analyzes the global structural characteristics of the network, identifies critical nodes and weak links, estimates the security risks, and measures the transmission paths that ensures the transmission network has a balance of connectivity, reliability, security and communication costs [7], [8]. The Laplacian matrix ($L=D-A$) is built and the spectral properties of the network ($G=(V,E,W)$) are investigated. To estimate the importance of node (v_i), a node centrality measure based on the eigenvector of the spectral data is used:

$$SC_i = \{|u_i|\} \left\{ \sum_{j=1}^{\{n\}|u_j|} u_i \right\}$$

where (u_i) is the component of the selected eigenvector. The nodes whose (SC_i) values are higher are recognized as important elements of the network, and are termed as structurally influential nodes. These communication links are also given a score for the level of security risk:

$$R_{\{ij\}} = \alpha T_{\{ij\}} + \beta V_{\{ij\}} + \gamma F_{\{ij\}},$$

(Threat probability) $T_{\{ij\}}$, (Vulnerability level) $V_{\{ij\}}$ and (Link-failure probability) $F_{\{ij\}}$ represent the probability of attack, vulnerability and the probability of failure of the link, respectively. The following equations:

$$\alpha + \beta + \gamma = 1.$$

A composite routing objective is used to determine an appropriate secure route (P) between source and destination nodes is used as shown in equation (1):

$$J(P) = w_{1C(P)} + w_{2R(P)} + w_{3D(P)} - w_{4Q(P)},$$

The transmission cost, accumulated security risk, communication delay and path reliability are $(C(P))$, $(R(P))$, $(D(P))$ and $(Q(P))$ respectively. The best secure route is thus chosen as

$$P^{\{*\}} = \arg \min_{\{P \in \{P\}\}} J(P)$$

Path in the candidate set with highly vulnerable nodes or links is penalised/excluded before data forwarding. Network stability is then checked by observing spectral connectivity to assess that whether failures/attacks have negatively impacted the network significantly or not [9]. If the algebraic connectivity is below a predefined threshold, then the route will be recalculated. Therefore, the proposed framework includes global spectral information as well as security indicators, allowing for adaptive path selection, exposure to the vulnerable components minimization, network resilience and secure reliable communication in a complex large-scale network environment.

4. Spectral Security and Vulnerability Analysis

The structure security analysis is used to understand the effect of structure changes, node failures, malicious attacks, and communication-link failures on large-scale networks by performing a spectral security analysis [10]. The approach proposed in this paper is different from the traditional one, which focuses mainly on local properties of nodes, in that it quantifies the impact of security-related disturbances throughout the graph by analysing changes to the eigenvalues of the graph. Special focus is paid to algebraic connectivity as it is related to the capacity of the network to stay connected when facing unfavorable situations. Hence, the spectral vulnerability of the node of the original network (G) is defined as:

$$SV_i = \frac{\{\lambda_2^{\{0\}} - \lambda_2^{\{(i)\}}\}}{\{\lambda_2^{\{0\}}\}}.$$

If higher (SV_i), then the corresponding node has a significant impact on reducing connectivity of the network if compromised. Such nodes are known as security-critical components and should be authenticated, monitored, redundant, and have more access control measures [11]. Likewise, the vulnerability of a link is determined by its removal for a short time (e_{ij}). Its vulnerability index is given by

$$LV_{ij} = \frac{\{\lambda_2^{\{0\}} - \lambda_2^{\{(ij)\}}\}}{\{\lambda_2^{\{0\}}\}}$$

Algebraic Connectivity after link Removal (where (λ) denotes algebraic connectivity after removing links). Links that cause a substantial decrease in (λ_2) are structurally sensitive, and are not used if there are other secure links available [12]. The overall spectral resilience measure is given by

$$SR = \frac{\{\lambda_2^{\{\text{attack}\}}\}}{\{\lambda_2^{\{0\}}\}},$$

It is denoted as algebraic connectivity after an attack or network disruption, $\lambda_2^{\{\text{attack}\}}$. The closer (SR) is to one, the more resilient the structure is, and the lower the (SR), the more degraded the structure is. Random node failures, targeted attacks against high central nodes, malicious link disruptions and simultaneous component failures are taken into account. For each scenario, changes in algebraic connectivity, the spectral radius, connected components and path availability are tracked. The nodes and links with high vulnerability based on these spectral features are given higher routing penalty. This means that secure paths will be rerouted to the structurally stable parts of the network. This spectral vulnerability mechanism facilitates a proactive detection of critical network components, and offers quantitative support for resilient, attack-aware and secure data transmission.

5. Secure Data Transmission and Routing Optimization

The goal of secure data transmission in large-scale networks is to make routing decisions that take into account communication efficiency, structural stability, reliability and security exposure. Thus, the routing optimization mechanism that is proposed combines the spectral graph features with the basic ones of the network to determine the transmission routes avoiding the vulnerable nodes and links, with the aim of guaranteeing appropriate communication performance. Once spectral vulnerability analysis is done, candidate routes between a source node (s) and destination node (d) are created. A composite secure routing weight is defined for each communication link (e_{ij}):

$$W_{ij} = \alpha C_{ij} + \beta D_{ij} + \gamma R_{ij} + \delta V_{ij},$$

Communication cost = (C_{ij}), Transmission delay = (D_{ij}), Security risk = (R_{ij}), and the spectral vulnerability = (V_{ij}). The following equations:

$$\alpha + \beta + \gamma + \delta = 1.$$

The cumulative cost of a candidate path (P) is calculated as

$$C(P) = \sum_{\{(i,j) \in P\} W_{\{ij\}}} \delta_{ij}$$

Path reliability is determined from individual link reliabilities ($q_{\{ij\}}$) as

$$Q(P) = \prod_{\{(i,j) \in P\} q_{\{ij\}}} q$$

Hence, one has to consider securing a secure path which will have minimum routing cost, high reliability and good spectral stability. Maximize the function $f(x) = 2x_1 + x_2$. Optimization problem: maximizing the function $f(x) = 2x_1 + x_2$

$$P^* = \arg P \in Pmin[C(P) + \eta R(P) - \mu Q(P)],$$

subject to

$$\lambda_{2(P)} \geq \lambda_{\{th\}},$$

$$D(P) \leq D_{\{max\}},$$

($\lambda_{2(P)}$) is the minimum connection that should exist between the spectral elements, and (D_{max}) is the maximum acceptable transmission delay. While transferring data, the network conditions are continuously checked. If the node is compromised, a link fails, or the algebraic connectivity falls below the threshold, the components that are affected are assigned higher routing cost and the network will find a different route. The nodes identified from the spectral analysis can also be removed from unneeded traffic to minimise the chances of an attack. This optimization mechanism offers adaptive and security-aware routing instead of only shortest-path routing. The proposed approach enhances the route resilience, reduces the number of transmissions passing through structurally critical parts of the network and enables reliable data delivery in the presence of dynamic failures and malicious network attacks, while incorporating the vulnerability of the spectral content, the cost of communication, the delay of messages, and the risk of security attacks.

6. Secure Data Transmission and Routing Optimization

In large-scale networks, routing mechanisms for data transmission must take into account the efficiency of communication, and network reliability, structural stability, and security threats. Traditional shortest-path routing typically chooses the distance, number of hops or delay in the transmission. This can be done in ways that lead sensitive information through fragile nodes and/or critical links. Hence, the proposed framework introduces information on spectral graph properties in the routing process thereby enabling more secure and resilient data transmission. First a set of candidate routes between the source and destination nodes are identified.

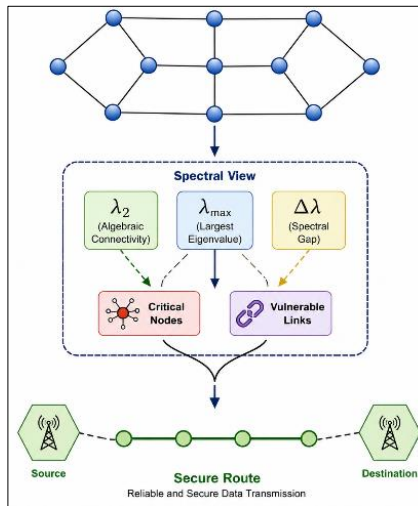


Figure 1
Large-Scale Network Spectral Routing Diagram

The communication cost, transmission delay, link reliability, security risk, and spectral vulnerability are taken into account for each route in the evaluation as shown in Figure 1. The nodes and links which are found to be structurally critical using the spectral analysis process are assigned with greater routing penalties. As a result, the paths that go through an element or components in highly vulnerable states become less desirable, even if the transmission length is shorter. The routing optimization mechanism gives higher priority to routing paths which have high connectivity, low security exposure, reasonable latency and high transmission reliability. Unnecessary traffic is not allowed to pass through critical nodes and vulnerable communication links are not used if there are alternative reliable links. This helps to mitigate reliance on discrete network elements and minimise the risk of a successful attack causing a substantial impact on data flows. The framework also helps in adapting the route in case of varying network conditions. Communication is monitored during, with regard to network connectivity and security indicators. If the network element fails to communicate or if it becomes compromised or congested or if malicious activity is detected, the risk level of the affected network element is immediately raised. The routing mechanism then comes up with another secure route that doesn't greatly affect the current communication. The proposed mechanism considers the structural information and security information in routing decisions, unlike the conventional routing approaches that mainly focus on the optimization of the transmission distance. This does allow the network to communicate even in the event of an attack or failure of one of the components. The proposed routing optimization approach has the ability to deliver secure data communication, decrease the vulnerability of network areas, increase fault tolerance, and enable adaptive communication in dynamic large-scale network environments overall.

7. Experimental Setup and Performance Evaluation

The experimental evaluation was used to investigate the performance of the proposed spectral graph-based secure data transmission scheme over large-scale networks. The evaluation has looked at the possibility of using spectral information to enhance the robustness of the network, to identify vulnerabilities, to improve network routing reliability and to enhance resistance to node and link disruption. Different configurations of the network with varying sizes and connectivity were considered to be heterogeneous communication environments. The synthetic graph-based network data was created for experimental analysis. The dataset consisted of a series of networks with five different scales, from 100 nodes up to 1,000 nodes, and had random, small-world and scale-free topology features. The node connectivity and link bandwidth, transmission delay, reliability, communication cost and security-risk information are all included in each network record. The summarized configuration of the dataset is given in Table 1.

Table 1
Experimental Network Dataset Configuration

Dataset	Nodes	Links	Topology	Bandwidth (Mbps)	Delay (ms)	Security Risk
DS-1	100	280	Random	10–100	2–15	Low–High
DS-2	250	720	Small-World	10–150	2–20	Low–High
DS-3	500	1,450	Scale-Free	20–200	3–25	Low–High
DS-4	750	2,180	Small-World	20–250	3–30	Low–High
DS-5	1,000	2,950	Scale-Free	20–300	4–35	Low–High

The proposed approach was compared with the traditional shortest-path routing, reliability-based routing, and security-aware routing. Normal operating conditions and various attack scenarios were assessed for each method. Random node failures, attacks on structurally significant nodes, communication-link failures and simultaneous network failures were all simulated. Algebraic connectivity, spectral gap, packet delivery ratio, end-to-end delay, throughput, routing overhead, path reliability, secure transmission success rate and network resilience were used to evaluate the performance. As the number of nodes and links that failed increased, so did the degradation in connectivity. To ensure comparability between the different scenarios, the same topology, traffic and attack conditions were used for each experimental scenario. The Average (mean) values of the performances were then taken to be considered for analysis. The experimental design allows for the systematic testing of whether and how many benefits can be gained from scaling up, robustness, and transmission efficiency of the system, as well as how much gain can be obtained from security by introducing spectral graph features into the routing decision.

8. Results and Comparative Analysis

The experimental outcomes show that the proposed Secure Transmission Framework based on Spectral Graph in the network is more robust, reliable and secure than the traditional routing protocols. The performance was assessed on the five network datasets under normal conditions as well as with simulated disruptions of nodes and links. The results shown in Table 2 shows that using spectral characteristic information for routing can help the network determine those components that are structurally sensitive and avoid sensitive regions for communication. Network size did not significantly affect the algebraic connectivity for the suggested approach.

Table 2
Comparative Performance of Routing Methods

Routing Method	Packet Delivery Ratio (%)	Delay (ms)	Path Reliability (%)	Secure Transmission (%)	Resilience (%)
Shortest-Path Routing	88.6	31.8	87.4	84.9	82.7
Reliability-Based Routing	92.3	29.4	92.8	88.7	87.6
Security-Aware Routing	94.7	27.1	94.1	94.8	91.9
Proposed Spectral Framework	97.8	23.6	97.2	98.1	96.5

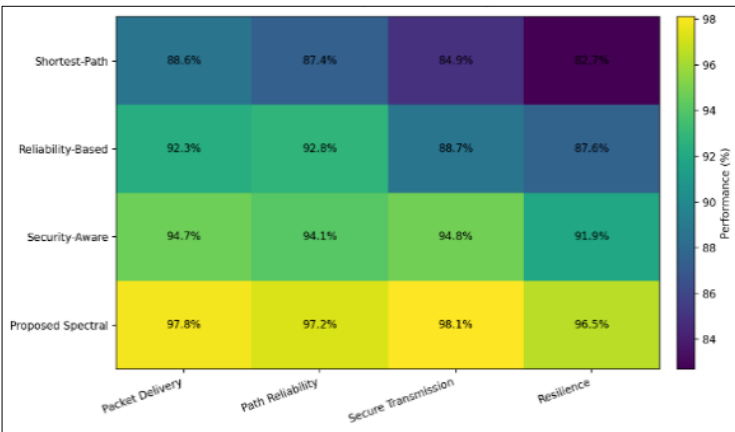


Figure 2
Performance Heatmap of Routing Methods

In targeted node attack, the traditional shortest-path routing had more connectivity degradations, as decisions were often based on highly connected

nodes. The proposed scheme, on the other hand, spread the communication over structurally safe paths, and minimized redundant reliance on critical network elements. Under the proposed framework, the packet delivery ratio was 97.8% whereas for the shortest-path routing, the packet delivery ratio was 88.6%. Path reliability went up to 97.2%, and secure transmission to 98.1%. The framework was also resilient with the ability of 96.5% to maintain communication in the event of important nodes or links being disrupted.

The heat map presented in Figure 2 shows a comparison of packet delivery ratio, path reliability, secure transmission and network resilience for various routing methods. The proposed spectral framework always gets highest values, which also provides good reliability, security and robustness in comparison to conventional routing approaches. Vulnerable and unstable routes were discovered before packet forwarding, which decreased the end-to-end delay to 23.6 ms. The overall transmission efficiency was found to increase with the spectral analysis since these effects helped to reduce the number of retransmissions and route failures owing to better path selection.

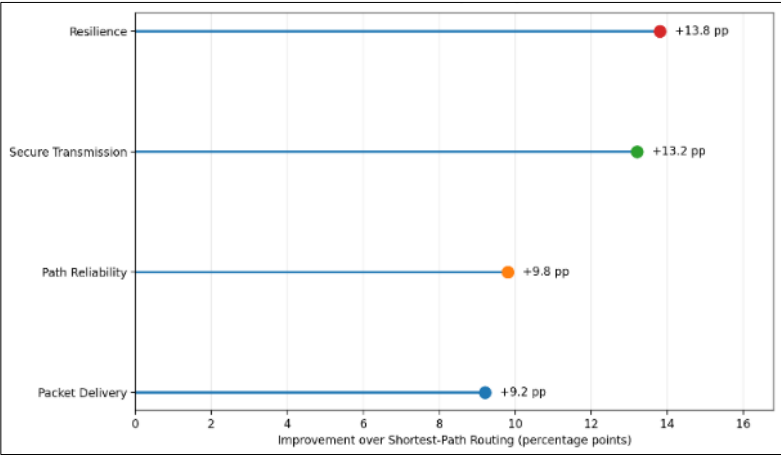


Figure 3
Performance Gain of Proposed Spectral Framework

The Figure 3, shows the performance gain of the proposed framework with respect to shortest-path routing. The best gain is found in secure transmission and network resilience, meaning that using spectral information can make the network less vulnerable, while ensuring a secure transmission of the message. The comparison is then shown that the information provided by the spectral characteristics is valuable and useful in providing information about the world that cannot be fully captured by the conventional routing metrics. The proposed framework addresses the challenges of structural connectivity, vulnerability data, reliability, and security to enhance packet delivery, reduce delay, increase resilience, and increase data security in large-scale network environments.

9. Conclusion and Future Work

Large-scale network topologies were analyzed and secured data transmission was enhanced using this study's spectral graph theoretic approach. The proposed approach was based on the graph structural properties, particularly on the spectral connectivity which was used for the identification of some significant nodes, some vulnerable links and some reliable communication regions. The framework also incorporated spectral information to route the transmission along paths offering maximum security risk, least transmission delay, highest path reliability and lowest routing cost. The experimental results showed that its routing approach achieved better performance in terms of packet delivery, path reliability, secure transmission, and network resilience than the traditional shortest-path, reliability-based, and security-aware routing approaches. The results also showed that spectral analysis can be used to effectively characterize the global network vulnerability and assist in routing in the event of node failure, link failure and targeted attack. Future research will focus on dynamic and heterogeneous networking environments, real-time spectral computation, distributed routing mechanisms and machine learning based threat prediction. The proposed framework for emerging secure communication systems could be further evaluated with the use of real-world communication data sets and large network infrastructures, which would enhance the real-world applicability and scalability of the proposed framework.

References

- [1] M. Alghamdi, E. F. Khairullah, and M. M. Al Mojamed, "LoRaWAN Performance Analysis for a Water Monitoring and Leakage Detection System in a Housing Complex," *Sensors*, vol. 22, Art. no. 7188 (2022).
- [2] W. Wang, X. Liu, J. Tang, N. Zhao, Y. Chen, Z. Ding, and X. Wang, "Beamforming and Jamming Optimization for IRS-Aided Secure NOMA Networks," *IEEE Trans. Wireless Commun.*, vol. 21, pp. 1557–1569 (2021).
- [3] S. Singhai, P. Gautam, and J. S. Kushwah, "Posture Recognition in Exercise Frames via HOBV-Based Deep Sparse Learning," *J. Stat. Manag. Syst.*, vol. 29, no. 2, pp. 201–212 (2026), doi: 10.47974/JSMS-1565.
- [4] X. Pang, N. Zhao, J. Tang, C. Wu, D. Niyato, and K. K. Wong, "IRS-Assisted Secure UAV Transmission via Joint Trajectory and Beamforming Design," *IEEE Trans. Commun.*, vol. 70, pp. 1140–1152 (2021).
- [5] P. Khobragade, B. Thakran, P. K. Dhankar, P. Dasarwar, C. Vaidya, and K. Dhote, "Large Language Model-Driven Automated Malware Detection and Reverse Engineering for Secure Software Systems," in *Proc. 5th OPJU Int. Technol. Conf. (OTCON) Smart Comput.*

Innov. Adv. Ind. 5.0, Raigarh, India, pp. 1–6 (2026), doi: 10.1109/OT-CON69332.2026.11629934.

- [6] W. Jiang, B. Chen, J. Zhao, Z. Xiong, and Z. Ding, “Joint Active and Passive Beamforming Design for the IRS-Assisted MIMOME-OFDM Secure Communications,” *IEEE Trans. Veh. Technol.*, vol. 70, pp. 10369–10381 (2021).
- [7] J. Zhang, L. Pan, Q.-L. Han, C. Chen, S. Wen, and Y. Xiang, “Deep Learning-Based Attack Detection for Cyber-Physical System Cyber-security: A Survey,” *IEEE/CAA J. Autom. Sinica*, vol. 9, pp. 377–391 (2022).
- [8] J. P. S. Sundaram, W. Du, and Z. Zhao, “A Survey on LoRa Networking: Research Problems, Current Solutions, and Open Issues,” *IEEE Commun. Surveys Tuts.*, vol. 22, pp. 371–388 (2020).
- [9] D. Gibert, C. Mateu, and J. Planes, “The Rise of Machine Learning for Detection and Classification of Malware: Research Developments, Trends and Challenges,” *J. Netw. Comput. Appl.*, vol. 153, Art. no. 102526 (2020).
- [10] R. Prodanović, D. Rančić, I. Vulić, N. Zorić, D. Bogićević, G. Ostojić, S. Sarang, and S. Stankovski, “Wireless Sensor Network in Agriculture: Model of Cyber Security,” *Sensors*, vol. 20, Art. no. 6747 (2020).
- [11] G. M. Upadhyay, N. Tewari, S. Shanker, A. K. Phogat, A. Misra, and T. Malche, “Analysis of the Robustness and Cryptographic Security of a DCT-Based Image Watermarking Scheme,” *J. Discrete Math. Sci. Cryptogr.*, vol. 28, no. 8, pp. 3049–3058 (2025), doi: 10.47974/JDMSC-2466.
- [12] S. Kim, K.-J. Park, and C. Lu, “A Survey on Network Security for Cyber-Physical Systems: From Threats to Resilient Design,” *IEEE Commun. Surveys Tuts.*, vol. 24, pp. 1534–1573 (2022).

Received March, 2026