

Graph-theoretic trust models for secure IoT and medical sensor networks

Ravindra S. Patil [‡]

Department of Emergency Medicine

Krishna Institute of Medical Sciences

Krishna Vishwa Vidyapeeth (Deemed to be University)

Karad 415539

Maharashtra

India

Deepika Sharma [†]

Department of Computer Sciences

Noida International University

Greater Noida 201312

Uttar Pradesh

India

Rahul A. Padgilwar [§]

Department of Engineering Science and Humanities

Vishwakarma Institute of Technology

Pune 411037

Maharashtra

India

Ramachandro Majji ^{*}

Department of Computer Science and Engineering (Artificial Intelligence & Machine Learning)

Vardhaman College of Engineering

Shamshabad

Hyderabad 501218

Telangana

India

[‡] E-mail: ravipatilich@gmail.com

[†] E-mail: deepika.sharma@niu.edu.in

[§] E-mail: rahul.padgilwar1@vit.edu

^{*} E-mail: ramachandro.m@vardhaman.org (Corresponding Author)

L. Yamuna[@]

*Department of Computer Science and Engineering (Artificial Intelligence & Machine Learning)
Pragati Engineering College
Kakinada 533437
Andhra Pradesh
India*

N. Muninathan[#]

*Central Research Laboratory
Meenakshi Medical College Hospital & Research Institute
Meenakshi Academy of Higher Education & Research
Kanchipuram 631552
Tamil Nadu
India*

Abstract

To secure IoT and medical sensor networks, mechanisms that are able to detect malicious and compromised devices or unreliable devices are needed. In this study a graph-theoretic trust model is suggested, where the sensors are the nodes and the communication relationship between the sensors is represented by a weighted edge. The trust is estimated directly from packet delivery, data consistency, responsiveness and authentication behavior, and indirectly is based on a collection of the recommendations of neighboring nodes. A composite score adaptively weights both direct, indirect and historical evidence and contextual factors. The operations performed on the nodes (adjacency-matrix operations) and the analysis of paths (path-based analysis) both enable scalable propagation of trust and isolation of suspicious nodes. The simulation results show better detection of malicious nodes, reliability of packets and the robustness of the network when compared to the traditional reputation methods. The framework offers an easy-to-understand and lightweight basis for secure distributed healthcare monitoring applications.

Subject Classification: 05C12.

Keywords: Graph theory, Trust management, Internet of Things, Medical sensor networks, Malicious-node detection, Network security.

I. Introduction

With the advent of IoT and medical sensor networks, continuous monitoring, fast clinical decision making is possible, remote patient care is feasible, and intelligent healthcare services can be provided. These networks are composed of sensor nodes with limited resources and sensitive physiological data is communicated between sensor nodes by wireless communication [1, 2,

[@] E-mail: lyamuna@gmail.com

[#] E-mail: muninathan@maher.ac.in

3]. But the open connectivity, dynamic topology, limited energy and unattended deployment result in increased susceptibility of sensors to spoofing, false-data injection, selective forwarding, collusion, and node-capture attacks [4, 5]. Typical cryptographic solutions ensure confidentiality and authentication but they are not sufficient to check the reliability of an authenticated node when communicating. Trust modeling based on the graph theory [6, 7, 8] gives a formal method to represent nodes, links, user interactions in the past and recommendation paths. All the elements of sensors, links, recommendations, trust, detection and security are combined in Figure 1.

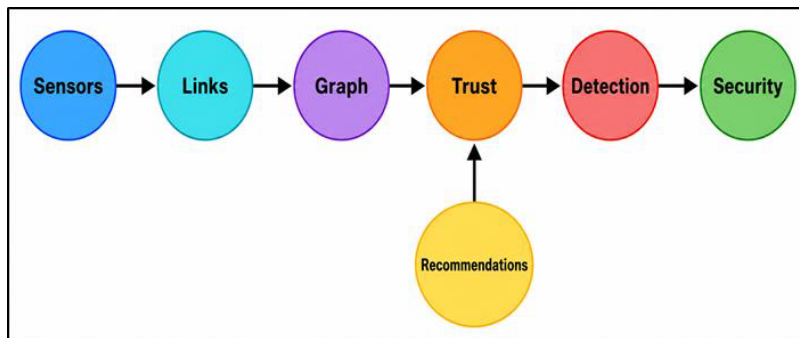


Figure 1

Graph-Theoretic Trust Framework for Secure IoT and Medical Sensor Networks

In this representation, vertex nodes represent sensor devices, edge nodes represent communication relationship and observation of trust are dynamic edge weights. Direct trust refers to direct behavior while indirect trust refers to the trust based on a recommendation by neighboring nodes [9, 10]. They come in handy for identifying suspicious devices, choosing safe routes to travel and ensuring that data is delivered securely. The aim of this study is to develop a composite graph based trust framework for the IoT and medical sensor environment. The model fuses together all the evidence related to behaviors, context, history, and recommendations, in a way that adapts the weights based on the evidence and the adjacency-matrix analysis [11, 12]. It strives to enhance the ability of detecting malfunctions, minimize propagation of misleading trust and ensure a reliable communication in healthcare networks under varying network situations. This approach is light, interpretable, scalable and has applications in medical contexts that are security-critical, such as medical devices [13, 14].

II. System Model and Problem Formulation

System model includes network entities, assumptions for communication, the behavior of the threats, and the constraints of the operation in the system; problem formulation specifies the trust evaluation goals for the network, malicious-node detection, and reliable data delivery for the system.

A. *IoT and Medical Sensor Network Architecture*

The architecture includes wearable sensors, implantable sensors, gateways, edge servers, cloud platforms, and medical applications for continuous sensing, secure transmission, processing and storage, analysis and medical decision support services.

$$x_{i(t)} = s_{i(t)} + n_{i(t)}, i \in S \quad (1)$$

The physiological data is acquired by the sensors, and physiological signal can be decomposed into the real biomedical signal (noise-free) and measurement noise, as shown in (1). This is a representation of practical uncertainty (uncertainty in the observations made with wearable technology).

$$D_{g(t)} = \sum_{i \in S_g} [\omega_{ig} x_{i(t)}] \quad (2)$$

In this case, gateway aggregation is a weighted sum of readings from related sensors (as defined in equation (2)). The weights are a measure of the relevance, reliability and/or quality of the sensor data for fusion prior to onward transmission and processing.

$$\sum_{i \in S_g} \omega_{ig} = 1 \quad (3)$$

All the aggregation weights in equation (3) are forced to add up to 1. This normalization preserves the measurement scale, avoids the amplification of measurement value by the sensors, and makes it possible for the fusion of different heterogeneous sensors running on the gateway architecture.

$$Q_{ig} = \sqrt{[\alpha P_{ig}^2 + \beta R_{ig}^2 + \gamma B_{ig}^2]} \quad (4)$$

The quality of communication-links, as calculated by equation (4) is obtained as a square root of the following squared measures: packet-delivery, reliability, and bandwidth. They rely on parameters alpha, beta and gamma to ensure that they are relative to reliable link-selection decisions without any doubts.

$$E_{i(T)} = \int_0^T [P_i^{sense(t)} + P_i^{process(t)} + P_i^{transmit(t)}] dt \quad (5)$$

Equation (5) is a sum of sensing, processing and transmission power over time, to calculate energy consumption of the sensor. This formulation can be used for evaluating battery life, routing in energy-aware networks, and operating constrained devices in a sustainable way.

$$D_{total} = \sum_{(i,j) \in P} [D_{ij}^{tx} + D_{ij}^{prop} + D_{ij}^{queue} + D_{ij}^{proc}] \quad (6)$$

End-to-end network delay is calculated by adding up the transmission, propagation, queuing and processing delays of all the links in the chosen path as given in equation (6). Assesses the appropriateness of responsiveness needed for timely, reliable and clinically sound healthcare monitoring.

B. *Graph Representation of Sensor Nodes and Communication Links*

Graph representation assigns a node to each sensor/gateway and an edge with a weight indicating connectivity, reliability and quality of interactions observed dynamically for each wireless communication link.

$$G = (V, E, W) \quad (7)$$

$$V = \{v_1, v_2, \dots, v_n\} \quad (8)$$

The medical sensor network is basically a weighted graph with vertices, edges and weights, as shown in Equation (7). Vertices represent devices, edges represent communication links and the weights represent the measure of reliability or connectivity or relationships of trust between the devices. The entries of the weighted adjacency-matrix are defined for each pair of nodes in Equation (8). If it is a positive value, it means that there is an existing communication link between the devices and its level of trust; if it is zero, then there is no direct link between the devices.

$$D_{ii} = \sum_{j=1}^n A_{ij} \quad (9)$$

The node-degree matrix is created with (9) by adding up the weights on the adjacent nodes. The values along the diagonal show the total weighted connectivity, and the off-diagonal ones are zeros for 'structured graph-analysis' operations.

$$L_{norm} = I - D^{-\frac{1}{2}} A D^{-\frac{1}{2}} \quad (10)$$

The graph Laplacian with inverse square-root degree scaling is given by equation (10). This transformation alleviates the high degree node bias, facilitates spectral analysis and allows a fair comparison of medical sensors with different connections in a secure way.

$$T(P_{ij}) = \sqrt[n]{\prod_{(u,v) \in P_{ij}} w_{uv}} \quad (11)$$

The communication-path trust (see equation (11)) is estimated as the geometric mean of individual edge-trust values. Using the nth root to normalize path length, helps to avoid giving longer routes an unfair disadvantage, and aids reliable routing.

$$\bar{w}_{ij(T)} = \left(\frac{1}{T}\right) \int_0^T w_{ij(t)} dt \quad (12)$$

The time-averaged edge reliability is computed in the following way, using equation (12): It includes the historical behavior, leads to a more stable estimation of trust and can smooth up the temporary fluctuations.

III. Mathematical Formulation of Graph-Based Trust

The mathematical formulation models direct, indirect, contextual and historical trust, integrates the use of graph structures, recommendation paths, adaptive weights and aggregation rules to provide dependable security decisions as the networks evolve.

A. Graph, Node, Edge, and Adjacency-Matrix Definitions

The network is represented by a weighted graph, $G=(V,E)$. A vertex refers to a device, an edge is a communication, and entries in the adjacency-matrix refers to the existence, direction and trust weight of communication.

$$G = (V, E, W) \quad (13)$$

$$V = \{v_1, v_2, \dots, v_n\} \quad (14)$$

$$E \subseteq V \times V \quad (15)$$

A sensor network weighted trust graph is defined by equation (13) which consists of sensor nodes, communication edges and weights, used to numerically represent the confidence in the interaction between the devices in a healthcare network. The vertex set is defined in equation (14) as an indexed set of all the sensor, gateway, edge and cloud devices that are involved in the networked medical monitoring operations. The edge set is a subset of the Cartesian node product, as defined by equation (15), and thus describes allowable directed communications relationships between network devices that are connected.

$$v_i = [ID_i, L_i, E_i, R_i, S_i]^T \quad (16)$$

Equation (16) defines each node by its identity, location, energy, reliability and security attributes, allowing for a contextual assessment of trust for each node, differentiating among devices, and making adaptive decisions securely.

$$e_{ij} = (v_i, v_j, w_{ij}) \quad (17)$$

Every edge in the equation is defined by a source, a destination and a trust weight, bounded values to which represent the level of trust in the communication from complete distrust to trustworthiness.

$$A_{norm} = D^{-\frac{1}{2}} A D^{-\frac{1}{2}} \quad (18)$$

Inverse Square-Root Degree Scaling in equation (18) scales the adjacency relationships to normalize the connectivity, which helps to alleviate the imbalance in the connectivity of the sensor nodes and ensures fair trust propagation among the sensor nodes with different connections.

$$D_{ii} = \sum_{j=1}^n A_{ij} \quad (19)$$

Each diagonal degree value is calculated as in Equation (19) by the sum of adjacency weights for neighbors, as a measure of the overall strength of node's network connectivity.

$$T_{ij(t)} = \left(\frac{1}{T}\right) \int_0^T A_{ij(t)} dt \quad (20)$$

The equation (20) takes account of the time evolution of the adjacency trust over the observation period and then averages it, which leads to reliable historical estimates of the reliability of the time series even in the light of short-term fluctuations of the behaviour of people securing.

B. Indirect Trust and Recommendation Aggregation

The idea of indirect trust is to mix recommendations from neighbouring nodes based on the level of credibility, trustworthiness, recency of interactions and consistency of the nodes, reducing the impact of biased, dishonest, collusive or outdated trust-information.

$$N_i = \{v_k \in V \mid (v_i, v_k) \in E\} \quad (21)$$

The set of neighbors of node i , is defined in equation (21) as the set of nodes that can directly communicate with node i . This set sets up other trust sources that can be used for indirect trust recommendations and evaluation processes.

$$IT_{ij} = \frac{\sum_{k \in N_i} C_{ik} R_{kj}}{\sum_{k \in N_i} C_{ik}} \quad (22)$$

Indirect trust is computed by the equation (22) as the weighted average of the trust of the neighbors (indirect recommendations) by their respective credibility. Reliable recommenders are given more influence, and normalization makes the total value understandable, restricted and comparable regarding the interactions of the sensors without risk.

$$PT_{ij} = \sqrt[n]{\prod_{(u,v) \in P_{ij}} T_{uv}} \quad (23)$$

Equation (23) is an estimate for path-based indirect trust which is based on the geometric mean of the weights of trust along a recommendation path. Normalization of the root serves to account for the different lengths of routes as well as discourages use of less reliable intermediary nodes when making trust-propagation decisions.

$$C_{ik} = 1 - \sqrt{\left[\frac{(R_{kj} - DT_{ij})^2}{M} \right]} \quad (24)$$

A recommender's credibility is assessed by the deviation of the recommender's recommendation from direct trust in the recommendation, as can be seen in Equation (24). The smaller the disagreement, the more credible the advice, and thus, the higher its influence in the aggregation and decision-making processes, the smaller the disagreement will be.

$$R_{kj}^t = R_{kj}^0 \exp[-\lambda(t - t_k)] \quad (25)$$

The exponential temporal decay equation in (25) is used in the case of previously generated recommendations. Recent evidence is more important, and older info fades over time, so that out-of-date behaviours don't have a big impact on current trust-assessment results.

$$CIT_{ij(T)} = \left(\frac{1}{T}\right) \int_0^T IT_{ij(t)} dt \quad (26)$$

In the above equation, equation (26) is an integration of the indirect trust over time and division of the observation duration. This adds up the short-term variations, reflects historical recommendations, and enhances the performance of detecting malicious nodes stably.

C. Composite Trust-Score Formulation

Working with contextual evidence, direct observation and indirect recommendation, historical behavior together, with adaptive normalized

weights, composite trust is used to create a composite score for classification, routing, access and isolation decisions.

$$T_{ij}^C = \alpha DT_{ij} + \beta IT_{ij} + \gamma CT_{ij} + \delta HT_{ij} \quad (27)$$

$$\alpha + \beta + \gamma + \delta = 1 \quad (28)$$

A composite trust is calculated by Equation (27) as a weighted average of the direct, indirect, contextual and historical evidence with weights of alpha, beta, gamma and delta respectively. This constraint, represented in equation (28), ensures that the four component weights are normalized, so that there is a normalized contribution along the trust dimensions.

$$T_{ij}^{RMS} = \sqrt{[\alpha DT_{ij}^2 + \beta IT_{ij}^2 + \gamma CT_{ij}^2 + \delta HT_{ij}^2]} \quad (29)$$

The root mean square trust (RMST) can be calculated using equation (29) by taking the weighted squared component scores. Squaring highlights strong evidence, the square root brings the measure back to its original scale and the outcome accentuates significant weaknesses in network interactions more clearly whilst rewarding nodes that are consistently strong.

$$\alpha_{r(t+1)} = \frac{[\alpha_{r(t)} \exp(-\eta e_{r(t)})]}{[\sum_{q=1}^4 \alpha_{q(t)} \exp(-\eta e_{q(t)})]} \quad (30)$$

The adaptive update of the weights of the components is performed with equation (30) based on the prediction errors, the learning rate and exponential weight adjustment. The smaller the error produced by the component, the more important it is, while an inaccuracy in evidence is downweighted, allowing trust estimation to appropriately react to the dynamic attacks and behavior.

$$\bar{T}_{ij}^{C(T)} = \left(\frac{1}{T}\right) \int_0^T T_{ij}^{C(t)} dt \quad (31)$$

The composite trust score is summed up during an observation period and divided by the duration of the observation period as sum of the trust score times the observation period. This helps minimize variations in short-term device behavior, provide long-term insights into device performance, and maintain secure isolation, authentication and communication in healthcare networks.

IV. Result and Discussion

Results show how graph-based trust enhances the detection of malicious nodes, packet delivery ratio, reliability of recommendations and robustness in the presence of compromised nodes, while decreasing the risk of communication and false acceptance in different healthcare network scenarios.

Table 1 shows that the performance of the trust-management gradually increases when using reputation-based method to using weighted graph trust. The detection accuracy of 94.83%, the precision of 94.12%, the recall of 93.56%, the F1-score of 93.84% and the packet delivery ratio of 95.62% are the best results that Weighted graph trust can obtain. These enhancements suggest that graph-based relationships and weighted interactions do serve as a more reliable identification of malicious nodes, trusted and secure communication and

more resilient medical sensor network operation amidst security challenges and attacks.

Table 1
Comparative Performance of Trust-Management Methods

Trust-Management Method	Detection Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Packet Delivery Ratio (%)
Reputation-Based Trust	86.42	84.75	83.68	84.21	88.35
Direct Trust Model	89.68	88.41	87.92	88.16	91.26
Recommendation-Based Trust	92.15	91.08	90.64	90.86	93.47
Weighted Graph Trust	94.83	94.12	93.56	93.84	95.62

Table 2
Performance of the Proposed Model Under Different Malicious-Node Ratios

Malicious Nodes (%)	Detection Rate (%)	Trust Reliability (%)	Packet Delivery Ratio (%)	Communication Delay (ms)	Energy Consumption (mJ)
5	98.72	98.35	98.94	24.6	18.3
10	97.85	97.62	98.21	26.8	19.7
15	96.94	96.78	97.46	29.4	21.2
20	95.71	95.48	96.32	32.7	23.5
25	94.36	93.92	94.87	36.9	26.1
30	92.84	92.37	93.15	41.3	29.4

Based on the results in Table 2, it can be observed that the detection rate, the trust reliability and the packet delivery performance of the system gradually decrease as the malicious-node ratio increases. For 5% malicious nodes the model can detect malicious nodes with 98.72% accuracy, reliability 98.35% and packet delivery 98.94%. Figure 2 is valid in assessing the resilience of the models with growing ratio of malicious nodes.

These metrics are still above 92% even if there are malicious nodes up to 30%. The delay of communication, however, is increased from 24.6 to 41.3 ms and the additional energy consumption is from 18.3 to 29.4 mJ, which is due to the added security-processing overheads.



Figure 2
Analysis of Varying Malicious-Node Ratios

V. Conclusion

In this study, a trust model has been provided based on graph theory to enhance the IoT and medical sensor network security. The framework used the nodes to represent the devices, the weighted edges to represent the communication links and the behavioral relationships to be represented by a dynamically changing adjacency matrix. Adaptive composite trust scores were generated by combining information from direct observation, indirect recommendations, contextual evidence and from historical behavior. The methodology enabled the detection of malicious nodes as well as the establishment of secure routing, reliable data exchange and timely isolation of malicious sensors. The comparative results showed that the accuracy of detection, packet delivery, trust reliability, network resilience were improved, and the number of false accept and the manipulation of recommendations were reduced. The proposed model thus provides a lightweight, scalable and interpretable security solution to a secure healthcare monitoring system. The federated trust learning will be explored in the future.

References

[1] M. J. C. S. Reis, "Trust-aware federated graph learning for secure and energy-efficient IoT ecosystems," *Computers*, vol. 15, no. 2, Art. no. 121 (2026), doi: 10.3390/computers15020121.

[2] L. Wang, K. Petrova, and M. L. Yang, "Trust models in wireless sensor networks for defending against denial-of-service attacks: A literature review," *Appl. Sci.*, vol. 15, no. 6, Art. no. 3075 (2025), doi: 10.3390/app15063075.

- [3] Y. Alghofaili and M. A. Rassam, "A trust management model for IoT devices and services based on the multi-criteria decision-making approach and deep long short-term memory technique," *Sensors*, vol. 22, no. 2, Art. no. 634 (2022), doi: 10.3390/s22020634.
- [4] A. Rodríguez, A. López-Chau, L. Dávila-Nicanor, V. Landassuri-Moreno, and S. Lazcano-Salas, "Lightweight protection mechanisms for IoT networks based on trust modelling," *IoT*, vol. 7, no. 1, Art. no. 18 (2026), doi: 10.3390/iot7010018.
- [5] K. Miličević, L. Omrčen, M. Kohler, and I. Lukić, "Trust model concept for IoT blockchain applications as part of the digital transformation of metrology," *Sensors*, vol. 22, no. 13, Art. no. 4708 (2022), doi: 10.3390/s22134708.
- [6] M. J. C. S. Reis, "Trust-aware and energy-efficient federated learning for secure sensor networks at the edge," *Sensors*, vol. 26, no. 8, Art. no. 2307 (2026), doi: 10.3390/s26082307.
- [7] S. M. Muzammal, R. K. Murugesan, N. Z. Jhanjhi, M. Humayun, A. O. Ibrahim, and A. Abdelmaboud, "A trust-based model for secure routing against RPL attacks in Internet of Things," *Sensors*, vol. 22, no. 18, Art. no. 7052 (2022), doi: 10.3390/s22187052.
- [8] A. Saleh, P. Joshi, R. S. Rathore, and S. S. Sengar, "Trust-aware routing mechanism through an edge node for IoT-enabled sensor networks," *Sensors*, vol. 22, no. 20, Art. no. 7820 (2022), doi: 10.3390/s22207820.
- [9] M. Ileana, P. Petrov, and V. Milev, "Secure integration of sensor networks and distributed web systems for electronic health records and custom CRM," *Sensors*, vol. 25, no. 16, Art. no. 5102 (2025), doi: 10.3390/s25165102.
- [10] T. A. Wani, P. P. Bedekar, S. Raut, T. Porwal, M. P. Rao, and B. N. M. Rao, "Analysis of edge colorings and $c'(G)$ in discrete structures using graph theoretic approaches," *J. Discrete Math. Sci. Cryptogr.*, vol. 29, no. 2-A, pp. 437–444 (2026), doi: 10.47974/JDMSC-2475.
- [11] T. Ngo, J. Yin, Y.-F. Ge, and H. Wang, "Optimizing IoT intrusion detection—A graph neural network approach with attribute-based graph construction," *Information*, vol. 16, no. 6, Art. no. 499 (2025), doi: 10.3390/info16060499.
- [12] M. A. Khan, R. N. B. Rais, O. Khalid, and S. Ahmad, "Trust-based optimized reporting for detection and prevention of black hole attacks

- in low-power and lossy green IoT networks," *Sensors*, vol. 24, no. 6, Art. no. 1775 (2024), doi: 10.3390/s24061775.
- [13] V. Aivaliotis, K. Tsantikidou, and N. Sklavos, "IoT-based multi-sensor healthcare architectures and a lightweight-based privacy scheme," *Sensors*, vol. 22, no. 11, Art. no. 4269 (2022), doi: 10.3390/s22114269.
- [14] M. S. Abdalzaher, K. Seddik, M. Elsabrouty, O. Muta, H. Furukawa, and A. Abdel-Rahman, "Game theory meets wireless sensor networks security requirements and threats mitigation: A survey," *Sensors*, vol. 16, no. 7, Art. no. 1003 (2016), doi: 10.3390/s16071003.

Received March, 2026