Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 47 (2026), No. 10, pp. 3837–3847
DOI : 10.47974/JIOS-2507

Graph-based modeling and optimization of secure routing mechanisms in wireless and sensor network architectures

Sanjivani Hemant Kulkarni [†]
Sulakshana Sagar Malwade *
Department of Computer Science and Engineering
MIT World Peace University
Pune 411038
Maharashtra
India

Abstract

In wireless or sensor networks, due to limited resources, dynamic network topology, unreliable communication links, and malicious intrusion, it is still difficult to find secure and energy efficient routing schemes. In this study, a graph based modelling and multi-objective optimization model for secure routing in wireless sensor networks is proposed. The sensor nodes and communication links are modelled as a weighted graph which includes link reliability, node trust, link energy consumption, transmission delay and security risks. A composite routing cost function dynamically assesses possible paths, and discards nodes that are malicious, unreliable or have little energy. The proposed framework provides a route selection mechanism that can be adapted to changing scenarios on network and security. Experimental examination indicates that the packet delivery, attack avoidance, energy efficiency, communication delay and network robustness are superior to the conventional shortest-path, energy-aware, and trust-based routing methods. Dynamic trust evaluation adds more to the anti-blackhole and anti-selective-forwarding protection. The system design proposed offers a scalable and resource-efficient solution to ensure reliable, adaptable, and secure communications for future wireless sensor and IoT systems.

Subject Classification: *68M12.*

Keywords: *Graph theory, Secure routing, Wireless sensor networks, Multi-objective optimization, Trust management, Energy efficiency, Network security, Internet of Things.*

This article has been corrected with minor changes. These changes do not impact the academic content of the article.

[†] *E-mail:* sanjivani.kulkarni@mitwpu.edu.in
* *E-mail:* sulakshana.malwade@mitwpu.edu.in (Corresponding Author)

© Taru Publications

1. Introduction

With these requirements, wireless and sensor network architectures have emerged as an integral part of communication systems, which are being used in a variety of applications like environmental monitoring and monitoring, smart cities, industrial automation, healthcare applications, military surveillance, smart transportation, Internet of Things services, etc. [1]. A network made up of distributed nodes communicate with each other via wireless links, and deliver sensed information to a destination or sink node. But, due to limited energy resources, dynamic topology, unreliable communication links, limited computing power and attacks by malicious users, secure and efficient routing is a tough job [2]. Traditional routing protocols tend to use shortest path, least energy or the least delay in transmission as their primary criterion, and security is usually treated separately [3]. These methods can choose vulnerable routes with compromised nodes or unreliable links and lead to more packet loss, information leakage, disruption of the route and energy consumption [4].

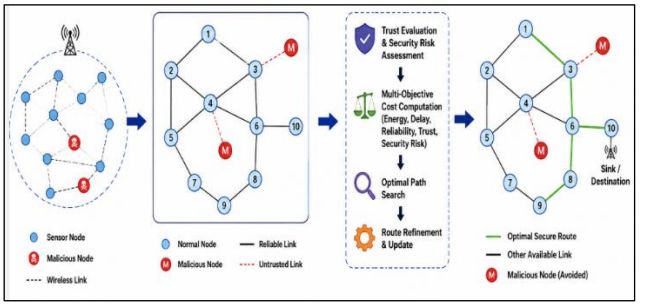


Figure 1
Secure Routing Architecture Info graphic

The mathematical model of graph theory is an effective tool to represent and analyze wireless and sensor networks [5]. The sensors are represented by the vertices of a graph and the links between them are represented by the edges of the graph, with weights on the edges indicating the likelihood of successful communication. A network can be modeled as a weighted graph, where the sensor devices are represented as vertices, and the communication links between them are represented as edges shown in Figure 1. The weight of each edge represents the probability that the link will be successful. Distance, residual energy, transmission cost, delay, trust, reliability, and security risk are some attributes that can be used in graph attributes [6]. This representation allows for an optimization problem to be defined, where optimized path routing is performed based on multiple performance and security target functions, while adhering to various constraints.

In this study, we introduce a graph-based modelling and optimization approach to secure routing in wireless and sensor networks. The framework combines energy efficiency, delay in communication, link reliability, node trust

and security risk into a single route selection mechanism [7]. To assess paths and determine routes that strike a balance between efficiency in communication and security, a multi-objective cost function is used. The proposed approach is designed to enhance the packet delivery, minimize energy consumption, routing overheads, avoid the presence of malicious or unreliable nodes and maximize lifetime of the network [8]. The framework thus offers a mathematically scalable foundation for the design of secure, reliable and resource-aware routing mechanisms for the next generation of wireless sensor networks.

2. Graph-Based Network and Security Model

The proposed framework formulates the wireless sensor network as a weighted graph (G= (V, E)), where (V={v_1,v_2,….,v_n }) is the set of sensor nodes (SN) and E⊆V×V is the set of wireless communication links between the sensor nodes [9]. A link eij∈E exists between nodes (v_i) and (v_j) if they are in the communication range and have a minimum connectivity requirement. The source node will generate the sensing information, the intermediate node will relay the packet and the sink node will receive the transmitted data. Instead of a distance-based weight, there are several attributes of each communication link. If the attribute is edge (E_{ij}), then the attribute vector is given by:

$$A_{\{ij\}} = \left[E_{\{ij\}}, D_{\{ij\}}, R_{\{ij\}}, T_{\{ij\}}, S_{\{ij\}}\right]$$

Transmission energy is represented by where, communication delay by (D_{ij}), link reliability by (R_{ij}), node or link trust by (T_{ij}) and security risk by (S_{ij}) [10]. The amount of energy used for transmission of an L bit packet over distance D_{ij} is given by

$$E_{\{ij\}} = L\left(E_{\{elec\}} + \varepsilon d_{\{ij\}}^{\{\varepsilon\}}\right),$$

Residual energy is always taken into consideration not to overuse the resource constrained nodes. Each node has a security level (T_in [0,1]). Packet-forwarding behavior, communication reliability and detected malicious behavior are used for calculating trust:

$$T_i = w_{1F_i} + w_{2R_i} + w_{3(1-M_i)},$$

Forwarding reliability is denoted as where (F_i), (R_i) represents the probability of communication to be reliable, (M_i) represents the probability that the communication carries malicious behavior, and (w_1+w_2+w_3=1). It is applied a security threshold (T_{min}) in such a way that the nodes that satisfy (T_i<T_{min}) are not considered for the formation of candidate routing paths. Therefore, acceptable nodes and communication links are only included in the resulting secure graph (G_s=(V_s,E_s)) [11], [12]. This graph-based formulation is used to find multi-objective secure route optimization along with energy efficiency, reliability, delay, trust and security risk [13].

3. Proposed Secure Routing Optimization Framework

The proposed SRO framework includes graph-based representation of the network, trust evaluation, energy awareness, link reliability, communication

delay and security risk to find an efficient and secure routing path between source and destination nodes as shown in Figure 2. The proposed approach is different from the traditional shortest-path approach in that more than just route length or hops is taken into account when computing the path.

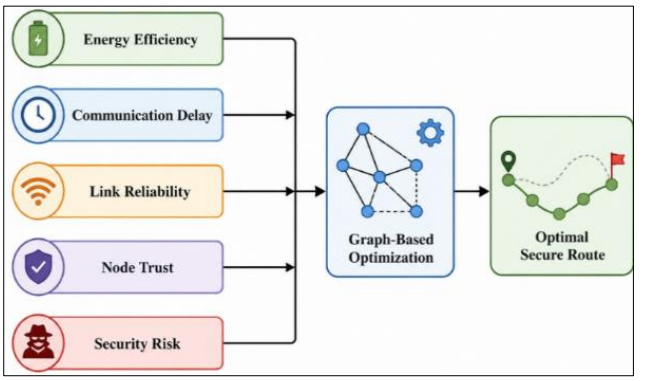


Figure 2
Graph-Based Secure Routing Architecture

For every candidate communication edge (e_{ij}), a composite routing cost is calculated as

$$C_{\{ij\}} = \alpha\{E\}\{ij\} + \beta\{D\}\{ij\} + \gamma\left(1 - R_{\{ij\}}\right) + \delta\left(1 - T_{\{ij\}}\right) + \mu S_{\{ij\}},$$

where ($\beta\{D\}\{ij\}$) *and* ($\alpha\{E\}\{ij\}$) represent normalized energy consumption and delay, respectively. ($\left(1 - R_{\{ij\}}\right)$) denotes link reliability, ($T_{\{ij\}}$) represents trust, and ($S_{\{ij\}}$,) indicates security risk. The weighting coefficients satisfy

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

For a candidate path (P) containing multiple communication links, the total routing cost is determined as

$$C(P) = \sum_{\{(i,j)\in P\}} Cij.$$

The optimal secure path is therefore selected according to

$$P^{\{*\}} = \arg_{min}\left\{P \in \{P\}_{\{s,d\}}\right\} C(P)$$

Subject to security, energy, and reliability constraints:

$$Ti \geq Tmin, Eires \geq Emin, Rij \geq Rmin.$$

The nodes with trust value less than the pre-set security value are deleted from the candidate graph before the process of route optimization. Likewise, nodes that have residual energy levels that are at or below given thresholds and links that have unacceptable reliability are excluded. The resulting secure subgraph will have only feasible routing alternatives. The trust function, residual energy, delay and link conditions are updated periodically during network

operation. This means that the weights of the edges are dynamically adjusted to the current situation in the network. When a node in the middle of the route is found to be malicious, unreliable, congested or energy deficient, the cost of that node is increased or it is not considered in the next route calculation. The proposed system thus implements a dynamic and secure path selection, instead of a static shortest-path routing. It is designed to optimize together security and network performance in order to minimize exposure to malicious nodes, balance energy consumption, increase packet delivery reliability, minimize unnecessary routing overhead, and increase overall sensor network lifetime.

4. Multi-Objective Secure Routing Model and Optimization

The secure routing problem is presented as a multi objective optimization problem on a graph, where the objective is to find the best and the most efficient path that doesn't go through malicious nodes. Assume the wireless sensor network is modeled as (G=(V,E)), where (V) is the set of sensor nodes and (E) represents a set of possible communication links between the nodes. Let {P}_{s,d} = {p} be the set of all possible paths between a source node (s) and destination node (d). A binary decision variable is a one that has two possible values, namely:

$$xij = \{1,0, if\ link\ (i,j)\ is\ selected, otherwise.$$

The optimization objective combines energy consumption, transmission delay, reliability, trust, and security risk:

$$minZ = (i,j) \in E\sum xij[\alpha Eij + \beta Dij + \gamma(1 - Rij) + \delta(1 - Tij) + \mu Sij],$$

where $\alpha, \beta, \gamma, \delta, \mu \geq 0$

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

To guarantee a continuous source-to-destination route, flow conservation is imposed as

$$j\sum xij - j\sum xji = 1, -1,0, i = s, i = d, \text{otherwise}$$

Energy feasibility requires that every selected node maintain sufficient residual energy:

$$E_i^{\{res\}} \geq E_{\{\backslash min\}}$$

Similarly, only trusted nodes are permitted to participate in routing. Communication reliability is maintained through

$$R_{\{ij\}} \geq R_{\{\backslash min\}}$$

while end-to-end delay is constrained by

$$\sum_{\{(i,j)\in E\}} R_{\{ij\}} \leq D_{\{max\}}$$

To represent overall route security, the cumulative path risk can be defined as

$$Risk(P) = 1 - \prod_{\{(i,j)\in P\}\left(1-S_{\{ij\}}\right)} S_{\{ij\}},$$

and constrained according to

$$Risk(P) \leq Risk_{\{max\}}.$$

The optimal solution (P^{*}) is thus the feasible solution that minimizes the composite objective value while meeting the energy, trust, reliability, delay and security constraints. Normalization of different routing parameters before optimization reduces the effect of variables that can have a large numerical value on the optimization objective function. This mathematical expression can support the adaptive routing mechanisms and can serve as a systematic framework for trade-offs between communication efficiency, resource conservation, reliability and cybersecurity in wireless and sensor network architectures.

5. Experimental Setup and Performance Evaluation

To test the proposed secure routing architecture based on graph, a simulated wireless sensor network is created to represent the changeable and limited communication environment. The sensor nodes are deployed randomly over a two dimensional monitoring region and a specific sink node is the last destination for information to be sent. Initially, energy, communication range, processing power, trust value and packet generation parameters are assigned to each sensor node. Wireless links are dynamically established based on communication distance, link quality and connectivity. To study the scalability of the proposed routing mechanism, different network densities have been considered. In each simulation round, the source nodes will produce data packets, which will be transmitted to the sink node via intermediate nodes. Energy used for packet transmission, reception and processing. The energy value of the nodes are continually updated to ensure that nodes that are coming close to minimum energy value can be avoided during the next route selection. Performance metrics include packet delivery ratio (PDR), end-to-end delay, energy consumption, network lifetime, routing overhead, throughput, secure packet delivery ratio and malicious-node avoidance rate. The ratio of packets delivered to the ratio of packets sent is called the packet delivery ratio and is given by:

$$PDR = \frac{\{N_{\{received\}}\}}{\{N_{\{sent\}}\}} * 100.$$

Various malicious activities are injected into the network to evaluate the security performance, such as blackhole attacks, selective forwarding, packet dropping attacks and compromised node attacks. The malicious nodes will actively drop or alter the transmitted packets that will lead to decrease in trust value. The proposed mechanism will dynamically update node trust and will delete nodes if the node trust is below the predetermined value. End-to-end delay is represented by the average value of:

$$D_{\{avg\}} = \left\{\frac{1}{PDR}\right\}\{N\} \sum_{\{k=1\}}^{\{N\}\left(t_k^{\{receive\}} - t_k^{\{send\}}\right)} PDR.$$

The operational rounds that a network can sustain before significant nodes become depleted or network disconnection are considered as the lifetimes of the network. The proposed approach is evaluated with traditional shortest path, energy aware and trust-based routing schemes while considering the same network environment. Experiments are repeated in various node densities, traffic loads and attack intensities. The resulting measurements offer a systematic framework to assess the possibility of improving routing security, communication reliability, energy utilization and overall sustainability of the network in a single stroke of multi-objective graph optimization.

6. Results and Comparative Analysis

The experimental shows that the proposed secure routing scheme has superior performance compared to the traditional shortest path, energy-saving and trust-based routing techniques. The improvement comes from the fact that the residual energy, the communication delay, link reliability, node trust, and security risk are taken into consideration simultaneously while making the route selection decision. The proposed approach is dynamic in nature that identifies routes which balance security, efficiency and network sustainability, while conventional approaches optimize only one or two routing parameters. The proposed approach had a higher packet delivery ratio (PDR) especially in the presence of malicious nodes. Conventional shortest-path routing was more susceptible, as the selection of a route was mainly done based on the path length and the behavior of nodes was not taken into consideration. Energy-aware routing enhanced network lifetime, but was insufficient to offer protection against compromised nodes. Trust-based routing provided higher security, but trust-based routing—choosing routes primarily based on trust—sometimes led to longer paths in the network and to higher delays.

Table 1

Comparative Performance of Secure Routing Methods

Routing Method	PDR (%)	Delay (ms)	Energy (J)	Attack Avoidance (%)
Shortest-Path	86.4	42.6	18.7	72.3
Energy-Aware	89.8	39.4	15.2	78.6
Trust-Based	93.1	44.2	16.8	91.5
Proposed Method	97.2	34.8	12.9	96.8

The proposed method had a PDR of 97.2%, which was higher than the PDR of 86.4% for shortest-path routing, as presented in Table 1. The attack-avoidance rate rose to 96.8%, showing that trust and security-risk evaluation was effective in preventing compromised nodes from taking part in selected routes. The average delay was shortened to 34.8ms with the multi-objective cost function avoiding unnecessary long secure paths.

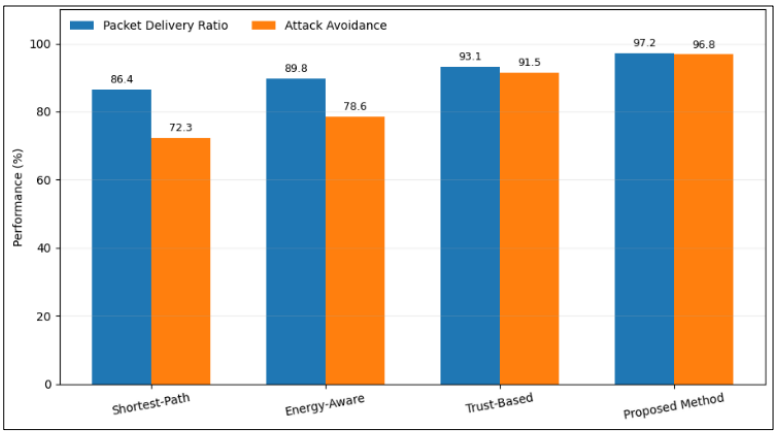


Figure 3

Secure Routing Performance Comparison

This (Figure 3) shows the comparison of packet delivery ratio and attack avoidance performance of various routing protocols. The proposed method is achieved with the highest PDR which is 97.2% and attack avoidance rate is 96.8%. This improvement proves that the evaluation of trust and risk of security is an effective way of avoiding malicious nodes and still ensuring reliable packet transmission using graph-based approach. There were also very significant enhancements in energy performance. The proposed routing algorithm used 12.9 J and conventional shortest-path routing used 18.7 J. This reduction was accomplished by taking into account the residual energy when calculating the edge weight and by not reusing energy constrained nodes. This results in more even energy usage throughout the network thereby prolonging the life of the network.

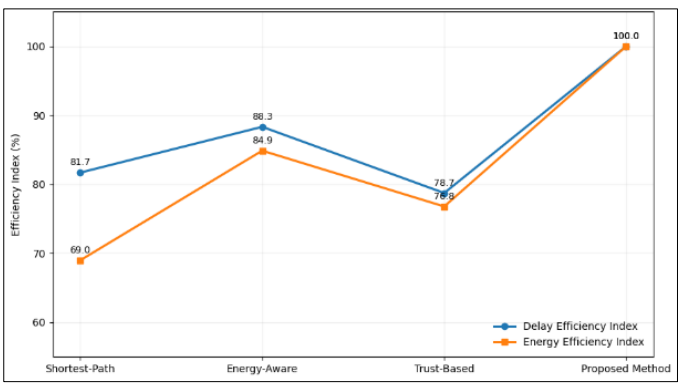


Figure 4

Routing Efficiency Comparison

The Figure 4, shows the normalized delay and energy efficiency for the routing methods evaluated. The proposed method has the highest efficiency index for both the above parameters. The results show that multi-objective route optimization can decrease the transmission delay and energy consumption by providing secure and resource efficient communication routes. The framework also had a stable performance for growing the number of nodes in the network and nodes joining the malicious set. The weights of the graphs were dynamically updated, enabling them to adjust to shifts in trust, residual energy, link reliability and security. If a node showed abnormal forwarding it lost trust and the routing cost of the node increased, which meant that the use of that node was avoided by the routing paths.

7. Security and Robustness Analysis

The security and strength of the proposed routing framework based on the graph were compared in different environments, such as varying number of malicious nodes, failures of links and changes of topology. The framework was able to successfully recognize nodes that were not trusted, and regularly adjust the trust values based on the quality of communication and packet-forwarding behavior. These nodes whose trust was below the trust threshold that was set beforehand were not considered in the candidate routes, therefore less vulnerable to blackhole and selective-forwarding attacks. Energy levels, congestion, and link quality were further taken into account by the routing mechanism as it was able to adjust the edge weight dynamically. Once an active route was no longer available the framework chose an alternate secure route, but did not cause any material disruption of packet transmission. The incorporation of trust and security risk but also of residual energy and reliability also ensured less reliance on individual nodes and increased resilience against node failures. In general, the proposed mechanism kept the wireless sensor network well connected and the routing function stable with dynamic network, which makes it suitable for resource-constrained wireless sensor networks with potentially hostile and unreliable communication environments.

8. Conclusion and Future Work

This research gave an overview of graph-based modeling and optimization for secure routing in wireless and sensor network architectures. The proposed approach is to model the sensor nodes and communication links as a weighted graph and to combine energy consumption, delay, reliability, trust and security risk into a single routing criterion. Multi-objective optimization helps choose secure and energy efficient routes and to eliminate malicious, unreliable and energy exhausted nodes. Experimental assessment showed its superior performance in terms of packet delivery ratio, attack avoidance, energy efficiency, communication delay and robustness to network compared to conventional routing approaches. Dynamic trust evaluation and adaptive edge weighting further enhanced the resilience to the blackhole attack, selective forwarding, node failures and varying network conditions. The framework is

thus a suitable platform for secure routing in resource-limited wireless networks. Scalability, adaptability, computational efficiency, and security can be further analyzed through future research on machine learning-based trust prediction, reinforcement learning-assisted routing, blockchain-based authentication, and mobile sensor networks, as well as real world hardware implementation, in larger and more complex environments.

References

[1] Q. Cappart, D. Chételat, E. B. Khalil, A. Lodi, C. Morris, and P. Veličković, "Combinatorial Optimization and Reasoning with Graph Neural Networks," *J. Mach. Learn. Res.*, vol. 24, pp. 1–61 (2023).

[2] Z. A. Dagdeviren, "Weighted Connected Vertex Cover Based Energy-Efficient Link Monitoring for Wireless Sensor Networks Towards Secure Internet of Things," *IEEE Access*, vol. 9, pp. 10107–10119 (2021).

[3] M. Majid, S. Habib, A. R. Javed, M. Rizwan, G. Srivastava, T. R. Gadekallu, and C. Lin, "Applications of Wireless Sensor Networks and Internet of Things Frameworks in the Industry Revolution 4.0: A Systematic Literature Review," *Sensors*, vol. 22, Art. no. 2087 (2022).

[4] X. Xie, Z. Dou, and Y. Zhang, "Reinforcement Learning-Based Intelligent Decision-Making for Communication Parameters," *KSII Trans. Internet Inf. Syst.*, vol. 16, pp. 2942–2960 (2022).

[5] Z. Al Aghbari, A. M. Khedr, W. Osamy, I. Arif, and D. P. Agrawal, "Routing in Wireless Sensor Networks Using Optimization Techniques: A Survey," *Wireless Pers. Commun.*, vol. 111, pp. 2407–2434 (2020).

[6] S. Sharma, P. Rathi, R. K. Popli, S. Tanwar, and P. Vats, "Algebraic Graph Models for Secure Distributed Networks and Cryptographic Systems," *J. Discrete Math. Sci. Cryptogr.*, vol. 28, no. 8, pp. 3071–3080 (2025), doi: 10.47974/JDMSC-2468.

[7] H. Abdulrab, F. A. Hussin, A. Abd Aziz, A. Awang, I. Ismail, and P. A. M. Devan, "Reliable Fault-Tolerant-Based Multipath Routing Model for Industrial Wireless Control Systems," *Appl. Sci.*, vol. 12, Art. no. 544 (2022).

[8] M. Abbasi, A. Shahraki, and A. Taherkordi, "Deep Learning for Network Traffic Monitoring and Analysis (NTMA): A Survey," *Comput. Commun.*, vol. 170, pp. 19–41 (2021).

[9] A. K. Sharma, N. Purohit, S. Joshi, I. U. Lakkewar, and P. Khobragade, "Securing IoT Environments: Deep Learning-Based In-

trusion Detection," in *Deep Learning for Intrusion Detection*, F. S. Masoodi and A. Bamhdi, Eds. Wiley, ch. 12, pp. 251–266 (2026), doi: 10.1002/9781394285198.ch12.

[10] M. Kol, E. E. Uslu, Z. A. Dagdeviren, and O. Dagdeviren, "Design and Analysis of Minimum Weighted Connected Capacitated Vertex Cover Algorithms for Link Monitoring in IoT-Enabled WSNs," *Sensors*, vol. 26, Art. no. 2752 (2026).

[11] L. Sixu, W. Muqing, and Z. Min, "Particle Swarm Optimization and Artificial Bee Colony Algorithm for Clustering and Mobile-Based Software-Defined Wireless Sensor Networks," *Wireless Netw.*, vol. 28, pp. 1671–1688 (2022).

[12] O. I. Khalaf, C. A. Romero, S. Hassan, and M. T. Iqbal, "Mitigating Hotspot Issues in Heterogeneous Wireless Sensor Networks," *J. Sensors*, vol. 2022, Art. no. 7909472 (2022).

[13] O. E. Oluyisola, F. Sgarbossa, and J. O. Strandhagen, "Smart Production Planning and Control: Concept, Use Cases, and Sustainability Implications," *Sustainability*, vol. 12, Art. no. 3791 (2020).

Received March, 2026