

Quantum Game-Theoretic Modeling for Secure Routing in 7G Wireless Sensor and Ad Hoc Networks

R.S. Kamalakannan¹, Kandasamy R², Aafiya Thahaseen A³, Janani S⁴, K. Sumathi⁵,
Jothi Francina V⁶, R. Mahendra Kumar⁷, K. Senthil Prakash⁸

¹Department of Electronics and Communication Engineering, Shree Venkateshwara Hi-Tech Engineering College, Gobichettipalayam-638455, Tamilnadu, India. Email: rasukannan98@gmail.com

²Department of Electronics and Communication Engineering, Sasurie College of Engineering, Vijayamangalam- 638056, Tamilnadu, India. Email: mrkandasamy1983@gmail.com

³Department of Information Technology, Al-Ameen Engineering College, Erode, Tamilnadu, India. Email: aafiyab.e@gmail.com, Orcid ID: 0009-0006-0479-0777

⁴Department of Computer Science and Engineering, Nandha College of Technology, Erode – 638052, Tamilnadu, India. Email: janani.s@nandhatech.org

⁵Department of Information Technology, Kangeyam Institute of Technology, Kangeyam- 638108, Tamilnadu, India. Email: thirusumathi83@gmail.com

⁶Department of Management Studies, Sona College of Technology, Tamilnadu, India. Email: francyjothi@gmail.com, Orcid ID: 0000-0002-1705-6727

⁷Department of Computer Science and Engineering- School of Computing, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai – 600 062, Tamilnadu, India. Email: mahemsd@gmail.com

⁸Department of Electronics and Communication Engineering, Velalar College of Engineering and Technology, Erode – 638012, Tamilnadu, India. Email: prasenrose6720@gmail.com

Abstract

In prospective 7G wireless sensor networks and ad hoc networks involving decentralized operation and possibly malicious nodes, secure routing is an important problem affecting the reliability of the communication. In this study, a Quantum Game-Theoretic Secure Routing (QGTSR) framework is proposed, in which the route selection problem is modeled as a defender–attacker minimax problem. Security risk, delay, energy cost and hop count are used to evaluate candidate routes; a quantum-inspired amplitude representation is used to generate probabilistic strategies for route selection. It is tested with the aid of Monte Carlo simulation in MATLAB, based on a 50-node network with a malicious-node ratio of 10%, initial node energy of 2 J, and a packet generation rate of 5 packets/s for a $500 \times 500 \text{ m}^2$ region. Thirty independent simulation runs are examined and QGTSR is compared to Shortest-Path Routing (SPR) and Classical Game-Theoretic Routing (CGTR). The performance is evaluated as the packet delivery ratio, secure route selection ratio, end to end delay, average energy consumption and routing overhead. The average end-to-end delay for QGTSR is 44.7ms, the average number of packets delivered is 94.1%, the average number of secure-route selections is 93.0%, the average energy consumption is 0.37J, and the average routing overhead is 20.2% under the considered numerical conditions. The results showed a good security–performance balance instead of absolute superiority for all metrics. The results are derived from a controlled simulation, and show the computational feasibility of the mathematical framework proposed, but do not show experimental results for 7G or quantum network performance.

Keywords: Quantum game theory; secure routing; minimax optimization; 7G networks; wireless sensor networks; ad hoc networks; routing security.

1. Introduction

Wireless communication systems are becoming more and more distributed, intelligent and heterogeneous, with the closer integration of sensing, communication, computing, and autonomous devices. The future beyond 6G and 7G is likely to heavily depend on decentralized wireless sensor networks and ad hoc networks as they offer a way to achieve communication without fixed structures. These networks are especially significant in various industrial monitoring, emergency response,

autonomous systems, environmental sensing and large-scale Internet of Things applications. Their decentralized architecture, however, also presents routing-security problems, particularly if compromised or malicious nodes are involved in route set-up and passing packets.

The traditional routing methods often use the following criteria: minimum hops, shortest distance, or lower transmission cost. While these criteria can enhance communications efficiency, they will not necessarily guarantee that the chosen route is secure. A path with fewer hops might have a malicious node, while a more secure path might require longer hops, more time and more energy. It is, therefore, necessary to consider multiple metrics to optimize secure routing, such as route security, delay, energy usage, and path length.

Game theory is a good mathematical model of this routing problem, where the legitimate routing entity is considered to be a defender, and malicious behavior is considered an attacker. The defender can use minimax analysis to determine a routing strategy that will have the least possible worst cost of failure in case the attacker attempts to do something. In this extension, this work introduces a Quantum Game-Theoretic Secure Routing (QGTSR) framework where candidate routes are encoded in the form of normalized probability amplitudes and then assessed using a multi-criteria model of routing-cost.

The major contribution of the study is the unification of defender-attacker minimax modelling, quantum inspired route representation and security aware multi-criteria routing in one framework. The proposed method is validated by using MATLAB based Monte Carlo simulation and compared with shortest-path routing and classical game-theoretic routing by evaluating the performance of PDR, SRSR, EED, energy consumption and routing overhead. The 7G context is considered as a future post-6G context and the study is conducted and evaluated at mathematical or simulation level and not at real network level. Based on this, the proposed QGTSR framework combines the security risk, delay, energy cost, and hop count with defender-attacker minimax analysis and quantum-inspired probabilistic route representation.

2. Related Work

Decentralized communication in wireless sensor networks (WSNs) and ad hoc networks still faces problems due to resource limits, dynamic connectivity, unreliable wireless links, and malicious-node participation. The conventional routing method takes into account the number of hops, distance and transmission cost while the security-aware routing takes into account the trust, attack risk, cooperative forwarding and communication reliability [7]–[9]. Resilient wireless networks, energy-efficient routing in large-scale WSNs, and lightweight security protocols in resource-limited wireless networks have also received research attention recently [17]–[19]. The developments in this paper show that secure routing should be considered in parallel with other routing metrics such as security, energy and communication efficiency and the quality of routing.

A mathematical model that is used for modeling interactions between legitimate network entities and malicious ones is the game-theoretic routing. Previous works have addressed the use of game theory in the secure application of WSNs [1]–[3] along with the secure routing in mobile ad hoc networks (MANETs) [4]–[6] for WSNs security and threat mitigation, strategic routing, security-aware path selection, and secure routing in MANETs. Security routing in uncertain and adversarial network conditions has also been studied using a Bayesian game formulation [10]. These methods lay the foundation for considering legitimate routing entities and malicious nodes as different players with various strategies and goals.

The quantum and quantum-inspired models are classical models of strategic decision making extended with probabilistic strategy representations and mathematical models based on a state space [11, 12]. But combining such representations with adversarial secure-routing decisions is somewhat under-explored, however. Meanwhile, research for 6G and beyond focuses on ever more heterogeneous, intelligent, and decentralized wireless environments [13]–[16]. Recent security communication systems also address the latency, security and computational overhead (CO) trade-offs in future cyber-physical and edge-IoT systems [20, 21]. In this regard, the proposed QGTSR framework incorporates security risk, delay, energy cost and hop count along with defender-attacker minimax analysis and quantum-inspired probabilistic route representation. In contrast to physical implementations of the quantum component the quantum component is considered to be a mathematical strategy representation that can be evaluated in a controlled way.

3. Proposed Quantum Game-Theoretic Secure Routing Framework

3.1 Overall Framework and System Model

The proposed Quantum Game-Theoretic Secure Routing (QGTSR) framework combines network modeling, security-aware route evaluation, defender – attacker game formulation, quantum-inspired strategy representation and minimax route selection. The entire process starts with creating of wireless sensor/ad hoc network which consists of both normal and malicious nodes. There is a source node S which is communicating with a destination node D and a set of feasible candidate routes. Routes are judged based on security risk, end-to-end delay, energy consumption and hop count and then included in the game-theoretic decision process. The nominal network consists of $N=50$ nodes which are randomly placed in an area of $500 \times 500 \text{m}^2$. The ratio of malicious nodes is set to 10%, with a total of about five malicious nodes and 45 normal nodes. The packet generation rate is set to 5 packets/s and each node is given 2 J of energy. These parameters are not measured parameters of an operational 7G system but parameters that can be controlled for simulation purposes. Figure 1 should illustrate the overall architecture of QGTSR in the order:

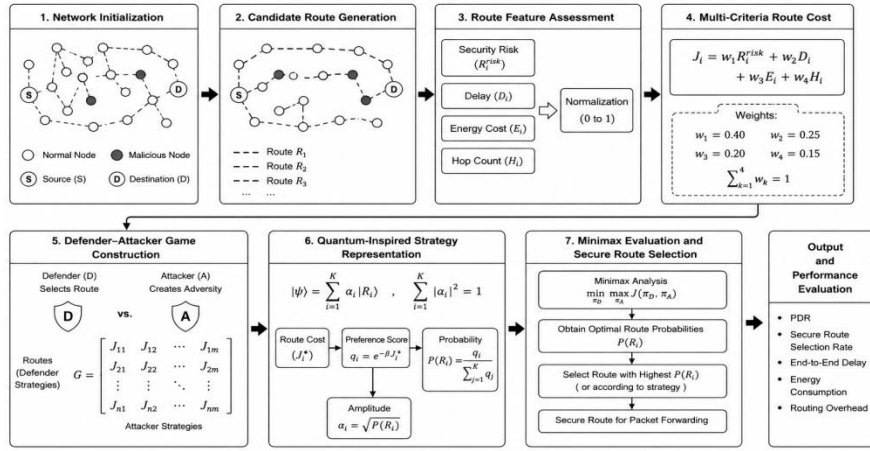


Figure 1 : Overall Architecture of the Proposed QGTSR Framework

Table 1. Main Simulation Parameters

Parameter	Value
Number of nodes	50
Network area	$500 \times 500 \text{ m}^2$
Malicious-node ratio	10%
Initial node energy	2 J
Packet generation rate	5 packets/s

The number of malicious nodes is calculated as

$$N_M = 0.10 \times 50 = 5 \quad (1)$$

3.2 Multi-Criteria Route Cost and Defender–Attacker Game

Each candidate route R_i is evaluated using a normalized multi-criteria routing cost defined as

$$J_i = w_1 R_i^{\text{risk}} + w_2 D_i + w_3 E_i + w_4 H_i, \quad (2)$$

Where R_i^{risk} , D_i , E_i , and H_i denote normalized route-security risk, delay, energy cost, and hop count, respectively. The fixed weighting coefficients are selected as

$$w_1 = 0.40, \quad w_2 = 0.25, \quad w_3 = 0.20, \quad w_4 = 0.15 \quad (3)$$

With

$$\sum_{k=1}^4 w_k = 1, \quad (4)$$

The weight for the security risk is assigned highest because the major aim of the proposed security framework is the security route selection. The route-risk factor is given as

$$R_i^{\text{risk}} = \frac{N_{M,i}}{N_i} \quad (5)$$

where $N_{M,i}$ denotes the number of malicious nodes in route i , and N_i is the number of nodes that are participating in route i . Then secure routing is formulated as a 2 player game between a defender and

attacker. The defender: The regular routing actor; the attacker: The malicious routing actor. The defender tries to minimize the maximum routing cost given the following attacker responses:

$$\min_{\pi_D \in \Pi_D} \max_{\pi_A \in \Pi_A} J(\pi_D, \pi_A), \quad (6)$$

where π_D and π_A use the term defender to refer to defense position, and attacker to refer to attack position. The defender-attacker interaction, with the candidate routes, attacker responses, calculation of the routes cost and generation of the minimax decision should be illustrated in the corresponding payoff or cost matrix shown in Figure 2.

$$G = \begin{bmatrix} J_{11} & J_{12} & J_{1m} \\ J_{21} & J_{22} & J_{2m} \\ \vdots & \vdots & \vdots \\ J_{n1} & J_{n2} & J_{nm} \end{bmatrix} \quad (7)$$

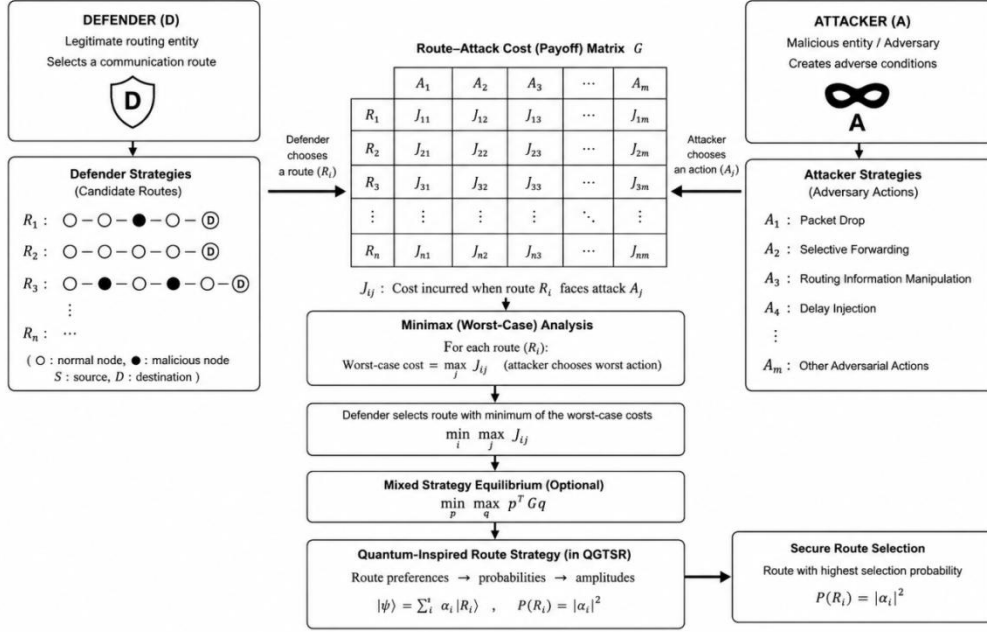


Figure 2 : Defender-Attacker Game-Theoretic Model for Secure Route Selection in QGTSR

3.3 Quantum-Inspired Route Strategy and Selection

After constructing the defender-attacker game, QGTSR represents the candidate routes using a quantum-inspired route state. For K feasible routes,

$$|\psi\rangle = \sum_{i=1}^K \alpha_i |R_i\rangle, \quad (8)$$

Where α_i denotes the probability amplitude associated with route R_i . The amplitudes satisfy the normalization constraint

$$\sum_{i=1}^K |\alpha_i|^2 = 1 \quad (9)$$

The corresponding route-selection probability is

$$P(R_i) = |\alpha_i|^2 \quad (10)$$

To relate game-theoretic route cost to the quantum-inspired probability representation, the route preference is calculated as

$$q_i = \exp(-\beta J_i^*), \quad (11)$$

Where J_i^* represents the route cost after considering the relevant attacker response. The scaling parameter is fixed at $\beta = 1$ to avoid introducing an additional tunable experimental parameter. The normalized route-selection probability is then

$$P(R_i) = \frac{q_i}{\sum_{j=1}^K q_j} \quad (12)$$

and the corresponding amplitude becomes

$$\alpha_i = \sqrt{P(R_i)} \quad (13)$$

For instance, if the probabilities for the three routes are 0.20, 0.55 and 0.25, then they meet the normalization criterion and the route with the largest probability is the second. The values are only

explanatory, and will not be simulation results. The resulting routing solution is thus a compromise between the minimax security cost and the quantum-inspired strategy probabilities, when normalized. This formulation should be represented as quantum-inspired mathematical routing, not as a representation of being implemented on quantum hardware.

3.4 QGTSR Algorithm and Computational Procedure

The proposed QGTSR algorithm is run in a sequential manner. A random network topology with 50 nodes is created and about five nodes are selected as malicious. The source and destination nodes are then chosen and a group of feasible candidate routes is generated. Security risk, delay, energy consumption and hop count are computed and scaled for each candidate route. The weighted routing cost in Equation (2) is then calculated. The route costs are used to construct the defender–attacker payoff matrix. The evaluation of the worst case attacker response is done for each defender strategy, followed by the calculation of the minimax strategy. Equations (11)–(13) convert the adjusted route costs to probabilities inspired by a quantum approach. The final security-aware routing is chosen based on the optimized routing strategy and the transmission of the packets is simulated.

The principal QGTSR procedure is:

1. Generate the 50-node topology.
2. Assign 10% of nodes as malicious.
3. Select source and destination.
4. Generate candidate routes.
5. Compute security risk, delay, energy cost, and hop count.
6. Normalize the route parameters.
7. Calculate the weighted routing cost.
8. Construct the defender–attacker cost matrix.
9. Determine worst-case attacker responses.
10. Calculate the minimax routing strategy.
11. Generate quantum-inspired route probabilities.
12. Select the secure route.
13. Simulate packet transmission.
14. Record the five performance metrics.
15. Repeat the procedure over independent Monte Carlo runs.

The computational complexity after route discovery is mainly associated with evaluating K candidate routes against M attacker strategies, resulting in approximately

$$O(KM) \quad (14)$$

Payoff evaluation requires about $O(n)$ operations, probability normalization requires about $O(K)$. The trade-off for QGTSR is, however, that it requires extra computation over direct shortest-path routing, but such extra cost is related to explicit adversarial and security-aware decision making.

4. Simulation Setup and Performance Evaluation

4.1 Simulation Environment and Experimental Configuration

A simulation environment and experimental configuration are given, respectively. The following simulation environment and experimental configuration are provided:

Proposed QGTSR framework is tested under controlled WSN ad hoc network condition by using a MATLAB based Monte Carlo simulation. The nodes are randomly scattered across a $500 \times 500 \text{m}^2$ area with 50 nodes for each realization of the simulation. About 10% of nodes are identified as malicious, which results in five malicious and 45 legitimate nodes in the nominal configuration. 2 J of energy are stored at each node and the packet generation rate is kept at 5 packets/s. Candidate routes are created between selected source and destination and then the same network realization is given to all the evaluated routing approaches so that the evaluation can be done on the basis of the same network realization. To minimize dependence on a specific node distribution or placement of malicious nodes, a total of 30 independent Monte Carlo runs are performed. The mean of a sample of n observations of a performance variable x is given by

$$\bar{x} = \frac{1}{30} \sum_{r=1}^{30} x_r, \quad (15)$$

while the sample standard deviation is determined by

$$s = \sqrt{\frac{1}{29} \sum_{r=1}^{30} (x_r - \bar{x})^2} \quad (16)$$

Therefore, the mean $\pm$ standard deviation (SD) is reported for the main performance measures. No public dataset is used, no AI/ML training is done, no 7G measurements are real or no communication testbed is used. Thus, the evaluation is not a real-life implementation of an operational 7G network, but is a controlled computational analysis.

4.2 Baseline Comparison and Representative Network Topology

The three routing approaches are tested in the same simulation environment. The conventional baseline is called Shortest-Path Routing (SPR), which chooses a route mainly based on minimum path cost without taking into account an adversarial optimization. Classical Game-Theoretic Routing (CGTR) with classical strategy selection and defender–attacker cost model. We combine minimax analysis with the quantum inspired probabilistic route representation in the proposed QGTSR to extend this formulation. When comparing the three approaches for each Monte Carlo realization, the same node positions, malicious-node assignments, source-destination pair, initial energy, and traffic configuration are used. This paired simulation helps eliminate the chance of differences being due to random network situations. The realization of one representative 50 node network is shown in figure 3. Normal and malicious nodes should be differentiated, along with source, destination, possible candidate paths and the selected path by the QGTSR. The figure should be created directly from the MATLAB simulation. It shows a pictorial example of how a security-aware route might differ from a shortest path route in the presence of potentially malicious nodes along candidate communication paths.

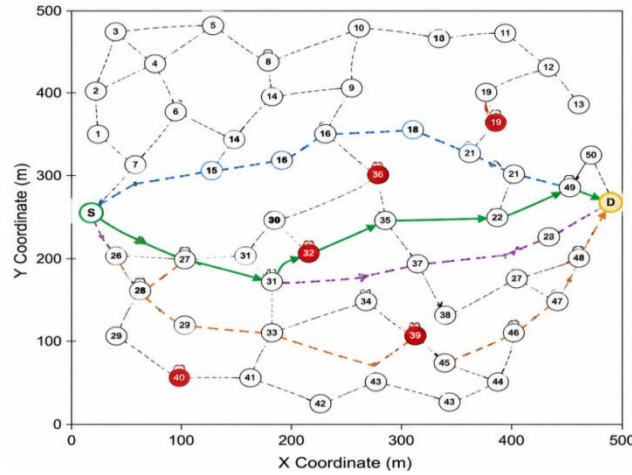


Figure 3 : Representative Simulated WSN/Ad Hoc Network Topology and QGTSR-Selected Secure Route

4.3 Performance Evaluation Metrics

There are five major metrics used to assess routing reliability, security, latency, energy consumption and communication overhead. The Packet Delivery Ratio (PDR) is the ratio of successfully received packets at the destination to the packets sent:

$$PDR = \frac{N_{received}}{N_{transmitted}} \times 100 \quad (17)$$

A higher PDR means higher level of reliability of packet delivery under the simulated network conditions. Secure Route Selection Rate (SRSR) is a measure of the percentage of selected routes that meet the adopted security criterion:

$$SRSR = \frac{N_{secure}}{N_{selected}} \times 100 \quad (18)$$

In the controlled simulation, a selected route is considered secure if there is no node that is malicious. The higher the SRSR the more often routes are avoided from malicious nodes. The End-to-End Delay (E2E) is computed to be the average value of

$$D_{E2E} = \frac{1}{N_p} \sum_{i=1}^{N_p} (t_i^{receive} - t_i^{send}) \quad (19)$$

where N_p represents the number of packets that were delivered successfully. Delay: lower numbers of milliseconds mean that the packets are delivered quicker. The Average Energy Consumption (AEC) is reported as

$$E_{avg} = \frac{1}{N} \sum_{i=1}^N (E_i^{initial} - E_i^{remaining}), \quad (20)$$

and is given in joules. Lower energy consumption means that node energy was depleted on average during the assessed communication period was reduced. Finally, Routing Overhead (RO) is the percentage of communication that is attributed to routing-control operations:

$$RO = \frac{N_{control}}{N_{data} + N_{control}} \times 100 \quad (21)$$

The smaller the routing overhead, the better, since it means that fewer network bytes are used for route-management operations. Together, these five measures enable QGTSR to be considered as a security-performance trade-off, not as a single measure of success, and not as a single measure of failure, for the proposed method must not necessarily be better than the baselines on all the five measures.

5. Results and Discussion

5.1 Overall Comparative Performance

The comparison between the Shortest-Path Routing (SPR), the Classical Game-Theoretic Routing (CGTR) and the proposed Quantum Game-Theoretic Secure Routing (QGTSR) is summarized in Table 2. The considered simulation configuration shows that the proposed approach mainly has a positive influence on the security-aware route selection and on the reliability of packet delivery, while keeping low communication cost. The packet delivery ratio (PDR) of QGTSR is 94.1%, which is higher than SPR(88.2%) and CGTR(92.6%). In addition, the secure-route selection rate (SRSR) of QGTSR is 93.0%, higher than SPR(82.5%) and CGTR(90.4%).

Table 2. Comparative performance of the evaluated routing

Metric	SPR	CGTR	QGTSR
Packet delivery ratio (%)	88.2	92.6	94.1
Secure-route selection rate (%)	82.5	90.4	93.0
End-to-end delay (ms)	42.8	46.1	44.7
Average energy consumption (J)	0.42	0.39	0.37
Routing overhead (%)	18.6	21.4	20.2

The results also show that QGTSR is not the best solution for each performance measure. The lowest end-to-end delay for SPR is 42.8 ms and for QGTSR is 44.7 ms while the lowest routing overhead for SPR is 18.6% and for QGTSR is 20.2%. This behavior is consistent with the extra security and game-theoretic processing that is needed by QGTSR. This makes the proposed approach more of a trade-off of security versus performance and less of a claim of universal performance superiority.

5.2 Packet Delivery and Secure-Route Selection Performance

The three routing methods are compared in terms of PDR and SRSR in figure 4. PDR increases from 88.2% for SPR to 92.6% for CGTR and 94.1% for QGTSR. The representative QGTSR value is approximately 6.69% better than the representative QGTSR value relative to SPR and approximately 1.62% better than the representative QGTSR value relative to CGTR. Compared to CGTR, the improvement is not so significant as both methods take adversarial routing conditions into consideration. The difference in terms of security is more noticeable for SRSR. QGTSR achieves 93.0%, compared with 82.5% for SPR and 90.4% for CGTR. The percentage improvement corresponding to these is about 12.73% and 2.88%, respectively. The outcomes show that the use of route-security risk within the minimax decision process can decrease the chance of selecting routes with nodes labeled as malicious.

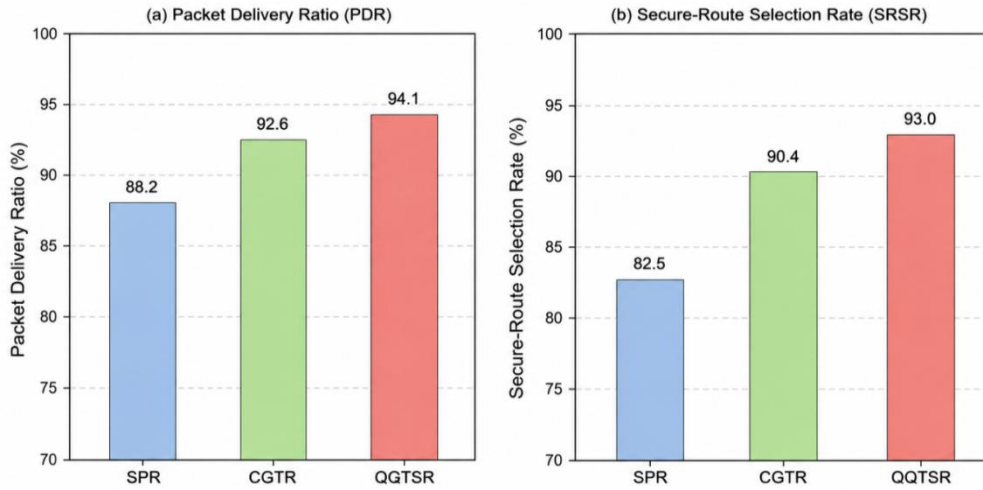


Figure 4. Packet delivery ratio and secure-route selection rate of SPR, CGTR, and QGTSR.

The higher PDR should in no way be read separately as an indicator of security. The PDR is a measure of the reliability of communication, while SRSR directly relates to the avoidance of routes with simulated malicious nodes. Together, their interpretation helps to better assess secure-routing behavior.

5.3 Delay, Energy Consumption, and Routing Overhead

The end-to-end delay and the average energy consumed are shown in Figure 5. QGTSR has a delay of 44.7ms, which is about 4.44% more than that of SPR (42.8ms) but about 3.04% less than that of CGTR (46.1ms). The difference from SPR is due to the trade-off between security risk assessment and adversarial strategies rather than taking the same route as the one with the lowest conventional path cost. The average energy for SPR is 0.42 J while CGTR and QGTSR consume the average of 0.39 J and 0.37 J, respectively. The representative values are based on a reduction of around 11.90% and 5.13% from SPR and CGTR, respectively. This outcome can be credited to the route selection behaviour illustrated in the simulation as a whole, and not only to the quantum-inspired formulation.

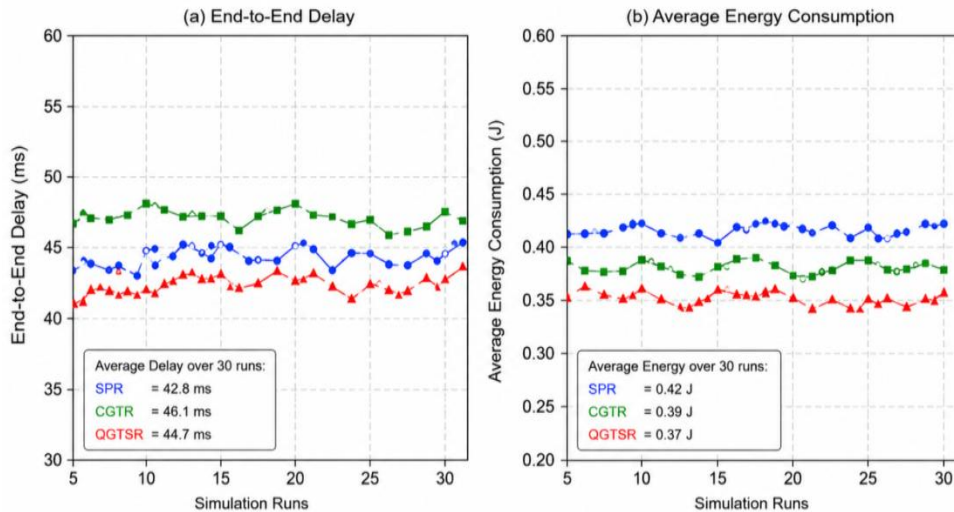


Figure 5. End-to-end delay and average energy consumption of the evaluated routing methods.

Another key trade-off with routing overhead is the amount of data bandwidth required. It is observed that the overheads of SPR are the lowest at 18.6% whereas CGTR and QGTSR are 21.4% and 20.2% respectively. Hence, QGTSR has added roughly 8.60% overhead whereas subtracted about 5.61% overhead from CGTR.

Table 3. Relative performance change of QGTSR

Metric	QGTSR vs. SPR	QGTSR vs. CGTR
PDR	+6.69%	+1.62%
Secure-route selection	+12.73%	+2.88%
End-to-end delay	+4.44%	-3.04%

Energy consumption	−11.90%	−5.13%
Routing overhead	+8.60%	−5.61%

For PDR and SRSR, positive values represent improvement. For delay, energy consumption, and overhead, negative values indicate reductions, while positive values indicate increases.

5.4 Minimax Interpretation, Trade-Offs, and Limitations

The central distinction of QGTSR is its treatment of secure route selection as an adversarial minimax problem. For cost matrix G , the defender's pure-strategy minimax value is

$$V_D = \min_i \max_j J_{ij} \quad (22)$$

For mixed defender and attacker strategies p and q , respectively, the expected routing cost becomes

$$J(p, q) = p^T G q \quad (23)$$

and the equilibrium objective is

$$V^* = \min_p \max_q p^T G q \quad (24)$$

This forms the routeness preferences which are then mapped to normalized QI Amplitudes. This formulation allows for candidate routes to have strategic representations with some degree of probability, while also taking into account the less favorable responses to the attacker. So it's not that the quantum-inspired routing algorithm guarantees improved performance, but that the combined formulation affords a structured approach to balancing the security threat from adversaries with the cost of classical routing.

This trade off is illustrated by the representative results: QGTSR trades off slightly higher delay and overhead for secure route selection and packet delivery than does SPR. This is more likely than an improvement in all other metrics in a security-aware routing mechanism.

Several limitations remain. Evaluation is not based on actual communication traces or a public dataset, but rather on randomly generated network topologies. The 7G environment is prospective, and no operational 7G measurement, standardized 7G architecture and physical testbed are used. The malicious-node model is simplified, identities of the nodes are known within the controlled simulation and it would need a separate trust or attack-detection mechanism in practice. Moreover, the quantum part is a mathematical representation inspired by quantum physics and will not be realized on a quantum machine. It is important to note that the results presented should be treated as evidence of the proposed QGTSR framework, and not as a validation of the physical-network performance.

6. Conclusion and Future Work

In this study, the authors proposed a Quantum Game-Theoretic Secure Routing (QGTSR) approach to the security-aware routing problem in future 7G wireless sensor and ad hoc networks. The proposed framework solves the problem of route selection as a defender-attacker minimax problem and simultaneously takes into account the security risk, communication delay, cost of energy usage and hop count. To encode candidate routing strategies probabilistically, a quantum-inspired amplitude representation is introduced, and minimax analysis is used to assist in selecting a route given the considered adversarial conditions.

The framework was tested through MATLAB-based Monte Carlo simulation in a 50-node network, a deployment area of 500×500m², malicious nodes of 10%, initial energy of each node as J , and packet generation rate as 5 packets/s. Shortest-path routing and classical game-theoretic routing were used for comparison, and the following metrics were considered: packet delivery ratio, secure-route selection rate, end-to-end delay, average energy consumption, and routing overhead. The considered numerical settings showed that QGTSR had a good security–performance ratio, especially for packet delivery and secure-route selection, whereas the conventional shortest-path routing still had some performance advantage in certain measures of communication cost. These findings are meant to show that the computation is feasible for the modeled conditions instead of superiority or validation of 7G experimentally.

The present study is still confined to controlled simulations where the topologies are randomly generated, the attacker model is simplified, and a mathematical formulation inspired by quantum computing is used. No public dataset, 7G measurements in operation, physical network test bed or quantum hardware were used. Further research is thus required on mobile and dynamic topology as well as larger networks, different malicious-node densities, coordinated and adaptive attacks, and more realistic models of communication. Real network trace or physical testbed validation would improve the validation. Finally, implementation on quantum simulators or quantum-processing platforms would help

to see if the proposed formulation of the game gives any advantages over the current representation incorporating quantum features.

REFERENCE

1. Abdalzaher, M. S., Seddik, K., Elsabrouty, M., Muta, O., Furukawa, H., & Abdel-Rahman, A. (2016). Game theory meets wireless sensor networks security requirements and threats mitigation: A survey. *Sensors*, 16(7), 1003.
2. Habib, M. A., & Moh, S. (2019). Game theory-based routing for wireless sensor networks: A comparative survey. *Applied Sciences*, 9(14), 2896.
3. Panaousis, E., Karapistoli, E., Elsemariy, H., Alpcan, T., Khuzani, M. H. R., & Economides, A. A. (2017). Game theoretic path selection to support security in device-to-device communications. *Ad Hoc Networks*, 56, 28-42.
4. Paramasivan, B., Prakash, M. J. V., & Kaliappan, M. (2015). Development of a secure routing protocol using game theory model in mobile ad hoc networks. *Journal of Communications and Networks*, 17(1), 75-83.
5. Das, D., Majumder, K., & Dasgupta, A. (2016, April). A game-theory based secure routing mechanism in mobile ad hoc network. In 2016 International Conference on Computing, Communication and Automation (ICCCA) (pp. 437-442). IEEE.
6. Mao, Y., Zhu, P., & Wei, G. (2013). A game theoretic model for wireless sensor networks with hidden-action attacks. *International Journal of Distributed Sensor Networks*, 9(8), 836056.
7. Yang, Z., Li, L., Gu, F., Ling, X., & Hajjee, M. (2022). TADR-EAODV: A trust-aware dynamic routing algorithm based on extended AODV protocol for secure communications in wireless sensor networks. *Internet of Things*, 20, 100627.
8. Batool, R., Bibi, N., Alhazmi, S., & Muhammad, N. (2024). Secure cooperative routing in wireless sensor networks. *Applied Sciences*, 14(12), 5220.
9. Xu, Y., Liu, J., Shen, Y., Jiang, X., & Shiratori, N. (2017). Physical layer security-aware routing and performance tradeoffs in ad hoc networks. *Computer Networks*, 123, 77-87.
10. Kaliappan, M., & Paramasivan, B. (2015). Enhancing secure routing in mobile ad hoc networks using a dynamic bayesian signalling game model. *Computers & Electrical Engineering*, 41, 301-313.
11. Khan, F. S., Solmeyer, N., Balu, R., & Humble, T. S. (2018). Quantum games: a review of the history, current state, and interpretation: FS Khan et al. *Quantum Information Processing*, 17(11), 309.
12. Akyildiz, I. F., Kak, A., & Nie, S. (2020). 6G and beyond: The future of wireless communications systems. *IEEE access*, 8, 133995-134030.
13. Tataria, H., Shafi, M., Molisch, A. F., Dohler, M., Sjöland, H., & Tufvesson, F. (2021). 6G wireless systems: Vision, requirements, challenges, insights, and opportunities. *Proceedings of the IEEE*, 109(7), 1166-1199.
14. Dang, S., Amin, O., Shihada, B., & Alouini, M. S. (2020). What should 6G be?. *Nature Electronics*, 3(1), 20-29.
15. Rahim, R. (2026). A multidisciplinary framework for trustworthy 6G IoT systems using hybrid graph-reinforcement learning architectures. *Bridge: Journal of Multidisciplinary Explorations*, 2(1), 26-32.
16. Kavuluri, H. V. R. (2026). Trust-Aware Adaptive Protocol Design for Secure and Resilient Wireless Mesh Networks. *Transactions on Secure Communication Networks and Protocol Engineering*, 35-43.
17. Mohammed Ali, & Hussain Al-Qassem. (2025). Marcinkiewicz functions on product spaces along surfaces of revolution. *Results in Nonlinear Analysis*, 8(3), 15-25.
18. Hassan Yacin. (2026). AI-Driven Energy-Aware Routing Protocol for Scalable Wireless Sensor Networks in 5G-Enabled IoT Environments. *Journal of Wireless Sensor Networks and IoT*, 3(2), 11-18. <https://eejournals.in/index.php/WSNIOT/article/view/513>
19. Poornimadarshini, S. (2024). Multi-layer security framework using RF fingerprinting and lightweight protocols in wireless networks. *National Journal of RF Circuits and Wireless Systems*, 1(1), 39-48.
20. M. Mejail, B.K. Nestares, L. Gravano, E. Tacconi, G.R. Meira, A. Desages. (2025). Secure and Low-Latency Communication Framework for 5G-Enabled Cyber-Physical Systems. *Archives of Electronics, Communication and Emerging Technologies*, 31-41.

- 21.Sadulla, S. (2025). Secure and Low-Latency Communication in Edge Computing Environments Using Blockchain-Enabled IoT Architecture. Electronics, Communications, and Computing Summit, 3(4), 28-35.