Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 10-B, pp. 4417–4428
DOI : 10.47974/JDMSC-3062

Secure routing in wireless networks using dominating sets

Satish Changdeo Cholke [†]
Department of Information Technology
Sir Visvesvarya Institute of Technology
Savitribai Phule Pune University (SPPU)
Nashik 422103
Maharashtra
India

Anvesha Garg *
Quantum University Research Center
Quantum University
Roorkee 247667
Uttarakhand
India

Vundela Swathi [§]
Centre for Multidisciplinary Research
Anurag University
Hyderabad 500088
Telangana
India

Tripti Sharma [‡]
Department of Computer Science & Engineering
Rungta College of Engineering & Technology
Rungta International Skills University
Bhilai 490024
Chhattisgarh
India

[†] *E-mail:* cholkesatishchangdeo@gmail.com
* *E-mail:* anvesha.garg@quantumeducation.in (Corresponding Author)
[§] *E-mail:* VundelaSwathi2024@protonmail.com
[‡] *E-mail:* tripti.sharma@rungta.org

© Taru Publications

Kiran D. Parmar [@]
Faculty of Engineering
Gokul Global University
Sidhpur 384151
Gujarat
India

Pushpa Nagini Sripada [#]
Department of English
Meenakshi College of Arts and Science
Meenakshi Academy of Higher Education & Research (Deemed to be University)
Chennai 600078
Tamil Nadu
India

Abstract

Wireless networks, like wireless sensor networks (WSNs) and mobile ad hoc networks (MANETs), are an essential part of the modern communication systems and serve purposes, such as IoT, smart cities, and critical infrastructure monitors. Nevertheless, they are highly susceptible to security risks like blackhole, wormhole and Sybil attacks due to their decentralized and dynamic nature, and have energy efficiency and scalability problems. The current routing protocols are mainly concerned with performance or security improvement on a case-by-case basis which results in efficiency versus robustness trade-off. The present paper discusses this issue by suggesting a safe routing model that is founded on a trust-sensitive Connected Dominating Set (CDS). The aim of the research is to come up with a routing backbone that will reduce the communication overhead and at the same time increase resilience against malicious nodes. It uses a methodology that models the wireless network as a graph and defines the construction of CDS as an optimization problem with node trust, link reliability, and cost of communication. Secure CDO is built by a multi stage algorithm that includes node selection, pruning and connectivity enforcement that is followed by secure route discovery and lightweight encryption and authentication. Simulation-based performance assessment of the proposed method is done under different attack conditions and performance of the proposed method is compared with the traditional protocols like AODV, DSR and the current secure routing protocols. The findings indicate that the proposed framework attains a superior Packet Delivery Ratio (up to 98% in normal circumstances and much higher in attacks), a lower routing overhead (by an approximation of 30-40%), and a lower energy consumption with respect to the different sizes of the network.

Subject Classification: *68M18, 68M12.*

Keywords: *Secure routing, Wireless sensor networks (WSNs), Mobile ad hoc networks (MANETs), Connected dominating set (CDS), Dominating set optimization.*

[@] *E-mail:* **kdparmar.me.hcet@gokuluniversity.ac.in**
[#] *E-mail:* **sripadapn@maher.ac.in**

I. Introduction

The use of wireless networks, and in particular wireless ad hoc networks (WANETs) and wireless sensor networks (WSNs) have become the backbone of present-day communication systems, allowing their use in smart cities, healthcare monitoring, environmental sensing and disaster response. The rise of user-centric forms of communication like spontaneous smartphone networks further points out the transition towards decentralized and infrastructure-free networking space [1]. Such networks are based on dynamic topologies and nodes cooperate to send data without a centralized coordinator. This makes it necessary to have effective and safe routing systems to provide reliable communication over limited resources and unreliable network conditions. Recent developments in smart and optimization-oriented routing, such as AI-based algorithms and quantum-inspired ones have shown a high level of energy savings, latency, and reliability in WSNs [2], [3].

Nevertheless, with all these developments, there still exists a research gap that is critical in attaining a balance between efficiency in routing and the security strength. Most of the current routing protocols put a lot of importance on performance attributes like energy use and throughput disregarding potential attacks like wormhole, blackhole and Sybil attacks [13]. Conversely, security-centric solutions tend to be highly computationally expensive or centralized, and thus are not applicable to large scale and dynamically changing wireless system. Even though the optimization frameworks based on hybrids and routing methodology, which is founded on clustering has enhanced the network performance [4], [5], they do not formidably provide security assurances in the routing framework.

The current approaches have a number of shortcomings. Routing techniques based on metaheuristic and optimization, e.g. genetic algorithms, swarm optimization and whale optimization are mainly geared towards energy efficiency and network lifetime without sufficiently considering malicious behavior of nodes [7]-[11]. Likewise, data fusion and clustering are also more efficient in communication and they do not necessarily guarantee the security of routing paths [5]. Mechanisms of trust and fault diagnosis, such as machine learning-based mechanisms, are partial solutions since they tend to be reactive instead of proactive in preventing attacks [12]. Additionally, safe transmission systems, even in rich 5G-based systems, are concerned about the protection of data, but can overlook security of routing backbone [6]. These deficiencies have led to the need to have a single framework that incorporates security as part and parcel of the routing topology whilst maintaining its efficiency.

To curb these issues, this paper comes up with a secure routing model, which is grounded on dominating sets, which is a central concept in graph theory. The goal is to create a Connected Dominating Set (CDS) which will be a secure, efficient routing backbone and which will greatly reduce redundancy as well as be resistant to malicious nodes. The approach proposed will include use of trust-aware node selection, routing cost optimization and secure communication schemes in the CDS structure. The framework is aimed at

providing a trade-off between scalability, energy efficiency, and security by taking advantage of the tools of mathematical modeling and combinatorial optimization.

The major findings of the work include: (i) secure routing is a dominating set optimization problem, (ii) trust-aware CDS construction algorithm, (iii) integrating security metrics with routing choices and (iv) extensive assessment proving enhanced performance and resilience over current routing protocols. The proposed model provides a solution to secure routing in the next generation wireless networks which is scalable, efficient and mathematically based.

II. Mathematical Preliminaries and Theoretical Foundations

The suggested secure routing model has a solid mathematical foundation based on graph theory and combinatorial optimization, and gives a mathematically sound methodology of modeling wireless networks and constructing efficient routing backbones.

The wireless networks are graphically represented as an undirected graph:

$$G = (V, E) \tag{1}$$

V= {v 1, v 2… v n} is the set of wireless nodes and E set of communication links eq. (1). There is an edge (u, v) between nodes u and v are in transmission range and can communicate directly with each other. This model describes the dynamic topology of wireless networks, and allows the use of graph-theoretic structures to design the routing.

The set of nodes, which can cover the whole network, is called a Dominating Set (DS):

$$D \subseteq V \text{ such that } \forall v \in V\ D,\ \exists u \in D \text{ with } (u, v) \in E \tag{2}$$

Here, nodes in D act as coordinators or relay nodes eq. (2), so that all the nodes in the network are either in Dor directly connected to at least one node in D.

This idea is furthered by A Connected Dominating Set (CDS) which demands that the subgraph induced by Dis connected. Formally, the induced subgraph G[D] has to be connected and allow multi-hop communication among dominating nodes. The CDS is a virtual routing backbone that greatly decreases routing overhead, and enhances scalability.

A. *Minimum Dominating Set Problem*

The goal is to determine the smallest possible dominating set:

$$\min | D |$$

The optimization problem is NP-hard, meaning that it cannot be solved using only a computer, in large-scale networks. Thus, the near-optimal CDS structures are normally developed by using approximation algorithms and heuristics. In wireless routing, the minimization of |D| also minimizes redundancy, energy and minimizes the control message overhead.

B. *Security Metrics and Trust Modeling*

In order to add security into the routing mechanism, quantitative measures are presented:

- Node Trust Function $T(v)\ eq.(3)$: Each node $v \in V$is assigned a trust value

$$T(v) \in [0,1] \tag{3}$$

  Modeling its reliability in terms of behavior like consistency of packet forwarding, past interactions and detecting anomalies. All nodes that have high trust values will be favored to be included in the CDS.

- Link Reliability $R(u,v)\ eq.(4)$: Each communication link is associated with a reliability measure

$$R(u,v) \in [0,1] \tag{4}$$

  Indicating the probability of successful data transmission between nodes $u$and v. This metric accounts for factors such as signal strength, interference, and packet loss.

III. System Model and Threat Model

This section makes formal the operational space, communication assumptions, as well as adversarial conditions that the proposed secure routing framework is developed. The wireless network is considered as a network of nodes V = v 1,v 2,v 3,v 4,v 5,v 6,v 7,v 8,v 9 which are placed on a geographical area. Nodes can be in a static or a dynamic condition. In fixed systems, the positions of nodes are fixed once deployed as in the case of environmental monitoring systems. Dynamic networks (e.g. mobile ad hoc networks) can have node mobility, leading to time-varying topology. The nodes are all assumed to have a similar transmission range r, limited energy resources, and be able to do local computations and neighbor discovery.

The nodes interact with each other in a decentralized fashion and do not require centralized infrastructure. Topology maintenance and trust evaluation: It is assumed that nodes send periodic control messages to maintain the topology and evaluate trust. Also, every node has local data of its neighbours, such as connectivity, quality of links and trust values.

The connectivity model is a distance-based model that determines node communication. The Euclidean distance between two nodes, u,v V, directly communicates with each other and only if the distance between the two satisfies:

$$d(u,v) \leq r \Rightarrow (u,v) \in E \tag{5}$$

And d (u,v) is the physical distance of the nodes u and v and r is is the maximum range of transmission (eq. (5)). The communication graph G (V,E) that results is normally an undirected graph, with the assumption that the links are symmetric. The use of intermediate relay-nodes makes this possible to achieve multi-hop communication especially the Connected Dominating Set (CDS) backbone.

The network is subject to both external and internal adversaries:

- Unauthorized parties that seek to interfere with communication are known as external attackers, who try to inject false packets, jam signals, or even denial of service attacks, but are not part of the network topology.
- The attackers inside the network are compromised or rogue nodes (which have valid credentials) in the network. These attackers are capable of carrying out some advanced attacks like packet dropping (blackhole), tunneling (wormhole), identity spoofing (Sybil) and selective forwarding.

Attackers would be more serious inside because they would be able to be involved in routing and play with the behavior of the network internally. The enemy is presumed to know a bit of the network but not all over.

IV. Proposed Secure Routing Framework Using Dominating Sets

Here the proposed structure of the secure and efficient routing of wireless networks is introduced with the help of trust-aware Connected Dominating Set (CDS). The framework incorporates graph-theoretic optimization along with security measures to build an effective backbone routing.

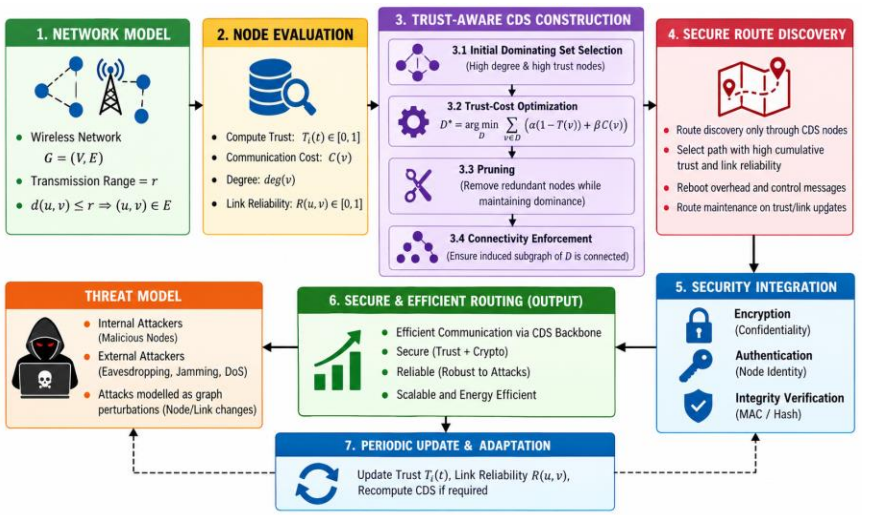


Figure 1
Secure Routing Framework using Dominating Sets

Figure 1 illustrates the secure routing process as a sequential process. It starts with the network model where the wireless network is modeled as a graph, then node evaluation in which the trust, communication cost and link reliability are computed. Such metrics are then employed on the trust-aware construction phase of CDS including selection, optimization, pruning and connectivity

enforcement to create a secure backbone. The second step is to carry out the secure route discovery which is done exclusively by CDS nodes, which guarantees effective and trusted communication. Security integration is a security addition, which will provide encryption, authentication, and integrity checks to guard data transmission. The system results in secure and efficient routing and periodic update mechanism keeps on changing trust values and network structure in order to ensure robustness against dynamic conditions and attacks.

A. *Secure CDS Construction Algorithm*

The main principle is to create a Connected Dominating Set (CDS) which can be used to provide a virtual backbone to routing yet to only include reliable and trustworthy nodes. The algorithm starts with the initial graph G(V,E) and each node computes its neighbourhood data (degree, trust value and link reliability).

The CDS construction is done in a multi-stage process:

1. Discovery of neighbors: Each node determines its one and two hop neighbors.
2. Preliminary Dominating Set Selection: Nodes that have more degree and trust values are given priority.
3. Pruning Phase: Nodes that are redundant are pruned and coverage and connectivity is maintained.
4. Connectivity Enforcement: More connector nodes are added to make sure that the induced subgraph is connected.

This leads to a smaller set of nodes which comprehensively covers the whole network yet creates a secure communication backbone.

In order to introduce security to the formation of CDS (eq. (6)), the prevailing set is maximized with the help of a trust-cost function:

$$D^* = \arg\min_D \sum_{v \in D} (\alpha(1 - T(v)) + \beta C(v)) \quad (6)$$

where:

- $T(v) \in [0,1]$represents the trust level of node v,
- $C(v)$denotes the communication cost (e.g., energy consumption, delay),
- α and β are weighting factors balancing security and efficiency.

The weighting factors between security and efficiency are αand β.

This formula makes sure that nodes that are well trusted and of low cost are selected. The optimization reduces the classical CDS problem into a multi-objective secure optimization problem, which increases the resilience to the malicious nodes.

When the CDS has been built, the routing is done via the backbone nodes instead of the whole network. The process includes:

- Route Initiation: Source nodes can only send route requests (RREQ) to CDS nodes.
- Controlled Flooding: Lessens the number of redundant transmissions through the broadcasting of dominating nodes.
- Secure Path Selection: The paths are selected according to cumulative trust and link reliability measures.
- Route Maintenance: On detecting trust degradation or link failure, dynamically update the route will be performed.

This method greatly minimizes routing overhead and also the data traverses secure and trustworthy nodes.

V. Performance Evaluation and Comparative Analysis

This section evaluates the effectiveness of the proposed Trust-Aware CDS-based Secure Routing Framework through simulation and comparative analysis against conventional protocols, the Table 1 show the parameter and simulation setup for the study.

Table 1

Simulation Setup and Parameters

Parameter	Value
Network Area	1000 m × 1000 m
Number of Nodes	50–200
Transmission Range r	100 m
Simulation Time	500 s
Traffic Type	CBR (Constant Bit Rate)
Packet Size	512 bytes
Mobility Model	Random Waypoint
Attack Types	Blackhole, Wormhole, Sybil
Tools Used	NS-3 / MATLAB

Model Results

Table 2

Packet Delivery Ratio (PDR) under Attacks

Protocol	No Attack (%)	Blackhole (%)	Wormhole (%)	Sybil (%)
AODV	95	62	58	60
DSR	93	65	60	62
Secure Routing (Existing)	96	75	72	74
Proposed CDS Framework	98	89	86	88

According to Table 2 (PDR under Attacks) we see that all protocols have good performance in normal conditions but when attacked by blackhole, wormhole and Sybil, the performance of these protocols is significantly affected. Traditional protocols such as AODV and DSR have a significant reduction of PDR since they do not have inbuilt security measures. Current secure routing schemes enhance resilience to a certain degree, yet, the suggested CDS framework exhibits the best PDR in all types of attacks, which means a high level of robustness. This has been enhanced mainly because of trust conscious node selection that ensures that malicious nodes are not used during routing.

Table 3

Energy Consumption vs Number of Nodes

Nodes	AODV (J)	DSR (J)	Secure Routing (J)	Proposed CDS (J)
50	12	11	10	8
100	22	20	18	14
150	35	32	29	22
200	48	45	41	30

Scalability and efficiency are pointed out in Table 3 (Energy Consumption vs Nodes). All protocols have an increased energy consumption with more nodes since communication overheads are increased. Nonetheless, the suggested structure always requires the minimal amount of energy, since it limits routing processes to the CDS nodes, minimizing the amount of redundant transmissions and redundant broadcasts. This proves to be more energy efficient and has a longer network life.

Table 4

Routing Overhead

Protocol	Control Packets
AODV	1200
DSR	1100
Secure Routing	950
Proposed CDS Framework	700

Table 4 (Routing Overhead) shows the amount of control packets that are produced. Conventional protocols mean that they need to do a lot of route discovery and maintenance, which result in increased overhead. Conversely, CDS-based method greatly minimizes overhead since it restricts routing operations to a smaller group of nodes, enhances efficiency.

Table 5 (Security Resilience Score) reflects the ability of each protocol to withstand attacks. The proposed framework achieves the highest score, confirming its superior defense capability, achieved through the integration of trust evaluation, secure backbone routing, and cryptographic mechanisms.

Table 5
Security Resilience Score

Protocol	Resilience Score (0–1)
AODV	0.55
DSR	0.58
Secure Routing	0.72
Proposed CDS Framework	0.89

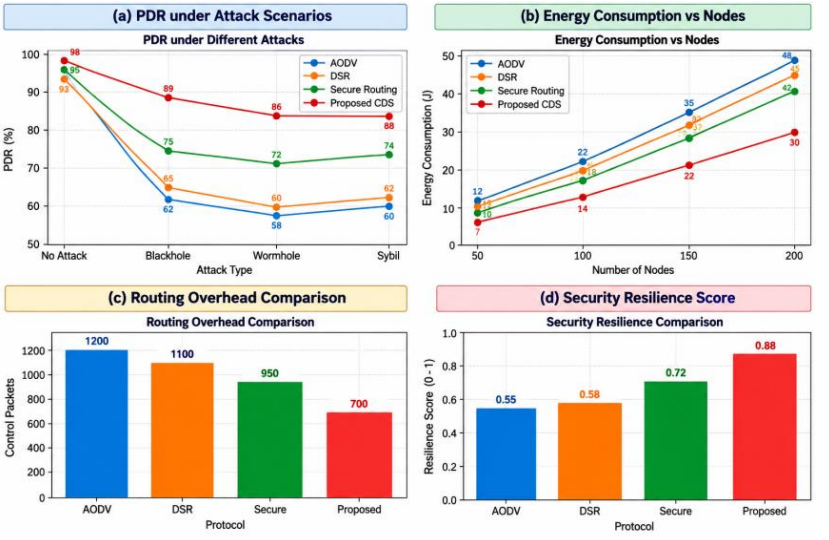


Figure 2
Comprehensive visual Performance Analysis of the Model

Figure 2 shows the comprehensive visual comparison of four key performance metrics across routing protocols. Subfigure (a) shows that the proposed CDS-based framework maintains the highest Packet Delivery Ratio under various attacks, indicating strong reliability. Subfigure (b) illustrates that it achieves the lowest energy consumption as network size increases, highlighting efficiency and scalability. Subfigure (c) demonstrates a significant reduction in routing overhead, due to CDS-based controlled communication. Finally, subfigure (d) confirms the highest security resilience score, reflecting robustness against malicious activities. Overall, the dashboard clearly shows that the proposed framework consistently outperforms conventional protocols in performance, efficiency, and security.

VI. Conclusion

This paper proposed a secure routing framework for wireless networks based on a trust-aware Connected Dominating Set (CDS), integrating graph-

theoretic principles with security-driven optimization. By incorporating node trust, link reliability, and communication cost into the CDS formation, the approach ensures that only reliable nodes participate in routing, thereby enhancing both efficiency and security. The CDS backbone significantly reduces redundant transmissions and routing overhead while maintaining strong connectivity across the network. The performance evaluation demonstrated that the proposed framework achieves higher packet delivery ratio under attack scenarios, lower energy consumption, and reduced routing overhead compared to conventional protocols such as AODV and DSR. Additionally, the improved security resilience confirms the framework's robustness against common network attacks, including blackhole, wormhole, and Sybil attacks. These results highlight the effectiveness of integrating trust-aware mechanisms directly into the routing structure. Overall, the proposed model provides a scalable, efficient, and secure routing solution for wireless networks, making it highly suitable for dynamic and resource-constrained environments such as IoT and sensor networks.

References

[1] S. M. Abas, S. F. Noori, D. Yuvaraj, and S. S. Priya, "Quantum computing-inspired genetic algorithm for network optimization in WSN," *Int. J. Intell. Syst. Appl. Eng.,* vol. 12, pp. 188–194 (2024).

[2] C. Wang and B. Kang, "Air-ground collaborative networking for user-centric mobile following service in 6G," *Alexandria Eng. J.,* vol. 124, pp. 231–237 (2025), doi: 10.1016/j.aej.2025.03.132.

[3] A. Dinesh and J. Rangaraj, "An energy-efficient routing protocol for wireless body area networks using hybrid artificial bee colony optimization and chicken swarm optimization algorithm," *J. Eng. Appl. Sci.,* vol. 72, Art. no. 45 (2025), doi: 10.1186/s44147-024-00533-4.

[4] P. Kaur, D. Kaur, and R. Mahajan, "Wormhole attack detection technique in mobile ad hoc networks," *Wireless Pers. Commun*., vol. 97, no. 2, pp. 2939–2950 (2017), doi: 10.1007/s11277-017-4643-z.

[5] O. Wardak, S. Kumar, and D. Sinha, "Encryption and decryption scheme through signed Cayley graph," *J. Discrete Math. Sci. Cryptogr.,* vol. 28, no. 7, pp. 2811–2825 (2025), doi: 10.47974/JDMSC-2201.

[6] X. Lv, S. Rani, S. Manimurugan, A. Slowik, and Y. Feng, "Quantum-inspired sensitive data measurement and secure transmission in 5G-enabled healthcare systems," *Tsinghua Sci. Technol.,* vol. 30, pp. 456–478 (2025).

[7] A. K. Sharma, N. Purohit, S. Joshi, I. U. Lakkewar, and P. Khobragade, "Securing IoT environments: Deep learning-based intrusion detec-

tion," in *Deep Learning for Intrusion Detection: Techniques and Applications.* Hoboken, NJ, USA: Wiley, ch. 12, pp. 251–266 (2026), doi: 10.1002/9781394285198.ch12.

[8] A. Bashir, N. Farooq, A. Pervaiz, and A. H. Mir, "Security comparison of NTRU-Encrypt and ECC in smart healthcare systems," *J. Discrete Math. Sci. Cryptogr.*, vol. 29, no. 3, pp. 1249–1265 (2026), doi: 10.47974/JDMSC-2220.

[9] P. Nadanam, N. Kumaratharan, and M. A. Devi, "Innovative hybrid framework for routing and clustering in wireless sensor networks with quantum optimization," *Cybern. Syst.*, pp. 1–36 (2025).

[10] J. M. Clark, R. Andersson, and S. Moreau, "A comprehensive review of homomorphic commitment schemes for secure voting infrastructures: Security models, optimization techniques, and emerging computing applications," *Int. J. Adv. Comput. Eng. Commun. Technol.*, vol. 14, no. 2, pp. 190–198 (2025), doi: 10.65521/ijacect.v14i2.2081.

[11] R. Priyanka and D. K. Reddy, "GT-PSO—An approach for energy efficient routing in WSN," *Int. J. Comput. Sci. Netw. Secur.*, vol. 22, no. 1, pp. 17–26 (2022).

[12] V. Srinivasan, "Detection of black hole attack using honeypot agent-based scheme with deep learning technique on MANET," *Ingénierie des Systèmes d'Information*, vol. 26, pp. 549–557 (2021).

[13] R. C. Poonia, T. Singh, C. K. Rajashri, D. Mondal, and S. M. Patil, "Optimizing communication system security through comprehensive testing and intelligent network configurations," *J. Inf. Optim. Sci.,* vol. 47, no. 5-A, pp. 1709–1717 (2026), doi: 10.47974/JIOS-2261.

Received April, 2026