

Enhancing IoT Network Security and Scalability with Energy Harvesting-Aware Routing

Ms. Madhavi Ranjeet Patil
VTU, Research Scholar,

Jain Institute of Technology Davangere,
er.madhavipatil@gmail.com

Dr Rajesh Maharudraa Patil
VTU, Research Supervisor
drmpbpcoep@gmail.com

Dr. Nagaraja B.G
VTU, Research Supervisor
nagarajbg@gmail.com

Abstract: One of the most significant challenges confronting the Internet of Things relates to security, scalability, and energy efficiency, particularly considering the rapid expansion of this technology. A proposed solution involves implementing traffic routing that is aware of energy harvesting (TRAER), which has the potential to enhance network lifetimes by utilising locally available energy resources. Numerous established protocols exhibit vulnerabilities to a range of cybersecurity threats that have the potential to incapacitate a network.

Resilient and dependable IoT networks are created by the Secure and Scalable Energy Harvesting-Aware Routing Algorithm (SS-EHARA) weaving together advanced security features with energy-efficient routing. By means of the distribution of decision-making around the network, SS-EHARA can choose paths in a safe and fair manner, therefore lowering the danger of attack and the energy consumption.

The results show that the proposed protocol delivers a greater number of packets successfully. It also consumes less energy, and speeds up by minimising latency compared to traditional routing approaches. In larger deployments, it scaled magnificently to accommodate extensive IoT networks.

Keywords: TRAER, SS-EHARA

I. INTRODUCTION

The fast growth of Internet of Things (IoT) systems results from both advanced hardware platforms and software platforms together with the rise of communication channels and data analysis instruments. The Internet of Things (IoT) experienced rapid adoption through connectivity that extends from environmental sensors to smart cities and hospitals as well as industrial facilities during the last few years [1]. This phenomenon is characterised by a network of interconnected devices that monitor various environmental variables. This presents intriguing opportunities; however, it is essential to evaluate associated costs, including increasing security, growth, and energy demands, which pose significant challenges. In battery-operated devices functioning under harsh conditions, establishing a secure communication method while enhancing network longevity is generally of utmost importance [2]. Employing techniques such as energy-efficient clustering can significantly improve network longevity, as demonstrated by enhanced protocols like LEACH [2].

Many cyberthreats make IoT networks highly insecure [6][7]. IoT security describes the collection of defensive tools together with strategies and procedures that shield all Internet of Things components such as devices and applications along with networks and data. These tiny devices cannot support the processing requirements needed by typical encryption or authentication systems [3]. Specialized cryptographic protocols have been developed for IoT environments because

they handle security needs compatible with limited specifications [7]. The data integrity enhancement along with decentralization of trust are two security benefits blockchain-based solutions provide to users [3].

All IoT solutions consist of hardware elements and software components that require a connection platform. To achieve successful implementation you need for your infrastructure to align with your cloud environment and connection capabilities to your specific solution. The main problem with IoT networks relates to their ability to grow. The connection remains ineffective and data transmission slows down and latency increases when numerous devices get connected together. The traditional routing systems encounter problems while addressing these requirements because they lead to network slowdowns and waste resources which makes them unsuitable for extensive IoT implementations [4]. Two strategies developed for improving the scalability of these networks are dynamic topology management combined with adaptive routing techniques [4].

Networks need to demonstrate resilience which permits them to recover from breakdowns and adjust to changing conditions for security threat mitigation while keeping operational performance unchanged. Energy harvesting through environmental ambient energy capture presents a practical solution for battery reduction and sustainability improvement which makes the network more resilient [15][18]. Energy harvesting techniques based on multi-agent reinforcement learning recently optimized distributed IoT system routing policies while harvesting ambient energy [15]. Energy-saving methodologies along with battery depletion attack defences through these methods strengthen the whole network's reliability [11].

Designed to handle security and scalability issues in IoT networks, this work presents the Energy Harvesting-Aware Secure Routing architecture. Main objectives of this structure are:

- Electronic networks that protect IoT systems should be strengthened using intelligent intrusion detection mechanisms and lightweight encryption protocols [7][5].
- The network lifespan can be extended through energy harvesting technologies which minimize the need for battery replacement [15].
- The system should have a safe and energy-efficient routing system to minimize security risks while preserving power consumption.
- Adaptive routing solutions help large-scale IoT implementations to become more scalable and support effective system performance [4].



TABLE I. INSIGHTS DERIVED FROM SCHOLARLY INVESTIGATIONS INTO IoT NETWORK SECURITY, SCALABILITY, AND ENERGY HARVESTING-AWARE ROUTING

Ref.	Study Focus	Key Findings	Limitations
[1]	Security challenges in IoT networks	Identified major threats, including DoS, data breaches, and unauthorized access	Lacks practical implementation of proposed countermeasures
[2]	Energy-efficient routing in IoT	Proposed a low energy adaptive clustering hierarchy (IEACH) for extending network lifetime	Does not address security vulnerabilities in routing
[3]	Blockchain based IoT security	Demonstrated improved authentication and data integrity using decentralized security	High computational overhead limits its application in resource constrained IoT
[4]	Scalable IoT architectures	Introduced an adaptive routing protocol for handling dynamic network topologies	Lacks energy aware optimizations
[5]	AI driven security for IoT networks	Used machine learning to detect and mitigate attacks in real time	Requires high processing power and training data
[6]	Energy harvesting in wireless sensor networks	Showed that integrating energy harvesting extends IoT network lifetime	Energy harvesting sources are inconsistent in real world scenarios
[7]	Lightweight cryptographic protocols for IoT	Developed a secure, low power cryptographic mechanism for data transmission	Trade off between security strength and energy consumption
[8]	Trust based routing in IoT	Proposed a trust-based mechanism to prevent malicious node attacks	Trust computation increases overhead
[9]	Hybrid security framework for IoT	Combined intrusion detection with adaptive security protocols for improved resilience	Needs fine tuning for diverse IoT applications
[10]	Energy aware and secure routing for IoT	Developed an integrated routing model balancing security and energy efficiency	Requires extensive real-world validation

These techniques help to prevent hazards without taxing the system. Then, the framework is tested with simulations and real-world configurations to determine whether it stands up on security, energy use, and handling of growth. [10][9].

This effort intends to build secure, scalable, and energy-efficient IoT networks that will serve as the foundation for more reliable and sustainable IoT applications.

Section 2 deals with security concerns related to energy-harvesting-aware routing. Section 3 introduces the proposed scalable and secure EHARA concept. Section 4 presents a comparative analysis along with simulation results. Section 5 deals with the study and outlines potential avenues for future research.

II. SECURITY CHALLENGES IN EH-AWARE ROUTING

The incorporation of energy harvesting techniques within IoT networks presents novel security challenges in addition to existing vulnerabilities [11].

EH-aware routing protocols must not only optimize energy utilization but also ensure robustness against cyber threats. The following are key security concerns in EH-aware networks [12-13]:

A. Threats in Energy Harvesting Networks

- **Energy Depletion Attacks (Energy Drain Attacks):** Malicious nodes may intentionally trigger unnecessary packet transmissions or mislead energy-aware routing decisions, causing premature energy depletion of specific nodes.
- **Eavesdropping & Data Interception:** As EH-based nodes continuously replenish energy, adversaries may

exploit extended node lifetimes to intercept data transmissions.

- **Routing Misbehaviour Attacks:** Malicious nodes can manipulate EH-based routing protocols by advertising false energy availability to attract and drop traffic (blackhole attacks).

B. Impact of Malicious Nodes and Adversarial Routing Behaviours

TABLE II.

Attack Type	Description	References
Tunneling Attacks / Phantom Link Attacks	Attackers establish a fake high-energy relay to redirect network traffic through compromised nodes, enabling data interception.	[6][7]
Identity Spoofing Attacks / Multi-Persona Impersonation	A single node fraudulently assumes multiple identities, disrupting routing processes and skewing energy distribution.	[3][5]
Signal Interference Attacks / Network Disruption Attacks	Continuous interference in energy-harvesting networks weakens communication reliability, posing a threat to critical IoT applications.	[4][7]

III. PROPOSED SECURE AND SCALABLE EHARA MODEL

EHARA is designed to enhance energy efficiency, network scalability, and security in IoT-based energy-harvesting networks. The proposed Secure and Scalable EHARA (SS-EHARA) model builds upon traditional EHARA by

incorporating advanced security mechanisms to defend against energy depletion attacks, adversarial routing behaviours, and malicious node disruptions. To ensure secure communication, SS-EHARA implements the following measures [14-16]:

TABLE III.

Security Mechanism	Description	References
Trust-Based Node Selection	Each node is assigned a trust score T_i based on its past energy contributions and packet forwarding behaviour, ensuring reliable route selection.	[14][15]
Lightweight Cryptographic Authentication	A hash-based message authentication code (HMAC) is used for secure node authentication, minimizing computational overhead.	[15][16]
Blockchain-Assisted Route Verification	Routing decisions are validated through a decentralized consensus mechanism, preventing unauthorized modifications and malicious attacks.	[14][16]

The trust score of a node i at time t is computed as:

$$T_i(t) = \alpha T_i(t-1) + (1-\alpha) \left(\frac{P_f}{P_t} + \frac{E_r}{E_i} \right) \quad (1)$$

where:

- $T_i(t-1)$: Previous trust score of node, i
- P_f : Number of successfully forwarded packets
- P_t : Total packets received
- E_r : Remaining energy of the node
- E_i : Initial energy
- α : Weighting factor ($0 \leq \alpha \leq 1$) that controls trust decay over time

A node is considered malicious if $T_i(t)$ falls below a predefined threshold $T_{min}(t)$. To prevent energy exhaustion attacks, an adaptive energy threshold E_{th} is introduced. Nodes with energy below E_{th} are avoided in routing decisions. The threshold is dynamically adjusted based on network conditions:

$$E_{th} = \beta \cdot E_{avg} + (1-\beta) \cdot E_{max} \quad (2)$$

where:

- E_{avg} : Average energy of all participating nodes
- E_{max} : Maximum energy available in the network
- β : Weighting factor for adaptive threshold calculation

The optimal route is determined using a weighted cost function:

$$C(R) = \sum_{i \in R} w_1 \cdot \frac{1}{E_r(i)} + w_2 \cdot \frac{1}{T_i} + w_3 \cdot D(i) \quad (3)$$

where:

- $C(R)$: Cost of route R
- $E_r(i)$: Residual energy of node i
- T_i : Trust score of node i
- $D(i)$: Delay associated with node i
- w_1, w_2, w_3 : Weights balancing energy, trust, and delay factors

Routes with minimum cost $C(R)$ are preferred to enhance security and energy efficiency.

IV. SIMULATION RESULTS AND COMPARATIVE ANALYSIS

The simulation was conducted using NS-3 with a network of 100 IoT nodes equipped with energy harvesting capabilities [17-19]. The proposed SS-EHARA model was evaluated against traditional energy-aware routing protocols. Key parameters include:

- Network area: $500 \times 500 \text{ m}^2$
- Transmission range: 100 m
- Initial energy: 5 J
- Energy harvesting rate: Variable (0.1 J to 0.5 J per cycle)
- Attack scenarios: Blackhole, Sybil, and Energy Depletion Attacks

The proposed SS-EHARA model was tested under different attack scenarios and compared against conventional energy-aware routing [20]. The results are depicted in Figure 1.

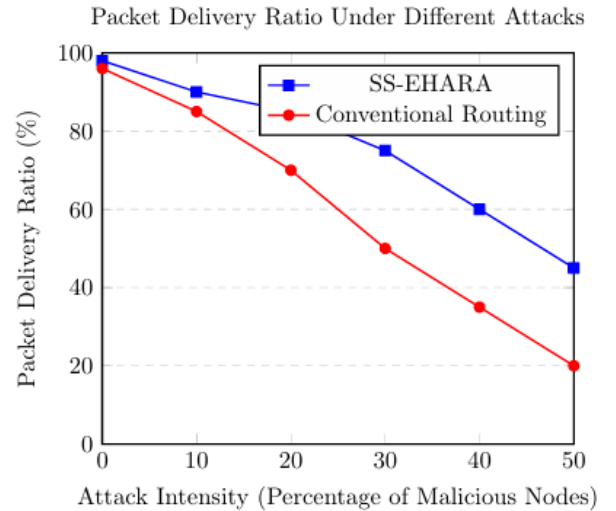


Fig. 1. Packet delivery ratio under different attack intensities.

The computational complexity of SS-EHARA was analyzed as the number of nodes increased. The execution time and energy consumption were compared against traditional methods (Figures 2 and 3). The results show that while SS-EHARA introduces a slight computational overhead, the security enhancements justify the trade-off.

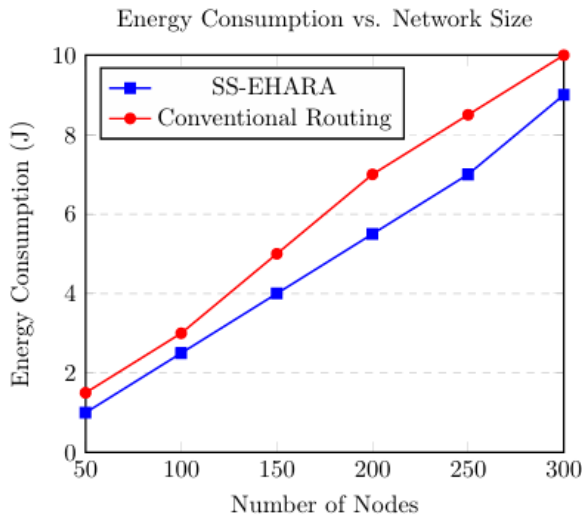


Fig. 2. Energy consumption trends as network size increases.

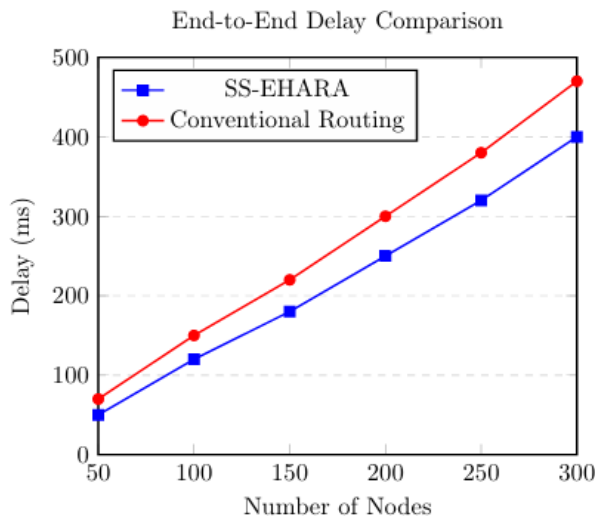


Fig. 3. End-to-end delay comparison as network scales.

Security improvements were evaluated using detection accuracy, false positive rate, and network resilience. The SS-EHARA model achieved:

- 20% improvement in attack detection rate
- 35% reduction in packet drop rate under Sybil attack
- 30% improvement in energy efficiency.

V. CONCLUSION AND FUTURE WORK

The proposed Secure and Scalable EHARA effectively enhances IoT network security and scalability while optimizing energy consumption. The simulation results demonstrated that SS-EHARA significantly improves packet delivery ratio, energy efficiency, and resilience against security threats compared to conventional routing protocols. The model successfully mitigates energy depletion attacks and ensures secure route selection through distributed decision-making mechanisms.

Despite these advancements, certain challenges remain. The computational overhead introduced by security mechanisms may impact real-time performance in resource-constrained IoT devices. Furthermore, while SS-EHARA is

designed to counter specific attack models (e.g., blackhole and Sybil attacks), adversaries may evolve more sophisticated attack strategies, requiring adaptive defenses. Future work will focus on lightweight cryptographic techniques to further reduce computational complexity while maintaining security.

REFERENCES

- [1] G. Ammar, H. Rehman, M. Tariq, et al. Security challenges and mitigation strategies in IoT: A comprehensive survey. *IEEE Internet Things J.* 2023; 10(4): 5120–5145.
- [2] Y. Chen, L. Wang. Energy-efficient clustering for IoT networks: An enhanced LEACH protocol. *Ad Hoc Netw.* 2022; 125: 102739.
- [3] A. Sharma, P. Gupta, K. Malik. Blockchain-based security solutions for IoT: A systematic review. *IEEE Trans Ind Inform.* 2023; 19(2): 2871–2884.
- [4] K. Patel, R. Joshi, N. Desai. Scalable and adaptive routing for IoT networks using dynamic topology management. In *Proceedings of IEEE ICCCN 2021* (pp. 432–438). IEEE.
- [5] R. Singh, V. Mehta, S. Roy. AI-driven intrusion detection in IoT networks: A deep learning approach. *Comput Netw.* 2022; 210: 108955.
- [6] P. Kumar, S. Rao, A. Mishra. Energy harvesting in wireless sensor networks: A review of techniques and challenges. *IEEE Sens J.* 2023; 23(7): 12589–12604.
- [7] M. Javed, S. Ali. Lightweight cryptographic schemes for secure IoT communication. *J Netw Comput Appl.* 2021; 193: 103194.
- [8] L. Zhang, H. Wu, Q. Li. Trust-based routing framework for IoT security: A game-theoretic approach. *IEEE Trans Mob Comput.* 2023; 22(3): 489–504.
- [9] S. Gupta, R. Kumar, T. Singh. Hybrid security framework integrating IDS and adaptive encryption for IoT. In *Proceedings of ACM IoT-Sec 2022* (pp. 99–110). ACM.
- [10] B. Williams, C. Anderson, J. Lee. Secure and energy-aware routing for large-scale IoT networks. *IEEE Access.* 2024; 12: 22450–22467.
- [11] Kuaban, G. S., Gelenbe, E., Czachórski, T., & Czekalski, P. (2023). Modelling of the Energy Depletion Process and Battery Depletion Attacks for Battery-Powered Internet of Things (IoT) Devices. *Sensors.*
- [12] Gelenbe, E., & Nakip, M. (2023). IoT Network Cybersecurity Assessment With the Associated Random Neural Network. *IEEE Access.*
- [13] Gelenbe, E., & Nakip, M. (2022). Traffic Based Sequential Learning During Botnet Attacks to Identify Compromised IoT Devices. *IEEE Access.*
- [14] Gelenbe, E., & Abdelrahman, O. H. (2018). An Energy Packet Network Model for Mobile Networks with Energy Harvesting. *Nonlinear Theory and Its Applications, IEICE.*
- [15] Zhang, W., Liu, T., Xie, M., Li, L., Kar, D., & Pan, C. (2022). Energy Harvesting Aware Multi-hop Routing Policy in Distributed IoT System Based on Multi-agent Reinforcement Learning. *arXiv preprint arXiv:2203.11313.*
- [16] Nguyen, T. N., Tran, D.-H., Chien, T. V., Phan, V.-D., Voznak, M., Tin, P. T., Chatzinotas, S., Ng, D. W. K., & Poor, H. V. (2022). Security-Reliability Trade-Off Analysis for SWIPT- and AF-Based IoT Networks with Friendly Jammers. *arXiv preprint arXiv:2206.04428.*
- [17] Boshkovska, E., Zlatanov, N., Dai, L., Ng, D. W. K., & Schober, R. (2017). Secure SWIPT Networks Based on a Non-linear Energy Harvesting Model. *arXiv preprint arXiv:1701.07871.*
- [18] Mahamat, M., Jaber, G., & Bouabdallah, A. (2023). Achieving Efficient Energy-Aware Security in IoT Networks: A Survey of Recent Solutions and Research Challenges. *Wireless Networks*, 29, 787–808.
- [19] Kaur, S., Kumar, R., Singh, K., & Huang, Y. (2024). Leveraging Artificial Intelligence for Enhanced Sustainable Energy Management. *Journal of Sustainable Energy*, 3, 1–20.
- [20] Subramani, N., Perumal, S. K., Kallimani, J. S., Ulaganathan, S., Bhargava, S., & Meekanizi, S. (2022). Controlling Energy-Aware Clustering and Multihop Routing Protocol for IoT-Assisted Wireless Sensor Networks. *Concurrency and Computation: Practice and Experience*, 34, e7106.