IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

# An Adaptive Trust-Aware Routing Framework Using Deep Reinforcement Learning for Secure Wireless Sensor Networks

**Janaranjani R* Dr. A. Senthilkumar****

***Ph.D., Research Scholar, Department of Computer Science,Thiruvalluvar Government Arts College, Rasipuram, Namakkal, Affiliated to Periyar University, Salem.**

****Assistant Professor, Department of Computer Science,Thiruvalluvar Government Arts College, Rasipuram, Namakkal, Affiliated to Periyar University, Salem**

## Abstract

Wireless Sensor Networks (WSNs) are widely used in applications such as environmental monitoring, healthcare, industrial automation, and smart infrastructure. However, the limited energy resources, dynamic network conditions, and vulnerability of sensor nodes create significant challenges for reliable and secure communication. Conventional routing protocols generally rely on static routing decisions and may not effectively respond to changing network conditions or malicious behaviour. This paper proposes an adaptive trust-aware routing framework that integrates trust evaluation with Deep Reinforcement Learning (DRL) to improve routing decisions in wireless sensor networks. The proposed approach continuously evaluates node behaviour based on communication reliability and network characteristics and incorporates the resulting trust information into the routing decision process. A DRL-based agent is designed to learn suitable routing actions according to the current network state, thereby enabling adaptive selection of reliable communication paths. The methodology focuses on improving secure and efficient data transmission while reducing unnecessary routing overhead and energy consumption. The proposed framework is designed to be evaluated using performance measures such as packet delivery ratio, end-to-end delay, energy consumption, routing overhead, and network lifetime. The study provides a methodology-oriented approach for combining intelligent decision-making and trust management in WSN routing and establishes a foundation for future simulation-based validation under different network and security conditions.

**Keywords:** Wireless Sensor Networks, Deep Reinforcement Learning, Trust-Aware Routing, Secure Routing, Energy Efficiency, Adaptive Routing

## Introduction

Wireless Sensor Networks consist of distributed sensor nodes that collect and transmit information through wireless communication. Due to their low-cost deployment and ability to operate in environments where conventional infrastructure may be difficult to establish, WSNs have become an important component of Internet of Things and intelligent monitoring applications. However, sensor nodes normally operate with limited computational capability, communication range, and battery energy. These limitations make routing an important factor in determining network reliability, security, and operational lifetime.[1,2,3,4]

The dynamic nature of wireless communication further complicates routing decisions. Changes in node availability, communication quality, congestion, and node behaviour can affect the reliability of established routes. In addition, sensor networks may be exposed to malicious or unreliable nodes that can disrupt data forwarding and reduce the overall performance of the network. Therefore, routing me reliability of participating nodeschanisms need to consider not only conventional network parameters but also the behavioural reliability of participating nodes.[6,7,8,9]

Recent developments in Artificial Intelligence and Machine Learning have created opportunities for developing adaptive routing mechanisms. In particular, Deep Reinforcement Learning can learn suitable actions from interactions with a changing network environment without depending entirely on predefined routing rules.[1,2,3,4,5] However, intelligent routing decisions can still be affected when unreliable or malicious nodes are selected during route formation. Integrating trust information into the learning process can therefore provide an additional mechanism for identifying reliable nodes and improving route selection.[6,7,8,9]

This study proposes an adaptive trust-aware routing framework using Deep Reinforcement Learning for Wireless Sensor Networks. The proposed methodology combines node trust assessment with intelligent routing decisions so that the learning agent can select communication paths according to both network conditions and node reliability. The framework is intended to improve secure data transmission while maintaining energy efficiency and reducing unnecessary routing overhead. The proposed approach is methodology-oriented and can subsequently be evaluated through controlled simulation experiments using standard WSN performance metrics.

## Related Work and Research Gap

Recent research has increasingly explored Artificial Intelligence and Reinforcement Learning for improving routing decisions in Wireless Sensor Networks. Traditional routing protocols generally depend on fixed metrics such as distance, residual energy, or hop count, which may not respond effectively to dynamic network conditions. Recent reinforcement learning-based approaches attempt to overcome this limitation by allowing routing decisions to adapt according to network state.[1,3,4,5] For example, recent work on reinforcement learning-based routing has demonstrated that combining residual energy and packet-loss information can improve throughput and network lifetime compared with conventional reinforcement learning approaches.[1,3]

Deep Reinforcement Learning has also been applied to adaptive routing in WSNs. EDRP-GTDQN combines game-theoretic clustering with Deep Q-Network-based path selection to respond to topology changes while balancing energy consumption and delay.[10] Similarly, recent research has investigated DRL-based clustering and routing to improve energy efficiency and network lifetime in dynamic WSN environments.[1,5,12] These studies indicate that learning-based routing can provide more flexible decisions than conventional static routing mechanisms.

Security remains another important challenge in WSN routing. Because sensor nodes communicate through an open wireless environment and often operate without continuous supervision, unreliable or malicious nodes can affect data forwarding. Recent research has therefore started combining intelligent routing with attack detection and trust-related mechanisms.[6,7,8,9] A 2025 study proposed a knowledge-based adaptive routing mechanism using reinforcement learning for attack detection and route adaptation, demonstrating the increasing importance of integrating security with adaptive routing.[6] Another recent study combined trust-aware routing, deep learning, and intrusion prevention to address both security and energy-efficiency requirements in WSNs.[9]

Although existing studies demonstrate the effectiveness of AI and reinforcement learning for WSN routing, several limitations remain. Many approaches primarily concentrate on energy consumption, network lifetime, delay, or throughput, while security and node reliability are treated separately. Other approaches introduce complex optimization or learning mechanisms that may increase the computational requirements of resource-constrained sensor networks. Recent studies also show that adaptive routing is still an active research area, particularly when network conditions and node behaviour change dynamically.[1,3,5,10,12]

## Research Gap

Based on the reviewed literature, there is a need for a lightweight and adaptive routing methodology that considers both **node trust and network conditions** during routing decisions. Existing energy-oriented reinforcement learning methods can select efficient paths, but they may not sufficiently distinguish between reliable and unreliable forwarding nodes.[1,3,4,5] Conversely, security-oriented approaches may increase computational or communication overhead.[6,8,9] Therefore, this study focuses on integrating trust evaluation with Deep Reinforcement Learning so that route selection considers both the behavioural reliability of nodes and the current state of the network.

## Proposed Methodology

The proposed methodology introduces a trust-aware Deep Reinforcement Learning framework for secure routing in Wireless Sensor Networks. The network consists of sensor nodes that periodically collect and forward data towards a base station. During communication, information such as successful packet forwarding, packet delivery behaviour, residual energy, and communication reliability is monitored to estimate the trust level of neighbouring nodes.[6,7,8,9] Nodes demonstrating consistent and reliable forwarding behaviour receive higher trust values, whereas nodes showing abnormal or unreliable behaviour receive lower trust values.

The calculated trust information is provided to the DRL-based routing agent along with relevant network-state information. The agent considers the current network condition and evaluates possible forwarding actions.[1,2,3] A reward mechanism is designed to favour routes that provide reliable data transmission while maintaining reasonable energy consumption and communication efficiency. Consequently, the routing process is not based on a single parameter; instead, it jointly considers node reliability and network performance.

The proposed methodology follows an adaptive decision-making cycle in which the network state is observed, neighbouring nodes are evaluated, candidate routes are identified, and the DRL agent selects an appropriate forwarding path. After data transmission, the resulting network behaviour is used to update the learning process. This allows the routing strategy to gradually adapt to changes in node reliability and network conditions. The framework is therefore designed to provide a balance between secure routing, energy efficiency, and communication reliability without depending entirely on predefined routing rules.

## Proposed Trust-Aware Deep Reinforcement Learning Framework

The proposed framework integrates trust assessment with Deep Reinforcement Learning to support adaptive and secure routing in Wireless Sensor Networks. The framework consists of four major stages: network-state observation, trust evaluation, intelligent route selection, and feedback-based learning.[1,2,6] Sensor nodes periodically observe their communication environment and provide information related to residual energy, packet forwarding behaviour, link quality, and neighbouring node status. This information is used to construct the current network state for the learning agent.

The first stage is trust evaluation. Each neighbouring node is assigned a trust value based on its observed forwarding behaviour and communication reliability. A node that successfully forwards packets and maintains stable communication is assigned a higher trust value, whereas repeated packet dropping, abnormal forwarding behaviour, or unreliable communication reduces its trust value. The trust value is continuously updated so that temporary changes in node behaviour can be reflected in subsequent routing decisions.[6,7,8,9]

In the second stage, the DRL agent receives the network state containing residual energy, link quality, trust level, hop-related information, and other relevant routing parameters. Based on the observed state, the agent selects a forwarding node from the available neighbouring nodes. The action space therefore represents the possible next-hop selections. Instead of using a fixed routing rule, the agent learns which forwarding decisions provide better long-term network performance.[1,2,4,5]

The reward function is designed to encourage reliable and energy-efficient routing. A successful packet transmission through a highly trusted and energy-efficient node receives a positive reward, while packet loss, excessive delay, low-trust forwarding, or unnecessary energy consumption results in a penalty. A generalized reward formulation can be expressed as:

[
$$R_t = w_1T_t + w_2E_t + w_3L_t - w_4D_t - w_5O_t$$
]

where ($T_t$) represents the trust level of the selected node, ($E_t$) represents the energy condition, ($L_t$) represents link reliability, ($D_t$) represents communication delay, and ($O_t$) represents routing overhead. The parameters ($w_1$) to ($w_5$) represent weighting factors that determine the relative importance of each routing criterion.

During the learning process, the agent continuously interacts with the network environment. After selecting a route, the resulting communication outcome is observed and the reward is calculated. The network state is then updated and the agent learns from the previous decision. Through repeated interactions, the routing policy gradually improves and becomes capable of selecting routes that provide a better balance between security, reliability, and energy efficiency.

### Framework Workflow

The overall workflow of the proposed methodology can be summarized as follows. Initially, sensor nodes are deployed and neighbouring relationships are established. The network periodically monitors node behaviour and communication conditions. Trust values are calculated for neighbouring nodes, after which the network state is provided to the DRL agent. The agent evaluates the available forwarding actions and selects the most suitable next-hop node. Data transmission is then performed through the selected route. The transmission outcome is used to calculate the reward and update the routing policy. This process continues throughout the network operation, allowing the routing mechanism to adapt to changing network conditions.

**Algorithmic Description**

**Algorithm: Trust-Aware DRL Routing**

1. Deploy sensor nodes and establish initial communication links.
2. Collect residual energy, link quality, forwarding behaviour, and node-status information.
3. Calculate and update the trust value of neighbouring nodes.
4. Construct the current network state using trust and routing parameters.
5. Provide the state to the DRL routing agent.
6. Select a suitable next-hop node based on the learned routing policy.
7. Forward the data packet through the selected node.
8. Observe packet delivery, delay, energy consumption, and forwarding behaviour.
9. Calculate the corresponding reward or penalty.
10. Update the DRL policy using the observed network feedback.
11. Repeat the process until the communication session is completed.

The main advantage of the proposed methodology is that trust information is incorporated directly into the routing decision rather than being treated as an independent security layer. Consequently, unreliable nodes can gradually receive lower routing preference while reliable nodes become more suitable forwarding candidates. At the same time, the learning mechanism enables the routing policy to adapt to variations in network topology and communication conditions.

## Performance Evaluation Strategy

The proposed framework can be evaluated through a simulation-based WSN environment. The performance of the methodology can be compared with conventional routing and existing reinforcement learning-based routing approaches under identical network conditions.[1,4,5] The evaluation should consider different node densities, traffic levels, energy conditions, and unreliable or malicious node scenarios.

The major performance indicators include **Packet Delivery Ratio (PDR), average end-to-end delay, energy consumption, throughput, routing overhead, and network lifetime**.[1,3,4,5,12] Security-related performance can additionally be examined by observing the framework's ability to reduce the participation of low-trust nodes in data forwarding. These metrics provide a comprehensive basis for determining whether the proposed trust-aware learning mechanism can improve routing reliability while maintaining acceptable energy and communication efficiency.

## Discussion

The proposed trust-aware Deep Reinforcement Learning framework provides an integrated approach to addressing the security and routing challenges of Wireless Sensor Networks. Unlike conventional routing mechanisms that primarily depend on fixed parameters such as hop count, distance, or residual energy, the proposed methodology incorporates node trust and network conditions into the routing decision. This enables the routing process to dynamically respond to variations in node behaviour and communication conditions.[1,2,4,5]

The integration of trust assessment with DRL can help reduce the selection of unreliable forwarding nodes while maintaining adaptive route selection. When a node repeatedly demonstrates poor forwarding behaviour, its trust value decreases and the routing agent can reduce its preference for that node. Similarly, reliable nodes can receive higher routing preference. This mechanism can potentially improve packet delivery and communication reliability while reducing the impact of malicious or unstable nodes.[6,7,8,9]

From an energy perspective, the proposed reward mechanism considers the energy condition of candidate nodes during route selection. Therefore, the learning agent is encouraged to avoid routes that unnecessarily consume the limited energy resources of sensor nodes. This can contribute to improved network lifetime and more balanced energy utilization. However, the computational requirements of DRL should also be considered because sensor nodes have constrained processing and energy resources. A practical implementation may therefore place the learning process at an edge or base-station level while maintaining lightweight trust monitoring at sensor nodes.[1,3,5,12]

The proposed framework is methodology-oriented and requires simulation-based validation before its practical effectiveness can be established. Future experimental evaluation should compare the framework with established routing protocols under different network sizes, node densities, traffic conditions, and malicious-node scenarios. Such evaluation would provide quantitative evidence regarding its advantages and limitations.

## Final Research Contribution

The primary contribution of the proposed study is the integration of **trust evaluation and Deep Reinforcement Learning within a unified adaptive routing methodology**. Rather than treating security and routing as completely separate processes, the framework incorporates node reliability directly into the routing decision. This provides a foundation for developing secure, adaptive, and energy-conscious routing mechanisms for future Wireless Sensor Network applications.

## Conclusion

This paper proposed an adaptive trust-aware routing framework using Deep Reinforcement Learning for Wireless Sensor Networks. The methodology combines node behaviour assessment, trust evaluation, network-state observation, and reinforcement learning-based route selection within a unified routing process. By considering both trust and network conditions, the framework aims to improve secure and reliable data transmission while maintaining energy efficiency.

The proposed reward-based learning mechanism enables the routing agent to learn from communication outcomes and gradually improve its routing decisions. The approach is particularly relevant to WSN environments where node reliability, limited energy, and changing communication conditions directly influence network performance. Although the proposed framework provides a conceptual methodology, simulation-based experimentation is required to quantitatively validate its performance against existing approaches.

Future work can focus on implementing the framework using a standard WSN simulation environment and evaluating its performance against different routing protocols. Further research can also investigate lightweight DRL models, multiple attack scenarios, federated learning, and edge-assisted intelligence to improve the practical applicability of intelligent and secure WSN routing.

**References**


1. Alsalmi, N., Navaie, K., & Rahmani, H. (2024). Energy and throughput efficient mobile wireless sensor networks: A deep reinforcement learning approach. *IET Networks*, *13*(5–6), 413–433. https://doi.org/10.1049/ntw2.12126

2. Jemla Naik, A. K., Parameswarappa, M., & Ramachandra, M. N. (2024). Multiobjective, trust-aware, artificial hummingbird algorithm-based secure clustering and routing with mobile sink for wireless sensor networks. *ETRI Journal*, *46*, 950–964. https://doi.org/10.4218/etrij.2023-0330

3. Suresh, S. S., Prabhu, V., Parthasarathy, V., Senthilkumar, G., & Gundu, V. (2024). Intelligent data routing strategy based on federated deep reinforcement learning for IoT-enabled wireless sensor networks. *Measurement: Sensors*, *31*, 101012. https://doi.org/10.1016/j.measen.2023.101012

4. Kim, B.-S., Suh, B., Seo, I. J., Lee, H. B., Gong, J. S., & Kim, K.-I. (2023). An enhanced tree routing based on reinforcement learning in wireless sensor networks. *Sensors*, *23*(1), 223. https://doi.org/10.3390/s23010223

5. Godfrey, D., Suh, B., Lim, B. H., et al. (2023). An energy-efficient routing protocol with reinforcement learning in software-defined wireless sensor networks. *Sensors*, *23*(20), 8435. https://doi.org/10.3390/s23208435

6. Khelkar, P. S., & Borkar, G. M. (2025). Trust-aware and optimization-driven secure routing in heterogeneous wireless sensor networks for Internet of Things applications. *International Journal of Communication Systems*, *38*(16), e70270. https://doi.org/10.1002/dac.70270

7. Jagan, G. C., Remya, V., Balachandran, G., & Ranjith, S. (2025). Trust-based multi-objective cluster head selection for optimal and secure routing in wireless networks. *International Journal of Communication Systems*, *38*(8), e70095. https://doi.org/10.1002/dac.70095

8. Jadidoleslamy, H. (2025). A distributed fuzzy trust-aware multipath routing protocol in wireless sensor networks. *International Journal of Communication Systems*, *38*(10), e70118. https://doi.org/10.1002/dac.70118

9. Selvi, M., Santhosh Kumar, S. V. N., Thangaramya, K., & Abdul Gaffar, H. (2025). Energy efficient trust aware secure routing algorithm with attribute based encryption for wireless sensor networks. *Scientific Reports*, *15*, 19724. https://doi.org/10.1038/s41598-025-03558-8

10. Pushpa, G., Babu, R. A., Subashree, S., et al. (2025). Optimizing coverage in wireless sensor networks using deep reinforcement learning with graph neural networks. *Scientific Reports*, *15*, 16681. https://doi.org/10.1038/s41598-025-01841-2

11. Robertson, A., & Moreau, L. (2025). Deep reinforcement learning-driven routing algorithms for high-performance wireless sensor networks. *International Journal of Circuit, Computer and Networking*, *6*(2), 63–70. https://doi.org/10.33545/27075923.2025.v6.i2a.104

12. Nagalingayya, M., & Mathpati, B. (2025). Deep reinforcement learning-driven cooperative routing for energy efficiency in wireless multimedia sensor networks. *International Journal of Communication Systems*, *38*(14), e70225. https://doi.org/10.1002/dac.70225