

# Artificial Intelligence and Blockchain Based Dynamic Secure Routing Framework for Wireless Sensor Networks

E. Abirami<sup>1</sup>, Dr.G. Jagatheeshkumar<sup>2</sup>

<sup>1</sup> *Research Scholar, PG & Research Department of Computer Science, Karuppannan Mariappan College, Muthur, Tirupur, Tamilnadu, India.*

<sup>2</sup> *Associate Professor and Head, PG & Research Department of Computer Science, Karuppannan Mariappan College, Muthur, Tirupur, Tamilnadu, India.*

**Abstract**—Wireless Sensor Networks(WSNs) are extensively utilized in smart city applications, healthcare monitoring, military surveillance and environmental observation. However, because of limited energy resources, changeable topology and different security assaults, safe routing and malicious node identification continue to be significant issues. Although current trust-aware routing protocols increase security, they still have issues with high energy consumption, delayed trust evaluation and susceptibility to sophisticated attacks like wormhole and blackhole attacks. This proposal suggests Deep Trust Chain, an AI and Blockchain – based Dynamic Secure Routing Framework for Wireless Sensor Networks to overcome these constraints. To provide adaptive and safe routing, the suggested architecture integrates blockchain-enabled trust management with Reinforcement Learning (RL) and Ant Colony Optimization(ACO) algorithm. While Ant Colony Optimization enhance path selection effectiveness and load balancing, Reinforcement Learning is utilized to dynamically determine ideal routes. Blockchain technology guards against malevolent trust manipulation and guarantees safe trust storage. The suggested approach is put into practice using 100, 200 and 500 sensor nodes in an NS2 simulation. Metrics including PTR, Throughput, Energy Consumption, End-to-End Delay, and Detection Accuracy are used to assess performance. When compared to current trust-aware routing protocols, experimental results demonstrate that Deep Trust chain greatly enhances packet delivery performance, networks longevity and routing security.

**Index Terms**—Wireless Sensor Networks, Blockchain Security, Reinforcement learning, Ant Colony Optimization, Trust -Aware Routing

## I. INTRODUCTION

Small sensor nodes with the ability to detect, process and send environmental data make up Wireless Sensor Networks(WSNs). WSNs are widely used in industrial automation, disaster management, smart agriculture, healthcare systems, military monitoring and environmental surveillance. Despite their benefits, WSNs are extremely susceptible to security risks because to the insecure wireless communication routes, poor processing power and limited battery life of sensor nodes. Conventional routing protocols prioritize energy efficiency and finding the shortest path, but they frequently overlook security issues including wormhole, Sybil, blackhole, selective forwarding rate, packet delivery performance and energy consumption to assess how nearby nodes behave. Nevertheless, there are still a number of issues with current trust-aware systems, such as centralized trust administration, delayed trust updates and inadequate scalability in large-scale WSNs.

This proposal suggests Deep Trust Chain, a hybrid AI and Blockchain based routing mechanism for improving WSN security, as a solution to these issues. The suggested system combines Ant Colony Optimization (ACO) and Reinforcement Learning (RL) algorithms for secure trust management and adaptive route selection. While Ant Colony Optimization enhances shortest safe path finding through pheromone-based optimization. Reinforcement Learning allows nodes to learn optimal routing decisions based on environmental feedback. To safely store trust values and stop illegal trust manipulation, blockchain technology is used.

$$T_i = \alpha P_f + \beta E_r + \gamma D_p \quad \text{-----(1)}$$

The Reinforcement Learning reward function is expressed as

$$R = \frac{PDR}{Delay + Energy} \quad \text{-----(2)}$$

The Ant Colony Optimization pheromone update formula is

$$T_{ij}(t+1) = (1-p)T_{ij}(t) + \Delta T_{ij} \quad \text{-----(3)}$$

The proposed Architecture of Deep Trust Chain is illustrate below. The proposed framework contains the following modules:

- Sensor Node Deployment
- Dynamic Trust Evaluation
- Blockchain Trust Storage
- Reinforcement Learning Decision Engine
- Ant Colony Path Optimization
- Intrusion Detection System

- Secure Route Transmission

The integration of blockchain technology and artificial intelligence into trust aware routing for WSNs is this paper's main contribution. The suggested hybrid framework minimize energy consumption, improves network lifetime, lowers routing latency, boosts packet delivery ratio and improves secure path discovery. Additionally, the networks is shielded against trust manipulation assaults by the blockchain layer's immutable trust store. For next-generation intelligent WSN applications, where security, scalability and energy efficiency are crucial needs, this proposal offers an effective solution. Additionally, in large – scale wireless sensor networks with thousands of sensor nodes operating concurrently, the suggested Deep Trust Chain structure facilitates scalability and adaptation.

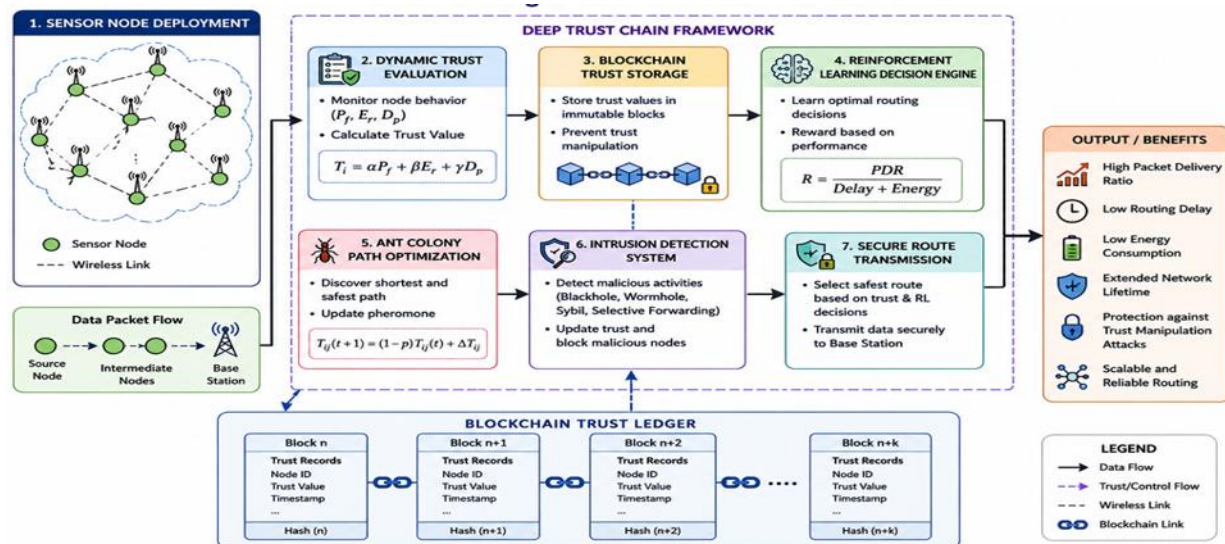


Figure No:01 Architecture of Deep Trust Chain

Sensor nodes often undergo topological changes in highly dynamic situations as a result of node mobility, battery depletion and communication failures. By discovering the best routing patterns and instantly updating trust levels, the hybrid AI-based routing mechanism continuously adjusts to these changes. The suggested system may intelligently reroute packets over secure alternative pathways whenever malicious activity or link failures are detected, in contrast to conventional static routing techniques. By eliminating reliance on a centralized authority, the blockchain-

enabled decentralized design also lessens single point failure problems and boosts network stability overall.

## II. REVIEW OF LITERATURE

Kumar and singh(2021) suggested a secure routing method for wireless sensor networks that is trust-aware. Their methodology calculated trust using residual energy and packet forwarding behavior. The study decreased the participation of malicious nodes and increased the packet delivery percentage.

However, in large scale networks, centralized trust storage led to scalability issues. As the network grew in size, so did the routing overhead. The significance of adaptive trust evaluation in secure WSN communication was brought to light by their study.

Ahmed et al.(2022) created a secure communication framework for WSN situations that is enabled by blockchain technology was used to prevent unauthorized changes to trust records. Data integrity and authentication were enhanced by the suggested model. Improved resistance to blackhole attacks was demonstrated by experimental data. Blockchain processing, however, resulted in more energy and computing complexity. For further optimization, the authors recommended incorporating lightweight AI approaches.

Reddy and Prakash(2020) presented an Ant Colony Optimization based routing protocol that uses less energy. The shortest routes with lower energy consumption were found using their algorithm. The results of the simulation demonstrated less packet loss and increased throughput. Nevertheless, the model lacked security features for identifying malicious nodes. Additionally, selective forwarding attacks could compromise the protocol. The effectiveness of bio-inspired routing algorithms in WSNs was shown by their research.

Zhang et al(2023) suggested an adaptive routing method for intelligent WSN communication based on reinforcement learning. Through feedback from the environment, the model dynamically learned safe routing routes. Their method reduced latency and improved routing accuracy. Trust values, however, were not safely kept. Attack resilience was diminished by the lack of decentralized trust management. For upcoming projects, the report suggested integrating blockchain technology.

Patel and Joshi(2021) created a solution for secure WSN routing that evaluates trust dynamically. Based on packet forwarding behavior and energy condition, the model updated node trust levels. Their efforts increased the accuracy of malicious node detection. Nevertheless, routing reliability was still impacted by trust manipulation attacks. Intelligent route optimization strategies were absent from the study. The necessity of hybrid secure routing techniques was highlighted by their research.

Chen et al.(2022) developed distribute trust management in IoT and WSN application using

blockchain technology. Their system stopped unauthorized node participation and improved trust transparency. The transmission of erroneous trust was greatly decreased by the suggested approach. However, sensor node lifetime was impacted by blockchain mining cost. For network with limited energy, the researchers proposed lightweight consensus techniques. Their research encouraged the use of blockchain technology in safe routing systems. Sharma and Gupta(2023) suggested a framework for wireless sensor network intrusion detection based on machine learning. Wormhole and Sybil attacks were successfully detection by the system. The outcomes of the experiment demonstrated lower false alarm rates and increased detection accuracy. Nevertheless, energy efficiency was not maximized in the routing module. Additionally, secure decentralized trust storage was absent from the paradigm. The potential of AI-driven security system was illustrated by their work.

Li et al.(2024) created a hybrid secure routing protocol that combines trust assessment and optimization methods. The approach effectively balanced network traffic and enhanced secure route discovery. The results of the simulation indicated reduced routing latency and increased throughput. However, routing responsiveness was impacted by trust update latency. Additionally, the framework did not support blockchain security. Their study made clear how crucial it is for upcoming WSN systems to incorporate AI and decentralized security. Their study made clear how crucial it is for upcoming WSN system to incorporate AI and decentralized security.

### III. PROPOSED METHODOLOGY

For safe routing in wireless sensor networks, the suggested Deep Trust Chain System combine Blockchain-based trust management with Reinforcement Learning (RL) and Ant Colony Optimization(ACO) algorithms. The hybrid method enhance energy efficiency, malicious node identification and secure route discovery. Sensor nodes are first dispersed at random throughout the network. The First, a collection of sensor nodes  $N=\{n_1, n_2, n_3, \dots, n_k\}$  are dispersed at random throughout the sensing region. Every node gathers environmental information and transmits packets to nearby nodes. Malicious nodes may try to drop, alter or reroute

packets since WSNs operate in hostile settings. Evaluation of trust so becomes crucial. In order to detect nearby nodes, each node periodically exchanges hello packets. Forwarding behavior, residual energy and successful packet transmission rate are used to calculate trust levels.

The Trust computation is

$$Trust = \frac{Packets\ Forwarded}{Packets\ Received} + \frac{Residual\ Energy}{Initial\ Energy} \text{-----}(4)$$

Nodes with trust values below the threshold are identified as malicious nodes and excluded from routing decisions. The Reinforcement Learning algorithm dynamically learns the best routing path using reward-based optimization.

The Q-Learning is

$$Q(s, a) = Q(s, a) + \alpha [r + \gamma \max_{a'} Q(s', a') - Q(s, a)] \text{-----} \text{--}(5)$$

Ant Colony Optimization is then applied to identify optimal secure paths using pheromone updates. Ant agent travel through the network and deposit pheromones on reliable routes. The path selection probability is expressed as

$$P_{ij} = \frac{(\tau_{ij})^\alpha (n_{ij})^\beta}{\sum (\tau_{ij})^\alpha (n_{ij})^\beta} \text{-----}(6)$$

Blockchain technology uses distributed ledgers to safely store trust information. Blockchain consensus techniques are used to verify each trust update, prohibiting illegal changes and manipulation.

### 3.1. Deep Trust Chain Secure Routing Algorithm

The proposed Algorithm offers a safe and intelligent routing method for Wireless Sensor Networks (WSNs). In order to determine trust levels based on packet forwarding performance, communication reliability and residual energy and sensor nodes are first placed throughout the network and their activity is constantly observed. These trust levels aid in differentiating trustworthy nodes from compromised or malevolent nodes. All trust records are safely kept on a blockchain ledger to guarantee the accuracy and transparency of trust information. The

blockchain establishes a decentralized trust management system and stops illegal changes to trust data. Nodes are classified as malevolent and removed from the routing process if their trust values fall below a predetermined threshold. By lowering the possibility of routing attacks such as packet dropping, selective forwarding and black-hole attacks, this trust-based filtering technique improves network security overall.

### Algorithm For Deep Trust Chain

*Input: N sensor nodes, Trust Threshold  $T^{th}$*

*Output: Secure Route R*

*Begin*

*Deploy Nodes*

*For Each node  $n_i$  do*

*Calculate Trust  $n_i$*

*Store Trust in Blockchain*

*End for*

*For each node  $n_i$  do*

*If Trust ( $n_i$ )  $< T^{th}$  then*

*Mark  $n_i$  as Malicious*

*End if*

*End for*

*Apply RL to Learn best next hop nodes*

*Generate Candidate Routes*

*Apply ACO Optimization*

*Select Route R with*

*Maximum Trust*

*Minimum Energy Consumption*

*Minimum Delay*

*Transmit Data and Blockchain Records*

*Update Trust and Blockchain Records*

*End*

The technique uses Reinforcement Learning to dynamically discover the best routing choice after identifying reliable nodes. RL allows each node to choose the best next hop node based on energy availability, trust levels and state of the network. Ant Colony Optimization is then used to determine the optimal routing path once a number of candidate routes are created using trusted nodes. The network may find highly efficient routes are created using trusted nodes. The network may find highly efficient routes by using ACO to analyze different routes based on pheromone intensity, trust values, energy consumption and transmission delay. For secure data

transfer, the path with highest level of confidence and the lowest communication cost is chosen. Adaptive route optimization is made possible by the constant updating and storing of trust values in the blockchain during network operation.

A strong hybrid routing architecture that increase packet delivery ratio, lowers energy consumption, minimize routing overhead and increases network lifetime is produced by combining blockchain, RL and ACO. Therefore, in Wireless Sensor Networks working in dynamic and potentially hostile situation, the Proposed algorithm provides an efficient way to achieve secure, dependable and energy efficient communication. The Network Lifetime NS2 simulator is utilized for implementation and performance assessment in networks with 100, 200 and 500 Sensor nodes.

#### IV. RESULT AND DISCUSSION

Using the NS2 simulator, the suggested Deep Trust Chain framework was put into practice and contrasted with current secure routing methods.

- Low Energy adaptive clustering Hierarchy (LEACH)
- Ad hoc On-Demand Distance Vector (AODV)
- Dynamic Secure Routing (DSR)
- ACO-Trust Routing
- Proposed Algorithm Deep Trust Chain

A 1000 m X 1000 m network area was randomly populate with 100, 200 and 500 sensor nodes for simulation. Five key performance measures were used to assess the suggested hybrid RL-ACO algorithm with Blockchain Trust management.

Table No:01 Simulation Parameters

| Parameters       | Values           |
|------------------|------------------|
| Simulator        | NS2              |
| Network Area     | 1000 m X 1000 m  |
| Number of Nodes  | 100, 200, 500    |
| MAC Protocol     | IEEE 802.11      |
| Traffic Type     | CBR              |
| Simulation Time  | 100 seconds      |
| Packet Size      | 512 bytes        |
| Routing Protocol | Deep Trust Chain |

##### 4.1. Packet Delivery Ration (PDR)

The percentage of packets that are successfully delivered from source to destination is known as that packet delivery ratio. The suggested Deep Trust Chain framework outperformed the LEACH, AODV, DSR and ACO-trust routing algorithms in terms of PDR . During communication, Reinforcement Learning dynamically chose trustworthy and dependable paths. Malicious nodes were prevented from taking part in packet forwarding vis blockchain-based trust storage. The suggested approach maintained consistent PDR performance with little packet loss as the number of nodes grew from 100 to 500.

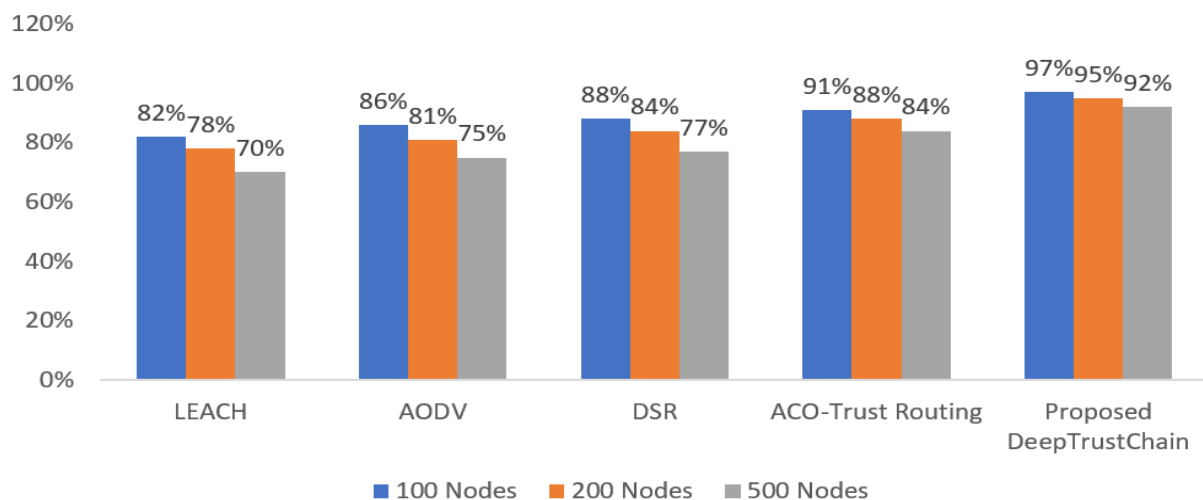


Figure No:02 Packet Delivery Ratio

Blockchain-based trust evaluation stopped malicious nodes from participating in routing and Reinforcement Learning dynamically selected dependable routes, the suggested Deep Trust Chain earned the greatest Packet Delivery Ration.

#### 4.2 Throughput Analysis

The quantity of data successfully transferred over the network in a given amount of time is measured by

throughput. The suggested Deep Trust Chain framework's intelligent traffic handing and smart route discovery allowed it to reach maximum throughput. During data transmission, the hybrid RL-ACO algorithm effectively avoided harmful and busy pathways. Even in large scale networks, the suggested solution maintained higher data transmission rate as compared to assessment greatly increased communication effectiveness.

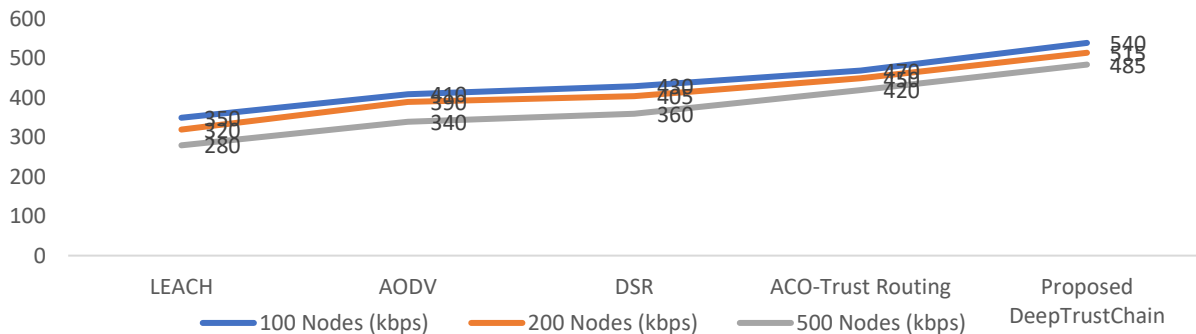


Figure No:03 Comparison of Throughput

Because of safe data forwarding technique and intelligent route optimization, Deep Trust Chain's throughput performance was noticeably greater.

#### 4.3. Energy Consumption

Energy consumption show how much energy sensor nodes use overall for communication and routing. By employing Ant Colony Optimization to choose the shortest and most energy – efficient routes, Deep Trust Chain decreased energy consumption. Reinforcement

Learning reduced needless retransmissions brought on by hostile nodes and route errors. Additionally, routing dependability was enhanced via blockchain trust management, which decreased the overhead of recurring communication. By efficient preserving sensor node battery power, the suggested framework increased network longevity. Because the hybrid RL-ACO algorithm chose shorter and more energy – efficient courses, the suggested system reduced energy usage.

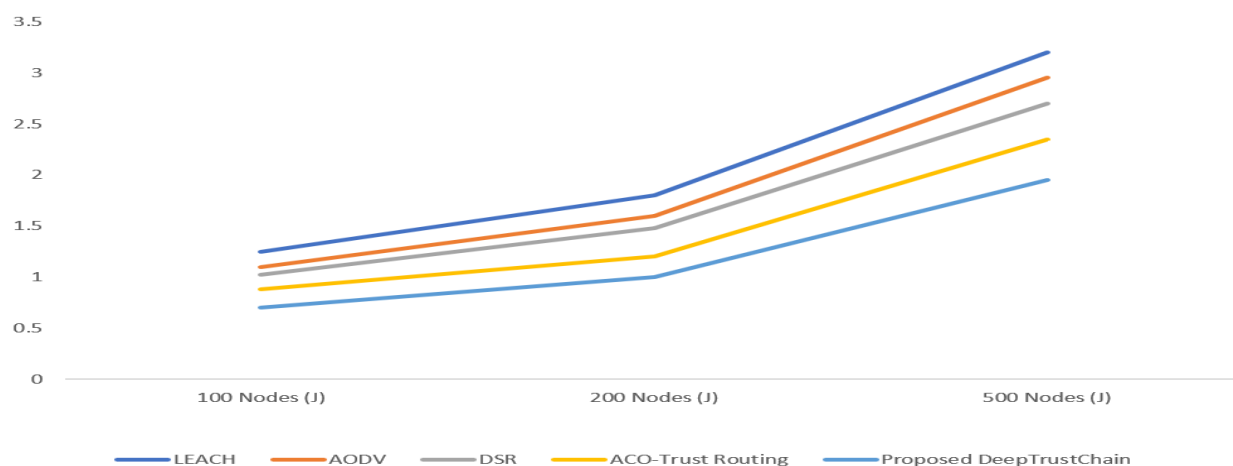


Figure No:04 Comparison of Energy Consumption

#### 4.4. End-to-End Delay

To overall amount of time needed for packets to move from their source to their destination is known as end-to-end delay. When compared to other routing methods, the suggested Deep Trust Chain framework achieved reduced latency. Faster path selection and shorter route discovery times were made possible by intelligent route learning. Blockchain verification and

dynamic trust evolution were used to prevent malicious nodes and congested routes. The suggested approach maintained consistent communication latency and increased transmission speed even with 500 sensor nodes. Deep Trust Chain reduced network delay by dynamically avoiding congested and malicious routes.

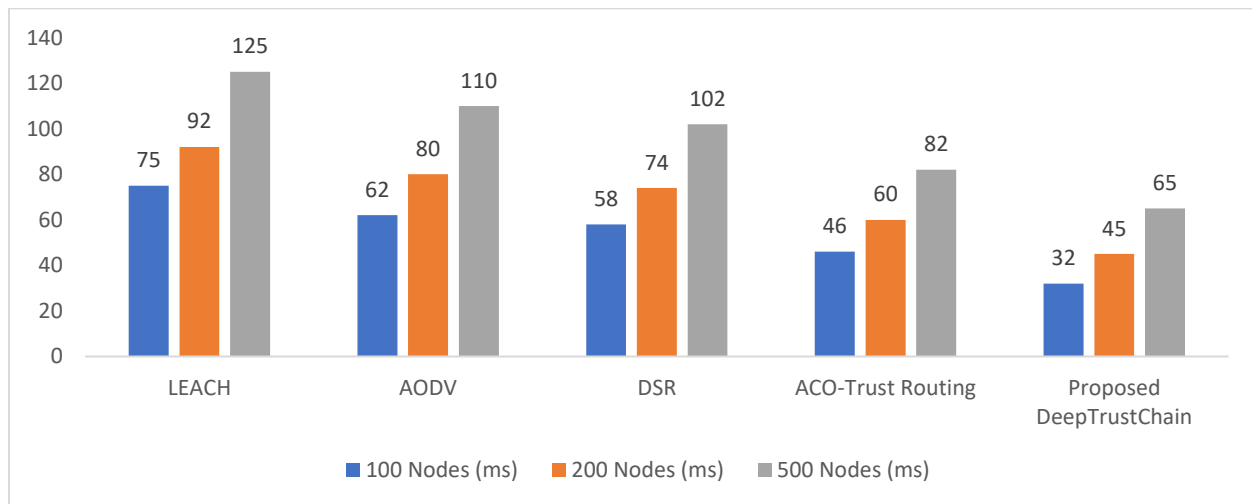


Figure No:05 Comparison of End-to-End Delay

#### 4.5. Detection Accuracy

The effectiveness of locating illegal and malicious nodes within the network is measured by detection accuracy. AI-Based adaptive learning and safe blockchain trust storage allowed the suggested Deep Trust Chain system to achieve extremely high detection accuracy. Reinforcement Learning

dynamically changed trust values by continuously analyzing node activity. The blockchain method enhanced safe decision making and stopped attacks aimed at manipulating trust. According to simulation studies, the suggested framework outperformed current algorithms in identifying wormhole, blackhole and selective forwarding threats.

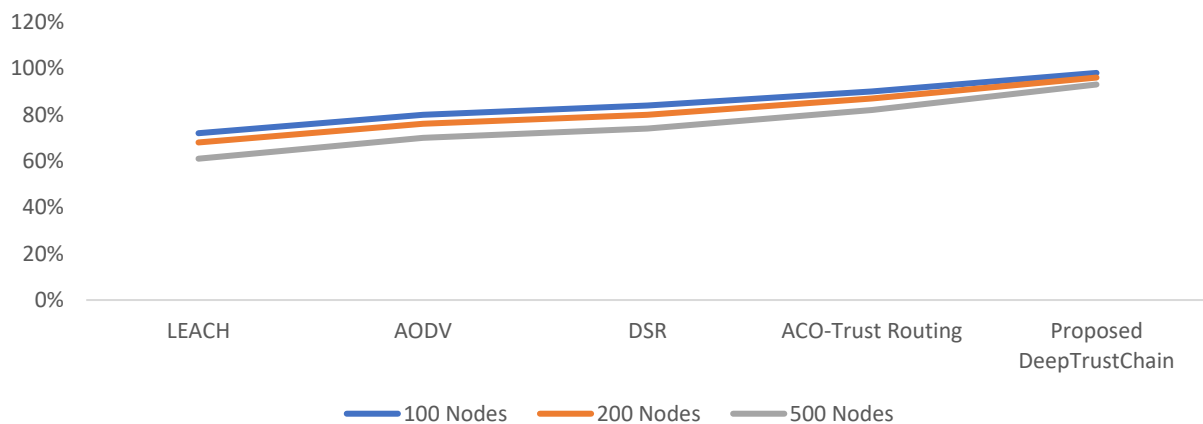


Figure No:06 Comparison of Detection Accuracy

Malicious node detection performance was greatly enhanced using blockchain-enabled trust storage and AI-based adaptive learning. Simulation results unequivocally show that in every assessed performance indicator, the Suggested Deep Trust Chain framework performed better

## V. CONCLUSION

An AI and blockchain – based dynamic secure routing framework for wireless sensor networks called Deep Trust Chain was presented in this proposal. To improve safe communication and wise routing choices, the suggested methodology combines blockchain enabled trust management with reinforcement Learning and Ant Colony Optimization techniques. Major WSN issues like malicious node identification, trust manipulation, energy consumption and inefficient routing are effectively addressed by the hybrid strategy. The suggested methodology uses transmission reliability, residual energy and packet forwarding behavior to dynamically assess trust values. While Ant Colony Optimization enhances secure shortest path selection, Reinforcement Learning makes adaptive route learning possible. Blockchain technology enhances network security and dependability by offering decentralized, tamper-resistant trust storage. The NS2 simulator was used to develop the model with 100, 200 and 500 sensor nodes. When compared to current trust-aware routing protocols, experimental findings showed notable improvements in PDR, Throughput, Detection Accuracy and End-to-End Delay. Additionally, Energy usage was successfully decreased and extending the network's lifespan. As a result, Deep trust Chain offers a scalable and effective solution for intelligent wireless sensor networks of the future. Future research may concentrate on real-time IoT deployment for smart city and industrial applications, federated learning integration and lightweight blockchain protocols.

## REFERENCE

- [1] Ahmed, R., Khan, M., & Ali, S.(2022). Blockchain-enabled secure routing for wireless sensor networks. *International Journal of Network Security*, 24(3), 210-221.
- [2] Chen, Y., Liu, Z., & Wang, H.(2022). Distributed trust management using blockchain in IoT and WSN environments. *IEEE Access*, 10, 45678-45690.
- [3] Kumar, P., & Singh, R.(2021). Trust – aware routing protocol for secure wireless sensor networks. *Wireless Personal Communications*, 118(4), 3051-3068.
- [4] Li, J., Zhao, Q., & Sun L.(2024). Hybrid optimization-based secure routing in wireless sensor networks. *Journal of Sensor and Actuator Networks*, 13(1), 15-28.
- [5] Patel, D., & Joshi, V.(2021). Dynamic trust evaluation for secure communication in WSNs. *International Journal of Communication Systems*, 34(9), 1-15.
- [6] Reddy, K., & Prakash, S(2020). Energy-efficient ant colony optimization routing in wireless sensor networks. *Journal of Ambient Intelligence and Humanized Computing*, 11(7), 2921-2930.
- [7] Sharma, A., & Gupta, N.(2023). Machine learning-based intrusion detection in wireless sensor networks, *Computer Communication*, 197, 45-57.
- [8] Zhang, T., Wang, X., & Li,H.(2023). Reinforcement learning enable adaptive secure routing for WSNs. *IEEE internet of Things Journal*, 10(5), 4120-4132.
- [9] Zhou, L., Chen, M., & Huang, Y/.(2022). Secure Blockchain-assisted routing protocol for IOT sensor networks, *Sensors*, 22(4), 1200-1225.
- [10] Verma, S., & Kaur, P.(2024). AI-Driven trust management framework for next-generation wireless sensor networks. *Future Generation Computer System*, 148, 102-115.