Cluster Based Scalable Adaptive Reputation Trust Management (Cb-Sartm) For Mobile Ad Hoc Networks

N.Thangamani[1], G. Dalin[2]

[1]Research Scholar, Hindusthan College of Arts and Science, Coimbatore, Tamilnadu, India.
[2]Professor, Hindusthan College of Arts and Science, Coimbatore, Tamilnadu, India.

Received: 05.04.2024 Revised : 10.05.2024 Accepted: 20.05.2024

ABSTRACT

This paper proposes a scalable trust management system for Mobile Ad Hoc Networks (MANETs) based on the Cluster Based Scalable Adaptive Reputation Trust Management (CB-SARTM) model. The system integrates Selective Trust Propagation and Distributed Trust Management to improve scalability, reduce network load, and enhance resilience to attacks. The approach allows nodes to calculate trust based on both direct interactions and recommendations from neighboring nodes within a limited range. Additionally, a distributed ledger mechanism ensures that trust updates are verified by multiple nodes, thus enhancing reliability. The system adapts to on-off attacks using a decay mechanism and includes an inconsistency check to detect malicious behavior such as collusion. By leveraging trust values for service discovery and routing, the proposed method ensures more secure communication in MANETs.

Keywords: Trust Management, Distributed Ledger Mechanism, Scalable, Decay Mechanism, Detect Malicious

1. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) are decentralized, self-organizing networks where nodes communicate without relying on fixed infrastructure. Trust management plays a critical role in ensuring secure and efficient communication in such environments. However, maintaining trust in MANETs presents significant challenges, including the dynamic nature of node mobility, limited resources, and the vulnerability to malicious attacks. Traditional trust management systems often struggle with scalability and accuracy in large-scale networks. This paper introduces a scalable version of the Cluster Based Scalable Adaptive Reputation Trust Management (CB-SARTM) system, designed to enhance the scalability of trust management in MANETs.

The Need for Trust Management in MANETs

In traditional networks, security is maintained through centralized authorities, firewalls, and other infrastructure-based mechanisms. However, MANETs lack this centralized control due to their ad hoc nature, which makes it challenging to ensure secure and trustworthy communication between nodes. Each node in a MANET relies on trust-based decision-making for routing and data forwarding, but the absence of a fixed, secure backbone makes this process vulnerable to attacks. Trust management systems in MANETs must dynamically assess the trustworthiness of each node to avoid malicious or uncooperative behavior.

Existing Trust Models and Their Limitations

Several trust models have been proposed for MANETs, primarily focusing on reputation-based or credit-based approaches. Reputation-based models evaluate the trustworthiness of nodes by calculating reputation scores based on past interactions. These scores can help nodes decide which neighbors are likely to cooperate. However, existing models often struggle to maintain scalability in large, dense networks. Additionally, since reputation information needs to be shared among nodes, they risk incurring significant communication overhead, especially when the network topology changes frequently.

Overview of CB-SARTM Approach

CB-SARTM introduces a cluster-based architecture where nodes are grouped into clusters, and trust management processes are handled at both the cluster level and the inter-cluster level. This clustering approach reduces communication overhead by limiting the dissemination of trust information within a cluster rather than across the entire network. Each cluster has a designated cluster head that manages trust evaluations and interactions within its cluster, reducing the need for each node to individually track.

Challenges and Future Directions

While CB-SARTM addresses several critical issues in trust management for MANETs, there are still challenges to consider. For example, determining optimal clustering criteria, adapting to highly dynamic topologies, and addressing potential vulnerabilities within cluster heads are areas that require further exploration. Additionally, CB-SARTM's performance could be enhanced by integrating machine learning techniques to predict node behavior patterns, further refining trust evaluations. Future work could also focus on hybrid trust management models that combine reputation, behavior, and transaction-based approaches for a more holistic trust assessment.

CB-SARTM presents a significant advancement in trust management for MANETs by combining clustering with a scalable reputation-based trust management system. By addressing the limitations of existing models and adapting trust evaluation criteria dynamically, CB-SARTM enhances security, reduces communication overhead, and improves the scalability of trust management in resource-constrained environments. With further research and optimization, CB-SARTM has the potential to become a robust and reliable trust management framework, making it an ideal solution for secure communication in MANETs across a variety of applications.

2. Review of Existing Work

1. Erman Ayday (2012) et.al proposed An Iterative Algorithm for Trust Management and Adversary. Detection for Delay-Tolerant Networks Reputation-Based Trust Management System To identify and stop MANET vulnerabilities, a reputation-based trust management system was suggested. While allowing for temporary malfunctions, this technique assists the nodes in preventing both active (malicious nodes) and passive (selfish nodes) attacks from entering the network. The method work with any on-demand routing protocol [7]

2. Huanyu Zhao (2011) et.al proposed Trust: Trust Management in Cyclic Mobile Ad Hoc Networks. Two methods are suggested by the Trust-enhanced Anonymous On-Demand Routing Protocol (TEAP) to prevent the abuse of anonymity.. In the first method, if any cooperative message is not sent upon receiving two warnings then the user is exposed as a trespassing user to other users. In the second method, if a user tries to send multiple claims across a specific user for the same reason it will also be treated as a trespassing user. Broadcast containing trapdoor information is the foundation of the TEAP protocol architecture, which is used to identify malicious users in a network anonymously [12].

3. Gayathri Dhananjayan (2016) et.al proposed T2AR: trust aware ad hoc routing protocol for MANET. Iterative Algorithm for Adversary Detection Delay/Disruption and Trust Management One of the key subfields of wireless communication was found to be Tolerant Networks (DTNs), wherein sparseness and delay are unusually high. Using reputation-based trust management system in MANETs is shown to be an effective way to handle the adversarial nature in Mobile Ad hoc Networks (MANETs). However, those conventional methods are inapplicable to DTNs due to their distinct features. ITRM is a recurring malicious node detection algorithm designed for DTNs. This scheme is a graph-based iterative algorithm inspired by the success of previous message passing methods for decoding low-density parity-check codes overbipartite graphs. Employing ITRM to DTNs for several mobility models, it is observed that this iterative reputation management scheme is effective than other well-known reputation management techniques such as the Eigen Trust and Bayesian framework. Additionally, it offers low latency, high data availability, and a packet-delivery ratio under a variety of adversary threats. [10]

4. Ing-Ray Chen (2013) et.al proposed Integrated Social and Quality of Service Trust Management of Mobile Groups in Ad Hoc Networks. Secure and dependable source routing The maintenance of a dependability factor by the nodes, which is raised when nodes successfully participate in data transmissions, results in improved security and reliability. This is determined through the use of positive and passive acknowledgments. Additional optimizations are included to increase the efficiency and performance of the network [13].

5. P. T. Selvi (2019) et.al proposed A novel algorithm for enhancement of energy efficient zone based routing protocol for MANET. Framework for Distributed Cooperative Trust-Based Intrusion Detection An intrusion detection system built on collaboration and trust is presented. It awaits on local and global determination of attacks within network and intrusion detection is carried out in a distributed fashion. Reputation mechanism is used for trust assessment, which is obtained by watching the neighbor nodes behaviors. IDS alert messages are used to disseminate evidence of an intrusion attempt The architecture's central component is a distributed intrusion detection system engine, which aims to address the drawbacks of node mobility by utilizing a cooperative trust-based intrusion detection system. [14]

3. Research Methodology

To design a Cluster Based Scalable Adaptive Reputation Trust Management (CB-SARTM) for Mobile Ad Hoc Networks (MANETs), we'll focus on a structured, step-by-step approach that integrates Selective Trust Propagation and a Distributed Trust Management System. These features enhance existing methods scalability, resource efficiency, and robustness against attacks. Here's a comprehensive breakdown of the trust management process:

1. **Direct Trust Calculation**: Compute trust based on successful and failed interactions.
2. **Indirect Trust Calculation**: Collect recommendations within two hops and weight them by relevance.
3. **Hybrid Trust Value Computation**: Combine direct and indirect trust with weights.
4. **Distributed Trust Management**: Use consensus among verifiers to validate and update trust values.
5. **Decay Mechanism**: Apply adaptive decay to penalize on-off attacks.
6. **Inconsistency Check**: Flag suspicious nodes based on collusion indicators.
7. **Trust-Based Routing**: Route packets based on the highest trust path.

In the proposed system, nodes calculate direct trust based on their interactions with neighboring nodes. Successful communications increase trust, while failed transmissions reduce it. To reduce network load, indirect trust is calculated only from nodes within a certain range (e.g., two hops), ensuring that trust propagation does not unnecessarily span the entire network. Hybrid trust values are then calculated by combining direct trust and indirect trust, weighted according to the network conditions. To further enhance the system's scalability and resilience, the model incorporates a distributed ledger mechanism. Trust updates are verified by multiple nodes in the network, ensuring that no single node can manipulate the trust value without being detected. This distributed consensus mechanism improves the reliability and robustness of the trust system, especially in highly populated networks prone to attacks.

To prevent on-off attacks, the system introduces a decay mechanism, where trust values decrease over time based on a node's recent behavior. Additionally, an inconsistency check is implemented to identify and flag suspicious behavior, such as collusion or bad-mouthing attacks, where malicious nodes provide false trust recommendations to manipulate routing decisions.

Finally, the trust values are used for service discovery and routing. Nodes select routes based on the highest trust values, ensuring that communication is routed through the most reliable and secure paths.

Step 1: Initial Trust Value Calculation (Direct Trust)

Each node calculates a direct trust value for its immediate neighbors based on direct interactions, assessing successful communication versus failed transactions.

The direct trust $T_{d_{i,j}}(t)$ of node j as observed by node i at time t is given by:

$$T_{d_{i,j}}(t) = S - F$$

where:

- S: Successful communication events (e.g., packet forwarding).
- F: Failed communication events (e.g., packet drops, delays).

This direct trust value is periodically updated and serves as the basis for further trust calculations.

Step 2: Indirect Trust Calculation (Recommendations from Neighboring Nodes)

Each node calculates indirect trust values based on recommendations from nearby nodes. This calculation considers recommendations from nodes within a limited range (up to two hops).

Let $T_{r_{i,j}}(t)$ represent the indirect trust of node j for node i based on recommendations.

The indirect trust value $T_{r_{i,j}}(t)$ is computed as an average of the trust values provided by the recommending nodes within two hops, weighted by the distance:

$$T_{r_{i,j}}(t) = \frac{\sum_{k \in N(i)} W_{⍰} . T_{k,j}(t)}{\sum_{k \in N(i)} W_{⍰}}$$

where:

- $N(i)$: Neighbor nodes within two hops of i.
- $W_{⍰}$: Weighting factor based on hop distance h (e.g. $W_1 = 1 \ W_2 = 0.5$ for two-hop neighbors).

Step 3: Hybrid Trust Value Calculation

Each node computes a **hybrid trust value** by combining the direct and indirect trust values. This hybrid value provides a comprehensive assessment of trustworthiness, considering both firsthand observations and recommendations from other nodes.

The hybrid trust $T_{i,j}\,(t)$ is given by:

$$T_{i,j}\,(t) = \, W_1.T_{d_{\,i,j}}(t) + \, W|_2.T_{r_{i,j}}(t)$$

where:

- W_1 and W_2 : Weights for direct and indirect trust, respectively, such that $W^1 + \, W_2 = 1$.

This formula ensures that both the direct and indirect trust factors are appropriately considered based on network settings and node behavior history.

Step 4: Distributed Trust Management and Consensus Mechanism

To enhance reliability, a distributed trust management system verifies each trust update through a consensus process. Multiple nodes within the network participate in verifying each trust update, similar to a blockchain or ledger system.

Step-by-Step Process

1. **Trust Update Proposal**: When a node $\boldsymbol{i}$ updates its trust value for node $\boldsymbol{j}$, it broadcasts a proposal $\boldsymbol{T_{i,j}(t)}$ to a subset of verifier nodes $\boldsymbol{V} = \{\boldsymbol{v_1}, \boldsymbol{v_2}, \ldots, \boldsymbol{v_n}\}$.
2. **Trust Verification by Verifiers**: Each verifier node $\boldsymbol{v\_k} \ \in \boldsymbol{V}$ independently calculates $\boldsymbol{T_{v_k,j}(t)}$ based on local or received information about node $\boldsymbol{j}$.
3. **Consensus Condition**: If the calculated trust values $\boldsymbol{T_{v_k,j}(t)}$ across verifiers agree within a tolerance ∈, the update is accepted and recorded. The consensus condition is:

$$|\boldsymbol{T_{v_k,j}(t)} - \boldsymbol{T_{i,j}(t)}| < \in, \forall \boldsymbol{v_k} \in \boldsymbol{V}$$

4. **Trust Ledger Update**: Upon reaching consensus, all verifiers update their local trust ledgers with $\boldsymbol{T_{i,j}(t)}$. ensuring a consistent trust record across the network.

Step 5: Decay Mechanism to Handle On-Off Attacks

To counteract on-off attacks where a malicious node alternates between good and bad behavior, an adaptive decay factor is applied to reduce the trust score over time if the node is inactive.

The decay factor $\boldsymbol{\alpha}$ adapts based on the behavior pattern of node $\boldsymbol{j}$ as perceived by node $\boldsymbol{i}$:

$$\boldsymbol{\alpha} = \begin{cases} \boldsymbol{\alpha_1 = e^{\rho_1 \cdot (t_c \ t_d)}}, & \boldsymbol{for\, positive\, behavior} \\ \boldsymbol{\alpha_2 = e^{\rho_2 \cdot (t_c \ t_d)}}, & \boldsymbol{for\, negative\, behavior} \end{cases}$$

where:

- $\boldsymbol{t_c}$: Current time.
- $\boldsymbol{t_d}$: Last communication time.
- $\boldsymbol{\rho_1 \ and \ \rho_2}$: Decay constants, where$\boldsymbol{\rho_1} \ < \ \boldsymbol{\rho_2}$ to penalize negative behaviors more strongly.

The decayed trust value is then:

$$\boldsymbol{T_{i,j}(t) = \alpha . T_{i,j}(t-1)}$$

Step 6: Inconsistency Check for Collusion Detection

To handle collusion and bad-mouthing attacks, an inconsistency check is introduced. In order to identify irregularities, this check confirms that direct and indirect trust is aligned.

Let $ic_{i,j}\,(t)$ denote the inconsistency check for node j observed by i:

$$ic_{i,j}\,(t) = |T_{i,j}\,(t) - \frac{\sum_{k \in N(i)} T_{k,j}\,(t)}{|N(i)|}|$$

If $ic_{i,j}\,(t) > \epsilon$ where ϵ is a threshold for acceptable trust variance, the recommendation data from node j is flagged as suspicious and possibly discarded.

Step 7: Service Discovery and Trust-Based Routing

The final step involves leveraging the computed trust values to perform service discovery and trust-based routing. Nodes select routing paths based on the hybrid trust values, prioritizing paths with higher trustworthiness.

Routing Decision Formula:

Given a set of neighboring nodes $N(i)$ from node i to destination d. the preferred route $R_{i\ \to d}$ is selected as:

$$R_{i\ \to d} = arg \ \max_{j \in N(i)} T_{i,j}\,(t)$$

where $T_{i,j}\,(t)$ is the hybrid trust value. The routing algorithm thus favors nodes with higher trust values, ensuring more secure data transmission.

4. Experiment Result

4.1 Packet Delivery Ratio (PDR)

It is the proportion between the number of packets transmitted and received.

Table 4.1: Comparison Table of Packet Delivery Ratio (PDR)

No of Nodes	RTAD	RESSR	Proposed CB-SARTM
100	75	71	85
200	78	75	90
300	80	75	92
400	83	77	94
500	85	79	97

The comparison table 4.1 of Packet Delivery Ratio (PDR) addressed the different values of existing (RTAD, RESSR) and proposed CB-SARTM. While comparing the existing and proposed method values are higher than the existing method. The existing values start from 75 to 85 and 71 to 79 and proposed CB-SARTM values start from 85 to 97. The proposed gives the best result.

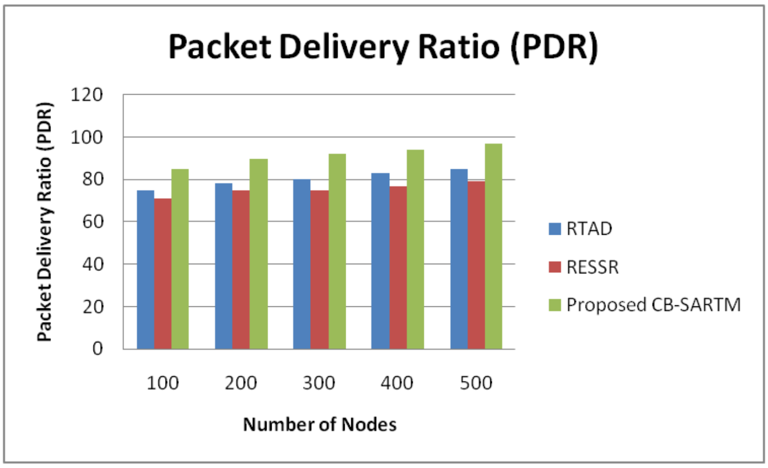

Figure 4.1: Comparison chart of Packet Delivery Ratio (PDR)

The figure 4.1 data Packet Delivery Ratio (PDR) describes the different values of existing (RTAD, RESSR) and proposed CB-SARTM. While comparing the existing and the proposed method values are higher than the existing method and No of Nodes in x axis and Packet Delivery Ratio (PDR) in Y axis. The existing values start from 75 to 85 and 71 to 79 and proposed CB-SARTM values start from 85 to 97. The proposed gives the best result.

4.2 Throughput

It indicates how many packets the recipient has successfully received.

Table 4.2: Comparison Table of Throughput

No of Nodes	RTAD	RESSR	Proposed CB-SARTM
100	60	63	70
200	64	66	74
300	66	68	77
400	67	73	79
500	70	77	82

The comparison table 4.2 of Throughput describes the different values of existing (RTAD, RESSR) and proposed CB-SARTM. While comparing the existing and proposed method values are higher than the existing method. The existing values start from 60 to 70, 63 to 77 and the proposed CB-SARTM values start from 70 to 82. The proposed gives the best result.

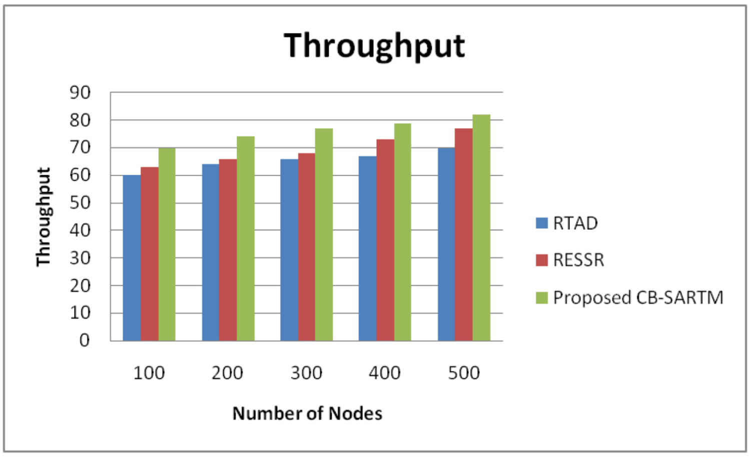

Figure 4.2: Comparison Chart of Throughput

The figure 4.2 data Throughput describes the different values of existing (RTAD, RESSR) and proposed CB-SARTM. While comparing the existing and the proposed method values are higher than the existing method and No of Nodes in x axis and throughput in Y axis. The existing values start from 60 to 70, 63 to 77 and the proposed CB-SARTM values start from 70 to 82. The proposed gives the best result.

7.4.3 Average Delay

Average Delay refers to the time it takes for a packet or data to travel from the source node to the destination node in a network.

Table 4.3: Comparison Table of Average Delay

No of Nodes	RTAD	RESSR	Proposed CB-SARTM
100	66	53	42
200	66	63	47
300	74	75	65
400	77	81	69
500	80	85	74

The comparison table 4.3 of Average Delay describes the different values of existing (RTAD, RESSR) and proposed CB-SARTM. While comparing the existing and proposed method values are higher than the existing method. The existing values start from 66 to 80 and 53 to 85 and proposed CB-SARTM values start from 42 to 74. The proposed gives the best result.

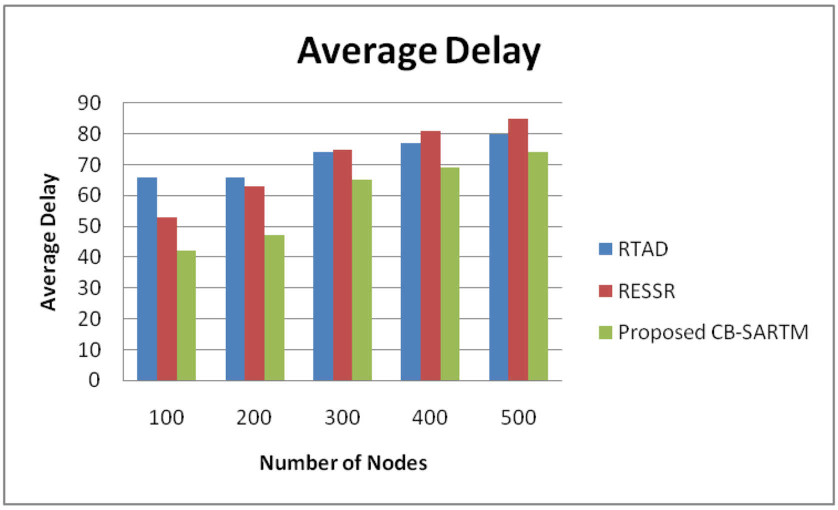

Figure 4.3: Comparison Table of Average Delay

The figure 4.3 Average Delay describes the different values of existing (RTAD, RESSR) and proposed CB-SARTM. While comparing the existing and the proposed method values are higher than the existing method and No of Nodes in x axis and Average Delay in Y axis. The existing values start from 66 to 80 and 53 to 85 and proposed CB-SARTM values start from 42 to 74. The proposed gives the best result.

7.4.4 Remaining Energy

Remaining Energy refers to the amount of energy that is still available or remaining.

Table 4.4: Comparison Table of Remaining Energy

No of Nodes	RTAD	RESSR	Proposed CB-SARTM
100	100	100	100
200	75	82	91
300	63	73	82
400	44	61	72
500	35	42	57

The table 4.4 comparison of Remaining Energy describes the different values of existing (RTAD, RESSR) and proposed CB-SARTM. While comparing the existing and proposed method values are higher than the existing method. The existing values start from 100 to 35, 100 to 42 and proposed CB-SARTM values start from 100 to 57. The proposed gives the best result.

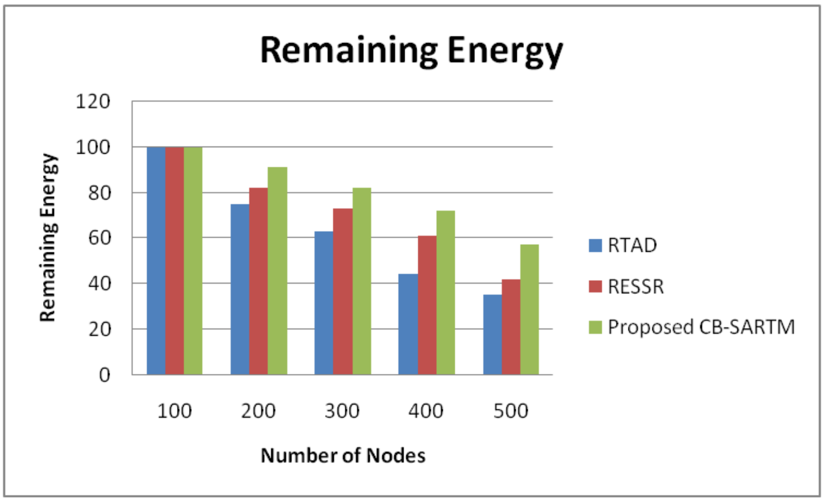

Figure 4.4: Comparison Chart of Remaining Energy

The figure 4.4 data Remaining Energy describes the different values of existing (RTAD, RESSR) and proposed CB-SARTM. While comparing the existing and the proposed CB-SARTM method values are higher than the existing method No of Nodes in x axis and Remaining Energy in Y axis. The existing values start from 100 to 35, 100 to 42 and proposed CB-SARTM values start from 100 to 57. The proposed gives the best result.

5. CONCLUSION

The Cluster Based Scalable Adaptive Reputation Trust Management (CB-SARTM) model presented in this paper provides a comprehensive solution for ensuring efficient and safe communication on massive MANETs. By integrating Selective Trust Propagation and Distributed Trust Management, the system significantly reduces the computational overhead and enhances scalability, making it appropriate for networks with a high node count. The incorporation of decay mechanisms and consistency checks helps to mitigate the impact of malicious nodes and attacks, ensuring the integrity of the trust model. Ultimately, this approach enables reliable service discovery and trust-based routing, ensuring that communication within the network remains secure and resilient to various attacks. Future work will focus on further optimizing the distributed ledger mechanism and extending the system to handle more complex attack scenarios and dynamic network conditions.

REFERENCES

[1] Erman Ayday, and Faramarz Fekri,"An Iterative Algorithm for Trust Management and Adversary Detection for Delay-Tolerant Networks ", IEEE IEEE Transactions On Mobile Computing, Vol. 11, No. 9, September 2012

[2] Fenye Bao, Ing-Ray Chen, MoonJeong Chang, and Jin-Hee Cho "Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection" By Ieee Transactions On Network And Service Management, Vol. 9, No. 2, June 2012

[3] Gayathri Dhananjayan and Janakiraman Subbiah SpringerPlus " T2AR: trust aware ad hoc routing protocol for MANET ", 2016 Elsevier

[4] Haojin Zhu, , Suguo Du, Zhaoyu Gao, Mianxiong Dong, Member, IEEE, and Zhenfu Cao,"A Probabilistic Misbehavior Detection Scheme toward Efficient Trust Establishment in Delay-Tolerant Networks" IEEE Transactions On Parallel And Distributed Systems, Vol. 25, No. 1, January 2014

[5] Huanyu Zhao, Xin Yang and Xiaolin Li "cTrust: Trust Management in Cyclic Mobile Ad Hoc Networks", Member, IEEE 2011 IEEE

[6] Ing-Ray Chen, Jia Guo, Fenye Bao "Integrated Social and Quality of Service Trust Management of Mobile Groups in Ad Hoc Networks" 2013 – IEEE

[7] K. Mabodi, M. Yusefi, S. Zandiyan, L. Irankhah and R. Fotohi, "Multi-level trust-based intelligence schema for securing of internet of things (IoT) against security threats using cryptographic authentication," Journal of Supercomputing, vol. 76, no. 6, pp. 7081–7106, 2020.

[8] L. Saganowski, T. Andrysiak, R. Kozik and M. Choras, "DWT-based anomaly detection method for cyber security of wireless sensor networks," Security and Communication Networks, vol. 9, no. 15, pp. 2911–2922, 2016.

[9] M. Biabani, H. Fotouhi and N. Yazdani, "An energy-efficient evolutionary clustering technique for disaster management in iot networks," Sensors, vol. 20, no. 9, pp. 2647, 2020.

[10] M. Desai and R. H. Jhaveri, "Secure routing in mobile adhoc networks: A predictive approach," International Journal of Information Technology, vol. 11, no. 2, pp. 345–356, 2019.

[11] M.D. Golam Kaosar,"Routing Protocol Based Shared and Session Key Exchange Protocol for Wireless Mobile Ad-hoc Network"

[12] R. T. Merlin and R. Ravi, "Novel trust based energy aware routing mechanism for mitigation of black hole attacks in MANET," Wireless Personal Communications, vol. 104, no. 4, pp. 1599–1636, 2019.

[13] S. K. Govindan and N. Prasant Mohapatra, "Trust computation and trust dynamics in mobile adhoc networks," IEEE Communications Surveys & Tutorials, vol. 14, no. 2, pp. 279–298, 2012.

[14] S. Kalaivanan, "Quality of service (QoS) and priority aware models for energy efficient and demand routing procedure in mobile ad hoc networks," Journal of Ambient Intelligence and Humanized Computing, vol. 12, no. 3, pp. 4019–4026, 2021.

[15] Seyedi and R. Fotohi, "NIASHPT: A novel intelligent agent-based strategy using hello packet table (HPT) function for trust Internet of Things," Journal of Supercomputing, vol. 76, no. 9, pp. 6917–6940, 2020.