An On-Off Attack Resilient Trust Framework for IoT

[1]Mohit Kumar Jain*, [2]Surendra Singh Dua, [3]Harsh Modi

[1, 2]Vivekananda Global University, Jaipur, Rajasthan, India
[3]Krishna Institute of Engineering & Technology (KIET), Ghaziabad, Delhi-NCR, Uttar Pradesh, India
[1]mohitjain02929@gmail.com
[2]harsh.modi@kiet.edu
[3]surendra.sdua@gmail.com

Abstract. The rapid growth of the IoT has led to the development of highly interconnected smart environments in which secure and reliable communication is crucial. `Trust management has proven to be an effective approach to evaluating the reliability of nodes in IoT environments while mitigating malicious interactions. However, existing trust models have failed to consider dynamic adversarial behaviors in which on-off attacks can occur. In on-off attacks, malicious nodes can exhibit both cooperative and adverse behaviors to escape detection. These behaviors can lead to an increase in trust value, which can undermine the reliability of the network. In this paper, we develop a coverage reliability-aware trust model that can improve the reliability of IoT networks while resisting on-off attacks. The proposed model incorporates cooperative trust, adverse trust, and energy-based trust to improve its reliability. To prevent trust value inflation that can result from on-off attacks, an exponential penalty is incorporated in the model. The efficacy of the proposed model is demonstrated in this paper using intensive simulations of dynamic IoT environments. The results obtained from the experiments show that the proposed model can quickly degrade the trust of malicious nodes while maintaining stable trust for legitimate nodes. Compared to existing trust management approaches, the proposed model has demonstrated improved reliability, achieved higher precision and recall while resisted on-off attacks.

Keywords: Internet of Things (IoT), Trust Management, Coverage Reliability, On-Off Attack, Trust, IoT Security, Malicious Node Detection.

1 Introduction

The Internet of Things (IoT) refers to a system of physical objects, or "things," that are equipped with sensors, software, and network connectivity, allowing them to collect and exchange data over a network [1]. IoT devices, with intelligent communication capabilities, can communicate between each other and make decisions independently for various applications, such as healthcare monitoring systems, smart homes, smart agriculture [2], smart parking systems, and intelligent traffic management systems. These intelligent systems are largely dependent on autonomous communication mechanisms to ensure efficient functioning by IoT devices. Security is crucial in ensuring

B. Singh et al. (eds.), *Proceedings of the International Conference on Advances in Computing Technology and Artificial Intelligence (COMPUTATIA 2026)*, Atlantis Highlights in Intelligent Systems 18,
https://doi.org/10.2991/978-94-6239-713-2_36

the efficiency and reliability of IoT systems [3]. The IoT system is defined by heterogeneous systems, wireless communication systems, battery-powered systems, and diverse protocols, making it difficult to implement security solutions for various applications in the IoT system. Thus, ensuring secure communication systems for IoT devices is a challenging area of research.

Trust management has been identified as a powerful security solution for IoT systems by evaluating the behavior of IoT devices over a period of time for detecting malicious activities while facilitating efficient communication among IoT devices [4]. Through continuous monitoring of interactions among nodes in a network, a trust management system can differentiate between nodes based on their reliability in a network. In spite of tremendous research efforts on developing efficient security systems for IoT applications through trust management systems, these systems still suffer from various limitations associated with dynamic adversarial behavior in IoT networks. Among these limitations is the On-Off attack, in which nodes can change their behavior from malicious to cooperative or vice versa [5]. Malicious nodes can accumulate sufficient trust in a network by behaving in a cooperative manner while evading detection by a trust evaluation system in a network. Once sufficient trust is accumulated in a network, these nodes can perform malicious activities in a network.

In this paper, we propose an improved trust evaluation mechanism for IoT networks to effectively detect malicious nodes in these networks. Existing trust evaluation models [6] are found to be inefficient in detecting On-Off attacks, in which nodes are found to maintain their trust values above a certain threshold by showing cooperative behavior in an intermittent manner. To overcome this drawback of existing trust evaluation mechanisms, we propose to improve cooperative trust evaluation and incorporate energy trust in the evaluation of trust.

The major contributions of this paper are as follows:

1. Improved cooperative trust evaluation for IoT networks.
2. Multiplicative evaluation of energy trust for accurate results.
3. Improved detection of On-Off attacks in IoT networks.
4. Performance evaluation of the proposed model using simulation.

The structure of this paper has been defined as follows: the next section discusses the existing literature on the Internet of Things (IoT) networks and the security mechanism for the purpose of ensuring high reliability in the network. After this, the methodology followed in this paper is discussed in the following sections. Accordingly, the simulation methodology followed in this paper is discussed in Section 4, followed by the results in Section 5. Finally, the conclusion is presented in Section 6.

2. Related work

The management of trust has received significant research attention as an essential approach to improve the security and reliability of distributed systems and IoT environments, where frameworks such as [4] evaluate trust using both qualitative and quantitative parameters. The essential steps included in the framework are information gathering, trust computation, trust dissemination, and trust maintenance. In [7], the authors

identified trust as an essential component in the development of secure computing, emphasizing the importance of trust management as a unique module that is responsible for the establishment of relationships, credentials, and authorizations based on prior experiences. Other related works, such as [8] and [9], focus on the incorporation of direct observations and recommendations in the assessment of trust in a distributed environment. In [10], the authors presented a direct trust approach based on parameters such as the success rate, user satisfaction, and node credibility in the IoT environment. However, the main disadvantage is that the approach does not incorporate recommendations and has a higher energy consumption, which is not desirable in IoT networks.
To incorporate the dynamic behavior of IoT nodes, the authors in [11] proposed the integration of the SMART multi-attribute rating method and the Long Short-Term Memory (LSTM) network approach. However, the disadvantage is that the proposed approach does not consider the energy cost incurred in the computation of trust in IoT networks.
Recommendation Aggregation is another significant issue in TMS, especially in IoT networks, which are characterized by memory and energy constraints. Storing and processing high amounts of recommendation data may compromise the overall scalability and energy efficiency of IoT networks. In order to reduce the overall computation associated with trust management in IoT networks. Authors in [12] presented a certificate-based approach in which nodes are issued trust certificates from a central authority and can communicate without the computation of trust values. Blockchain-based trust management frameworks are also emerging as an alternative solution to traditional trust management approaches in IoT networks. The lightweight blockchain-based trust management scheme presented in [13] is designed to support trust evaluation in Social IoT networks. Similarly, the T-RCIC model presented in [14] integrates trust management with confident information coverage (CIC) for categorizing nodes as malicious, critical, and trustworthy and limiting their activities accordingly.
Despite the progress, the problem of the standardization of the trust metrics is still open, as discussed in [15], where the authors proposed a comprehensive IoT trust framework. Dynamic mechanisms for managing the trust in industrial scenarios are critical, considering the dynamic nature of the IIoT, where the composition of the network is constantly changing, i.e., devices join or leave the network, as discussed in [16]. Trust, apart from security, is also used to perform reliability analyses in WSNs. For instance, the area coverage reliability (ACR) metric, proposed in [17], relies on Monte Carlo simulations to evaluate the sensing reliability. D-S evidence theory-based approaches, as discussed in [18], also estimate the sensing belief degrees to calculate the coverage. Trust-based frameworks, such as TrusDet, proposed in [19], utilize the trust metrics to perform intrusion detection and faulty node detection. Coverage-based intrusion detection is also discussed in [20].
Trust-based approaches are also used to perform industrial anomaly detection scenarios. For instance, the approach proposed in [21] discusses the abnormal behavior detection in industrial scenarios, but the applicability is limited to uniform anomaly patterns. For fog-based cyber-physical systems, the authors proposed a lightweight multi-factor trust management model based on the random forest regression algorithm, as

discussed in [22]. Decentralized trust computations have been proposed, and the authors have derived trust values based on first-hand experiences and second-hand observations in heterogeneous IoT environments, as mentioned in [23]. In socially connected IoT environments, social IoT trust models have been proposed, wherein social aspects have been included, as mentioned in [24]. NOTRINO is a hybrid trust model that considers the trust value at the transport layer as well as the application layer and has been proposed for the Internet of Vehicles, as mentioned in [25]. In order to solve the problem of scalability, adaptive trust models have been proposed. In the adaptive IoT trust protocol mentioned in [26], peer evaluation is used in conjunction with collaborative filtering for the accuracy of the trust model, but the protocol is applicable only for on-off attacks.

3. Proposed Methodology

In this paper, an advanced framework of trust management for IoT networks is introduced to mitigate on-off attacks and improve the reliability of network coverage. The framework considers an exponential penalty in cooperative trust evaluation and introduces an energy-aware aspect by using multiplicative trust aggregation. Unlike existing additive trust definitions in [6], in this framework, artificial inflation of trust caused by on-off attacks is avoided to prevent the risk of misclassifying energy-constrained nodes as trustworthy nodes.

3.1 Conventional Trust Metrics

An Existing Internet of Things (IoT) trust model [6] uses the following three major metrics to determine the reliability of the nodes in the network:

- Cooperative Trust
- Adverse Trust
- Energy Trust

3.1.1 Conventional Trust Metrics

This metric measures the extent to which a node participates in and contributes to network operations through successful interactions. Each interaction outcome is classified into three categories: successful cooperation (Res_G), malicious behavior (Res_M) or no response at all (Res_N).

The cooperative trust value of a node s_i, denoted as $T_{coo}(s_i)$, is calculated as:

$$T_{coo}(s_i) = \frac{\sum_{j=1}^{N_{s_i}} \sum_{k=1}^{K_{i,j}} F_{i,j}^{k}(res) \cdot I_{i,j}^{k}(\omega)}{\sum_{j=1}^{N_{s_i}} \sum_{k=1}^{K_{i,j}} I_{i,j}^{k}(\omega)} \quad (1)$$

where N_{s_i} represents the total number of neighboring nodes of node s_i, and $K_{i,j}$ denotes the number of interactions between nodes s_i and s_j. The function $F_{i,j}^{k}(res)$ indicates

the interaction outcome, while $I_{i,j}^{k}(\omega)$ represents the corresponding weight assigned to that interaction based on its importance.

The function $F(res)$ is defined as:

$$F(res) = \begin{cases} 1 & if\ res = Res\_G \\ 0.0 & if\ res = Res\_N \\ 0.5 & if\ res = Res\_M \end{cases}$$

3.1.2 Conventional Trust Metrics

Adverse trust [6], quantifies the proportion of negative interactions and is defined as:

$$T_{adverse}(s_i) = \frac{\sum_{j=1}^{N_{s_i}} \left(Q_{i,j}^{Res\_M} + Q_{i,j}^{Res\_N} + Q_{i,j}^{Res\_R}\right)}{\sum_{j=1}^{N_{s_i}} Q_{i,j}^{*}} \tag{2}$$

where $Q_{i,j}^{Res\_M}$, $Q_{i,j}^{Res\_N}$ and $Q_{i,j}^{Res\_R}$ denote malicious, no-response, and refusal interactions, respectively.

3.1.3 Conventional Trust Metrics

Energy trust [6], ensures that a node has sufficient residual energy to sustain communication and routing operations:

$$T_{ene}(s_i) = \begin{cases} 1 & if\ \ \widetilde{E_{s_i}} < \min E_{i,j} \quad \left(j \in N_{s_i}\right) \\ 0 & else \end{cases} \tag{3}$$

where $\widetilde{E_{s_i}}$represents the residual energy of node s_i, and $E_{i,j}$ represents the energy required for transmission from node s_i to its neighboring node s_j. If the residual energy is lower than the minimum required transmission energy, the node is considered energy infeasible and is given a trust value of 0. Otherwise, it is given a trust value of 1.

3.2 Limitations of Existing Trust Models

Conventional trust models [6] use a weighted additive model to aggregate trust as follows:

$$T(s_i) = \mu_1 T_{coo}(s_i) + \mu_2\left(1 - T_{adverse}(s_i)\right) + \mu_3 T_{ene}(s_i) \tag{4}$$

Although it is a balanced integration of all trust types, it is still vulnerable to on-off attacks. The weighted average used to calculate cooperative trust makes it easy for a node to manipulate trust by alternating between adversarial and cooperative behavior. Moreover, incorporating energy trust as a component of trust could allow a node to have a certain level of trust even if it is energy infeasible.

3.3 Data Preprocessing

To address the problem of trust inflation caused by intermittent malicious activities, the exponential penalty is introduced to the cooperative trust calculation process, given by:

$$T_{coo}(s_i) = \frac{\sum_{j=1}^{N_{s_i}} \sum_{k=1}^{K_{i,j}} F_{i,j}^{k}(res) \cdot I_{i,j}^{k}(\omega)}{\sum_{j=1}^{N_{s_i}} \sum_{k=1}^{K_{i,j}} I_{i,j}^{k}(\omega) \cdot e^{P\left(1-F_{i,j}^{k}(res)\right)}} \tag{5}$$

where $P \geq 2$ is the penalty factor.

The above equation shows that the exponential penalty function is used to exponentially increase the value of the denominator, thereby reducing the value of the cooperative trust for the malicious node. This is unlike the linear penalty function, which cannot prevent the rapid recovery of the malicious node.

3.4 Sentiment Analysis

To ensure the logical correctness of the proposed trust model, the energy trust is integrated into the final trust value calculation process, given by:

$$T(s_i) = \left(\beta_1 T_{coo}(s_i) + \beta_2\left(1 - T_{adverse}(s_i)\right)\right) \cdot T_{ene}(s_i) \tag{6}$$

where $T(s_i)$ represents the final trust value of node s_i. The terms $T_{coo}(s_i)$, $T_{adverse}(s_i)$, and $T_{ene}(s_i)$ denote the cooperative trust, adversarial trust, and energy trust of the node, respectively.

The above equation shows the multiplicative relationship between the cooperative trust, the adversarial trust, the energy trust, and the final trust value. The parameters β_1 and β_2 are weighting coefficients that determine the relative contribution of cooperative and adversarial trust components in the overall trust computation. These coefficients satisfy the condition $\beta_1 + \beta_2 = 1$, ensuring a balanced contribution between the two factors.

3.5 On-Off Attack Case Analysis

To ascertain the efficacy of the developed framework, a simulated analysis was conducted to test the on-off attack case where nodes exhibit both cooperative and malicious behavior. In accordance with the additive model, it was found that malicious node trust levels remained higher than the decision threshold despite continuous adversarial behavior. However, by employing the exponential penalty function and multiplicative energy integration, it was found that the trust levels remained below the threshold value. These results affirm that the developed framework is effective in countering intermittent adversarial behavior while preventing trust inflation.

4. Experimental Setup

The proposed trust evaluation model was evaluated using simulations carried out using the MATLAB environment. The MATLAB environment is a powerful tool that can be used to simulate the dynamic behavior of the network and is commonly used to evaluate IoT systems using the simulation approach. The simulation was carried out using a

Windows 10 operating system with an Intel Core i5 processor running at 2.50 GHz and 8 GB RAM.

4.1 Simulation Environment

To emulate a realistic IoT network environment, sensor nodes were randomly distributed over a two-dimensional plane of size 100 x 100 m². Although initial experiments were conducted by varying the number of nodes between 50 and 100, all results reported in this work are based on a network consisting of 100 nodes, ensuring consistency in comparative evaluation. Among these, 50% of nodes were configured as malicious nodes (p_{mali}) exhibiting dynamic attack behavior, with an initial energy level of 100 units and a trust value of 0.5. The communication range was set at 30 m, while the sensing range was set at 15 m. In addition, node mobility was taken into account with a constant average velocity of 5 m/s. The calculation of trust values occurs periodically based on interactions with neighboring nodes and the response received from them. Each node in this network observes the behavior of its neighboring nodes based on three parameters: cooperative trust, adverse trust, and energy trust. The values obtained from these parameters are further used by combining them with weighted parameters and comparing them with a threshold value in order to determine the trust values for all nodes in the network. Nodes in this network having a value higher than the threshold are classified as trustworthy nodes, while nodes having a lower value than the threshold are classified as malicious nodes.

The parameters used in this simulation scenario were taken from references [15], [6], and [27]. The details of the parameters used in this scenario are presented in Table 1.

Table 1. Simulation Parameters

Variable	Value
Field dimensions (Δ)	100 m × 100 m
Number of nodes (n)	[50-100]
Initial energy (E)	100 units
Node velocity (v)	5 m/s
Sensing radius (R_s)	15 m
Communication radius (R_c)	30 m
Duty cycle (α)	0.8
Probability of communication unit operational (p_{com})	0.95
Probability of sensing unit operational (p_{sen})	0.8
Link stability probability (p_{link})	[0.1-1]
Weight (β_1)	0.6
Weight (β_2)	0.4

4.2 Simulation Evaluation

Table 1 The simulation experiments have been performed to measure the effectiveness of the suggested trust model in differentiating trustworthy nodes from malicious nodes in a dynamic Internet of Things environment. In addition, the evaluation focuses on the impact of the nodes' behavior, energy consumption, and the dynamic nature of the nodes on the computation of the trust value. At the start of the simulation environment, the nodes are distributed uniformly at random in the specified region. An initial trust value of 0.5 is assigned to all nodes. In addition, the nodes' connectivity is determined based on the specified communication radius. Moreover, the stability of the links during the simulation is determined based on the probability parameter p_{link}. During the simulation period, the nodes may react in different ways, including cooperative response, malicious response, and non-response.

Energy consumption for nodes in a network is tracked in a simulation environment for different types of activities, including sensing, sending, receiving, and abnormal activities performed by nodes in a network. Therefore, on the basis of these activities, cooperative trust values, adversarial or malicious trust values, and energy trust values can be determined for nodes in a network. In addition, different states for nodes in a network, including ACTIVE, RELAY, SLEEP, and FAIL states, can be dynamically determined based on trust values and duty cycle values in a network.

In the proposed framework, nodes with trust values above the threshold are considered trustworthy and that nodes are allowed to continue participating in network operations. On the other hand, malicious nodes tend to exhibit abnormal behavior, which leads to higher energy consumption which lead to a gradual decline in their trust values. When a node's trust value falls below the trust threshold, it is identified as malicious and is subsequently suspended from further participation in network activities Discussion

The key components contributing to the improved performance of this system are (a) the thorough preprocessing of data prior to analysis and (b) the decision to combine two separate sentiment analysis tools [5], [8]. By doing so, noise in the text is effectively reduced, and more reliable drug rankings are produced, regardless of the total number of reviews available. The set of drug rankings has been validated against both variations in population characteristics and the number of reviews submitted, giving a robust ranking system [9]. Clinicians can also rely on the transparent and traceable nature of the drug recommendation process since recommendations are based solely on sentiment scores [7].

5. Results

To evaluate the effectiveness of the suggested trust evaluation mechanism, two attack behaviors were simulated: On-Off type of attack behavior and the gradual transition of nodes from cooperative to malicious behavior. The simulation results are presented to compare the performance of the suggested OOA-resilient trust model with the existing T-ITCR trust, which is implemented using the same simulation parameters and trust computation framework as described in [6]. The value of trust threshold is fixed at 0.6 based on analysis of results generated from multiple simulations. Low trust thresholds

led to increased number of false positives, and high thresholds resulted in difficulty in identifying malicious nodes. Nodes with trust value greater than or equal to 0.6 are trusted, while those Nodes below than 0.6 are malicious.

5.1 Accuracy Evaluation of the Trust Model

To For evaluating accuracy of the suggested model, simulations are performed using a network of 100 nodes, 50 nodes belong to trustworthy behavior and 50 malicious nodes within an IoT environment. The results obtained using the simulations in relation to the classification performance of the algorithm were then examined through a confusion matrix, providing a well-structured representation of the correct and erroneous classifications made using the model. Using the confusion matrix, the conventional performance measures like Precision and Recall were calculated in relation to both models being considered. The confusion matrix represents the number of both accurately and erroneously classified data, allowing a deeper understanding of the algorithm's performance. In particular, Recall (true positive rate) is the proportion between the number of correctly identified malicious nodes and the total number of actual malicious nodes in the network, while Precision is the ratio between the number of correctly identified malicious nodes and the total number of all nodes recognized as malicious. [28]

These performance measures are formulated in the following way:

$$Recall = \frac{True\ Positive}{True\ Positive + False\ Negative} \tag{7}$$

$$Precision = \frac{True\ Positive}{True\ Positive + False\ Positive} \tag{8}$$

Whereas True Positive is the number of identified malicious nodes (malicious nodes), False Negative represents malicious nodes recognized as trustworthy, while False Positive represents the number of trustful nodes wrongly classified as malicious nodes.

As seen values obtained are presented in Table 2, the proposed model performs better than T-ITCR with regard to both Recall and Precision. Namely, whereas Recall equals 0.84 for the proposed model, for the T-ITCR model this measure is lower (0.76), indicating a better ability to correctly detect malicious nodes. Furthermore, while Precision is equal to 0.89 for the proposed model, its value for the other model is 0.81.

Table 2. Confusion matrix

Model		Malicious Actual	Trustworthy Actual
Proposed Model	Malicious Predicted	42	5
	Trustworthy Predicted	8	45

T-ITCR Model	Malicious Predicted	38	9
	Trustworthy Predicted	12	41

5.2 Accuracy Evaluation of the Trust Model

Fig. 1 illustrates the variation in trust components under the On–Off attack model. In this fig, the x-axis represents the total iterations, while the y-axis represents the values of trust components ranging from 0 to 1. In this fig, the trust parameters include cooperative trust (T_{coo}), calculated using both the OOA-resilient model and the T-ITCR model, along with adverse trust (T_{adverse}), and energy trust (T_{ene}). From the Fig. 1, it is observed that the T-ITCR model maintains a high level of cooperative trust, even in the presence of malicious activities by the node, since the trust value is always greater than or equal to the threshold in most iterations, except in the malicious iterations. This shows that the model is not significantly affected by the On–Off attack model.
In contrast, the OOA-resilient trust model maintains a low level of cooperative trust, always keeping the trust value below or at the threshold in the presence of malicious activities by the node, thereby showing the effectiveness of the model in penalizing the nodes that exhibit On–Off attacks. In addition, the adverse trust level is also high in the presence of malicious activities, thereby resulting in a low trust level for the attacking node.

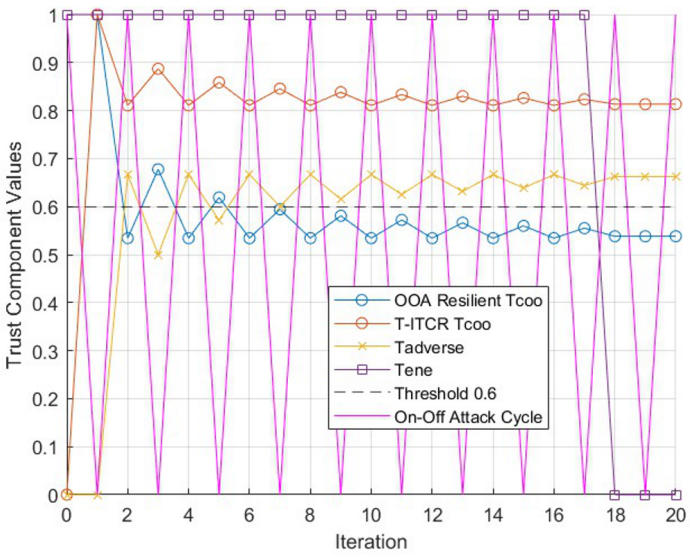

Fig. 1. Trust component variation under the On–Off attack scenario.

5.3 Trust Value Comparison Under On–Off Attack

As shown in Fig. 2, it represents the trust value of the nodes under the On-Off attack scenario. In this fig, the x-axis represents the simulation time in terms of iterations, and the y-axis represents the trust value of the nodes. Additionally, the dashed line represents the threshold for the trust value, which is set to 0.6. Based on the results, it is evident that the T-ITCR model is able to maintain the trust value of the nodes above the threshold for most of the simulation time, even when malicious behavior is observed in the network. This allows the malicious node to continue with its malicious behavior as it is still considered trustworthy in the network. However, in the case of the proposed OOA-resistant trust model, it is evident that the trust value of the malicious node is significantly reduced when malicious behavior is observed in the network. Furthermore, as the simulation time progresses, the trust value of the malicious node is reduced significantly below the threshold and approaches zero, indicating the accuracy of the proposed model in detecting malicious nodes performing On-Off attacks and ensuring they cannot maintain a high trust value in the network.

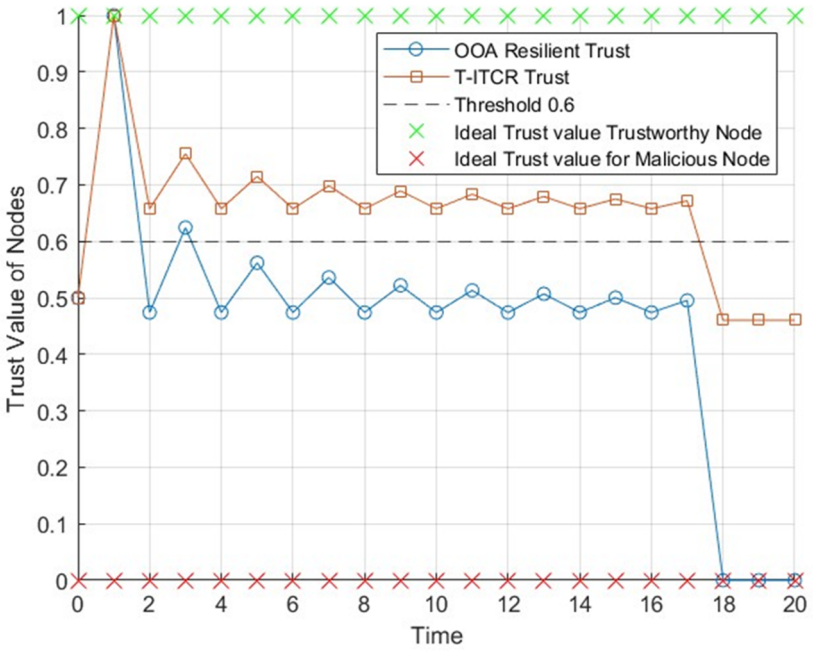

Fig. 2. Trust value comparison under On–Off attack behavior.

5.4 Gradual Shift from Cooperative to Malicious Behavior

The second experiment focuses on a scenario where a node exhibits initial adherence to a cooperative model, followed by the adoption of malicious behaviors. Fig. 3 illustrates the time progression of trust components within this scenario. On the x-axis, the time of the simulation process is indicated, while the values of different trust components are indicated on the y-axis. Initially, the values of the cooperative trust of both models are close to unity, reflecting the normal behavior of a node. However, as the node begins to exhibit malicious behaviors, the values of the OOA resilient trust of a node diminish significantly, reflecting the sensitivity of the model to changes in node behaviors. In contrast, the values of the T-ITCR trust diminish gradually, potentially masking the detection of a malicious node. At the same time, the adverse trust values increase, reflecting the detection of a node's malicious behaviors. This detection of a node's transition in behaviors allows the proposed model to better capture this transition.

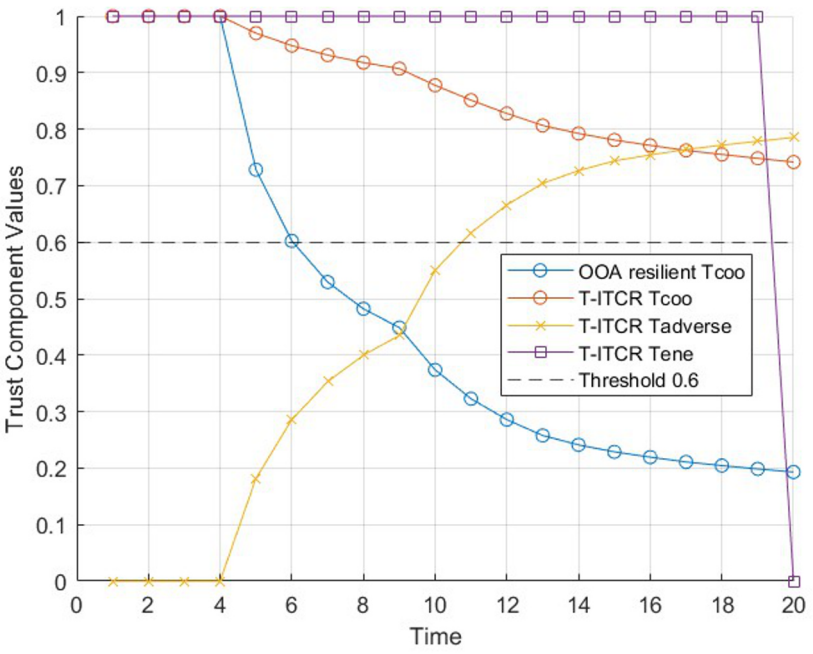

Fig. 3. Trust component evolution during gradual transition from cooperative to malicious behavior

5.5 Trust Evaluation During Behavioral Transition

Fig. 4 shows a comparison of the total node trust values during the gradual transition of nodes from a cooperative state to a malicious state. In this fig, the x-axis represents the simulation time, and the y-axis represents the trust values of the nodes. The results show that the proposed trust model for OOA resiliency results in a significant reduction in trust values when a node transitions to a malicious state. This means that the trust value will reduce rapidly and go below the threshold, thus identifying the malicious node. In contrast, the T-ITCR model shows a gradual reduction in trust values, which could allow malicious nodes to stay in the network for a long time. The significant difference in the trust values of the trustworthy and malicious nodes shows the effectiveness of the proposed model in maintaining reliable trust evaluation in dynamic IoT environments.

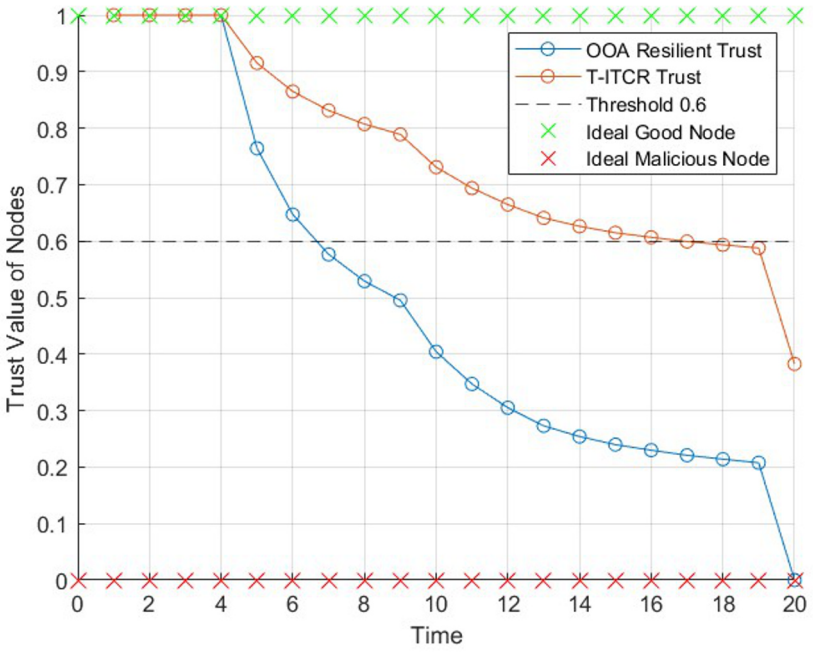

Fig. 4. Trust value variation during behavioral transition of a node.

6. Conclusion

In this study, a new trust evaluation mechanism has been presented, which aims to improve the detection of malicious nodes, especially under adverse conditions such as On-Off attacks and gradual changes in node behavior. This new mechanism combines aspects of cooperative trust, adversarial trust, and energy trust to improve the accurate assessment of node behavior in the IoT network. The results of this study show that this mechanism more effectively decreases the trust values of malicious nodes compared to

the current T-ITCR method, detecting the malicious nodes more quickly and achieving higher Precision (0.89) and Recall (0.84) compared to 0.81 and 0.76, respectively. In this mechanism, under On-Off attacks, the nodes are not able to sustain a high trust level during the intervals of cooperation, while a gradual change in node behavior from cooperative to non-cooperative results in a more rapid reduction in trust values.

7. Future Work

Although the proposed framework demonstrates strong resilience against dynamic attacks, several extensions can further enhance its applicability in real-world IoT systems. First, future work will explore the integration of indirect trust mechanisms, enabling nodes to incorporate recommendations from neighboring devices. This will be particularly useful in large-scale IoT environments where direct interactions are limited. Second, scalable and secure trust storage mechanisms will be investigated to support deployment in distributed IoT ecosystems. Emerging technologies such as blockchain or distributed ledgers can be leveraged to ensure transparency, tamper resistance, and decentralized trust management. Finally, future research will focus on validating the framework in real-world IoT testbeds and extending it to heterogeneous environments involving mobile nodes, edge computing, and federated learning scenarios. These enhancements will further strengthen the robustness, scalability, and practical applicability of the proposed trust management framework.

References

1. International Telecommunication Union, "Overview of the Internet of Things," ITU-T Recommendation Y.2060, June 2012.
2. F. K. Shaikh, S. Karim, S. Zeadally, and J. Nebhen, "Recent trends in internet-of-things-enabled sensor technologies for smart agriculture," *IEEE Internet Things J.*, vol. 9, no. 23, pp. 23583–23598, 2022.
3. E. Shaikh, I. Mohiuddin, and A. Manzoor, "Internet of Things (IoT): Security and privacy threats," in *Proc. 2nd Int. Conf. Comput. Appl. Inf. Secur. (ICCAIS)*, 2019, pp. 1–6.
4. A. Sharma, E. S. Pilli, A. P. Mazumdar, and M. C. Govil, "A framework to manage trust in internet of things," in *Proc. Int. Conf. Emerg. Trends Commun. Technol. (ETCT)*, 2016, pp. 1–5.
5. C. V. Mendoza and J. H. Kleinschmidt, "Mitigating on-off attacks in the internet of things using a distributed trust management scheme," *Int. J. Distrib. Sens. Netw.*, vol. 11, no. 11, Art. no. 859731, 2015.
6. Y. Xia et al., "Trust-based intrusion-tolerant coverage reliability in intelligent IoT systems," *IEEE Internet Things J.*, vol. 11, no. 15, pp. 25637–25647, 2024.
7. M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized trust management," in *Proc. IEEE Symp. Secur. Privacy*, 1996, pp. 164–173.
8. S. Dhelim, N. Aung, M. T. Kechadi, H. Ning, L. Chen, and A. Lakas, "Trust2Vec: Large-scale IoT trust management system based on signed network embeddings," *IEEE Internet Things J.*, vol. 10, no. 1, pp. 553–562, 2022.

9. Y. Liu, C. Zhang, Y. Yan, X. Zhou, Z. Tian, and J. Zhang, "A semi-centralized trust management model based on blockchain for data exchange in IoT system," *IEEE Trans. Serv. Comput.*, vol. 16, no. 2, pp. 858–871, 2022.
10. A. Sharma, E. S. Pilli, and A. P. Mazumdar, "BD-Trust: behavioural and data trust management scheme for internet of things," *J. Ambient Intell. Humaniz. Comput.*, vol. 14, no. 12, pp. 16195–16207, 2023.
11. W. Sherchan, S. Nepal, and C. Paris, "A survey of trust in social networks," *ACM Comput. Surv.*, vol. 45, no. 4, pp. 1–33, 2013.
12. K. A. Awan, I. Ud Din, A. Almogren, and H. Almajed, "AgriTrust—a trust management approach for smart agriculture in cloud-based internet of agriculture things," *Sensors*, vol. 20, no. 21, p. 6174, 2020.
13. J. Guo, R. Chen, and J. J. Tsai, "A survey of trust computation models for service management in internet of things systems," *Comput. Commun.*, vol. 97, pp. 1–14, 2017.
14. Y. Xia et al., "A trust-based reliable confident information coverage model of wireless sensor networks for intelligent transportation," *IEEE Trans. Veh. Technol.*, vol. 72, no. 7, pp. 9542–9554, 2023.
15. Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for Internet of Things," *J. Netw. Comput. Appl.*, vol. 42, pp. 120–134, 2014.
16. C. Boudagdigue, A. Benslimane, A. Kobbane, and J. Liu, "Trust management in industrial internet of things," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 3667–3682, 2020.
17. S. Chakraborty, N. K. Goyal, and S. Soh, "On area coverage reliability of mobile wireless sensor networks with multistate nodes," *IEEE Sensors J.*, vol. 20, no. 9, pp. 4992–5003, 2020.
18. R. Sun and Y. Deng, "A new method to determine generalized basic probability assignment in the open world," *IEEE Access*, vol. 7, pp. 52827–52835, 2019.
19. S. He et al., "Efficient fault-tolerant information barrier coverage in internet of things," *IEEE Trans. Wireless Commun.*, vol. 20, no. 12, pp. 7963–7976, 2021.
20. S. Sun, X. Fan, Y. Xia, C. Zhu, S. Liu, and L. Yi, "Coverage reliability of IoT intrusion detection system based on attack-defense game design," in *Proc. IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom)*, 2022, pp. 74–82.
21. J. Wang, Z. Zhang, and M. Wang, "A trust management method against abnormal behavior of industrial control networks under active defense architecture," *IEEE Trans. Netw. Serv. Manage.*, vol. 19, no. 3, pp. 2549–2572, 2022.
22. A. K. Junejo, N. Komninos, M. Sathiyanarayanan, and B. S. Chowdhry, "Trustee: A trust management system for fog-enabled cyber physical systems," *IEEE Trans. Emerg. Topics Comput.*, vol. 9, no. 4, pp. 2030–2041, 2019.
23. Y. B. Saied, A. Olivereau, D. Zeghlache, and M. Laurent, "Trust management system design for the Internet of Things: A context-aware and multi-service approach," *Comput. Secur.*, vol. 39, pp. 351–365, 2013.
24. M. Nitti, R. Girau, L. Atzori, A. Iera, and G. Morabito, "A subjective model for trustworthiness evaluation in the social internet of things," in *Proc. IEEE 23rd Int. Symp. Pers., Indoor Mobile Radio Commun. (PIMRC)*, 2012, pp. 18–23.
25. F. Ahmad, A. Adnane, F. Kurugollu, and R. Hussain, "A comparative analysis of trust models for safety applications in IoT-enabled vehicular networks," in *Proc. Wireless Days (WD)*, 2019, pp. 1–8.
26. F. Bao and I. R. Chen, "Scalable, adaptive and survivable trust management for community of interest based Internet of Things systems," in *Proc. 2013 IEEE International Symposium on Autonomous Decentralized Systems (ISADS)*, 2013, pp. 1–8.

27. X. Fan, X. Deng, Y. Xia, L. Yi, L. T. Yang, and C. Zhu, "Tensor-based confident information coverage reliability of hybrid Internet of Things," *IEEE Trans. Mobile Comput.*, vol. 23, no. 3, pp. 2171–2185, 2023.s
28. M. Buckland and F. Gey, "The relationship between recall and precision," *J. Amer. Soc. Inf. Sci.*, vol. 45, no. 1, pp. 12–19, 1994.