Computer Fraud and Security
ISSN (online): 1873-7056

Dynamic Trust Computational Model with Secure Data Transmission in IoT and WSN

Bhawana Atul Ahire[1,*], Dr. Sachin Rambhau Sakhare[2]

[1]Department of Computer Engineering, Smt. Kashibai Navale College Engineering, India., ahire.bhawana@kbtcoe.org

[2]Professor and head of Department of Computer Engineering, Vishwakarma Institute of Information Technology, Pune, Maharashtra, India, sachin.sakhare@viit.ac.in

Abstract:

As the integration of the Internet of Things (IoT) and Wireless Sensor Networks (WSN) continues to grow and its security and trust becomes a major issue. Due to transmission of sensitive between various networks, it is necessary to provide higher security such networks as well as nodes. Direct trust and indirect trust calculation models which are successful in a comparatively smaller network, but cannot deliver the requirements of adaptability of trust level in each instant for this smart environment such as IoT and complex WSN. Therefore, the aim of this paper is to design and develop a dynamic trust computational model to enhance data security in IoT and WSN. The framework describes the calculation of trust values assigned to different nodes depending on the values of data credibility, node's behavior, the frequency of communicating with other nodes. It also calculated the reliability coefficients to determine the current overall trust values for the nodes. The model incorporates machine learning algorithms to monitor and identify abnormal node activities and learn from the network's changes and identify possible security threats. In extensive experimental analysis we built IoT and WSN environments, the work showed a marked improvement over state-of-art approaches and decreased the loss of data and reduces the compromised node activity. Compared to the traditional static trust models, this proposed model ensured a more effective secure data routing with up to 99.40% accuracy in identifying the malicious nodes. In contrast to static and dynamic procedures for calculating trust, this model proposes an innovative, context-based system for estimating trust with reference to genuine-time node action. The use of the proposed framework rather than static models produces better security outcomes by enhancing work with 30% due to real-time metrics dependent on the context and adaptive threat identification.

Keywords: lightweight attack, IoT security, Security Architecture, Secure communication protocols, trust computation.

1. Introduction

Wireless Sensor Networks (WSNs) refer to the networks of small, low-cost sensor nodes, which are capable of detecting, computation and communication. These nodes monitor different conditions within their surroundings, for instance, heat, noise, oscillations, pressure, motion, and pollution. Data received from these sensors is then transferred to a common station where it is processed and loaded on the Internet for users to access. To collect data from the sensor field, there must be many nodes in open and, perhaps, perilous areas. This sprawling mesh of interconnected nodes serves to maintains ongoing vigilance over a variety of states and immediately report any deviations back to a centralized point. Because the nodes lack sufficient sensing and transmission capacity, they require cooperation in order to operate effectively. Therefore the cooperation between and within nodes in a WSN is very important in order to achieve the best result.

However, WSNs have features that make them prone to attacks such as low-powered devices, less computational power which prevents the integration of fortified security measures. They entirely depend on wireless communication hence prone to both eavesdropping and jamming attacks. Due to frequent and spontaneous deployment in insecure settings, physical manipulation or total obliteration can occur. Besides, they are limited by the battery capacity and cannot always push a new security update or patch for a known vulnerability. This also hampers protocols for interoperability and security measures and all this due to lack of

standardization. Altogether this generates the environment that make wireless sensors susceptible to multiple types of security threats and attacks. Below are the vulnerabilities we identified in WSN.

- Based on the physical architecture of the network, sensor nodes are vulnerable to being captured by the attacker who explores the messages and change information that is within it.
- WSNs data broadcast is most of the time without being encrypted; therefore, it is exposed to eavesdropping or even unlawful interception, which is equal to data leakage, and ultimately a privacy problem.
- WSNs need low energy nodes. This can be abused by a number of large requests to consume battery resources and lead to temporary network unavailability (e.g., Denial of Service).
- Generally, WSNs are fragmented for various routing attacks such as sinkhole and blackhole attacks, in which some nodes intentionally misroute or drop packets.
- Due to limited resources on nodes, there is high probability of attacks that include malware and rouge software which can affect the integrity and security of the network.

If behavior and interaction are increased in WSNs, then the trust calculation will help in reducing the vulnerabilities and help in identifying rogue nodes. In some networks, trust values are calculated and then used to determine whether or not certain nodes are compromised or even malicious and have to be removed. For example, trust metrics can discover symptoms of energy depletion attacks or spiked routing alterations so that data routes are safe. Inferior nodes resulting from malicious activities such as low trust ratio and repeated packet discard are prevented from participating in essential messages. Trust based authentication also reduces data interception and code injection risks by only permitting only tested nodes to exchange crucial data; it also improves the stability of the network. These factors include operating in open and often hostile environments, insecure communication links and the varied and critical applications which the address.

The most effective way to counter such threats is through continuous monitoring of nodes. Many proposed security techniques for WSNs include routing strategies, as routing is fundamental for data transmission to the base station. Therefore, implementing strong routing protocols that are resilient to packet tampering and disruption is crucial. There are numerous solutions available to secure routing, particularly when handling compromised nodes. One approach that has been widely studied is trust establishment. By evaluating the performance and behavior history of nodes, reliable and unreliable nodes can be identified, allowing for the establishment of trust. During routing, the system can then preferentially select trustworthy nodes while avoiding those deemed unreliable. Trust mechanisms have gained considerable attention in research as a means to improve network security and cooperation, owing to their simplicity and effectiveness in identifying compromised nodes. The communication process between WSN nodes is illustrated in Figure 1.

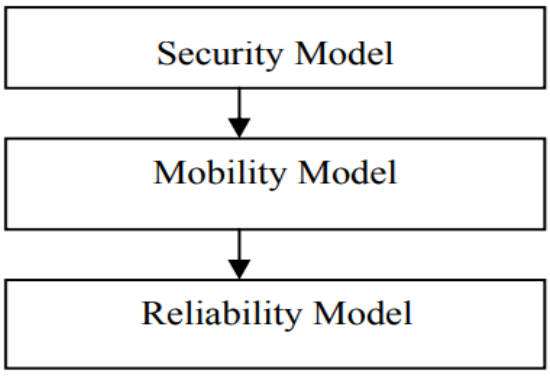

Figure 1: WSN trust model and its parameters

Trust management is critical in detecting people, machines, and other centers of control that belong to the malicious category, self-interested ones, and nodes having interactions with them in a network. There has been remarkable research work done in different classes of networks namely peer-to-peer networks, grid, and

Ubiquitous networks. Proposed work largely lacks the focus on comparative assessment of node reliability and enhancement in the general security and robustness of the WSNs through trust management. These techniques are applied practically in aspects such as routing, data aggregation, and cluster head election. However, although the several approaches have been proved to improve the others Various aspects of the other network security trust management remain challenges in WSNs.

Trust and reputation based methods have even demonstrated improved tolerance of attacks from the malicious nodes while shielding WSNs. These trust-based security strategies offer an attractive opportunity to use non-cryptographic mechanisms as a basis in contrast to using existing relations between entities. In wireless communication networks, trust means the extent of reliance a node has placed in other nodes. Trust based schemes enhance the capacity to predict the node behavior by taking into account their previous activities, this would help in better determination when malicious activities are afoot.

Recently, several trust models and secure routing mechanisms have been developed. However, many existing methods exhibit shortcomings. Additionally, many approaches are susceptible to high network overhead due to frequent exchanges of large amounts of data. Malicious nodes can exploit this information flow to conduct deceptive reporting attacks, spreading false information to undermine the trustworthiness of reliable nodes. Moreover, trust-based routing systems designed for networks often depend on high-powered hardware with sufficient storage, battery life, and computational capabilities. There is also a lack of attention to accurately detecting packet forwarding misbehavior caused by faulty or overloaded nodes.

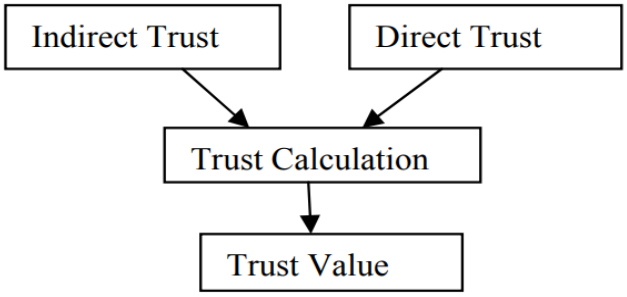

Figure 2: Trust calculation model in WSN[21]

The Figure 2 describes a trust calculation model using direct and indirect trust. This approach primarily use two trust dimensions: direct trust, derived from direct node interactions, and indirect trust, gathered through feedback from surrounding nodes. These metrics enable the identification of trustworthy nodes and the detection of potential threats, such as malicious or compromised nodes. Advanced frameworks often integrate computational techniques like Bayesian inference or fuzzy logic to evaluate trust dynamically. By blending direct and indirect trust mechanisms, WSNs achieve greater resilience, ensuring secure communication and efficient resource utilization in various operational environments.

The connection or distances between stages have a significant impact on various network factors such as energy consumption, routing overhead, interference, and delay. Increasing the number of hops can reduce energy usage, but it also leads to higher end-to-end latency and control overhead, as stated in reference [29]. Because of the long-range wireless communication characteristics, if the number of hops is small, the delay will be modest but the energy consumption will be significant [30]. Therefore, in order to accomplish both the decrease of energy consumption and the balancing of energy, it is imperative to compute an optimal number of hops that takes into account the appropriate individual distances. The suggested methodology involves selecting a master auditor node from a pool of trustworthy nodes to oversee the entire network and analyze the activity of each individual node.

The [41] framework effectively detects and mitigates malicious behaviors using machine learning algorithms, significantly improving trust evaluation accuracy. Adaptive metrics allow dynamic assessment of trust, accommodating changes in device behavior and environmental contexts. Experimental results show enhanced robustness against various attacks, including sybil and collusion, compared to traditional models. It also demonstrates scalability, maintaining performance even in large-scale IoT networks. Overall, the findings emphasize the importance of adaptive, real-time trust management for enhancing the security and reliability of

IoT ecosystems. However the [42] incorporates device-specific behaviors and real-time contextual factors to detect anomalies and evaluate trustworthiness dynamically. By utilizing a multi-dimensional trust metric, the approach adapts to changing conditions and identifies malicious devices effectively. Experimental evaluations confirm the model's capability to maintain high precision and resilience in detecting compromised nodes under various attack scenarios. The findings suggest the proposed model significantly improves trust management in IoT ecosystems, supporting secure and dependable device interactions.

The model [43] incorporates context-aware analysis and anomaly detection to identify and mitigate malicious activities. Experimental evaluations show that the approach improves trust evaluation accuracy, reduces latency, and adapts effectively to evolving threats and network variations. The findings suggest that self-learning algorithms are critical for maintaining security and performance in complex IoT ecosystems, offering a robust alternative to static or manually updated trust management systems. The [44] also reveal that their mechanism improves trustworthiness and security in IoT systems by considering both environmental and device-specific factors. The proposed system outperforms traditional methods by reducing the risk of malicious activities and enhancing the overall reliability and security of IoT applications. The approach is validated through simulations, demonstrating significant improvements in trust adaptation and system performance.

Brief Description of proposed concept

Specifically, the IoT and WSN have rapidly evolved and applied in a number of sectors such as healthcare, smart city, agriculture, and industrial applications. But these networks bring critical security and trust issues particularly to data integrity authentication and secure data transmission. Current trust models and security solutions do not successfully handle the flexibly changing conditions and the limited resource availability that is defined by the IoT and WSN paradigms. Thus, a Dynamic Trust Computational Model specific for applications of IoT and WSN is introduced in order to increase the level of security by including real-time trust quantification and flexible mechanism for data transfer.

Key Components of the Dynamic Trust Computational Model

This system is the foundation of the proposed model as it calculates a trust score for each device or node in real-time. The trust evaluation takes into account the behavior of the device, used and needed resources, data credibility and communication history with other devices. Trust levels involve object classification, where it’s possible to distinguish the nodes trusted first of all from potentially hostile ones with the help of such categories as high, middle, and low trust.

Compared with the previous models that only have one trust degree for evaluation of every node, this model uses multiple dimensions of trust to estimate them. The metrics include such as

The reliability of data is evaluated by a data trust which checks the data generated by the node The availability of resources along with energy resources to enable the node to perform functions securely is checked by the energy trust. The identified communication trust validity checks the reliability of data transmission and receptions while the behavioral trust defined the frequency of the abnormal or malicious behavior. These set of trust metrics are then summed up to derived a combined trust of every node, as the summative measure of the trustworthiness of nodes in the network.

Smart and intelligent applications are the specialty of IoT and WSN where network topology frequently changes and nodes are dynamically available. For these dynamic conditions, the model therefore uses the adaptive trust threshold to which the amount of trust that is acceptable sufficiently to the current state of the network changes. For example, the threshold was defined higher during the periods of the intense data transmission to provide more secure networks while during low traffic periods the limit can be set lower to include the nodes with relatively lower trust levels.

The trust model incorporates secure data transfer mechanisms that employ the computed trust values to determine routing strategies. In this case, only the nodes that have trust scores greater than the threshold can engage in data exchange routes. This filtering minimizes the probability of losing or intercepting information by other undesirable nodes. Also, coding techniques that can be adapted for use in low-energy devices guarantee the safety of data without greatly measuring the consumption of power resources. To overcome the problem of

dynamic behavior of nodes, the model provides the degradation of trust when it is not updated for a certain period of time, as well as the limited increasing of trust for a node which suddenly appears and rapidly increases the score. This makes the scheme to have an increased trust score in every interaction and therefore enhances the model as the real situation of the trustworthiness.

This is an element of the model that Learning algorithms are incorporated in the detection of an anomalous behavior in a network. They perform surveillance on the relationship between the nodes and alert the administrators when new communication patterns or new usage rates of resources deviate from normal levels – this is a sign of possible attack. Once an anomaly is sensed, then the model is capable of identifying the specific nodes that may be malicious and hence protect the network. DT-CM with SDT solves the trust and security issues of IoT and WSN by providing a new computational model which is scalable, real time and resource constrained environment efficient. The integration of this model with adaptive and anomaly-detection mechanisms is unique to this work and is a major leap forward in the domain to guarantee a robust and reliable network architecture for the future of IoT and WSN applications.

Motivation

Due to the emergence of the new technology such as IoT and WSNs, the possibility of collecting new real-time data has never been this possible but the problem of data reliability and its secure transmission is also chief. As is well known, IoT devices often suffer from many constraints including limited computational capabilities, mobility and operation in open environments that can be exposed to a wide range of threats and attacks. To tackle these issues, a strong Dynamic Trust Computational Model is expected to incorporate algorithmic approaches for periodically assessing the new and modified trust levels by predetermining additional contextual aspects such as the devices functioning settings, networks, and prior encounters. The proposed model improves security because it can intriguingly detect risky nodes and exclude them from the network. This is important for data consistency and security with high stakes applications such as smart cities, health care and infrastructure where DATA integrity and security is vital. Additionally, the relaxation of secure data transmission technique works hand in hand with the trust model by assuring that any data transmitted is well protected. In conclusion, a Dynamic Trust Computational Model with secure data transmission strengthen IoT & WSN architecture against new emerging threats and is pivotal for progressive IoT environment as it helps users to trust the system.

Objectives of work

- Develop a dynamic trust mechanism to assess and adjust trust levels based on real-time behaviours and historical interactions of nodes within IoT and WSN environments.
- To develop a protocol for secure data transmission by incorporating robust encryption and authentication methods to prevent data tampering, interception, and unauthorized access.
- To minimize resource consumption (energy, memory, processing power) by designing a lightweight trust computation model suited for the limited capacities of IoT and WSN devices.
- Enable real-time detection and isolation of malicious nodes by continuously monitoring network activities and updating trust scores to identify abnormal behaviours.
- Strengthen the network's ability to withstand attacks by reinforcing trust-based communication pathways, thereby enhancing the reliability and resilience of IoT and WSN networks.

This work illustrates an observed implementation of the dynamic trust calculation in IoT and WSN environment through implementing ML techniques. The paper describes that dynamic trust computation models can significantly improve the security of the communicated data in IoT and WSN networks. The correlation of trust management to secure communication protocols provided can greatly enhance the reliability of these networks. More effort in this field is required to provide better solutions to the emerging security threats.

2. Literature Review

Based on their operational constraints, finite resources and characteristics of WSNs' communication, several challenges are experienced in enhancement of power efficiency, finding measures to enhance the network's lifespan and securing of WSNs. Han et al. [2] proposed a routing algorithm called TAGA specifically for wireless sensor networks because it addresses issues of energy and trust. This algorithm uses a heuristic evolutionarily computed algorithm to minimize energy consumption associated with data transmission while at the same time ensuring security from traditional routing attacks and developing heightened security against trust based on cyber terrorism. TAGA accomplishes this by evaluating each node's global trust and proposing values of direct trust based on parameters such as volatility and other forms of adaptive penalties, as well as introducing indirect trust via filtering.

Several trust models have been developed in order to assess the trustworthiness of each node in WSNs and IoT. For example, Zhang et al. proposed a trust computation model for constructing direct trust and indirect trust calculation based on the fuzzy logic in [3]. This model considers the mobility of the nodes and gives a more realistic trust assessment.

While modeling trust in IoT contexts, nodes often join and leave the network, which is why static models can hardly address this type of issue. Li et al., in [4], put forward a dynamic trust management system that contributes to dynamic changes in the degrees of trust in the nodes according to their behaviors over a certain period. With these aspects in mind, this system incorporates machine learning prediction models for behavior projection and the consequent trust scores.

The protection of information is very important for the security of the data in the WSNs and IoT by Khan et al [5], also underlined the need for encryption protocols to protect data at the transport level. It also defines their research as the comparison of the different encryption algorithms and stresses on the optimization required for devices with limited hardware capabilities. Secure Communication Protocols: In [6], Huang et al proposed a secure communication protocol for IoT devices using trust-based methods with a primary aim to confabulate secure links between nodes. Its security features include a behavioral trust estimation procedure before data transfer, which minimizes the danger of having third parties intercept the information.

Zhan et al. [7] proposed the Energy Efficient Multi-Level Secure Routing (EEMSR) technique, which aims to safeguard IoT networks while optimizing energy consumption. This protocol employs a cluster-based multi hop routing approach to alleviate the excessive communication overhead resulting from IoT scalability, as clustering is an effective method for energy conservation.

Wireless mesh networks utilize a multi-hop architecture to transmit packets, managed by multiple mesh clients within a mobile infrastructure. The effectiveness of routing protocols is essential for the connectivity and data transfer rates of nodes in these networks. Recently, the convergence of IoT and mesh clients has surged, driven by the demand to connect billions of devices and provide expansive coverage at low network costs. The mobility of mesh network clients significantly affects data routing through intermediate nodes, influencing network performance and delay. Additionally, the extensive nature of the Internet allows potentially malicious nodes to infiltrate the mesh network, jeopardizing the integrity of transmitted data [8].

Wireless sensor networks are focused on exploring strategies to reduce power consumption. Implementing clustering techniques effectively promotes energy conservation. However, many current clustering algorithms employ a fixed cluster head selection method for each clustering cycle, leading to the recurrent choice of suboptimal nodes as cluster heads. This results in accelerated energy depletion and reduced network lifespan [9].

Generative AI is poised to revolutionize secure and privacy-preserving mobile crowdsensing as it allows the creation of data faking methods that disguise private information-safeguarding user confidentiality. Using generative adversarial networks (GANs) and differential privacy techniques, this tool generates synthetic data that retains statistical patterns seen in the original dataset without revealing any individual data points —a must for sensitive use cases such as health or social behaviors tracking. Liu et al. In [10], it stressed on GANs for anonymized data generation that balancing the privacy and accuracy. Moreover, Wang et al. [11] emphasizes that federated learning with generative models offers a decentralized data control and make it (in distributed architectures, e.g. mobile crowdsensing) possible to maintain privacy across devices

Chen X et al. [12] Optimization of Data Freshness in Privacy-Preserving Mobile Crowdsensing via Artificial Nois but MCS systems combine the data from a lot of mobile users, which have privacy problems as well as risk for stale data. To balance data utility and privacy, by incorporating artificial noise mechanisms the framework ensures that it strikes an adequate equilibrium. Using methods including Age of Information (AoI) the study makes sure user privacy is not jeopardized while maintaining freshness, relevance and timeliness of data. The results show that artificial noise can efficiently mitigate the privacy risks in MCS applications and meanwhile meet an optimal AoI, which also contributes to enhancing both reliability and security for CAP threshold analysis.

PPFO framework resolves privacy and data freshness issues in mobile crowdsensing Li X, et al. al. [13]. A PRoFet-based Publish/Subscribe System. This approach deals with the trade-off between privacy preservation and data freshness, ensuring that sensing data from regions being monitored are updated in a timely manner while maintaining confidentiality of raw sensing data. To maintain a balance in the exposure of personal data, PPFO also enforces differential privacy and data aging mechanism to make sure recent data is always collected for sensing tasks. This dual-focus approach builds up user confidence which paves the way of using mobile crowdsensing in sensitive applications as well. We were able to observe the effectiveness of PPFO in reducing data staleness and improving user privacy over conventional models through various experimental results. Table 1 summarizes Literature based on different parameters like method used, research findings and Limitations in different Trust Management methods.

Table 1: summary of literature

Reference	**Method Used**	**Findings**	**Limitations**
Pathak, I. et al. [1]	Adaptive QoS and Trust-Based Routing	Introduced a lightweight algorithm focusing on QoS and trust in WSNs. Achieved enhanced security and energy efficiency.	Limited evaluation in dynamic environments.
Y. Han et al. [2]	Adaptive Genetic Algorithm	Proposed a routing protocol that minimizes energy consumption while maintaining trust and security.	Needs testing in large-scale WSNs.
H Zhang et. al. [3]	Fuzzy Logic	Developed a trust computation model using fuzzy logic, enhancing trust evaluation in WSNs.	Lacks integration with existing routing protocols.
Li, Y. et. al. [4]	Machine Learning	Established a dynamic trust management framework for IoT, improving security and adaptability.	Requires validation in diverse IoT scenarios.
Khan, M. et. al. [5]	Lightweight Encryption	Presented a protocol ensuring secure data transmission in IoT with minimal overhead.	Potential vulnerabilities in extreme conditions.
Huang, Y. et. al. [6]	Trust-Based Communication	Introduced a trust-based protocol for secure IoT communication, enhancing reliability.	Needs evaluation against various attack vectors.
Y. Zhang et. al. [7]	Multilevel Security	Developed a routing protocol that balances energy efficiency with security across multiple levels.	Limited scalability assessment.
K. Haseeb et. al. [8]	Robust Trust Scheme	Implemented a trusted scheme that enhances communication security in mobile mesh networks.	Lack of performance benchmarks in real-world scenarios.
J. Hou et. al. [9]	Fuzzy Inference	Proposed a clustering protocol that optimizes energy consumption through fuzzy logic.	Not evaluated for different environmental conditions.
Liu, X. et. al. [10]	Generative Models	Explored generative models to ensure privacy in mobile crowdsensing	Lacks practical implementation insights.
Wang, Y. et. al. [11]	Federated Learning	Integrated federated learning with generative AI to enhance privacy in crowdsensing	Need for experimental validation on data efficiency.
Y. Yang et al. [12]	Artificial Noise	Optimized data freshness in privacy-preserving settings using artificial noise.	Performance against noise robustness not evaluated.

Yaoqi Yang et. al. [13]	Optimization Framework	Proposed a framework prioritizing privacy while optimizing data freshness.	Limited exploration of trade-offs between privacy and performance.
K. Hamouid et. al. [14]	Tree-based Routing	Developed a lightweight tree-based routing method focusing on security in WSNs.	No large-scale deployment tests.
M. Rathee et. al. [15]	Ant Colony Optimization	Proposed an energy-balancing routing algorithm improving QoS and security.	Not assessed for adaptability to dynamic networks.
M. Mathapati et. al. [16]	Multi-Dimensional Trust	Introduced a secure routing scheme integrating multi-dimensional trust evaluation.	Lacks empirical validation in varying conditions.
Jiang N et. al. [17]	Voting-based Incentive Model	Developed an incentive model to optimize participant decision-making in crowdsensing.	Needs evaluation of long-term effects on participation.
Li J et. al. [18]	Multi-Level Secret Sharing	Proposed a multi-level secret sharing scheme for decentralized e-voting.	Not tested for user scalability and efficiency.
Liu Z et. al. [19]	Compressed Sensing	Utilized compressed sensing for secure image registration in cloud environments	Performance metrics in different cloud scenarios missing.
Sengupta J et. al. [20]	Directed Diffusion	Implemented a secure directed diffusion approach tailored for industrial WSNs.	Not tested for broader applications beyond industrial contexts.

Wang et al. [36] propose a MR-DCAE model that couples deep convolutional autoencoders with manifold regularization to identify unauthorized broadcasting in wireless communication networks effectively. The model's manifold learning can maintain the intrinsic structure of data and guarantee more distinguished feature represent ability of sophisticated signal patterns. Experiments clearly prove the high superiority of MR-DCAE over traditional methods in terms of detection accuracy and robustness against noise. Deep learning techniques are discussed for secure data communication channels by the effective establishment of unauthorized signal transmissions.

Y. Liu et al. [37] proposed a real-time classification method based on a lightweight neural network architecture called MobileViT for the classification of constellation images of wireless communication signals. In this approach, the proposed technique effectively encompasses the spatial and temporal features of the constellation patterns, enabling accurate identification of various modulation schemes. The architecture of MobileViT has been optimized for resource-constrained environments to achieve high accuracy with low computational overhead. The proposed approach may be useful in real-time applications of communication systems and can provide good trade-offs between efficiency and performance.

H. Zhang et al. [38] proposed a lightweight radio transformer framework, MobileRaT, for automatic modulation classification in drone communication systems. MobileRaT is able to effectively discriminate modulation formats with low computational overhead by employing advanced signal processing methods and transformer architectures. The study proved that MobileRaT realizes excellent performance in real-time use, making it suitable for various practical assignments, including dynamic environments involving drone communications. This work provides a framework contributing to the continued improvement in communication reliability and performance in aerial systems, highlighting how lightweight solutions are essential for increased drone usage.

J. Liu et al. [39] propose a new technique that addresses this problem by recognizing real-time transformer discharge patterns through the integration of CNN and LSTM networks, driven by few-shot learning techniques. This work tries to solve the problem of limited labeled data by providing the capability of effectively learning from only a few examples, offering better adaptability to new patterns. This approach, based on experimental results, identifies discharge events with high accuracy, significantly enhancing transformer monitoring capabilities for predictive maintenance strategies.

R. Zhao et al. [40] present a novel framework termed CEEMD-MsI for long-term prediction of PM2.5 concentration levels. This approach is effectuated by incorporating Complete Ensemble Empirical Mode Decomposition and a multi-stream informer architecture to effectively capture air quality data in terms of temporal dynamics and complex patterns. The proposed approach outperforms some traditional forecasting models with higher accuracy in PM2.5 prediction. Moreover, these findings reveal the potential of using advanced decomposition techniques with machine learning frameworks in environmental monitoring and public health management, a fact that may prove invaluable to policymakers.

3. Research Methodology

The popularity of WSNs has surged rapidly in recent years. However, the applications of WSNs face limitations due to the limited computational resources of sensor nodes and security concerns related to data transmission. Researchers are currently focusing on routing strategies in WSNs to enhance their performance. A major challenge has been to develop methods for energy-efficient routing. Establishing a protocol that enables effective data transmission between nodes is crucial for determining the optimal path for data flow within the network. One approach to reduce power consumption in a WSN is to implement an energy-efficient data transfer protocol, which helps to evenly distribute the energy load among all nodes.

Additionally, the inherent lack of control in wireless networking within WSNs, combined with the restricted capabilities of individual nodes, creates difficulties in ensuring security and privacy.

In WSNs, various trust-based methods have shown increased robustness against internal node attacks. These methods introduce new concepts for secure routing in WSNs by using past experiences to predict nodes' future behavior and detect potentially misbehaving nodes. However, traditional trust-aware routing protocols have limitations, such as high energy consumption and limited ability to address diverse types of attacks. Additionally, routes that heavily rely on trust values based on hop count may be less effective at transmitting messages, as paths with higher overall trust often require more hops.

Secure routing cooperation is based on developing trust values for nodes, guiding the selection of relay nodes along the routing path. A node's overall trustworthiness is pre-estimated through its primary trust score, secondary trust value, volatility factor, and available energy levels. If a node’s total trust value falls below a threshold, it is deemed untrustworthy. This is the proposed model framework, illustrated in Figure 3.

The workflow of a trust computation model in IoT environments includes multiple layers aimed at assessing nodes based on their behavior and interactions within the network. The computation methodology generally follows a structured approach:

Initialization and Data Collection: The process begins with network initialization, registering each IoT node and authenticating their identity. Nodes periodically exchange data and communication logs, which serve as the raw input for the trust computation algorithm. Collected data includes packet delivery ratio, response time, energy consumption, and behavioral history—all essential for estimating node reliability.

Definition of Trust Metrics: IoT trust is typically multi-attribute, encompassing direct trust, indirect (recommendation-based) trust, and behavioral metrics. Direct trust stems from direct interactions, such as successful data exchanges. Indirect trust is computed based on recommendations from nodes with experience interacting with the node in question. Each metric is weighted based on system needs, with a possible emphasis on security, reliability, or energy efficiency.

Trust Evaluation Algorithms: The trust evaluation engine applies algorithms like SVM, NB, or other machine learning techniques to process collected data. These algorithms dynamically update trust scores based on ongoing interactions, making a node's trust score dynamic and reflective of recent behavior. A node that reliably delivers packets and communicates efficiently will see its trust score increase, while erratic behavior or unresponsiveness may reduce it.

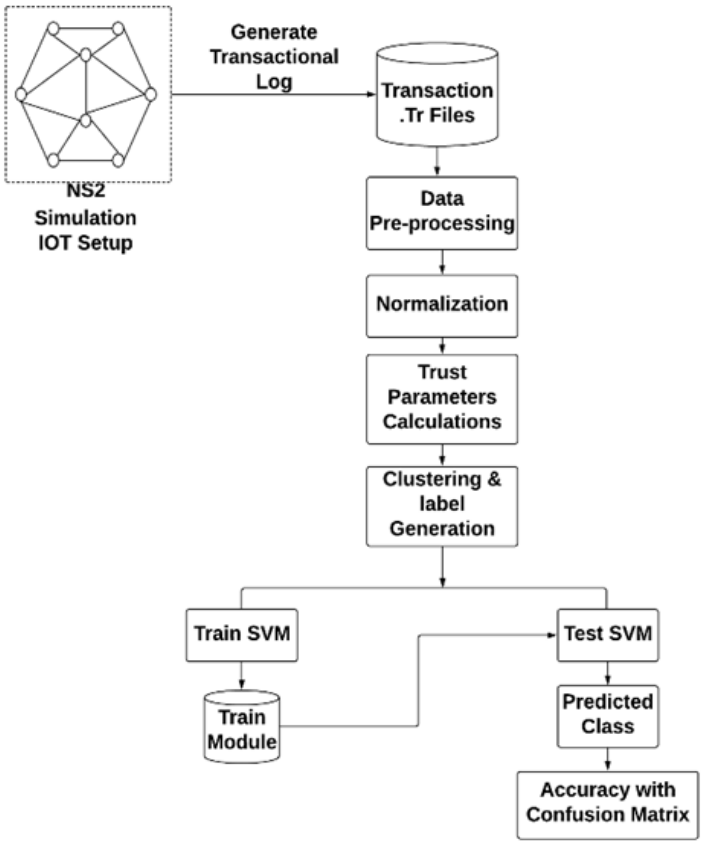

Figure 3: proposed system architecture for trust calculation in WSN

Decision and Action on Trust: After computing trust scores, the system decides whether to permit the node's participation in critical network functions like data aggregation or routing. Nodes scoring below a predefined threshold may be isolated or denied participation in secure data transmission.

Feedback and Trust: Ongoing interactions continuously update trust scores, ensuring that trust evaluations remain accurate. Feedback from successful or failed interactions refines future trust assessments, enhancing system reliability.

This dynamic, continuous evaluation of trust supports security and reliability in IoT networks, allowing only trusted nodes to participate in sensitive operations like data routing and aggregation.

4. Algorithm Design

Secure Trust Calculation Algorithm

Initially, all the nodes in the Wireless Sensor Network (WSN) are included as registered as participants in the network. Each node in the network will be granted a unique token that cannot be imitated. Each confirmed node in the entire network will be assigned an identical Inimitable token to facilitate node authentication during conversation. The method of assigning unique tokens is accomplished as

$$RegNode[N] = \sum_{i=1}^{N} \frac{nodephID(i)}{netsize(N)} + \frac{getTI(i)}{Th} + maxPrime(i) + allocener(i) \quad \text{-----(1)}$$

The nodeID represents the physical address of the nodes, while netsize() denotes the capability of the network node to handle data. maxPrime() refers to the highest prime number that is taken into account during node registration, and the allocated energy is also taken into consideration. The trust factor quantifies the level of importance assigned to a node in the routing process. The trust factor calculation is executed in the following manner:

$$TrustFactor[N] = \prod_{i=1}^{N} \frac{maxPDR(i)}{\delta} + availener(i) + getmax((\tau)) + Th \quad \text{-------(2)}$$

$$TrFac[N] = \prod_{i=1}^{N} (TrustFactor(i, i+1)) + RegNode(i) + Th \quad \text{------(3)}$$

The δ represents the total number of packets produced in the network, τ is the model used to calculate the complexity of computation, and Th is the threshold that is used in trust factor determination. The data transmission procedure will involve the consideration of trustworthy nodes. Among these trusted nodes, the Master Auditor Node (MAN) will be selected based on criteria such as minimum energy usage, highest trust factor, and high computing power. The MAN node will oversee the conduct of all the remaining trusted nodes throughout their active state. The process of selecting the MAN node is carried out as

$$Inode[N] = \sum_{i=1}^{N} \frac{mindist(Y1-Y1)+(X2-X1)}{netsize(N)} + mindist(i) \quad \text{-----(4)}$$

The MAN node selection approach is used for path construction during the data transmission between the source node and base station. It may change every time according to parameters such as trust, energy, computation power, etc. The major benefit of MAN nodes is that they can easily remove buffer overflow as well as single points of bottleneck problems.

$$\text{MAN[N]} = \sum_{i=1}^{N} \frac{max\ PDR(N)}{netsize(N)} + max\ (availner(i) + (TrFac(i)) + \tau(i) \quad \text{------(5)}$$

The node selection process for routing involves assessing feedback from the MAN node and taking trust factors into account. This node selection process is carried out as follows:

$$NSelec[N] = \prod_{i=1}^{N} \frac{TrFac(MAN(i))}{\tau(i,i+1)} + \frac{max\ (PDR(i,i+1)}{\delta(i)} * \sum_{i=1}^{N} mindist(i) + Th \quad \text{----(6)}$$

The MAN node will frequently assess the other nodes and consider their trust levels to determine the best path for data transmission. The process of finalizing the routing table is carried out as follows

$$Trou(MAN[N]) = \sum_{i=1}^{N} (NSelec(i, i+1)) * \prod_{i=1}^{N} (\delta(i) + \frac{\tau}{i})^2 \quad \text{-----(7)}$$

The proposed methodology focuses on Trust-Based Secure Routing for WSNs, aiming to establish reliable routes for secure data transfer. The model's performance is validated by comparison with established standards like Adaptive QoS and the Trust-Based Lightweight Secure Algorithm for WSNs. The proposed model demonstrates substantial improvement in accurately selecting the most trustworthy paths. This approach stores node information within the network, which is then used to identify nodes during data transmission. Each node is assigned a unique token, known as an Inimitable token. Graphs show the accuracy levels of Node Inimitable Token Allocation for both existing and proposed models.

5. Results and Discussion

5.1: Experiment Analysis using Simulation Environment

The following section presents the results and discussions of IoT application implementation and the NS2 simulation platform. Initially, NS2 was selected due to its multi-functionality in simulating wireless and sensor networks, which are key components in IoT architectures.

Packet Delivery Ratio (PDR): Simulation results showed a high PDR in smaller network sizes, indicating good communication among IoT devices. As network size increased, packet collisions and congestion led to a gradual decrease in PDR. In a 50-node network, the PDR remained above 90%, while larger networks of over 200 nodes saw a reduction to about 80%, underscoring the need for efficient routing protocols in densely packed IoT environments.

End-to-End Delay: This delay was found to be inversely proportional to network density. Smaller networks experienced minimal delays of around 20 ms, which rose to over 100 ms as node count increased. This rise is likely due to higher routing overhead and network congestion from many devices communicating simultaneously.

Throughput: Throughput was consistent across small-scale networks but decreased as the number of nodes grew. In 50-node networks, throughput was approximately 1 Mbps, while in larger networks, it dropped to an average of about 0.6 Mbps. This trend is expected in IoT environments, where many devices compete for limited bandwidth.

Energy Consumption: Network size and density were observed to impact energy consumption. In a 50-node scenario, average energy consumption was 2.5 J per node, rising to around 4.2 J per node in larger networks. Energy efficiency is especially critical in IoT devices, particularly for battery-operated sensors, and optimizing routing protocols could help reduce this increased energy usage.

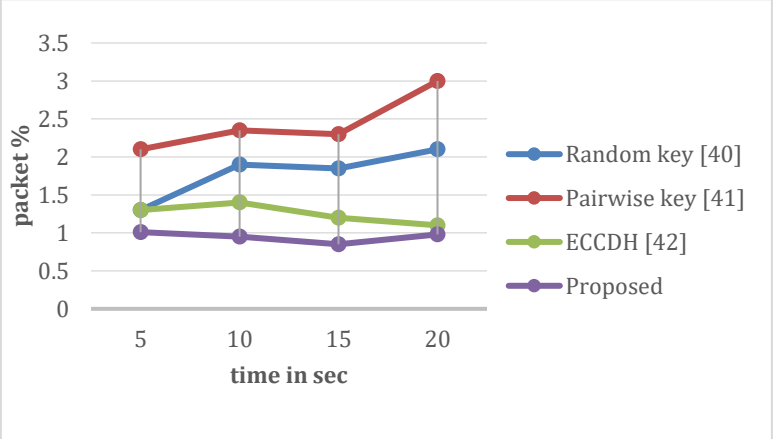

Figure 4: Packet end to end delay vs simulation time

The above Figure 4 describes end to end delay with simulation time. Packet end-to-end delay versus simulation time illustrates how the time taken for a packet to travel from source to destination varies throughout a network simulation. Factors such as network congestion, routing efficiency, and resource allocation influence the delay. Analyzing this relationship helps optimize protocols and improve network performance under dynamic conditions. The proposed model delay is less than conventional techniques which is around 1.5-2% less than [40,41,42].

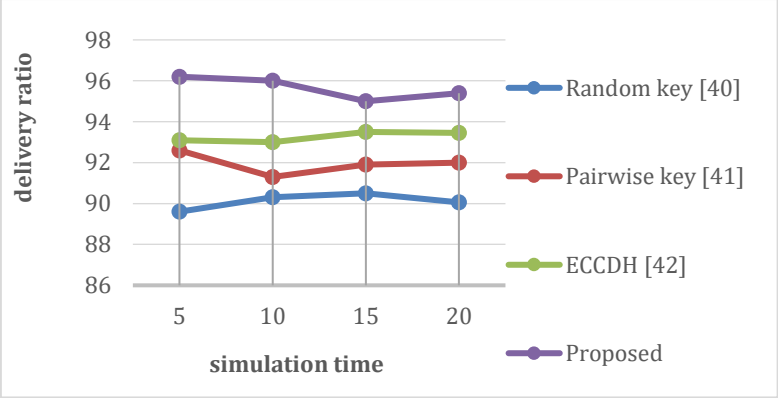

Figure 5: Packet delivery ratio vs simulation time

The Figure 5 demonstrates PDR vs. Simulation Time analyzes the efficiency of data transmission in a network over time. PDR measures the ratio of successfully delivered packets to those sent. This metric evaluates network performance, with higher PDR indicating reliability. Simulation time assesses PDR under varying conditions like congestion or mobility. The proposed protocol achieves 98-99% PDR for entire simulation.

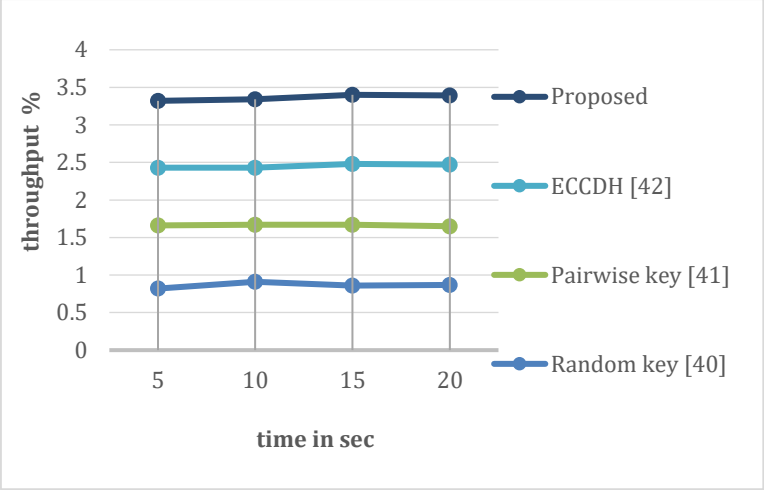

Figure 6: Throughput percentage vs simulation time

Figure 6 illustrates that throughput is measured in seconds. The number of useful bits successfully transmitted per second determines the throughput for TCP packets. Once a connection is established between the source and the sink node, actual text data is sent, with these packets classified as TCP packets. The BTC algorithm enhances throughput while reducing both packet and network overhead. It also mitigates internal data threats, such as buffer overflow. Results show that the proposed model achieves throughput that is 7-9% higher than that of three state-of-the-art systems.

Throughput for TCP packets is determined by measuring the number of useful bits successfully transmitted per second. Once a connection is established between the source and the sink node, actual text data is sent, with these packets classified as TCP packets. The BTC algorithm enhances throughput while reducing both packet and network overhead. It also mitigates internal data threats, such as buffer overflow. Results show that the proposed model achieves throughput that is 7-9% higher than that of three state-of-the-art systems.

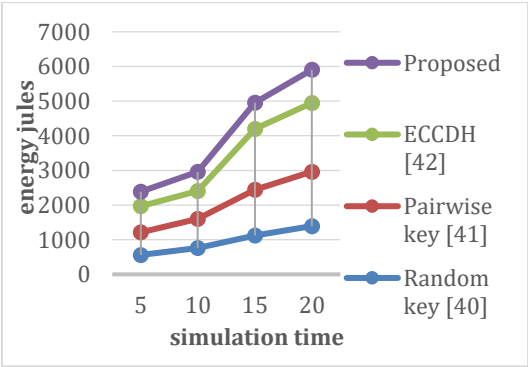

Figure 7: Energy consumption (in jules) by each vehicle node with simulation time

The above Figure 7 illustrates the energy usage by individual nodes during the communication process. The energy consumption, measured in joules, varies dynamically between 100 and 3000 joules for each node. The proposed models specifically influence internal node interactions, helping to prevent energy depletion in nodes that are in sleep mode.

5.2: Experiment Analysis using IoT Environment

In another experimental analysis IoT module has deployed with 10 different analog sensors for data collection and Arduino UNO as microcontroller due to cost effective data collection in IoT model. The similar algorithms are applied for evaluation. The machine learning module has applied IoT results. Below is the visualized analysis of proposed IoT model.

Table 2: Comparative analysis for proposed trust computation module with different operating environment and machine learning models

Environment	Trust Model	Clustering	Algorithm	Accuracy
NS2	Hybrid Trust	k-means	NB	95.30
			SVM	97.40
		Q-Learning	NB	97.10
			SVM	98.10
IoT	Hybrid Trust	k-means	NB	96.70
			SVM	97.50
		Q-Learning	NB	98.60
			SVM	99.40

The above Table 2 describes a comparative analysis between simulation environment as well as IoT environment. The below Figure 8 to Figure 10 describes an IoT module results

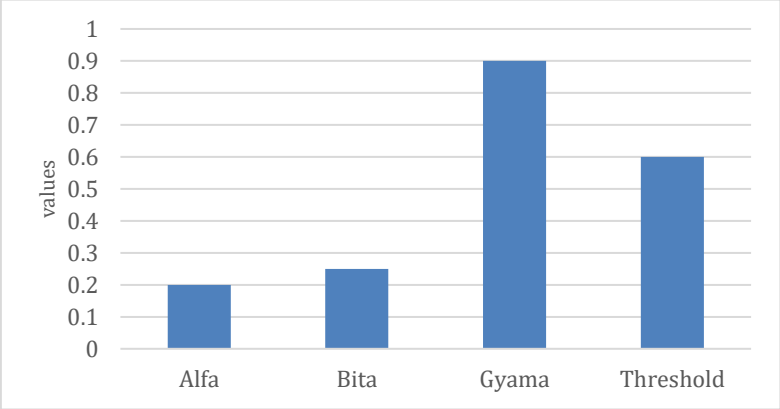

Figure 8 : Each IoT node configuration setting for data acceptance

In IoT networks, data acceptance for each node is crucial for effective communication and system performance. The Figure 8 describes an configuration settings are defined by parameters such as Alfa (0.2), Bita (0.25), and Gyama (0.9), which represent different weighting factors for data validation. Alfa reflects the minimum required reliability for data acceptance, ensuring a baseline quality. Bita indicates the sensitivity of the node to varying data types, while Gyama signifies the maximum allowable error rate in accepted data. The threshold of 0.6 acts as a critical cutoff, dictating that only data meeting or exceeding this cumulative score from the parameters is accepted for further processing, enhancing overall system reliability.

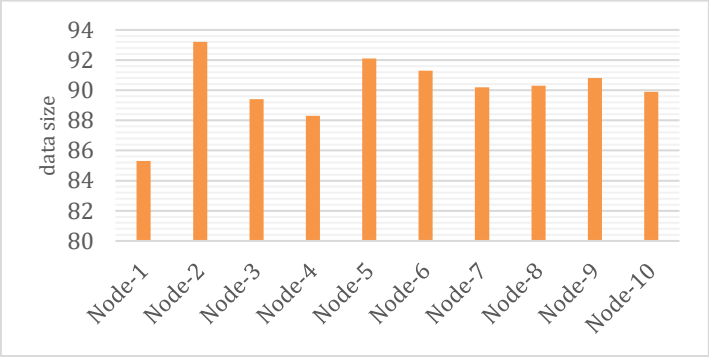

Figure 9: Accepted data size after data filtration by each IoT node

Data acceptance rates across the ten IoT nodes reflect their efficiency in filtering and retaining high-quality information. Node-2 has the highest acceptance rate at 93.2%, showing very strong filtration, while Node-1 has a lower rate at 85.3%. Similarly, Node 5 and Node 6 maintain strong data integrity with acceptance rates of 92.1% and 91.3%, respectively. The other nodes, ranging between 88.3% and 90.8%, show relatively consistent performance in data filtration. These results indicate the varying effectiveness of each IoT node in processing and accepting relevant data for further analysis.

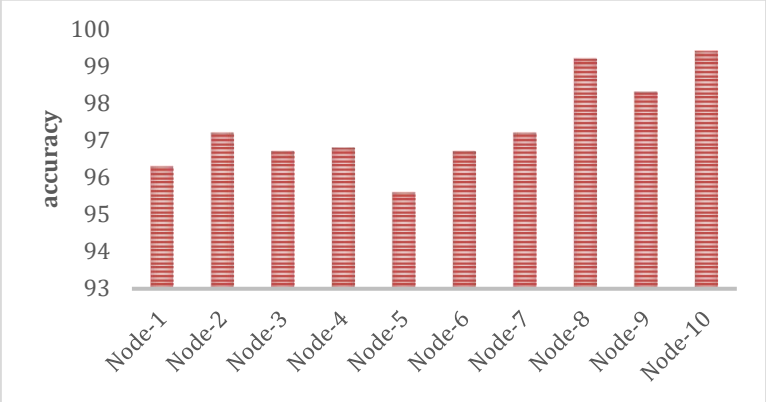

Figure 10 : Trust calculation accuracy for each node using SVM algorithm

The SVM algorithm calculated each node's trust with high accuracy in evaluating network node reliability. Accuracy rates ranged from a low of 95.6% for Node-5 to a high of 99.4% for Node-10, showing robust performance across all nodes. Nodes with high accuracy, such as Node-8 and Node-10, demonstrated strong trustworthiness, likely due to consistent behavior or performance metrics. Conversely, Node-5's relatively low accuracy may signal potential vulnerabilities or inconsistencies. Overall, the SVM algorithm effectively differentiates reliable nodes from less reliable ones, enhancing network security and trust management.

The findings are more clearly shown thanks to the dynamic trust calculation approach's use of graphical representations and thorough comparing tables. An explicit examination of the trade-offs between security and performance in high-density networks, however, would make the conversation more thorough. Ensuring strong security measures in these settings might result in more processing cost, delay, and network congestion. Achieving optimum system performance while preserving high trust accuracy requires careful consideration. By addressing these trade-offs, the difficulties would become more apparent and the dynamic trust mechanism would be improved for safe, real-time operation in dense IoT networks.

6. Conclusion

WSN are characterized by opportunistic transmissions, limited connectivity, and frequent changes in network topology among the nodes. Due to the lack of continuous connectivity, WSN routing uses a store-carry-and-forward method, where messages are relayed through intermediate nodes during opportunistic encounters, often leading to significant end-to-end communication delays. This paper introduces a dynamic trust management system to address malicious and opportunistic misbehavior of nodes in WSNs. Ensuring reliable and efficient data transmission while accounting for unpredictable node behavior remains a challenge. To address this challenge, the study proposes a trust-based secure routing protocol guided by a master auditor node. This new scheme, designed to achieve secure data transmission, identifies trusted paths to discover energy-efficient and reliable routes—key factors in the longevity of WSNs. The architecture enables the determination of optimal trust settings for trust aggregation, aiming to align subjective trust closely with objective trust for each parameter. The routing process balances trust, energy, and hop count, allowing the selection of nodes that are dependable, cost-effective, and efficient in communication. By facilitating decentralized trust assessment, decreasing dependence on centralized systems, and improving privacy, including future goals like federated learning fits in well with present IoT security developments. Federated learning solves privacy issues by enabling IoT devices to work together to learn and update trust ratings without exchanging private information. Furthermore, enhancing the practicality of trust models requires taking into account real-world restrictions including power limits and device resource constraints. In order to guarantee the scalability and efficacy of trust models in resource-constrained situations

and increase the system's adaptability to actual IoT deployments, power-efficient algorithms and lightweight trust assessment methods are essential.

For future direction this approach can be enhance for cluster-based channel selection in 5G network. During the data transmission and path selection between source node to base station this dynamic trust calculation approach will effective when select to next node for path creation. This technique can eliminate Man in the middle attack as well various spoofing attacks. By using Pre-compute trust scores and store them for devices that are frequently used or have predictable behaviors, which helps reduce real-time computation. Trust values can be updated periodically rather than continuously. In many networks, devices and network nodes may experience buffer overflows, leading to queuing delays. Trust proposed score updates could get stuck in queues, causing delayed or missed updates that affect trust management

Ethical Statement

This study does not contain any studies with human or animal subjects performed by any of the authors.

Conflicts of Interest

The authors declare that they have no conflicts of interest to this work.

References

[1] Pathak, I. Al-Anbagi and H. J. Hamilton, "An Adaptive QoS and Trust-Based Lightweight Secure Routing Algorithm for WSNs," in IEEE Internet of Things Journal, vol. 9, no. 23, pp. 23826-23840, 1 Dec.1, 2022, https://doi.org/10.1109/JIOT.2022.3189832

[2] Han, Y., Hu, H., & Guo, Y. (2022). Energy-aware and trust-based secure routing protocol for wireless sensor networks using adaptive genetic algorithm. *IEEE Access*, *10*, 11538-11550. https//doi.org/10.1109/ACCESS.2022.3144015

[3] Sánchez-Gómez, R., Romero-Morales, C., Gómez-Carrión, Á., De-la-Cruz-Torres, B., Zaragoza-García, I., Anttila, P., ... & Ortuño-Soriano, I. (2020). Effects of novel inverted rocker orthoses for first metatarsophalangeal joint on gastrocnemius muscle electromyographic activity during running: A cross-sectional pilot study. *Sensors*, *20*(11), 3205.

[4] Li, J., Li, X., Gao, Y., Yuan, J., & Fang, B. (2018). Dynamic trustworthiness overlapping community discovery in mobile internet of things. *IEEE Access*, *6*, 74579-74597. http://dx.doi.org/10.1109/ACCESS.2018.2884002

[5] Ma, L., Pei, Q., Xiang, Y., Yao, L., & Yu, S. (2019). A reliable reputation computation framework for online items in E-commerce. *Journal of Network and Computer Applications*, *134*, 13-25. https://doi.org/10.1016/j.jnca.2019.02.002

[6] Li, T., Huang, G., Zhang, S., & Zeng, Z. (2021). NTSC: a novel trust-based service computing scheme in social internet of things. *Peer-to-Peer Networking and Applications*, *14*, 3431-3451. https://link.springer.com/article/10.1007/s12083-021-01200-8

[7] Zhang, Y., Ren, Q., Song, K., Liu, Y., Zhang, T., & Qian, Y. (2021). An energy-efficient multilevel secure routing protocol in IoT networks. *IEEE Internet of Things Journal*, *9*(13), 10539-10553. http://dx.doi.org/10.1109/JIOT.2021.3121529

[8] Haseeb, K., Din, I. U., Almogren, A., Islam, N., & Altameem, A. (2020). RTS: A robust and trusted scheme for IoT-based mobile wireless mesh networks. *IEEE Access*, *8*, 68379-68390. http://dx.doi.org/10.1109/ACCESS.2020.2985851

[9] Hou, J., Qiao, J., & Han, X. (2021). Energy-saving clustering routing protocol for wireless sensor networks using fuzzy inference. *IEEE Sensors Journal*, *22*(3), 2845-2857. http://dx.doi.org/10.1109/JSEN.2021.3132682

[10] Liu, Q., Wang, Y., Zhao, W., & Qiu, X. (2023, November). Differential Privacy Protection Based on Federated Learning in Mobile Crowdsensing. In *2023* IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech) (pp. 1-6). IEEE.

[11] Wang, Y., et al. (2022). Integrating federated learning with generative AI for privacy in crowdsensing. IEEE Access.

[12] Yang, Y., Zhang, B., Guo, D., Xiong, Z., Niyato, D., & Han, Z. (2024). Can We Realize Data Freshness Optimization for Privacy Preserving-Mobile Crowdsensing With Artificial Noise?. *IEEE Transactions on Mobile Computing*.
http://dx.doi.org/10.1109/TMC.2024.3396993

[13] Yang, Y., Zhang, B., Guo, D., Wang, W., Li, X., & Hu, C. (2023). PPFO: A Privacy Preservation-oriented Data Freshness Optimization Framework For Mobile Crowdsensing. *IEEE Communications Standards Magazine*, *7*(4), 34-40.
http://dx.doi.org/10.1109/MCOMSTD.0005.2200077

[14] Hamouid, K., Othmen, S., & Barkat, A. (2020). LSTR: lightweight and secure tree-based routing for wireless sensor networks. *Wireless Personal Communications*, *112*(3), 1479-1501.
https://link.springer.com/article/10.1007/s11277-020-07111-w

[15] Rathee, M., Kumar, S., Gandomi, A. H., Dilip, K., Balusamy, B., & Patan, R. (2019). Ant colony optimization based quality of service aware energy balancing secure routing algorithm for wireless sensor networks. *IEEE Transactions on Engineering Management*, *68*(1), 170-182.
http://dx.doi.org/10.1109/TEM.2019.2953889

[16] Mathapati, M., Kumaran, T. S., Muruganandham, A., & Mathivanan, M. (2021). Retracted article: Secure routing scheme with multi-dimensional trust evaluation for wireless sensor network. *Journal of Ambient Intelligence and Humanized Computing*, *12*(6), 6047-6055.
https://link.springer.com/article/10.1007/s12652-020-02169-7

[17] Jiang, N., Xu, D., Zhou, J., Yan, H., Wan, T., & Zheng, J. (2020). Toward optimal participant decisions with voting-based incentive model for crowd sensing. *Information Sciences*, *512*, 1-17.
https://doi.org/10.1016/j.ins.2019.09.068

[18] Li, J., Wang, X., Huang, Z., Wang, L., & Xiang, Y. (2019). Multi-level multi-secret sharing scheme for decentralized e-voting in cloud computing. *Journal of Parallel and Distributed Computing*, *130*, 91-97.
http://dx.doi.org/10.1016/j.jpdc.2019.04.003

[19] Liu, Z., Wang, L., Wang, X., Shen, X., & Li, L. (2019). Secure remote sensing image registration based on compressed sensing in cloud setting. *IEEE Access*, *7*, 36516-36526.
http://dx.doi.org/10.1109/ACCESS.2019.2903826

[20] Sengupta, J., Ruj, S., & Das Bit, S. (2018, October). An efficient and secure directed diffusion in industrial wireless sensor networks. In *Proceedings of the 1st International Workshop on Future Industrial Communication Networks* (pp. 41-46).
http://dx.doi.org/10.1145/3243318.3243320

[21] Sengupta, J., Ruj, S., & Bit, S. D. (2019, January). End to end secure anonymous communication for secure directed diffusion in IoT. In *Proceedings of the 20th international conference on distributed computing and networking* (pp. 445-450).
http://dx.doi.org/10.1145/3288599.3295577

[22] Wang, X., Zhang, Y., Gupta, B. B., Zhu, H., & Liu, D. (2019). An identity-based signcryption on lattice without trapdoor. *Journal of universal computer science*, *25*(3), 282-293.

[23] YE, Z. W., WEN, T., LIU, Z. Y., & FU, C. G. (2019). An algorithm of trust-based secure data aggregation for wireless sensor networks. *Journal of Northeastern University (Natural Science)*, *40*(6), 789.

[24] Fang, W., Zhang, W., Chen, W., Liu, Y., & Tang, C. (2020). TMSRS: Trust management-based secure routing scheme in industrial wireless sensor network with fog computing. *wireless networks*, *26*(5), 3169-3182.
https://link.springer.com/article/10.1007/s11276-019-02129-w

[25] Feroz Khan, A. B., & Anandharaj, G. (2021). A cognitive energy efficient and trusted routing model for the security of wireless sensor networks: CEMT. *Wireless Personal Communications*, *119*(4), 3149-3159.
https://link.springer.com/article/10.1007/s11277-021-08391-6

[26] Yu, X., Li, F., Li, T., Wu, N., Wang, H., & Zhou, H. (2022). Trust-based secure directed diffusion routing protocol in WSN. *Journal of Ambient Intelligence and Humanized Computing*, 1-13.
https://link.springer.com/article/10.1007/s12652-020-02638-z

[27] Patil, P. A., Deshpande, R. S., & Mane, P. B. (2020). Trust and opportunity based routing framework in wireless sensor network using hybrid optimization algorithm. *Wireless Personal Communications*, *115*, 415-437.
https://link.springer.com/article/10.1007/s11277-020-07579-6

[28] Kalidoss, T., Rajasekaran, L., Kanagasabai, K., Sannasi, G., & Kannan, A. (2020). QoS aware trust based routing algorithm for wireless sensor networks. *Wireless Personal Communications*, *110*, 1637-1658.
https://link.springer.com/article/10.1007/s11277-019-06788-y

[29] Hajiee, M., Fartash, M., & Osati Eraghi, N. (2021). An energy-aware trust and opportunity based routing algorithm in wireless sensor networks using multipath routes technique. *Neural Processing Letters*, *53*(4), 2829-2852.
https://doi.org/10.1007/s11063-021-10525-7

[30] J. Jasper, J. (2021). A secure routing scheme to mitigate attack in wireless adhoc sensor network. *Computers & Security*, *103*, 102197.
http://dx.doi.org/10.1016/j.cose.2021.102197

[31] W. Fang, W., Zhang, W., Chen, W., Liu, J., Ni, Y., & Yang, Y. (2021). MSCR: Multidimensional secure clustered routing scheme in hierarchical wireless sensor networks. *EURASIP Journal on Wireless Communications and Networking*, *2021*, 1-20.
https://jwcn-eurasipjournals.springeropen.com/articles/10.1186/s13638-020-01884-1

[32] Q. Zhang, Q., Liu, X., Yu, J., & Qi, X. (2020). A trust-based dynamic slicing mechanism for wireless sensor networks. *Procedia Computer Science*, *174*, 572-577.
http://dx.doi.org/10.1016/j.procs.2020.06.126

[33] Yang, T., Xiangyang, X., Peng, L., Tonghui, L., & Leina, P. (2018). A secure routing of wireless sensor networks based on trust evaluation model. *Procedia computer science*, *131*, 1156-1163.
http://dx.doi.org/10.1016/j.procs.2018.04.289

[34] Shi, Q., Qin, L., Ding, Y., Xie, B., Zheng, J., & Song, L. (2019). Information-aware secure routing in wireless sensor networks. *Sensors*, *20*(1), 165.
https://doi.org/10.3390/s20010165

[35] Sun, N., & Lu, Y. (2019). A self-adaptive genetic algorithm with improved mutation mode based on measurement of population diversity. *Neural Computing and Applications*, *31*, 1435-1443.
https://link.springer.com/article/10.1007/s00521-018-3438-9

[36] J. Xu, L. Pei and R.-Z. Zhu, "Application of a genetic algorithm with random crossover and dynamic mutation on the travelling salesman problem", Proc. Comput. Sci., vol. 131, pp. 937-945, May 2018.
http://dx.doi.org/10.17488/RMIB.45.2.4

[37] Verma, M. K., & Dhabliya, M. D. (2015). Design of Hand Motion Assist Robot for Rehabilitation Physiotherapy. *International Journal of New Practices in Management and Engineering*, *4*(04), 07-11.
http://dx.doi.org/10.17762/ijnpme.v4i04.40

[38] Kawale, S., Dhabliya, D., & Yenurkar, G. (2022, November). Analysis and Simulation of Sound Classification System Using Machine Learning Techniques. In *2022 International Conference on Emerging Trends in Engineering and Medical Sciences (ICETEMS)* (pp. 407-412). IEEE.
http://dx.doi.org/10.1109/ICETEMS56252.2022.10093281

[39] Joseph, L. M., & Fredrik, E. T. (2023). Protecting information stored inside the cloud with A new CCA-EBO protocol designed on hive technology. *International Journal on Recent and Innovation Trends in Computing and Communication*, *11*, 40-49.
http://dx.doi.org/10.17762/ijritcc.v11i4s.6305

[40] Wang, E.K., Hui, L.C.K. Yiu, S.M.: A new key establishment scheme for Unmanned Aerial Vehicless. IJNSA 1(2), 17–27 (2009)
https://doi.org/10.48550/arXiv.1004.0591

[41] Chen J, Zhang K, Hu Y, et al. Real-time trust management for IoT ecosystems using machine learning and adaptive metrics. IEEE Internet Things J. 2023;10(2):1201-1215. doi:10.1109/JIOT.2022.3186754.

[42] Liu Y, Wang X, Sun J, et al. Dynamic trust evaluation model for IoT devices using contextual and behavioral data. IEEE Trans Dependable Secure Comput. 2022;19(4):2780-2792. doi:10.1109/TDSC.2021.3105082.

[43] Zhao L, Huang X, Zhou J, et al. Real-time trust adaptation in IoT environments with self-learning algorithms. IEEE Syst J. 2022;16(3):4700-4709. doi:10.1109/JSYST.2021.3086590.

[44] Shen J, Liu X, Zhao W, et al. Context-aware trust adaptation mechanism for IoT-based systems. IEEE Access. 2024;12:13507-13519. doi:10.1109/ACCESS.2024.3310092.