Peer-to-Peer Networking and Applications (2026) 19:79
https://doi.org/10.1007/s12083-026-02222-w

RESEARCH

TITAN: Logarithm-based trust-aware integrated technique for robust anomaly neutralization in industrial WSNs

Khushboo Tripathi[1] · Shalu[2,8] · Sheetal Kaushik[3] · Shubham Vyas[4] · Mohd Anas Khan[5] · Ali Ahmadian[6,7]

Received: 10 July 2025 / Accepted: 14 March 2026

Abstract

Trust between sensor nodes is very essential to improve security, dependability, energy efficiency, scalability, and cooperation in Industrial Wireless Sensor Networks (IWSNs). In order to enhance cooperation and security on a large scale in IWSNs, we suggest a Trust-based Integrated Techniques for Anomaly Neutralization (TITAN), where unequal clustering can be used to detect and shrink unacceptable sensor nodes and save resources. Disparate strategic clustering helps in boosting energy efficiency through the creation of smaller clusters close to the sink and larger ones at the distances, therefore encouraging the more tolerable distribution of power and communication encumbrance. Heads of the clusters are dynamically selected depending on the fitness of the nodes within the cluster through a new Optimal Cluster Representative Election Algorithm (OCREA). The fitness of a node is based on its residual power, connection quality, signal strength and distance to the sink. TITAN applies distributed intra-cluster trust to make decisions combining with centralized inter-cluster methodologies, merging attack-resistant trust evaluations and effective trust aggregation. In addition, TITAN applies an appealing dynamic logarithmic trust fund distribution of rewards and sanctions based on the actions of sensor nodes, it is possible to distinguish between reliable and faulty nodes. Also, it includes key indicators of communication trust, data trust, and energy measurement to allow proper trust measurement. TITAN considers a dynamic aging factor and damping factor, which ensures that reliability of sensor nodes is considered on account of recent exchanges, and, therefore, minimizing the influence of old information. To a larger extent, the model incorporates a logarithmic penalty term that punishes the node when the rate of unsuccessful interactions goes up hence effectively isolating with untrustworthy nodes. TITAN enhances better and reliable and robust trust assessment as it incorporates feedback provided by trustworthy neighbor's nodes and the manipulation of trust levels using an extensive analysis. The combination of these features contributes to the overall performance and improves it's security of IWSNs, which enables them to be better resistant to attacks and use less resource to run in resource-constrained environments. Due to its communication overhead, trust evaluation and detected malicious nodes, the solution proposed is superior in its capabilities compared to other solutions authenticated with extensive simulations. TITAN manages to recognize the presence of the malicious nodes with 87 percent even when the malicious nodes are less than 60 percent, meaningfully better than such comparative models as SDTS and DTMS. The positive error rate and the negative error rate is minimized with a precision in detection increased to 9% and 6% respectively. TITAN also maintains high packets delivery ratio of above 89% and reduced the average packet loss to only 36 as compared to more than 60 in the baseline schemes. Also, the energy consumption is lowered by about 14% that confirms the effectiveness of TITAN. These findings all indicate the strength and scalability of TITAN Energy-constrained environment performance and threat-prone IWSN environments performance.

Keywords Trust · Reliability · Dependability · IWSN security · Attacks · Fitness score · Unequal clustering

Extended author information available on the last page of the article

Published online: 10 April 2026

1 Introduction

The industrial wireless sensor networks (IWSNs) are the key aspect of the modern industrial-based settings as they allow real-time management and observation of industrial processes and machines. These networks are made up of a group of small powered sensor nodes (SNs) distributed throughout industrial plants and that measure and transmit data in parameters like temperature, pressure, humidity and vibration[1]. Such large amount of information facilitates prompt decision making, optimization of processes and enhancement of work efficiency in industries [2]. The industrial set-up is bound to consist of varied and intricate assembly of machines, SNs, communication systems, control system and computing functionality, and these should be coo-ordinated. This heterogeneity forms many vulnerability points, which could be exploited by attackers. In addition, the working conditions in industries are largely hostile, and there are elevated levels of electromagnetic interference, extreme temperatures and physical impediments. It may influence the reliability of wireless communication and the functioning of sensors. However, there are special issues involved in wireless communications within industrial set ups especially regarding security [3]. IWSNs possess a number of most serious problems including reliability and robustness, heterogeneity, interoperability, scalability, energy constraints and security vulnerabilities [4]. In IWSNs, security and reliability are most essential, as the data and processes in question may be considered too sensitive [5, 6]. Such networks are running some vital industrial processes where any attack or malfunction may cause Destructive consequences that may include disruption of operations, safety incidents, and financial damages. Security also guarantees the confidentiality of data and freedom of tampering against malicious usage and authorized access. Reliability embodies reliable and accurate transmission of data which is significant when it comes to making timely decisions and optimization of processes. Malicious players are interested in the industrial systems having high priority to destroy the work of the infrastructure, to steal the sensitive information, or to sabotage the work. Different types of attacks pose serious risks to the integrity, confidentiality and availability of the data in IWSNs [7]. A few of them include eavesdropping, where attackers monitor communications in order to obtain sensitive information, and tampering, where unauthorized alteration of data or SNs is implemented. The stakeholder network can be intentionally sabotaged by disgruntled workers or contractors, or unauthorized access to sensitive data can be affected by the machines inside the network [8]. These attacks can go years without being caught and this would cause havoc in the production process, data leakage and loss of money, intellectual property theft or loss of essential infrastructure [9]. Insider attack also undermines trust in the IWSN, which undermines cooperation and collaboration of legitimate actors as well as influence in making effective decisions [10]. Outsider attackers may attack IWSNs via different types of sophisticated attacks in order to exploit flaws in network protocols or software and hardware components [11]. Such attacks might be eavesdropping in passive form, distortion of data packets, the introduction of harmful code or even interference with the communications channel. Specifically, DoS attacks can saturate the network resources that will lead to failure of communications and distortion of regular industrial operations [12]. Moreover, other attacks may have economic reasons or competitive spying, or geopolitical intentions. They are able to present serious threat to industrial organizations to take action against new threats. Attacks of IWSNs by external entities have non-monetary results. They can produce a blow to the reputation, a loss of client faith, and a possibility of the legal blow-back. It emphasizes the importance of strong security procedures and active risk mitigation methods [13]. The intensive security practices are important to counter any form of external and internal threats [9–14]. These approaches need to provide confidentiality, integrity as well as availability of the data in the network. Confidentiality ensures the data is not compromised with unauthorized entities whereas integrity assures the data is not compromised. Availability refers to making the services and network accessible to the parties supposed to access them where necessary [13]. Conventional security techniques, such as encryption and authentication are needed and may not be adequate on their own due to the high-risk environments, individual or complex nature of the challenges in IWSNs [12, 15, 16]. More enhanced regulations and progressive security solutions are demanded, which should be able to grow in line with the threats and anomalies that come [17, 18]. The trust mechanisms are needed to protect IWSNs against malicious activity and protect integrity of communications and data [19]. The mechanisms provide SNs with the ability to measure the trustworthiness and credibility of the information provided by their respective counterparts due to the establishment of trust relations among the SNs [20]. Decision-making based on trust allows SNs to be smart on the data aggregation, routing and cooperation. It minimizes the effect of attacks and the effect of network resilience maximization [21]. The trust models are good solution to the security problem in the IWSNs because it introduces a model of quantifying and managing the trust between the SNs in the network [22].

These models can be employed to make use of the different trust factors such as history of the past behavior of SNs, the context of interaction and the feedback of other SNs. By continuously monitoring and updating the level of trust, these models can identify and isolate malicious SNs before they can disrupt the network [23]. Figure 1 shows the different categories of trust.

In this paper, our objective is to design a lightweight trust mechanism (TITAN) for IWSNs to support decision-making at minimal energy cost. Our proposed solution is meant to provide structured as well as scalable attack detection and countermeasures utilizing trust as a primitive building block in order to support security. Adding energy-efficient mechanisms for trust assessment, the designed model minimizes security operation overhead, ensuring efficient network performance as well as resource utilization in IWSN. Our suggested approach involves several key components. Since In IWSNs unequal clustering is superior to equal clustering. To begin with, we outline a new unequal topology of strategic clustering because it allows balancing energy consumption and lowering funnel overheads around the sink and enhancing network longevity by stopping the premature depletion of nodes in high-traffic areas [24]. More data traffic is normally in SNs near the sink in IWSNs resulting in faster energy consumption [25]. Unequal clustering takes care of this by having smaller clusters closer to the sink, which is less burdened by the cluster heads, and larger clusters more distant, which distributions have fewer SNs relaying data [26]. This is because early energy congestion of vital SNs close to the sink is avoided, which leads to increased efficiency of resources use, reduction on load balancing and a prolonged network life time. We then construct an effective lightweight calculation of trust system that can be implemented on the resource constrained SNs. Such mechanism consider different new aspects of trust such as first-hand observation of SNs behavior, suggestions of other SNs, and data trust. Second, we develop a distributed trust management system where Jed SNs provide SNs with trust information and work together to identify and react to threats.In order to make sure that our proposed solution is effective and realistic, we thoroughly test and experiment the system in the industrial conditions. Our trust mechanisms are compared with various attack models that have been proposed in subsection attack model. This argument is substantiated by our experimental data, which confirms that our solution makes a great contribution to security position of IWSNs by increasing their resistance against attacks without reducing energy consumption and operation reliability.

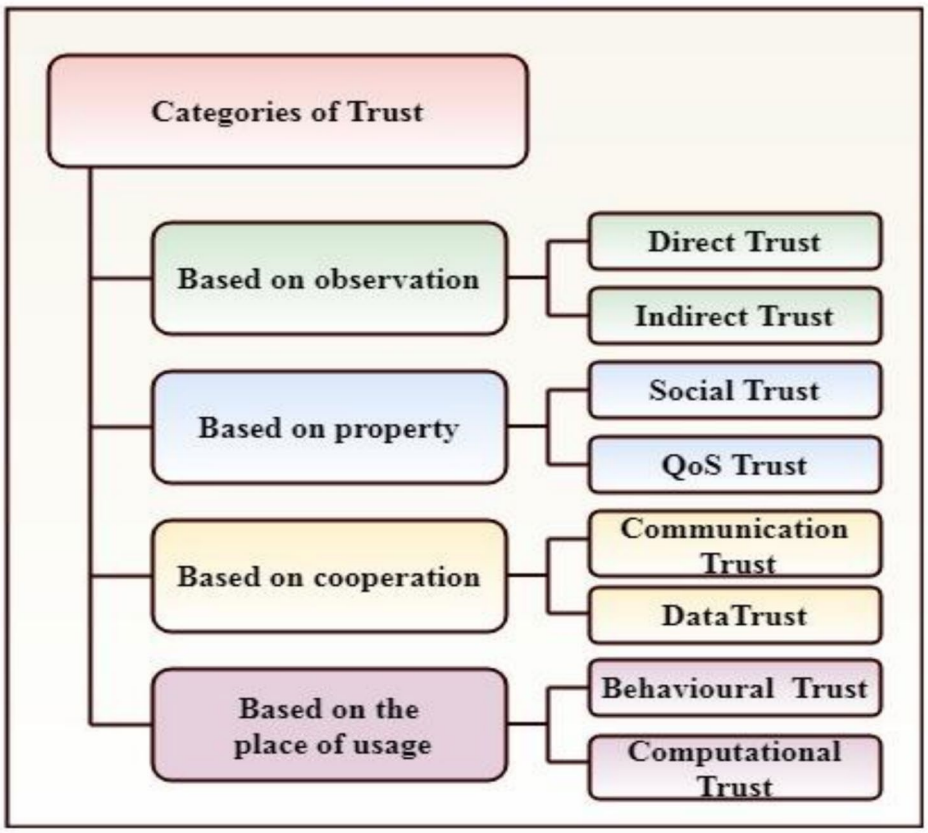

Fig. 1 Categories of trust

1.1 Motivation

The growing demand of secure and reliable communication in IWSNs renders the availability of new solutions in dealing with the sufficient problems of resource limitation and dynamic settings like security attacks [1], load balancing [2], energy and bandwidth limits, and inconsistency of data [3]. Traditional security measures rely on computationally infeasible cryptography and intrusion detection and some of the processes [4]. These do not fit in with the small energy and processing capacity.

of SNs [5]. The limitations cause vulnerability and inefficiency of industrial use in the real world [7]. This requires the availability of lightweight, adaptable trust models like the one that was proposed by the authors and is called TITAN which can guarantee strong security, improve energy efficiency and adaptively respond to the changing network conditions in IWSNs. Lightweight trust models are the most effective way out of above-mentioned problems [27]. The trust relationships that exist between SNs in these models are formed on behavior [8], which enables SNs to determine credibility and reliability of information [9]. Based on the measure of trust, SNs are capable of making intelligent decisions on data like aggregation, routing and collaboration, which improves the overall level of security and reliability of the IWSN. Trust models are adaptive in nature, whose trust levels are constantly updated depending on constant interactions and feedback, which is essential to guarantee strength in changing industrial settings [18–23]. Lightweight trust models use less energy and have low levels of computation overhead, which renders them applicable to SNs with a resource constraint [28, 29]. These models are based on simple and effective algorithms in order to be evaluated. These are reliable which guarantees security is brought without highly depleting battery life, or processing power. This is primarily crucial in the industrial setting where SNs are commonly used in places that are difficult to access, and constant battery changes are not feasible. In addition, insider threats are especially difficult to detect and counter with the help of trust models to fight with conventional security [30]. The trust models have the ability to detect likely anomalies in SN behavior. Due to monitoring it regularly, it denotes indicative of ill intentional operations in the IWSN [31]. With proactive security, it is possible to isolate and nullify easily within a short period of time, things such as threats, and blocking the possibilities of interruption and safeguarding sensitive industry procedures [32, 33]. Also, trust models support decentralized security control, reducing the reliance on a central control that may be a failure point [23]. For large-scale, this decentralization is the most important to IWSNs in order to ensure resilience and scalability. All SNs are assessing trust singly,

which distributes security decisions throughout the network, and resists attackers trying to attack central control points[34].

1.2 Novel scientific contribution

The suggested TITAN trust model is an efficient and strong security system, and it is accurately designed to enhance the security of IWSNs. The implementation of TITAN experiences radical changes in terms of trust management that introduces a new age of innovation and safety to these mission-critical systems. TITAN provides the following major contributions to the security of IWSNs offering reliability and performance in the mission critical industrial setting.

a. TITAN uses unequal strategic clustering as opposed to equal clustering to balance the consumption of energy and increase the network lifetime. TITAN uses an Optimal Cluster Representative Election Algorithm (OCREA), which enhances the choice of a cluster head (CH) in IWSNs. It takes into account network density, link quality, Traffic Load, distance to BS, Signal Strength and remaining battery life, which gives an efficient aggregation of data and the load balancing. It also periodically chooses healthy CHs and this offers some stability as it switches to backup CHs and limits the effects of low CHs battery levels.
b. TITAN is a multi-level, multi-factor, trust computation scheme that works at both distributed intracluster and centralized intercluster levels. It applies a dynamic logarithm trust function which allocates dynamic rewards and punishments on the behavior of SNs. It differentiates reliable and untrustworthy SNs and keeps whitelists and blacklists, respectively.
c. In order to identify positive and negative SN behaviors we use an adaptive sliding time window of variable length, which is directed by the trust levels. This improves the accuracy of monitoring and flexibility and performs better than fixed length windows in identifying and acting upon network abnormalities.
d. To incorporate the effective methodology used in estimating the trust (direct, indirect trust, data trust) in TITAN, it includes aging factor and damping factor, which are empirically validated to have good resistance to threats. TITAN reduces the communication

and computational overhead by interesting and unique trust operations over an unequal clustered architecture, and does not need superfluous trust measures such as entropy. Dynamic assignments of weights to system/application requirements. The effectiveness of TITAN is compared with the current schemes SDTS [23], DTMS [35], DST-WOA [36], which demonstrates the effectiveness of the system in an open environment.

IWSN data sharing security is significantly enhanced by the proposed clustered trust model that will efficiently address the myriad of limitations. The suggested approach is the interaction of success and failures, logarithmic rewards and penalties, direct trust and feedback trust to provide good security. The best feature with the method is that it can improve the level of security by detecting and utilizing SNs that will never be insecure when communicating. This implies that confidential information is shared with only trusted SNs hence the risks of unauthorized access and security attacks are reduced. The model proactively identifies and eliminates threats by constantly evaluating failed interactions. This allows using preventive measures, e.g. limited access or alerts to prevent possible data destruction. The dynamic system of rewards and penalties provided in the framework makes SNs take safe action. A high level of trust is likely to be enjoyed by individual SNs who assume responsibility in sharing data, hence making them comply with the security policy and ensure the integrity of the network. Instead, SNs with ill intentions will be punished, such as limited access, a powerful weapon to potential criminals. Also, the approach places precedence to interactions with trusted SNs using direct trust which is established by prior interaction. This reduces the probability of communication with unreliable SNs, which increases the network security.

The rest of this research paper has been structured into different sections to give a detailed analysis. Section 2 will discuss the current research studies concerning this study with references to their strengths and limitations. Section 3 shows the proposed methodology, which highlights its novelty. Section 4 outlines simulation experiments which shed light on the findings. And finally, Section 5 draws the conclusion of the research and offers possible directions of future research. This structure of organization facilitates conformity and homogeneity in the way the study methodologies, analysis and findings have been presented.

2 Related work

In this section, other models of trust in the context of the Industrial Wireless Sensor Networks (IWSNs) have been reviewed to develop a clearer picture of the current state of the art. An in-depth literature review reveals the limitations, strengths and gaps in the research of the current strategies and provides a basis upon which the new approach can be compared and confirmed. The analysis of the existing methods of building trust also demonstrates the historical developments, prevents duplication, and reveals the future lines of research. Fang et al. [9] presented an alternative by developing a trust management system called Gaussian distribution-based trust management system (GDTMS) to enhance security and performance of fog-based IWSNs. Their work addresses important challenges e.g. the minimization of the latency, the possibility to use the real-time control, the possibility to plan the resources, and the protection against inner security threats that are usual in the distributed industrial networks. The framework of the GDTMS uses sensor-node reliability to determine credibility of the sensor-node to trade off security, energy efficiency and transmission performance, which is very essential in industrial applications that require quick processing of data and low energy usage. The authors created a multidimensional selective forwarding scheme based on the grey decision -making theory to secure and simplify the transmission of data mitigating attacks by specific persons such as bad-mouthing within an organization. The technique also seals network holes and reduces the load distribution to maximize network survivability and reliability. The outcome of simulation indicates that GDTMS is more stable and robust than other related trust-based secure routing algorithms. Nevertheless, it might not be scalable in large resource limited industrial applications due to its greater computational complexity.

Yang et al. [10] presented a secure clustering framework of an IWSN in form of clustered networks named SCFTO. The protocol involves fuzzy trust estimation and outlier detection mechanism to enhance security of the network against internal attacks. In order to manage the uncertainties that are realized due to transmission in an open wireless setting, SCFTO uses an interval type-2 fuzzy logic controller that determines the reliability among sensor nodes (SNs). An outlier detection algorithm based on density is then used to enhance security by creating an adaptive trust threshold which eliminates malicious SNs during the selection of cluster-heads. To effectively select cluster-heads, the SNs with

more residual energy and smaller trust-value uncertainty are determined more highly through a fuzzy logic-based scheme, which offers a tradeoff between energy efficiency and security. The scheme is complete distributed and easy to carry out. According to performance assessments, SCFTO provides more protection against internal attacks as compared to cloud model-based and weight-based mechanisms.

Demertzis et al. (2016) introduced a security model of the Industrial Internet of Things (IIoT) on the blockchain. The framework uses deep learning-based smart contracts to prevent the increase of security threat levels in the industrial environment and to mitigate the drawbacks of existing security control methods. It facilitates safe, open communications between Industry 4.0-ready IIoT pervasive devices through real-time abnormal detection of network traffic utilizing a profound autoencoder neural network analyzing network traffic. In comparison to traditional approaches, AI is implemented at the core of the blockchain as opposed to the addition. As a result, decentralized, autonomous transactions of critical infrastructure are achievable, without relying on the central authority.

Smart contracts implement a bilateral traffic-control system which is a distributed, fault-tolerant anomaly-detection system, and provides high security with minimal computational overhead. The study is one of the earliest studies that uses deep learning enabled smart contracts in blockchain, which preconditions the development of intelligent security frameworks in IIoT environments. The deep autoencoders can further enhance the ability of the system to identify sophisticated multi-dimensional cyber threats.

The research by Rathee et al. [18] proposed a blockchain-based IIoT security model to improve transparency, data integrity, and traceability of sensor activity in the industrial processes. The framework records all sensor interaction in the blockchain and this will address unauthorized access and manipulation of data. Blockchain is used to store processed sensor data resulting in an immutable ledger enabling safe wireless communication between sensors. The simulations of the appraisal of performance of the framework were done based on the measurements of the probability of attack success, the rate of detection, the falsification resistance, and the authentication delay, and the performance is compared to the traditional security protocols. The outcomes have shown that the blockchain-based solution can greatly enhance the level of data protection and transparency, lessen unauthorized operations, and increase the detection of attacks.

Yang et al. [19] suggested a complex trust-management scheme to IWSNs, which employs Generative Adversarial Networks (GANs) to enhance safety and add resilience capabilities to IWSNs in the face of new threats. Trust models of conventional machine-learning based are still not as efficient at identifying malicious sensor nodes (SNs) as they are not labeled, and the attack patterns involved are not known. In order to handle uncertainty in sensor values, the framework uses type-2 fuzzy logic to determine SN reputation. A longer GAN-based codec structure also increases the level of trust, with a computation as high as 96 per cent detectable and the error-rate low below 8 per cent. The proposed GAN-based trust-redemption system aims to improve resiliency in the network by admitting those SNs, which have been mistaken, to the network in the future, thus not being rejected forever. The other module is the trust-adaptation which dynamically updates the trust analysis to follow the changing conditions of the industries to provide secure clustering and real time complement of data communication. The effectiveness of the framework is confirmed by the simulation results of protection against the dynamic and advanced threat, with a high detection accuracy, flexibility, and stability.

To enhance security and collaboration in an Industrial Wireless Sensor Networks (IWSN), Khan et al. [23] came up with the Secure and Dependable Trust Assessment Scheme (SDTS) with the aim of strengthening the security against severe internal attacks such as; on–off and bad-mouthing attacks as well as garnished attacks. SDTS evaluates the trustworthiness of a sensor node (SN) based on direct trust, indirect trust, data-communication trust and misbehavior in the SNs. It incorporates a dynamically adaptable trust range which is responsive to the application requirements. The network is partitioned into optimum clusters and abnormal attenuation variables in addition to dynamic sliding windows are implemented to overcome the natural interference and malicious intrusions. The computations in trust are founded on behavior-pattern analysis, the rate of misbehavior, misbehavior frequency and a misbehavior weighted and formula. The detection precision is 91% false-positive and false-negative ratings are 2.5 and 2 percent respectively and the energy use is high (0.40 J) and bandwidth is high (108Kbps) at the worst case when half the SNs are malicious. SDTS has better rates of detection and accuracy as compared to more recent state-of-the-art approaches, where its false positives are lowered by over 80 percent and its detection rates are enhanced by up to 23 percent.

Kumar et al. [24] has presented Energy Efficient Unequal Multilevel Clustering (EEUMC) algorithm on the underwater wireless sensor networks. The idea is to optimize the use of energy and enhance efficiency in data transmission to be used in the maritime tasks like monitoring the environment and exploring its resources. EEUMC also is used to extend the network lifetime by clustering sensor

nodes in unequal multilevel clusters. The grouping is made by the residual energy of each node and the distance led to the sink. This organization assists in efficient data routing and transmission minimization which is energy consuming. Heads of clusters (CHs) are dynamically chosen. This will be selected according to the energy level and distance of the node to the sink. This dynamic decision enables aggregation of data in an adaptable manner, removes redundant data and saves on energy. EEUMC ensures that energy consumption is balanced across sensor nodes even differently (when conditions in the network change) by routing around energy-efficient paths and adjusting aggregation strategies. Simulation finding indicates EEUMC is by far better than traditional clustering schemas in network surviving time and data transmission speed. This is a disadvantage of the model because it re-clusters very often. This is the case since the cluster relay points consume a great amount of energy, particularly at the varying water levels.

Mir et al. [26] proposed a protocol clustering (UDCOPA) (Unequal Distributed Clustering based on Objects Performances Aggregation), which was designed to enhance the energy consumption, scalability, and allow the network to live in WSN-based IoT networks. Unlike conventional clustering schemes whereby these schemes apply a fixed radius to all the cluster head (CHs), UDCOPA uses adaptive clustering radius (ARC) that corresponds to the characteristics of each CH such as the remaining energy and the distance between the BAS and the CH. The ARC is based on a multicriteria modeling and allows each CH to vary its radius on its own depending on its energy and spatial location relative to the BS. The results of simulation provide that UDCOPA is more efficient than current models such as DCOPA and LEACH, extending the network lifetime by 62.61% compared to LEACH and by 32.72% compared to DCOPA. The unequal clustering strategy balances network load by creating smaller clusters around the BS and larger ones more distant, hence saving energy. However, this solution can result in CHs near the BS being chosen more frequently, resulting in more energy usage, with CHs more distant possibly receiving more communication cost.

Another suggested routing protocol by Ravikumar et al. [32] is the one that is energy-saving and focuses on optimizing the sustainability of Industrial Wireless Sensor Networks (IWSNs) in industrial settings that are complex. The biggest problem to IWSNs is unpredictable environmental conditions and high-power consumption. The protocol addresses the latter concerns through the use of a grid system (region-based) and a heterogeneous placement of mobile sensor nodes (SNs). The base SN in any grid is chosen depending on the remaining energy and distance to other SNs which is a parameter that balances the energy consumed and enables successful transfer of data. A hybrid optimization algorithm COOT- HOA identifies the most optimal SN of each grid. In addition to this, LSTM deep-learning model predicts future path of moving mobile SNs by predicting direction of the SNs which allows the generation of effective routing paths. To ensure communication remains energy-aware, the protocol employs ESPRIT (Estimation of Signal Parameters via Rotational Invariance Technique) in order to create an active area between sending and base SNs. The tests have been conducted on the protocol and the findings reflect that it has a 94-percentage packet delivery ratio, a 7 percent ratio packet loss and an average remaining energy of 9.5 10 by J and has an average throughput rate of 3.4 Mbps.

Another hybrid trust management structure was proposed by Khan et al. [37] to enhance the security and reliability of IWSNs, the Multi-layered Assessment System for Trustworthiness Enhancement and Reliability (MASTER). The key goal of MASTER is to improve the level of trust through the combination of data-based and communication-based trust assessment, and, therefore, provide the successful prevention of malicious attacks and internal ones. The architecture of the system is clustered where the trust is measured within three hierarchies which are: cluster members (CMs), cluster heads (CHs) and base stations (BSs) and it is calculated dynamically through weighting mechanism which give more emphasis to recent interactions. Experimental findings indicate that MASTER has a 97 percent malicious behavior detection rate in the situation where 30 percent of the SNs have been compromised and this compares to some of the trust models currently in existence. Secondly, the framework is energy saving because it reduces the number of unneeded transactions but ensures high throughput of 150 kbps even in unfavorable network conditions. Nevertheless, it can be rather limiting on high-dynamics environments where the SN behavior varies rapidly due to reliance on precise estimates of trust.

As a solution to enhancing trust estimation in clustered WSNs, Khan et al. [34] introduced a trust management scheme, called the Reliable Trust Model (RTM), a weight-based scheme. The principal idea of RTM is to increase security, reliability, and decision-making by integrating communication-based trust (direct and indirect) and data-based trust, but overcome the drawbacks of the current methods, including the waste of communication and poor use of resources. RTM embraces data trust to reflect data consistency, which together with communication trust allows making trustworthy collective decisions. To minimize even more resource usage, RTM uses hybrid clustering strategy which reduces the number of inter-cluster communication.

Adaptive weighting is applied to the assignment of the issue of weight depending on the specific needs of the application, and it offers flexibility and adaptability. According to experimental assessments, RTM exists as either better or similar to the traditional models, including LDTS [2], LWTM [4], and ADCT [3] in their ability to detect malicious SNs by 15.78 per cent, the accuracy of selfish behavior detection, and cooperation. In addition, RTM also cuts communication overheads by up to 98 percent in networks consisting of 500 SNs and 100 clusters over ADCT as well as other comparable schemes. Although its performance is very effective, the performance of RTM is very much dependent on proper weight allocation that can be influenced by alteration of network conditions.

The hybrid metaheuristic protocol, which was developed by Dinesh et al. [33] to improve the energy efficiency and security in a hostile environment, is called GWO-MSLO, and is used in a Wireless Sensor Networks (WSNs). The main aim is to eliminate the energy and security constraints of WSNs through Grey Wolf Optimization (GWO) to cluster sensor node (SN) and an improved Sea Lion Optimization (SLO) to provide efficient routing. To provide the security of data transmission, Elliptic Curve Cryptography (ECC) is used with the help of a certificate-less aggregate signature algorithm that will ensure the conditional privacy and protection against malicious attacks. The protocol also introduces a Protection Trust Mechanism to assess SN trustworthiness in terms of effective packet delivery and hence offer trusted and secure communication paths. Simulation of NS3, the GWO-MSLO protocol performed better than the current protocols with 12 percent saved energy, 8 percent improvement in the ratio of packet delivery, 15 percent decreased end-to-end delay and 11 percent improvement in the network lifespan and throughput. Such outcomes have shown an increase in security and resource optimization. Nevertheless, the protocol has shortcomings related to the use of fixed SNs and absence of sophisticated data aggregation methods.

Khan et al. [35] admitted the topical problem of Sybil attacks in WSNs when a malicious SN creates several identities in order to compromise network security and trust. They came up with a Dual Trust-based Multi-level Sybil (DTMS) attack detection model where a multi-tier trust verification system is executed at three levels of the network: Cluster Manager (CM), Cluster Head (CH) and Base Station (BS). Trust values are determined at every level, which is based on SN behavior and uses both communication trust and data trust to provide accurate identity and location verification. DTMS uses dynamic reward-penalty mechanism to analyze the intensity of SN behavior and experiences data aggregation methodology to minimize energy use. Simulation findings show that DTMS can identify Sybil SNs with 100% detection rate, and shows significant improvements on detection accuracy, energy consumption, network life and packet loss as compared to the currently used models. The CH evaluates the trust of its members, separating malicious SNs, and the BS validates the trustworthiness of the CH and organizes secure data forwarding. Although DTMS has strong features in Sybil detection and network performance, the further research can streamline the use of the system in a highly dynamic or large-scale WSN deployment where high mobility or density can affect multi-level trust calibration.

Singh et al. [38] address the current problem of wormhole attacks in clustered WSNs, particularly in the frameworks of the IoT, and work on the two aspects of network security and energy efficiency, which are essential to the resistance of the network. Conventional clustering strategies have optimized the energy consumption without paying much attention to security weaknesses. Though the earlier trust models tried to identify the packet-dropping SNs based on the observation of the packet forwarding behavior, the current study takes a different approach using the Ant Colony Optimization (ACO) principles. It relies on pheromone concentration rather than promiscuous packet monitoring as a method to provide direct trust, which reduces packet loss. The model suggested computes the trust by the pheromone level between SNs, producing a strong and consuming less energy model, which is not needy of standard packet monitoring, thereby decreasing the overhead and detection delay. The model, tested under Network Simulator 2.35, provides better results than current model like the ESRT trust model and significant better results were achieved in metrics like packet delivery ratio, throughput and energy consumption. This ACO-based trust model is effective in detecting malicious SNs with minimum energy consumption and does not need packet forwarding monitoring, which makes it an ideal choice in energy-representative internet of things. Despite its success, it requires further enhancement to cover scalability in highly dynamic or heterogeneous networks of the IoT.

A trust-aware optimization framework of WSNs introduced by Singh et al. [36] addresses smart healthcare and IoT systems applications. Understanding the key importance of trust to achieve efficient data transmission among sensor nodes (SNs), the authors introduced the DST-WOA solution that integrates Dempser-Shafer Theory (DST) to trust-based clustering with Whale Optimization Algorithm (WOA) to energy-efficient routing. The structure improves network reliability and energy consumption by including trust measures in the cluster formation process and route selection. The simulations with MATLAB prove that DST-WOA is superior to the current models, such as TBSIOP, SQEER,

and SSDBN-TAA; it has a 23-percent longer network lifetime, a 22-percent higher level of energy efficiency, and a 4-percent better throughput. The findings show a high resilience to the usual WSN challenges like trust related attacks, high power consumption, and inefficient communications thus enhancing the overall network performance in dynamic environments. The method, however, has the drawback of not being able to sustain the true trust assessment in highly dynamic networks and it operates under the assumption of homogeneity of sensor nodes, which can restrict its scalability. Future research of the work should be aimed at improving accuracy of trust in dynamic situations, heterogeneous node support, and scaling and resilience proven on real-world deployments.

Baharloo et al. [39] addressed the issue of trust and reliability in ad hoc network in IoT by developing a three-valued (3v) model of trust that considers smart settings. Through three-valued logic, this method is used in dealing with uncertainty in complex trust relationships, where the traditional binary models of trust fail to work effectively, particularly those that involve social commitments. In order to substantiate this model, the authors developed a new modeling language, 3v-TCTLC, that is based on the traditional two-valued logic provided with an additional trust state. Furthermore, the MACMAS-interactor tool was improved to accommodate 3v-TCTLC, enabling the implementation of it in an IoT environment. The model was proven to be effective in a highly uncertain environment as indicated in case studies of smart healthcare monitoring and smart home applications. The suggested model exhibits the benefits of integrity, scalability, and flexibility, which is more efficient in time and space than traditional trust management strategies. These results suggest that the model has been adequately adapted to trust management in efficient future smart systems. Future studies would be able to extend this framework to a broader scope of IoT ad hoc applications that would further increase the dependability of interconnected smart environments.

To enhance the security of IoT-WSN networks, Kumar et al. [40] developed a route selection model based on security considerations designed to minimize the risk of compromised data integrity of data at critical points where security data is required like in health care and industrial automation. To overcome the weaknesses of data transmission, the model combines the ITrust mechanism of detecting malicious sensor nodes with an Improved Grey Wolf Optimization (IGWO) algorithm of trust-based routing. IGWO groups sensor nodes according to trust, remaining energy and connection requirements and allows the selection of secure and energy-optimal communication paths. The proposed solution provides an end to end secure routing architecture, and has superiority over the current frameworks like IOP and SQEER in power-use, transmission latency, and information integrity. The authors also mention the possibility of incorporating the emerging technologies like artificial intelligence and blockchain to improve the flexibility in dynamic IoT-WSN environments. The industrial application of modeling has shown to enhance operational efficiency, cost-effectiveness, and reliability of communication, which is why the model can be an effective and scalable method to secure IoT-WSN deployments. Table 1 offers a comparative study of the current WSN trust models and their shortcomings.

A new framework known as DL-HEED that was proposed by Juwaied et al. [41] will improve the classical HEED protocol by adding deep learning to enhance energy efficiency and increase the lifespan of heterogeneous wireless sensor networks (WSNs). The major value of the work lies in the fact that it proposes a novel intelligent, context-sensitive cluster head selection method involving explicit modeling of the relational structure of the network, which is not typical of the heuristic-based methods. Here, the WSN can be represented as a graph, where a Graph Neural Network (GraphSAGE) architecture is used to keep both the node-level and topological data. To make the model, the complete list of features, such as residual energy, node degree, coordinates, distance to the base station, and signal strength, is used to estimate the node suitability scores. Such learned scores are then incorporated into the iterative action of clustering of HEED that allows more balanced and adapting cluster formation. The outcomes of the simulation of different network size demonstrate significant gains in network lifetime, residual energy, ratio of packet delivery and end-to-end latency; the gains being significant in dense network cases. Consequently, DL-HEED is a scalable and robust solution to next generation IoT-enabled WSNs clustering. Nevertheless, the authors note that the computational and communication cost associated with the GNN component is a serious drawback, which is why future research on the lightweight and realistic applications should be conducted to apply in the real world.

Juwaied et al. [42] went ahead to extend machine learning-based clustering by proposing two improved versions of the Distributed Energy-Efficient Clustering (DEEC) protocol; DEEC-KNN and DEEC-KM, in particular, of heterogeneous WSNs. The main aim of the work is to add probabilistic and energy-aware cluster head selection on DEEC with the addition of spatial awareness and adaptive clustering by the means of lightweight unsupervised learning methods. The DEEC-KNN strategy uses the K-Nearest neighbors algorithm to dynamically allocate sensor nodes to cluster heads, both in terms of proximity and remaining

Table 1 Comparison of WSN Trust functions

Trust management Scheme	Observation	Trust function	Limitations
TMA [1]	Only communication trust	$\frac{S}{S+U}$	Not Scalable, Less Robust Against Internal Attacks, static trust function, Not Consider Effect of Environmental Factors, Limited Adaptability To Application-Specific Needs, Non-flexible trust domain, no punishment and reward system
LDTS [2]	Only communication trust	$\frac{S}{S+U} \times \frac{1}{\sqrt{U}}$	Static trust function, Poor Scalability, Static Clustering Structure, Increased Communication Overhead, CH Overload, Reduced Network Lifetime, vulnerable to various attacks such as On–Off attack, Non-flexible trust domain, no reward system, fixed size logical time window
GTMS [5]	Only communication trust	$\frac{S^2}{(S+U)\times(s+1)}$	Not consider data trust and energy trust, no againg factor and damping factor, high communication overhead, equal size clustering, less scalable, Non-flexible trust domain, no punishment and reward system, fixed size logical time window
ADCT [9]	Communication and Data trust	$\frac{S}{S+U}^{(1-\frac{S}{S+U})\alpha}$	no againg factor and damping factor, Static Clustering Structure, Increased Communication Overhead, CH Overload, Reduced Network Lifetime, vulnerable to various attacks such as On–Off attack, fixed size logical time window
LWTM [21]	Only communication trust	$\frac{(S^{G1}+S^{G2})}{(S^{G1}+S^{G2}+U^{G1}+U^{G2})} \times \frac{1}{\sqrt{P1\times U^{G1}+P2\times U^{G2}}} \times (\frac{p1\times S^{G1}+p2\times S^{G2}}{1+p1\times S^{G1}+p2\times S^{G2}})$	Not consider data trust and energy trust, no againg factor and damping factor, high communication overhead in multihop topology, equal size clustering, less scalable, Non-flexible trust domain, fixed size logical time window
ETERS [17]	Communication Trust, Data trust and Energy Trust	$\mathrm{R}\times \frac{S+1}{S+q\times U+2}^{\frac{U+1}{S+q\times U+2}}$	No againg factor and damping factor, high communication overhead in multihop topology, equal size clustering, less scalable, not consider various misbehaviours, No optimal CH selection, not consider link quality, not consider signal strength, not consider fitness score, weak trust function
SDTS [23]	Communication and Data trust	$T_{x,y}(\Delta t) = \left[T_{max} \times \left(\frac{S_{x,y}(\Delta t)}{(S_{x,y}(\Delta t)+q\times U_{x,y}(\Delta t))}\right) \times \frac{1}{\sqrt{U_{x,y}(\Delta t)+1}} \times \phi^{S_{x,y}(\Delta t)}\right]$ $DT^{D}_{x,y} = \left[T_{max} \times (\frac{Sx,yD(\Delta t)+1}{(Sx,yD(\Delta t)+q\times Ux,yD(\Delta t)+2)})^{\left(\frac{Ux,yD(\Delta t)+1}{Sx,yD(\Delta t)+q\times Ux,yD(\Delta t)+2}\right)}\right]$	No againg factor and damping factor, high communication overhead in multihop topology, equal size clustering, less scalable, fixed size logical time window, No optimal CH selection, not consider link quality, not consider signal strength, not consider fitness score, weak trust function

Table 1 (continued)

Trust management Scheme	Observation	Trust function	Limitations
ETDMA [29]	Communication trust with 4 trust features (CLR, CWR), CFD and Reward)	$w_1 \times \left[\left(\frac{S_{x,y}(\Delta t)+1}{(S_{x,y}(\Delta t)+U_{x,y}(\Delta t))+2} \right) \times \left(\frac{n-(S_{x,y}(\Delta t)+U_{x,y}(\Delta t))}{n} \times e^{\frac{-U_{x,y}(\Delta t)}{n}} \right) \right] + w_2 \times \left[\left(\frac{\sum_{j=1}^{z} T_{x,j} \times T_{j,y}}{\lvert z \rvert} \right) \right]$	No againg factor and damping factor, high communication overhead in multihop topology, equal size clustering, less scalable, fixed size logical time window, No optimal CH selection, not consider link quality, not consider signal strength, not consider fitness score, weak trust function
MASTER [37]	Direct trust and Indirect trust	$T_{x,y}(\Delta t) = \left[10 \times \left(\frac{S_{x,y}(\Delta t)+1}{(S_{x,y}(\Delta t)+U_{x,y}(\Delta t))+2} \right) \times \frac{S_{x,y}(\Delta t)}{S_{x,y}(\Delta t)+1} \times \frac{1}{\sqrt[2]{\varphi \times U_{x,y}(\Delta t)}} \right]$	No againg factor and damping factor, high communication overhead in multihop topology, equal size clustering, less scalable, fixed size logical time window, fixed trust domain, No optimal CH selection, not consider link quality, not consider signal strength, not consider fitness score, weak trust function
RTM [34]	Considers communication trust as well as data trust, focus on accurate trust values	$\left(\frac{S_{x,y}(\Delta t)}{(S_{x,y}(\Delta t)+U_{x,y}(\Delta t))} \right) \times \frac{1}{\sqrt{\eta \times U_{x,y}(\Delta t)+1}} \times \phi^{S_{x,y}(\Delta t)}$	No optimal CH selection, not consider link quality, not consider signal strength, not consider fitness score, weak trust function, No againg factor and damping factor, high communication overhead in multihop topology, equal size clustering, less scalable, fixed size logical time window
DTMS [35]	Communication and Data trust	$T^{C}_{CH,CM} = \frac{3\times(S+1)}{S+U+2} \times \frac{1}{\sqrt{\rho \times (U+1)}} \times \bar{\mathrm{R}}$ where $\bar{\mathrm{R}} = \left\{ 1 - \frac{1}{(S+1)} \right\}^{\alpha}$	Suitable for few attacks like sybil attack, No againg factor and damping factor, high communication overhead in multihop topology, equal size clustering, less scalable, fixed size logical time window, No optimal CH selection, not consider link quality, not consider signal strength, not consider fitness score, weak trust function
DST-WOA [36]	Employ Dempster-Shafer Theory (DST) for trusted clustering and the Whale Optimization Algorithm (WOA) for routing	$\mathrm{A1(Y)} \oplus \mathrm{A2(Y)} = \frac{1}{W \times [A1(Y)A2(Y)+A1(Y)A2(Y'')+A1(Y'')A2(Y)}$	High Computational Complexity, narrow security focus, lack of practical validation, Limited Accuracy in Dynamic Environments, No againg factor and damping factor
TITAN (Proposed)	Consider Robust Direct Trust, Indirect Communication Trust, Data Trust, energy factor and fitness score, quality and intensity of interaction	$Tx,yC(\Delta t) = \left[R \times \lambda_1 \times \left(\frac{Sx,yC(\Delta t)+\alpha}{(Sx,yC(\Delta t)+Ux,yC(\Delta t))+\beta)} \right) \times \frac{1}{\sqrt{\psi \times Ux,yC(\Delta t))}} \times \left[\lambda_2 \times \frac{Sx,yC(\Delta t)}{Sx,yC(\Delta t)+\gamma} \right]^{\widehat{r}} \times \frac{1}{\sqrt{1+\delta A_{(x,y)}}} \right]$ and $Tx,yD(\Delta t) = \sum_{i=1}^{Z} w_i \times q_i \times loglog\left(1 + \frac{Sx,yD(\Delta t)}{1+Ux,yD(\Delta t)}\right) \times \frac{1}{1+E_i \times D_i}$	**Advantage:** flexible trust domain, Employ optimal CH selection, consider link quality and signal strength, consider fitness score, Robust trust function, Employ againg factor and damping factor, dynamic logical time window, consider multi-trust approach, flexible punishment and reward system well suited for industrial applications

energy and hence enables cluster formation to be locality-aware. Depending on it, the DEEC-KM version uses K-Means to form spatially even clusters, and the most energetic node in each cluster is selected as the cluster head. Simulations with MATLAB have shown that with the traditional DEEC protocol performance can be significantly improved, by as much as 110 percent higher packet delivery ratio, longer network stability, and greater conservation of residual energy and more balanced cluster sizes. These findings attest to the suitability of machine learning-controlled adaptive clustering in improving the reliability and scalability of WSNs. The research, however, assumes that the nodes are deployed in a fixed manner and communicate without fading, which creates extra computation costs in terms of machine learning. Such constraints have highlighted the necessity to validate dynamically, in large scale, and in realistic WSN settings in the future.

A thorough survey of available trust models demonstrates that there are some significant drawbacks to the applications of trust in the case of the Industrial Wireless Sensor Networks (IWSNs). The majority of existing solutions rely on equal clustering and fixed trust computation which is not very useful in the dynamic industrial setting where energy efficiency, communication reliability, scalability, and security need to be weighed carefully. Most models do not have energy aware trust mechanisms, do not offer much flexibility to changing node behavior and offer weak protection against other more advanced attacks like Sybil, sinkhole, wormhole and collusion attacks. In addition, other important elements like delay in propagation of trust, variation in density of the network, and node mobility are also often ignored. Heterogeneous device type support and role-based trust differentiation, lightweight architectures that fulfill strenuous industrial latency and resource requirements are under-supported.

Despite the fact that the current literature offers important insights to trust management in WSNs and IoT-based application, the literature fails to consider a number of parameters that are necessary towards effective and dynamic trust modeling in IWSNs. Specifically, unequal clustering and fitness-based evaluation, where residual energy, link quality, signal strength, and distance to the base station are used as inputs, are seldom used towards effective sensor node assessment. Also, the development of multi-factor trust assessment, which encompasses communication trust, data trust and energy trust is still in its early stages, making the trust decision less accurate and responsive. Most models do not also have advanced mechanisms, such as dynamic reward and punishment policies, dynamic trust update, outlier detection and aging considerations to reject obsolete information in trust. These weaknesses reduce the capacity to determine unreliable nodes with great precision and undermine the general network resilience. It is of significant importance to address these gaps in order to create secure, robust and energy efficient IWSNs that can function efficiently under the resource limited environmental conditions and withstand the dynamic security threats.

2.1 Problem formulation

Considerable research work has already been accomplished in the development of trust models for IWSNs, but some of these limitations and knowledge gaps still exist. Existing trust models [33–40, 43–50] have demonstrated promising performance in energy efficiency, security, and network performance. The important parameters which are required for adaptive and accurate trust modeling are yet to be fully explored. Existing literature only discusses elementary trust metrics like communication trust, energy trust, link quality, and SN distance to the BS but doesn't include vital metrics such as dynamic aging factor, damping factor, multifactor trust, dynamically adjustable SV-LTW, and optimal CH selection that consider the global evaluation of SNs [9, 10]. Moreover, most trust models [2, 5, 9, 17, 21, 34–37] also lack consideration for advanced mechanisms, like unequal clustering based on residual energy and fitness scoring. It would potentially optimize network longevity and performance by prioritizing resource-rich SNs for sensitive tasks. This knowledge gap makes existing models susceptible to shortcomings in adaptability and scalability, leading to inefficient trust calculations in dense or industrial IoT applications [15]. Moreover, the absence of a dynamic ageing parameter makes obsolete or unnecessary information be retained within the calculations that build trust, potentially enabling compromised SNs to remain undetected in the future. Our proposed trust framework fills these gaps by incorporating trust factors. However, there exist vulnerabilities that could result in compromised adaptive, multi-factor models coupled with tools such as dynamic punishment & reward mechanisms and outlier filtering mechanisms that can help precision and robustness. The inclusion of these hitherto unaccounted parameters in the framework aims at enhancing the accuracy of unreliability identification in unreliable SNs and also reducing the false trusts. The issue of these knowledge gaps, which is important to enhance trust modeling in IWSNs. This facilitates reliable, secured, and robust networking operation with respect to competing with the demands of industrial IoT applications under changing security threats [18, 19]. These models need to balance security, reliability, and energy efficiency without imposing excessive computational overheads [23–26]. The identified research challenges in the ZigB gaps point towards the need for innovative and reliable trust mechanisms which can adapt

themselves accordingly in the growing industrial settings of strong security and highest performance. The key challenge is the design of a lightweight trust model that can provide real-time decision making [32]. It shall integrate novel predictive trust assessment algorithms, adaptive real-time threat countermeasures, and energy-efficient protocols to maximize network lifetime [23]. Besides, the trust model should be scalable, support a huge number of SNs and be resistant to a large range of cyber-attacks both external and internal attacks [33, 33]. These are going to be addressed by incorporating different trust measures, including direct and indirect trust, behavioral. It analyses reputation systems and combines them into one framework [35, 38, 49].

2.2 List of assumptions

Our proposed scheme, called TITAN, operates on a number of foundational assumptions in order to enhance efficiency and reliability in IWSNs. The SNs are fixed and agglomerated into clusters [24] of various sizes using established methodologies, wherein each SN is able to its cluster through information exchanging. The OCREA algorithm will select resourceful CHs that are responsible for managing the cluster. activities. It keeps track of records regarding the SN identities, locations, and energy levels and forwarded aggregated data to the BS for final decisions. Each SN has a unique identifier and spatial coordinates to enable communication. SNs are homogeneous in energetic level, buffer size, processing capacity, and interfaces, and each interaction spends 0.009217 of energy. CHs play a critical role within a cluster. Within the same cluster, they have a larger communication range than other SNs and enjoy higher power. These CHs are responsible for calculating the trust scores of SNs to enable better decision-making. The BS works as the main controller unit is provided with enough resources and is secured against internal attacks. It initializes the trust values for the SNs and handles requests from monitoring centers. Being the main command authority, the BS can replace any malicious SN with a reliable one, and assign unique identities to the SNs. This will improve the security of the communication mechanism and protect it against any outside threats. Moreover, the important management strategy [2] applied for generating the secure communication links is to ensure the values of trust. will remain secure. Trust levels extend from 0 through R, offering simplicity, detail, and optimization, achieving the smallest dissemination and memory overhead. The trust threshold is chosen at half of the maximum value, considering that all SNs above the threshold are trustworthy. A The dynamic logical timing window [34] monitors interactions, assessing SN experiences. All SNs are modeled as stationary and fixed. Various Misbehaviors, like packet drop attacks or misinformation dissemination, are detected and prevented. Trustworthy SNs, source SN, CHs, BS, and destination SNs, are assumed to behave selfishly, focusing on optimizing packet transmission, processing, and maintaining accurate forwarding tables. Selfish SNs that might drop packets or give erroneous routing directives, these effects are balanced through monitoring the behaviors and the data being sent through trusted paths, thereby maintaining the data throughputs in the networks and integrity.

3 Proposed method

The proposed IWSN network is separated into unequal clusters in order to deal with large amounts of data effectively based on grouping devices into clusters of different sizes. Inequal and unbalanced clustering configuration enhances the process and management of information within the network and provides more reliable and scalable operations resulting to enhancing better and faster decision-making [25]. Equal size clustering cannot work effectively in IWSNs because unequal clustering assigns the data load based on cluster size and equalizes the use of energy among SNs [26]. The strategy avoids fast consumption of energy in larger groups, enhances data processing speed, and increases network duration and is therefore suitable to IWSNs. TITAN has two levels: intra-cluster (Level 1) and inter-cluster (Level 2). At Level 1, within every cluster, TITAN computes trust in permitting the communication between the group heads (GHs) and group members (GMs). In this case, SNs are able to interrelate directly to each other to build trust by sharing data. In the case of indirect trust, GHs send request packets to all GMs. TITAN is also efficient on the basis of its unequal clustering design, which allocates part of the load of data to smaller clusters to preliminarily process it. This helps to relieve the congestion of high populated clusters and guarantee smoother data flow. Level 2, which deals with trust between clusters, involves the BS and GHs in TITAN. Information in larger clusters is first digested in smaller clusters before it is sent to the BS to distribute the load and ensure energy consumption is efficient.

Both the levels are using the dual strategy of TITAN which takes into consideration both, the direct trust and the indirect one on the basis of feedback and thus make the network more accurate in identification of intrusions. Gateways Hosts (GHs) determine the score of trust at the intra-cluster levels and the BS at the inter-cluster levels. In order to increase the security of the IWSN, TITAN applies one of the key management strategies [2, 27] to encrypt the information of trust, where each score is encrypted as an unsigned integer, and the range of values lies within a predetermined set. This is a

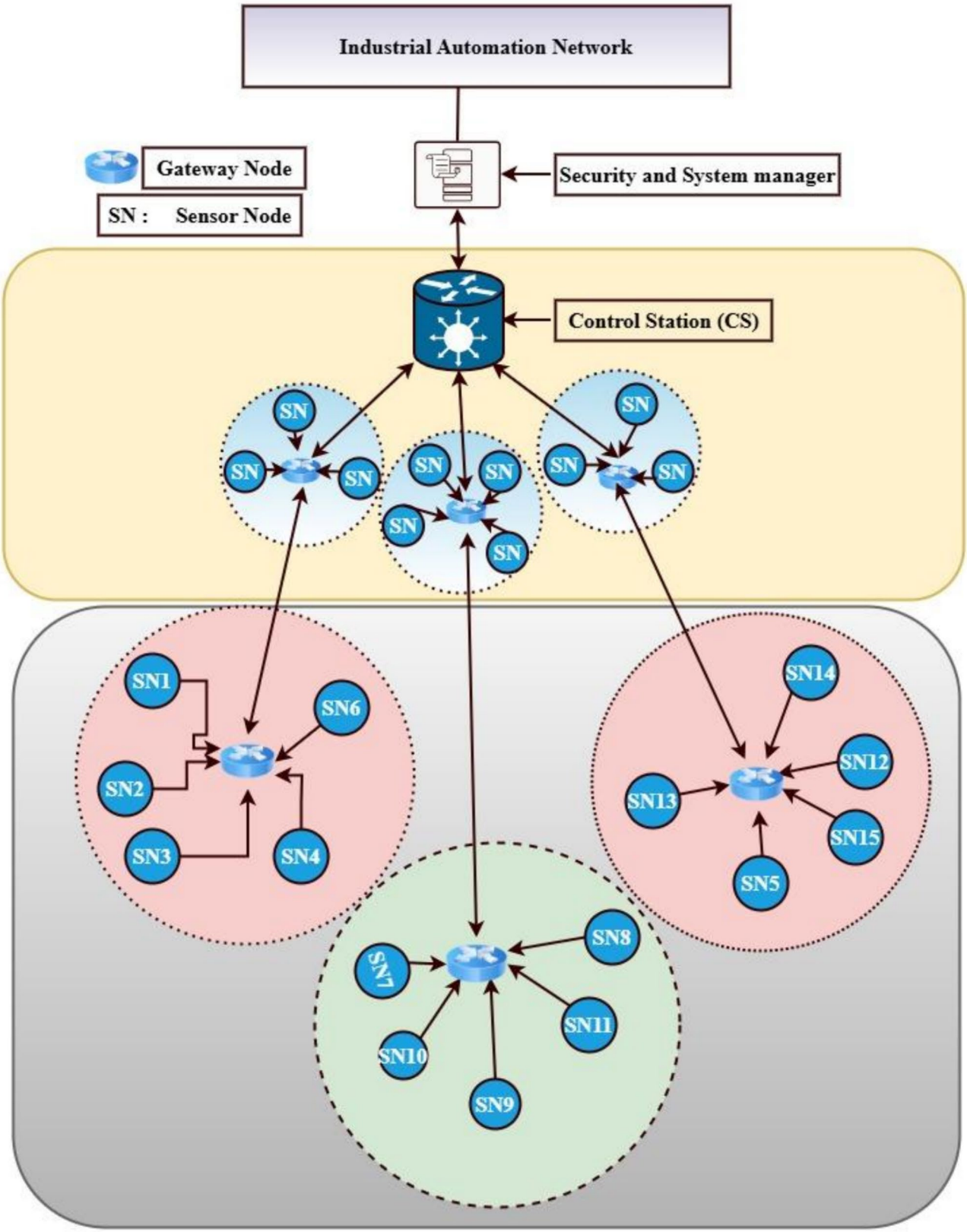

Fig. 2 Framework of proposed method

successful way of lowering the transmission and power costs as it lowers the data bits per communication. TITAN therefore uses a SV-LTW [34] to keep track of the trust levels every now and then and records interactions between SNs, GHs and the BS. As the new interactions occur, the old logs in the SV-LTW get updated thus it is only the most recent activities that affect the trust calculations. The dynamicity of the SVLTW helps TITAN to determine collaborative and non-collaborative activities within SNs. On a regular basis, the SV-LTW moves forward, forgetting outdated information and holding on to the most relevant interactions to ascertain trust adequately. Also, TITAN maintains a whitelist of trusted SNs that are allowed to participate in network monitoring and routing and a blacklist of SNs that are not allowed to sense data and transmit. Figure 2 demonstrates that the management of trust has a structured framework to address, which enables TITAN to be easily scaled to other network sizes and environments. The unequal clustering and distributed trust evaluation of TITAN enable it to be flexible and highly successful. It allows scaling effectively and merges with bigger networks and provides consistent, high-performance results. The proposed scheme trust assessment is divided into subsequent subsections as enumerated below.

Table 2 Threat model and corresponding detection and mitigation mechanisms in TITAN

Attack type	Detection feature(s) Used	Expected symptom in network	Mitigation action in TITAN
Packet dropping attack	Packet Delivery Ratio (PDR), End-to-End Delay, Throughput	Reduction in trust score, logarithmic trust penalty, isolation of malicious node	Reduction in trust score, logarithmic trust penalty, isolation of malicious node
Dissemination of misleading information	Data conformity, sensual deviation, data credibility	Incorrect sensor readings, wrong routing or control decisions	Data trust degradation, exclusion from aggregation and decision process
Bad-mouthing attack	Feedback inconsistency, indirect trust verification, reputation trend analysis	False negative feedback against legitimate nodes	Feedback filtering, cross-validation using neighboring nodes, trust correction
Blackhole attack	Packet forwarding behavior, route consistency, throughput drop	Sudden and complete packet loss after route attraction	Rapid trust decay, route avoidance, blacklist entry
Greyhole attack	Intermittent packet forwarding rate, interaction history	Random packet losses, unstable trust values	Aging factor and dynamic punishment, gradual isolation
Sybil attack	Identity verification, location consistency, trust threshold violation	Multiple fake identities, routing instability	BS-level validation and permanent node removal
On–off attack	Interaction frequency, trust fluctuation pattern, sliding window analysis	Alternating cooperative and malicious behavior	Dynamic aging factor, reduced trust recovery speed
Ballot-stuffing attack	Feedback bias detection, reputation inflation trend, cross-feedback validation	Artificially increased trust of malicious nodes	Weight reduction of biased feedback, indirect trust correction

4 Attack model

Malicious SNs in IWSNs may have a devastating effect on network integrity and efficiency through internal attacks. These evil SNs track network operations and traffic and use deceptive techniques to corrupt measures of trust, impoverish resources and suppress network efficiency [12]. The below is an elaborate attack model that defines six critical situations, which describe possible behaviors and the trust evaluation techniques to be used to identify and mitigate such threats [12].

First scenario: Packet dropping attack A packet-dropping attack is one that is perpetrated by an evil SN by intentionally omitting certain packets rather than passing them on. It causes high loss of packets and disruption of relay of data. It is quite crucial to monitor such metrics as the PDR, throughput and end-to-end latency to identify such activity. SNs with a persistent poor PDR and above average latency are labeled as suspicious. Dynamic monitoring of such measures allows the timely identification and separation of packet-dropping SNs, which guarantees reliability in the delivery of data and stability of the networks.

Scenario 2: Dissipation of misleading information In this regard, malicious SNs disseminate any fake routing data or spoofed sensor measurement that might influence other SNs or the BS to make the wrong decision. This threat is overcome by reputation-based trust models. Every SN creates a score of trust that illustrates the precision and reliability of its data with time. SNs who persist in acting abnormally or spreading fake news decrease the scores of trusts. Through this, the network is able to identify and reduce wrong data transmission. This enhances the accuracy of the decision and integrity of the data.

Bad mouthing attack: Scenario 3 Bad mouthing attack can be associated with stolen SNs sending messages that falsely identify authentic SNs as malicious or unreliable to destroy their reputation and disrupt network stability. This attack

isolates real SNs and causes inefficiency in routing of data and decision making. Trust models resist such attacks with key parameters: SN behavior history to trace past performance, consistency of feedbacks to confirm reports between SNs, reputation scores depicting long term trustworthiness, data authenticity to verify integrity, and indirect trust with corroborative feedbacks of surrounding SNs. All of these parameters work together to detect discrepancies, avoid false accusations and provide the stability of the network.

Scenario 4: Blackhole and greyhole attack Blackhole attack is a malicious attack that is carried out when an SN pretends to have the optimal path to a destination in order to lure data packets and then drop them resulting in loss of data and network instability. Greyhole attack is an event in which the packets are dropped randomly and it is difficult to detect. The parameters used in trust models to detect such an attack, use behavior parameters like packet forwarding to detect SN reliability, throughput to detect successful transmission, route consistency checks to detect sudden route change, and indirect trust assessment to use neighbor SN feedback. These parameters are used to detect suspicious SNs and keep the network intact.

Scenario 5: Network infiltration through sybil attack The Sybil attack is a type of attack that takes place when an attacker SN generates many identities to intrude into the WSN, thus, breaching routing and trust regulations. Deployment matrices are important in position verification and identification evaluation to detect such attacks. Trust estimation methods evaluate the performance of SNs and put under suspicion those that do not meet a pre-determined trust threshold. The BS is extremely important in erasing Sybil SNs to maintain structural integrity of the network and keep illegal entry.

Scenario 6: On–off attack (Laupery participation) An on–off attack is a situation whereby malicious SNs switch between collaborative and uncollaborative behavior to evade detection. They are allowed to use the network temporarily only to leave abruptly and create unpredictability with regard to the data transmission. Frequency of interaction is monitored to deal with this issue by creating a benchmark of regular involvement. The SNs with abnormal engagement patterns and who do not meet the required trust levels are identified as a possible threat hence maintaining regular engagement and data consistency in IWSN.

Background: The camp has been assaulted by the French and one of the guardians appears to have removed numerous ballots from the bag and replaced them with soldiers' name tags, whose colors are akin to those displayed on their hats. <|human|> Background.

Scenario 7: Ballot-stuffing attack The camp has been attacked by the French and one of the guardians seems to have taken a large number of ballots out of the bag and to have put into it the name tags of the soldiers, which are in colors similar to those that appear on their hats.

Ballot-stuffing attack involves malicious SNs enhancing the credibility of certain compromised SNs with random positive feedback. Such SNs are artificially increased in their trust values so that they could misbehave unnoticed in such an attack. In order to identify these attacks, trust models employ feedback consistency parameters that verify that feedback is consistent with observed behavior by other SNs, reputation trends that guard against abrupt, unjustified trust increases and cross-validated trust ratings by several SNs. They are able to take into account the history of interaction and indirect verification of trust by the second sources of information. These parameters find irregularities in trust rating and give network reliability through finding biased feedbacks.
Table 2 describes various threat model and corresponding detection and mitigation mechanisms in TITAN.

4.1 Optimal cluster representative election algorithm (OCREA)

In this sub-section we present an advanced method of the effective optimal CH election. Our answer is also not similar to the previous ones [3, 4, 13], as they are based on distance measurements to select CH. It considers other essential factors like residual energy, quality of link, distance between BS and signal strength. These are also significant in good data aggregation in the direction of the drain. In addition, the previous methods may have the disadvantage of overlooking the problem of CH selfishness since low battery capacity may cause the impact of the problem to be disregarded, but on the contrary, our Optimal Cluster Representative Election Algorithm (OCREA) provides a full solution to the problem of CH selfishness. OCREA aims at optimizing the performance of WSN through the use of regular election of trustful CHs, load balancing between CHs, and the removal of the effects of malicious behavior because of the low CH battery levels. Considering the significant role of CHs in gathering and sending data to the BS, OCREA ensures reliability and continuity of data by ensuring that data is passed on to the standby CHs in case the current one fails to process sensitive data. A thorough description of the ORCEA, which is abbreviated as algorithm 1 is as

follows. The clustering approach is clearly stated by the use of inequality clustering strategy in the form of rings whereby the network space is partitioned into a defined number of concentric rings around the BS. Each ring clustering boundary is calculated by the parameters of $D_{j,min}$ and $D_{j,max}$ are based on the proportional sections of the greatest distance between each SN and the BS. This will guarantee that smaller clusters are found closer to the BS to minimize the relay loading whereas larger clusters are found further away with less forwarding load. The weights of the fitness scores w1 to w4 derived based on residual energy, link quality, distance to the BS and signal strength are not learned or optimized, to maintain the lightweight and deterministic nature of the algorithm and to ensure that the algorithm does not introduce the extra load and complexity of additional training or computation that are otherwise not feasible in resource-constrained industrial WSNs. List of symbols used is as described in Table 3.

Table 3 List of symbols and their descriptions

Symbol	Description
N	Total sensor nodes deployed
m	Number of cluster heads
E_i	Initial Energy of SNs
T	Periodic reelection interval
E_{th}	Threshold energy for CH reelection
$D_{BS}^{n_i}$	distance of n_i from BS
CH_i	i[th] cluster head
$D_{j,min} and D_{j,max}$	Minimum and maximum distances defining the range of Cluster j
$FS(n_i)$	Fitness score of node n_i
$LQ\,(n_i)$	Link Quality of node n_i
$SS\,(n_i)$	Signal strength of node n_i
C_j	Cluster j
D_{th}	Transmission threshold
$Tx, yC\,(\Delta t)$	Communication trust of SN (x) on SN(y) at time (Δt)
$Tx, yD\,(\Delta t)$	Data trust of SN (x) on SN(y) at time (Δt)
$FT_{x,y}\,(\Delta t))$	Feedback Communication Trust
R	Global maximum trust value
$Sx, yC\,(\Delta t)$	Successful Communication interaction of SN (x) on SN(y) at time (Δt)
$Ux, yC\,(\Delta t)$	Unsuccessful Communication interaction of SN (x) on SN(y) at time (Δt)
$\lambda_1 and \lambda_2$	Weight factors that adjust the impact of the success ratio and the reward term respectively
$\alpha, \beta and \gamma$	Constants for maintaining numerical stability
Ψ	Punishment factor
$A_{(x,y)}$	Aging factor
Z	Total number of interactions considered
q_i	Quality of each interaction
t_i	Time elapsed since the i-th interaction
K	sensitivity coefficient
l_1 and l_2	Dynamic sliding window
$\zeta_1 and \zeta_2$	Sensitivity coefficients
ϵ	Buffer threshold
a	Good (positive) feedback
b	Bad (negative) feedback
w_p	Weight assigned to positive feedback
w_b	Weight assigned to negative feedback
E_{CH}	Current energy level of the CH
LQ_{CH}	Link quality between the CH and the CMs
$\varnothing$	Decay constant
$f_{x,y}^{T}\,(\Delta t)$	Final trust value

Algorithm 1: Optimal cluster representative election algorithm (OCREA)

Input: Set of N SNs, Position and ID of SNs, Initial Energy of SNs (E_i), Periodic reelection interval (T), Threshold energy for CH reelection (E_{th})
Output: Set of optimal Cluster Heads { $CH_1, CH_2, \ldots\ldots\ldots\ldots CH_m$}

Step1: Deployment Phase: Deploy N SNs accurately within the designated area where N= $\{n_1, n_2, n_3, \ldots\ldots\ldots\ldots n_k\}$
Step2: Unequal Cluster Formation Phase using following substeps
Step2.1: ∀ SNs, calculate the distance from BS ($D_{BS}^{n_i}$) as follows

$$D_{BS}^{n_i} = \sqrt{x_i - x_{BS})^2 + (y_i - y_{BS})^2}$$

where (x_i, y_i) are the coordinates of SN n_i and (x_{BS}, y_{BS}) are the coordinates of the BS.
Step 2.2: Determine the maximum distance from the BS as: $D_{max} = max\ (D_{BS}^{n_i})$
Step 2.3: Divide the network area into J concentric rings centered at the BS.
For each ring j, compute the cluster boundaries as:

$$D_{j,min} = (j-1)\ \times \frac{D_{max}}{J}, D_{j,max} = j\ \times \frac{D_{max}}{J}$$

Step 2.4: Assign SN n_i to cluster C_j where $C_j = \{n_i |\ \ D_{j,min} \leq D_{BS}^{n_i} \leq D_{j,max}$, Where $D_{j,min}\ and\ D_{j,max}$ are the minimum and maximum distances defining the range of Cluster j. Clusters closer to the BS contain fewer SNs to reduce forwarding load, while farther clusters contain more SNs.
Step 3: Cluster head selection phase using following substeps
Step 3.1: for all SNs $n_i \in C_j$, *calculate its fitness score* $FS\ (n_i)$ *using following score function*

$$FS\ (n_i) = \ w_1 \times \frac{E_i}{E_{max}} + \ w_2 \times \frac{LQ\ (n_i)}{LQ_{max}} + \ w_3 \times \left(1 - \frac{D_{BS}^{n_i}}{D_{max}}\right) + \ w_4 \times \frac{SS\ (n_i)}{SS_{max}}$$

Where E_i is the residual energy of SN n_i and $LQ\ (n_i)$ is the Link quality of SN n_i normalized to [0,1]. w_i denotes the respective weights associated and Fixed heuristic weights are used. $The\ term\ E_{max},\ LQ_{max}\ , D_{max}\ and\ SS_{max}$ are the maximum possible values for energy, link quality, distance, and signal strength respectively.
Step 3.2: Select a SN as cluster head (CH_j) for a cluster j (C_j) as follows $CH_j = arg\ arg\ FS\ (n_i)$
where **arg max** refers to the argument (or input value) that maximizes a given function.
Step4: Cluster head reelection :At every interval T, monitor the residual energy of each Cluster Head j (CH_j)
Step 4.1: If residual energy of CH_j i.e. $E_{CH_j} < enrgy\ threshold\ (E_{th}$)
then Re-elect a new CH_j
for C_j by recomputing $FS\ (n_i)$ for all remaining SNs in C_j, and select: $CH_j = arg\ arg\ FS\ (n_i)$
Step 5: Data Aggregation and Transmission phase:
∀ **Cluster Head** CH_j
Step 5.1: Aggregate data from all member SNs ($n_i \in C_j$)
Step 5.2: If $D_{BS}^{CH_j} \leq$ transmission threshold (D_{th})
then CH_j transmits data **directly** to the BS.
Else, use multi-hop routing to forward the data through neighboring CHs closer to the BS.
Step 6: If any CH fails due to energy depletion (i.e. $E_{CH_j} \approx 0$)
Then seamlessly switch to the next best candidate SN in C_j using following method
$CH_j = arg\ arg\ FS\ (n_i)$
Step 7: End

OCREA has a linear complexity on runtime with respect to the amount of SNs; the computation of node fitness is only simple arithmetic computations done on each node within the cluster of the node. To choose a cluster head of a particular cluster of Nj nodes, O (Nj) operations are required and hence the overall complexity of the network is O (N), where N denotes the number of nodes. This performance can be obtained without an iterative optimization, training steps, and convergence-dependent process, so that the approach is lightweight and deterministic. OCREA also has low messaging costs in communication overhead. Only periodic local exchange of parameters like residual energy, quality of link, signal strength and distance within each cluster is allowed but not a broadcast on a network wide basis. The re-election of cluster head is only elicited at specified intervals or when the energy of a cluster head falls below a pre-set threshold, this also suppresses unwarranted signaling. Moreover, the protocol uses unequal clustering, cutting down the message congestion at the base station by establishing smaller clusters in the high-traffic areas hence restricting the control packet build-up.

4.2 Trust assessment scheme

The trust evaluation proposal uses intracluster and intercluster level combination. Intra-cluster trust assessment has the goal of determining the suitability and credibility of particular SNs in every cluster. The variables considered are the consistency in data reporting and adherence to protocols. The intercluster trust assessment on the other hand measures the credibility of the clusters on the premise of cluster contribution to the WSN and their collaboration. This consists of the review of uniformity of intercluster communicational and cooperation effectiveness. By combining these assessments, one will have an end-to-end test of the credibility of SNs and clusters. This makes informed decisions to be taken over the network access control, resource allocation, as well as data forwarding. This technique, when combined, increases the stability and the security of the industrial clustered IWSNs. The scheme of suggested trust assessment is separated into multiple subsections as will be discussed in detail below. The proposed trust model flowchart is presented in Fig. 3.

4.2.1 CM to CM evaluation scheme

In IWSN, direct trust evaluation among sensor nodes is vital for the assurance of correctness, reliability, and security of data collected and transmitted. When untrustworthy nodes are identified and removed, trust assessment enhances resource allocation to support swift responses to emergencies and helps the network maintain functionality and perform swift, effective decisions. Here we consider communication and data trust in intracluster communication. We calculate the trust about communication to verify that the nodes communicating are reliable; this will ensure timely and accurate communication of information. Data trust further investigates the dependability of data emanating from a specific SN to assess the credibility and quality of the information sensed to avoid tampering with or false readings of data. This will leverage the incorporation of these trust measures to assure the use of trustworthy data sources, optimize resource usage, mitigate the influence of compromised sensor nodes, enhance the resilience of IWSNs, and thereby improve performance in critical industrial applications. The communication and data trust of SN(x) relative to SN(y) are computed by using Eqs. (1) and (3), respectively.

$$
\begin{aligned}
&Tx, yC\,(\Delta t) \\
&= \left[R \times \lambda_1 \times \left(\frac{Sx, yC\,(\Delta t) + \alpha}{(Sx, yC\,(\Delta t) + Ux, yC\,(\Delta t)) + \beta)} \right) \right. \\
&\times \frac{1}{\sqrt{\psi \times Ux, yC\,(\Delta t))}} \times \left[\lambda_2 \times \frac{Sx, yC\,(\Delta t)}{Sx, yC\,(\Delta t) + \gamma} \right]^{\widehat{r}} \\
&\left. \times \frac{1}{\sqrt{1 + \delta A_{(x,y)}}} \right]
\end{aligned}
\tag{1}
$$

In the Eq. (1), all the terms are having a particular role in providing a good and proper calculation of the trust of SN(x) on SN(y) within time interval Dt. The communication trust is denoted by the superscript C. The gurus of the trust assessment are the number of successful interactions and the number of unsuccessful interactions S(x,y) and U(x,y). The influence of success ratio and the reward term are moderated by weighting the factors l1 and l2, so that the recommended model can be capable of increasing or decreasing these factors accordingly. The value of a, b and g is critical in avoiding numerical instability like dividing by zero which would dislodge the values of trust. The factor of punishment decreases the trust of SNs with more failures, which gives a correctional measure to the proposed model. Symbol tunes the term of the reward. The Aging factor A(X,Y) causes the effect of past interactions to diminish with time. Weight factor d controls the strengths of the last interactions on the current level of trust-a process which secures best values and demonstrates nearer to recent conduct. The A(x,y) aging factor is obtained by use of the following equation:

$$
A_{(x,y)} = \sum\nolimits_{i=1}^{Z} w_i \times t_i \times q_i \times \frac{1}{1 + k \times I_i} \tag{2}
$$

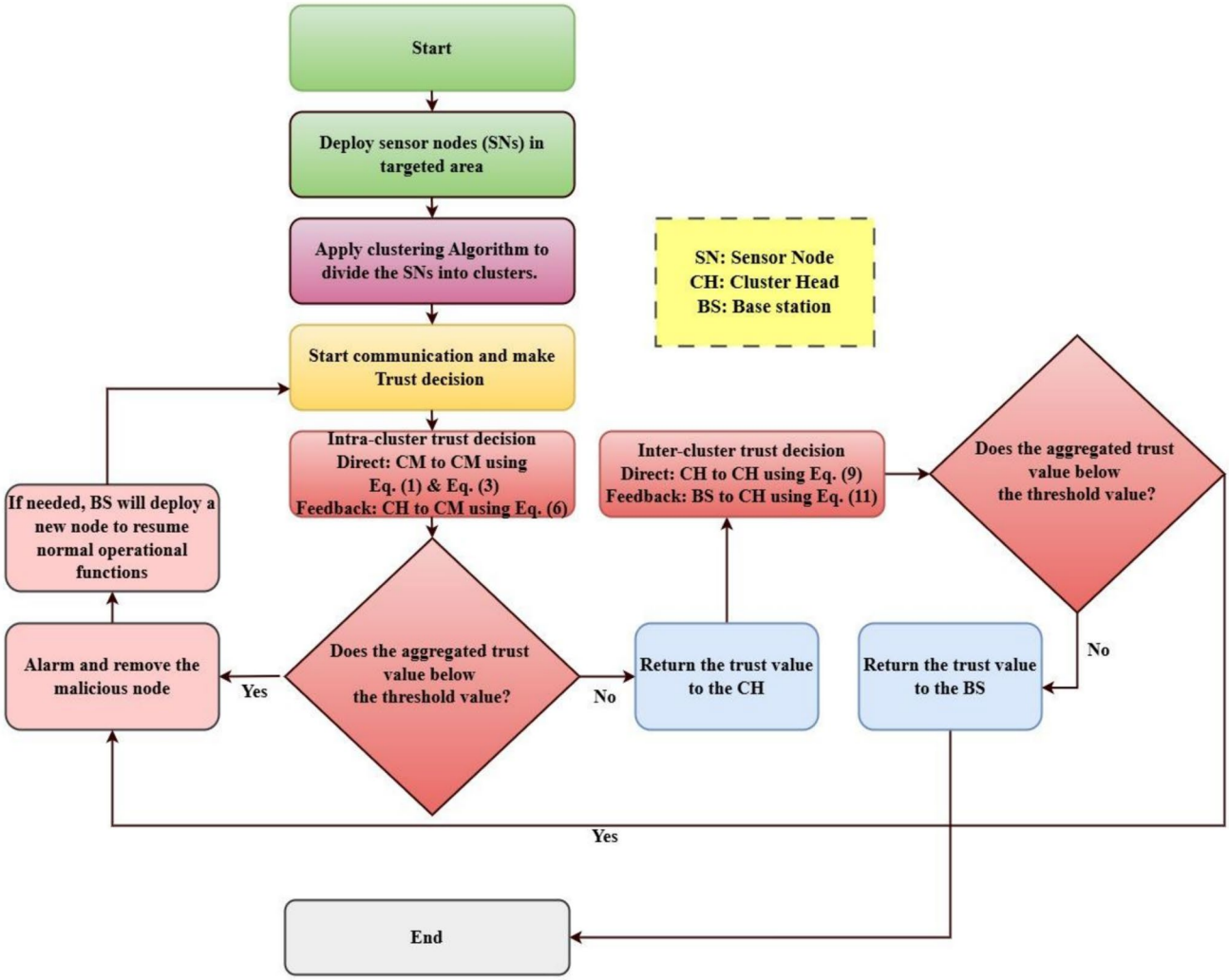

Fig. 3 Flow chart of proposed Trust model

$$Tx, yD(\Delta t) = \sum_{i=1}^{Z} w_i \times q_i \times loglog\left(1 + \frac{Sx, yD(\Delta t)}{1 + Ux, yD(\Delta t)}\right) \times \frac{1}{1 + E_i \times D_i} \quad (3)$$

There are a number of material parameters associated with the data trust. These involve the ratio between the success and failures in data interactions between successful and unsuccessful interactions, to make the trust established based on robust data interactions and one logarithmic ratio to reduce the influence of such a ratio; damping factor $\frac{1}{1+E_i \times D_i}$ to represent the efficiency of a data interaction, where an increased number of attempts Ei and delay Di decreases the value of the trust. The weight wi is given to each interaction to signify the importance with qi indicating the quality of data with different layers of significant aspects including accuracy, consistency and relevance of data exchanged. With qi in consideration, the trust model guarantees that the value of trust is not only attributed to the frequency of interaction that was successful, but also the internal reliability and utility of the information. This brings a general stability of the trust model where only high-quality effects are utilized to build trust other than to result in secure and efficient network activities. The Eq. The signification of (3) is that it establishes a more refined, accurate and life-like model of trust within IWSNs because it is able to strike a balance between success, failure, efficiency and quality of data. Thus resulting in safer and more trustworthy network systems. The adaptive sliding variable length logical time window (SV-LTW) changes accordingly to the levels of trust to the data trust and the direct communication trust. This is to show whether the actions of the SNs are good or bad. The introduction of a dynamically adjustable SV-LTW that is conditioned by trust levels of direct communication trust as well as the data trust can be considered a substantial advantage compared to the fixed-length windows. In dynamic adaptation of the fluctuations in trust, the monitoring system will achieve greater accuracy and flexibility

better than the performance of fixed time windows. The emergence of this has helped to have a better understanding of network dynamics, and thus, improve the effectiveness of anomaly detection and response measures. Simply put, it promotes a robust and flexible network infrastructure, which is capable of responding immediately to the increasing threats and do so without blacksighting its operational efficiency. The length of the SV-LTW would be computed according to the Eq. (4) where l1 is bigger than l2.

$$slidelength = \left\{ \left\{ if Avg \geq \frac{R-1}{2} + +\epsilon \right\} \left\{ if Avg < \frac{R-1}{2} - \epsilon \right\} \right\} \tag{4}$$

The l1 and l2 variables are actually the length (size) of SV-LTW with the cases when CMs are regarded as good and bad, respectively. The 1 and 2 are sensitivity parameters, and they define the extent to which window length needs to be modified towards variations in the average trust threshold. E is a symbol of which is a buffer threshold that introduces a point of transition between the various sizes of the window which eliminates the occurrence of sudden changes in the observation lag. The idea behind Eq. To enhance the responsiveness and the accuracy of the trust evaluation, the dynamic depending of the trustfulness of the interactions and the size of the window is to be adjusted dynamically. If the trust value is high ($Avg \geq \frac{R-1}{2} + +\epsilon$), the window size is also enlarged to give consideration of the stable and reliable interactions that reduce the overhead of computation. When the trust value is small, the size of the window is reduced to detect and react faster to possible misbehavior which enhances the security. The importance of Eq. Its capacity to balance computational efficiency to the estimation of various trusts is (4). The proposed model can react fast to the variation in the network behaviour by dynamically adjusting the observation window to ensure that there is healthy communication in various circumstances. The dynamic sizes of the sliding window mechanism can be explained by the necessity of the flexible monitoring periods that should indicate the credibility of the SNs. This will be critical in ensuring the security and functionality of WSNs in general. The Avg is an average of the direct communication trust)) and data trust and calculated by using Eq. (5).

$$Avg = \frac{Tx, yC\,(\Delta t) + Tx, yD\,(\Delta t))}{2} \tag{5}$$

4.2.2 CH to CM feedback communication trust estimation $\boldsymbol{FT_{x,y}\,(\Delta t))}$

Another significant issue of security in IWSN system is CH to CM feedback communication trust estimation that ensures integrity and reliability of information, supports security control, facilitates resource allocation and utilization in an efficient way, and reduces response time. Such benefits are achieved by the process of identifying and eliminating unreliable CMs. It pays more attention to the fact that trustful information is collected and distributed and ensures only trustful information is handled and processed. The CH to CM feedback communication trust estimation to CH integration is a necessity that is critical to the optimization of the IWSN system, and the functionality of the network, as well as making better-informed decisions. In the feedback trust estimation, CH communicates with CMs and directly estimate interaction trust score of (n-1) CMs by periodically transmitting a request packet and storing in a (n-1)×(n-1) matrix with the help of Eq. (6) as follows:

$$CH = \begin{bmatrix} T_{1,1} & T_{1,2} & \cdots & T_{1,n-1} \\ T_{2,1} & T_{2,2} & \cdots & T_{2,n-1} \\ \cdots & \cdots & \cdots & \cdots \\ T_{n-1,1} & T_{n-1,2} & \cdots & T_{n-1,n-1} \end{bmatrix} \tag{6}$$

Stimulated from the beta distribution function [19], feedback communication trust is evaluated using Eq. (7) as follows

$$FTx, yC\,(\Delta t) = R \times \left[\frac{a+1}{a+b+2} \right] \times \frac{E_{CH}}{E_{max}} \times \frac{LQ_{CH}}{LQ_{max}} \times e^{-\varnothing t} \tag{7}$$

where a and b are the good and bad feedbacks, respectively. It is claimed that a feedback is good when FTx,yCΔtR2 and bad when FTx,yCΔt<R2. The trust score is always in the range of 0 to R as the symbol R denotes the maximum trust value. ECH is the current energy level of the CH and Emax is the maximum energy level achievable of the CH. Also, LQCH is the quality of the link between the CH and the CMs, and LQmax is the maximum quality of link in the network, which is usually set to 1 in order to show ideal conditions. The e-∅t factor describes the time (t) since the time of the last interaction and is denoted as ∅. To determine final trust value (fx,yTΔt) is calculated using the Eq. (8) by summing Eq. (5) and Eq. (6). (7) as follows

$$(f^{T}_{x,y}\,(\Delta t)) = \frac{w_1 \times Avg + w_2 \times FTx, yC\,(\Delta t) + w_3 \times ET^{x}\,(\Delta t)}{3} \tag{8}$$

The energy trust of an SN (x) at Δt time(ExΔt) is calculated using a set value of a predetermined threshold amount of energy Eth of 20 percent of the total energy. In case the energy level ((ExΔt) exceeds half of the total energy, then SN(x) is much trusted. When 20% of the total energy<ExΔt≤50% of the total energy it becomes SN(x) trusted and otherwise non-trusted. To determine the signal level of a SN at the CM level, the fx,yTDeltaT element is imposed in line with the Eq. 9. R is customizable to meet the requirements of the application or system.

$$f_{x,y}^{T}(\Delta t) = \{Highly\ trusted\ node\ Malicious\ node\ Legitimate\ node\} \quad (9)$$

4.2.3 CH to CH direct communication trust estimation

CH-to-CH direct communication can be trusted by any means such that only trusted CHs are relied upon to transmit data and any compromised or malicious CHs will be identified and eliminated out of the network. This helps in enhancing the security of the IWSN system and eliminating possible cyberattacks. Moreover, because direct communication can be entrusted more to dependable CHs to transmit and communicate information, more efficient allocation of resources can be achieved by means of trust estimation. The asset makes it easier to respond faster to crucial events and situations and thus improves the effectiveness of the system as a whole. Eq. is used to provide the direct interaction trust between cluster heads CHi and CHj. (10) as follows. Each term of Eq. (10) represents the same purpose as at CM level in Eq. (1).

$$TCH_i, CH_jC(\Delta t) = \left[\begin{array}{l} R \times \lambda_1 \times \left(\frac{SCH1,CH2C(\Delta t)+\alpha}{(SCH1,CH2C(\Delta t)+UCH1,CH2C(\Delta t))+\beta)} \right) \\ \times \frac{1}{\sqrt{\psi \times UCH1,CH2C(\Delta t))}} \times \left[\lambda_2 \times \frac{SCH_i,CH_jC(\Delta t)}{SCH_i,CH_jC(\Delta t)+\gamma} \right]^{\alpha} \\ \times \frac{1}{\sqrt{1+\delta A_{(CH_i,CH_j)}}} \end{array} \right] \quad (10)$$

4.2.4 BS to CH feedback trust calculation

The BS transmits a request packet to m CHs and store the obtained direct interaction trust score of CHs into a matrix using Eq. (11) as follows

$$B = \begin{bmatrix} CH_{1,1} & CH_{1,2} & \ldots & CH_{1,m} \\ CH_{2,1} & CH_{2,2} & \ldots & CH_{2,m} \\ \ldots & \ldots & \ldots & \ldots \\ CH_{m,1} & CH_{m-1,2} & \ldots & CH_{m,m} \end{bmatrix} \quad (11)$$

Since the beta distribution increases the truthfulness of the trust assessment procedure because it provides a robust way to model probabilistic trust based on binary outcomes, such as positive (good) and negative (bad) feedback. This makes it highly suited for trustworthiness evaluations in dynamic environments like IWSNs. The beta distribution, as a conjugate prior to the binomial distribution, offers a mathematically sound means to continuously update trust values with new observations, effectively balancing past and recent feedback. This continuous updating is crucial in feedback-based trust systems, as it allows trust scores to dynamically reflect the latest network conditions and SN behavior without discarding historical data. The Eq. (12) can be utilized for predicting the trust in feedback communication.

$$FT_{BS,CH_j}(\Delta t) = R \times \left[\frac{w_p \times p + 1}{w_p \times p + w_b \times b + 2} \right] \times e^{-\varnothing t} \quad (12)$$

where w_p and w_b are dynamic weighting factors for positive and negative feedback, respectively during BS to CH Feedback Trust calculation. The weights can be dynamic depending on recent trends. These recent feedback is assigned higher weights to ensure trust calculations give more importance to latest network conditions. This dynamic weighting enhances resilience by enabling the trust model to adapt in real-time according to the behavior of the network. The term $e^{-\varnothing t}$ adds a time-decay function, where $\varnothing$ is a decay constant which diminishes the impact of older feedback progressively. This decay allows trust scores to represent more recent interactions, making the model more relevant to the current state of the network. All these components together present a strong and adaptive measure of trust that is very relevant to dynamic and potentially hostile WSN environments. A global trust score $G_{CH_i,CH_j}^{T}(\Delta t))$ is assessed at CHs using Eq. (13).

$$(G_{CH_i,CH_j}^{T}(\Delta t)) = \frac{T_{CH_i,CH_j}(\Delta t) + FT_{BS,CH_j}(\Delta t)}{2} \quad (13)$$

5 Simulation results

To test the performance of TITAN, we implemented a sequence of experiments in the MATLAB R2023b over a collection of conditions, systematically changing N, M, f̂, and ψ. The experimental protocol included 500 repetitions, and the evaluation of misbehavior was to be done after every 100 repetitions. Simulation outcomes revealed that the TITAN system has a very high resilience to internal attacks. To provide a full-fledged evaluation of its efficiency, the comparative study was conducted with the existing methodologies, i.e., SDTS [23], DTMS [35], and DST-WOA [36]. Special focus was given to essential measures, such as false-negative rate (FNR), false-positive rate (FPR), detection accuracy, average energy use, and throughput. The comparative analysis shows clearly that TITAN is better than these antecedent approaches. SDTS uses equal clustering to minimize the overhead of communication and counter active attacks like Sybil and Blackhole by laying emphasis on the communication-based trust. Nevertheless, this focus brings about inaccuracies in the values of trust, hence constraining flexibility in the dynamic environment. DTMS [35] implements a multi-level system of trust evaluation which combines both communication and data trust so as to obtain admirable detection power. However, there are limitations in the model that the trust is not absolute in a highly dynamic network and the model assumes

sensor-node (SN) homogeneity, thus limiting this model to a heterogeneous SN environment. The DST -WoA model combines the Dempster-Shafer theory of clustering with the Whale Optimization Algorithm of routing, and thus, the model is more efficient in terms of energy conservation and throughput. However, its fixed trust judgement and the use of homogenous SN properties do not allow realistic trust evaluation and flexibilities in networks in contexts of fast transformation. The TITAN framework eliminates these shortcomings by bringing in a number of new functionalities. It includes a multi-dimensional evaluation of trust, including communication trust, data trust, and energy trust to provide an all-inclusive evaluation of trust. Unequal strategic clustering balances the energy consumption through the creation of different cluster sizes depending on the distance of a sink and, in this way, energy consumption is distributed efficiently and network sustainability is increased. The OCREA method is a dynamic elector of cluster heads, computing the fitness score based on residual energy, quality of links, signal strength, and distance to the base station, thus both providing energy efficient leadership and supporting SN heterogeneity. The TITAN adaptive logarithmic trust function has dynamic rewards and penalties which change over time and are used to reflect the SN behavior. Moreover, a dynamic aging aspect keeps the recent interactions relevant and the impact of old information weakens and reinforces the identification of unreliable SNs. TITAN is more adept at providing the benefits of enhanced accuracy of trust and flexibility, energy efficiency to SDTS [23], DTMS [35], and DST -WOA [36], i.e. offering strong, secure, and power-efficient services to industrial wireless sensor networks. Moreover, TITAN has limited storage requirements of trust values, and the maximum trust value would be limited to ten, thus minimizing the use of memory. Moreover, clustered IWSN networks are inherently quadratic on communication overhead [26]. To determine the efficacy of the TITAN trust model, simulations were done which included successful and malicious behaviors at every time interval of the sliding variable length logical time window (SVLTW). In the TITAN model, malicious SNs were inserted into the IWSN network in random numbers before each round had been initiated. Table 4 shows the parameters of simulation employed in evaluation of our proposed model, TITAN. An analysis of the end performance of TITAN was carried out fully by choosing simulation settings in the domain of reference [23, 35, 36]. In the assessment, we had set up the initial energy of SNs (€) at 4 J. The hypothesis of trust threshold was expected to be 50 percent of the maximum trust value [12]. Since our values of trust will be in the range [0, 10], we have the trust threshold of 5. The role of the reward term in the model is very unique and crucial in the control of non-cooperative SNs.

Table 4 Simulation parameters

Network size	$100 \times 100m^2$
Network topology	$Random$/Clustered
Node deployment	Fixed
Number of sink node	1
IWSN nodes (N)	$100to500$
Malicious nodes	10
Number of rounds	100
No. of Cluster Heads	$2to7$
Transmission range	$30m$
Optimal number of clusters	$2to7$
Each simulation iteration	100
Range of trust values	$[0R]$
Cluster size	20 nodes to 70 nodes
Initial energy of SN	4 J
Packet size	512 byte
Position of the sink	(50,50)
Minimum length of sliding window	(2,5)
Buffer size	30 packets
Weight assignment strategy	Equal
Punishment coefficient (ψ)	[1, 3]
Reward $coefficient(\widehat{r})$	[1, 3] neutral tuning when $\widehat{r}$=1
Pause time interval	0.01 s
Energy Usage During Data Transfer for One Packet	0.004096 J
Energy Usage During Data Collection for One Packet	0.005121 J
α	1
β	2
Γ	0.1

Parameters and thresholds that are used in the simulation have been thoroughly tested and verified. However, it is still imperative to note that there are also other parameter values which could be interesting to examine since they can be adjusted to suit the unique needs of different applications. In the military arena, say two to three, values may be increased to enhance reliability of information depending on the level of confidence required. The TITAN model defines the percentage levels by using the previously done work [3, 23, 23, 35], which give invaluable information on the suitability of the parameter range. As shown in Fig. 4, success rate is a critical factor when it comes to the outcome trust levels. The higher the success rate, the higher the trust scores which SNs were given. However, in adversarial situations, the level of trust decreases in comparison with the usual operating conditions, since the TITAN trust model decreases the scores of SNs who show inappropriate behavior as demonstrated in Fig. 5. The TITAN trust model is skillful in isolating evil SNs that do not adhere to the protocol of packet-forwarding. Both the CM and the CH level are calculated and used to measure trust, so that any negative tendencies that are exhibited by SNs can be identified and prevented.

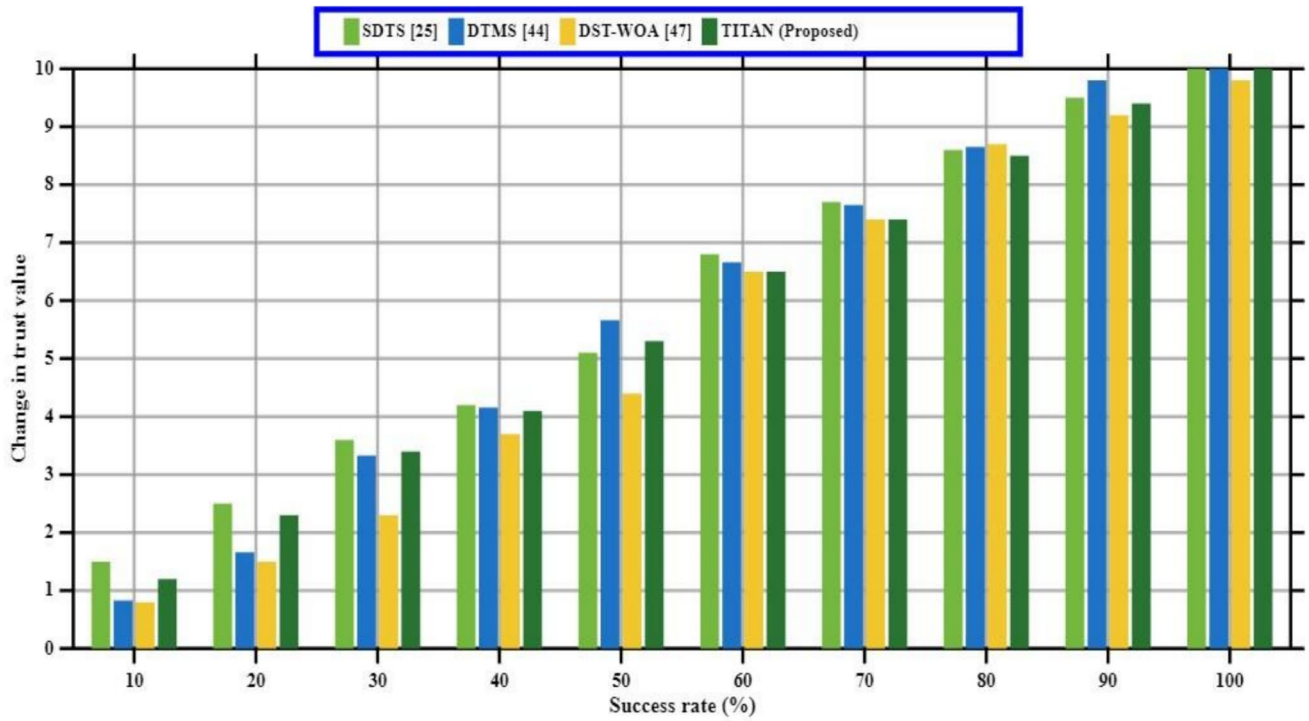

Fig. 4 Effect of success rate on trust values in normal environment

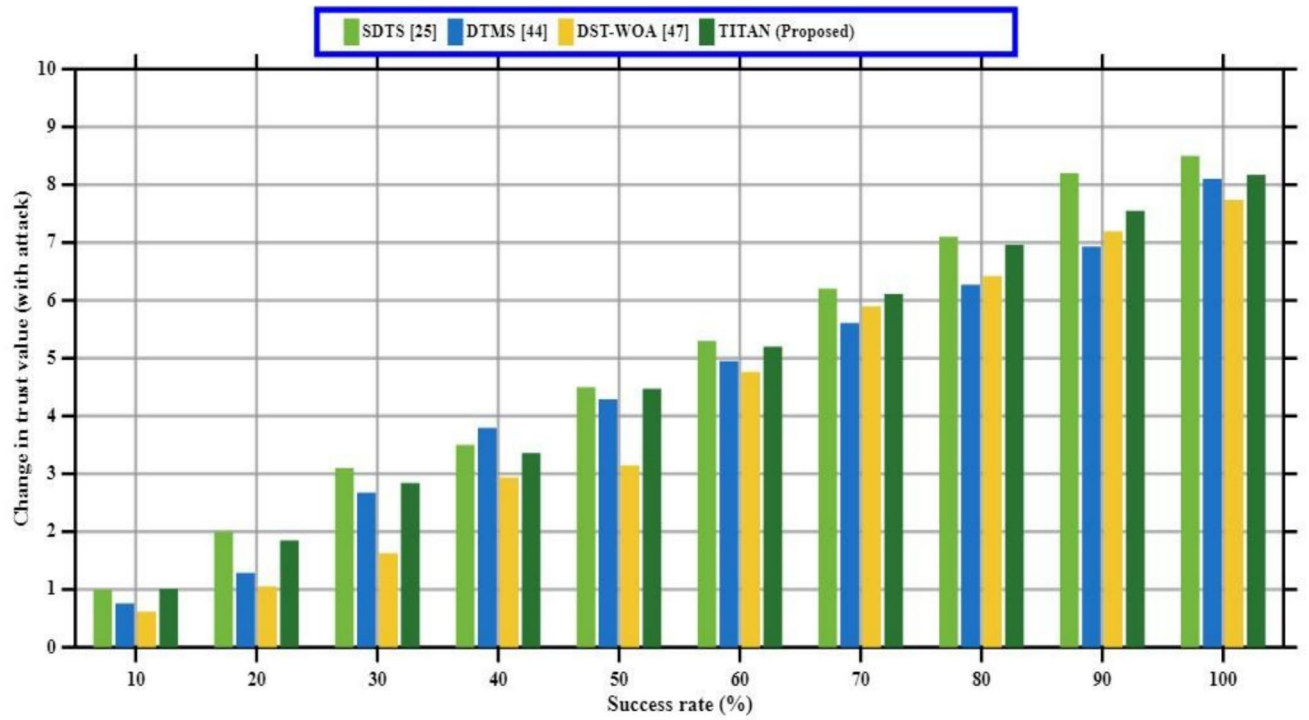

Fig. 5 Effect of success rate on trust values in attack environment

There are numerous internal attacks in the industrial wireless sensor networks (IWSNs), which can seriously hurt both the integrity of the network and efficiency. MATLAB is an effective instrument that can be used to simulate such malicious situations and to estimate the effect they have on trust-related parameters. This discussion will describe some of the attack paradigms and show how certain MATLAB functions and procedural methods can be used to model these

paradigms in a principled and efficient way. In the packet-dropping attacks, the adversary sensor node (SN) chooses to selectively drop packets sent by the sender instead of forwarding the packets. This can be recreated in MATLAB by calling a function like simulatePacketDropping which adjusts the probability of transmitting packets to replicate this malicious intent of the node. The performance indicators are packet delivery ratio (PDR), throughput and end-to-end delay, which may be periodically recorded using time-series collection functions like measurePDR and calculateLatency. Setting a threshold on PDR and delay enables one to signal SNs with low reliability to be viewed more closely. In order to simulate the spread of false data, we can design a function called *disseminateFalseInfo() [7] that can be used to inject false sensor data into the data stream of the network. All SNs participating could then have their trust scores trailed with the aid of *updateTrustScore()* which is a routine that punishes those nodes that keep on giving false information. In a bad-mouthing attack, a node under compromise falsely charges really honest nodes with deviant behavior. This adventure can be modeled with the help of applying the idea of trackNodeHistory which logs every SN interaction and the feedback that they will get. Measures like feedback consistency and reputation scores can then be calculated using the function called calculateReputation hence being able to identify SNs who have been involved in dishonest behavior. Similarly, an attack based on black holes may be defined as a regular routine, such as advertiseBestRoute, in which rogue SNs announce themselves to be the best route to use but responsibly discard any packets they receive. In the case of greyhole attacks, it is possible to use the command simulateSelectiveDropping where SNs are occasionally allowed to drop packets in an uneven distribution. A MATLAB subroutine, called checkIdentity, can be used within the application of Sybil attacks by using a deployment matrix to highlight discrepancies in the reported locations of SNs. Trust estimation measures can then mark any node that does not meet set trust limits as a possible malicious node. In order to simulate an on/off attack, the SN may be made or broken a participant of the IWSN randomly by invoking the function: simulateOnOffBehavior. Similarly, the frequency of engagement is tracked regularly and is monitored by the routine process, which aids in identifying the presence of anomalous and sporadic behavior through regular monitoring. In the case of ballot-stuffing methods, the function of boostReputation allows the malicious SNs to engage in positive feedback on the commodity artificially increasing the trust granted to them. Such inflation may be detected by consistency checks on feedback and trend analysis using the functions analyzeFeedbackConsistency and monitorReputationTrends, which, when combined, can be used to isolate such components and fix over valued scores on trust.

TITAN's proposed trust model is unique because of realistic, incremental trust assessments directly associated with the success rate observed as demonstrated by the progressive increase in the trust values shown in Figs. 4 and 5. The success rate which is formally defined as the ratio of successful interactions to the total number of interactions among the SNs is a determining factor in the output of the trust value by the TITAN model. An increased rate of success is an indication of a stable, dependable communication, hence, producing high scores of trust. On the other hand, a reduced success rate, which is usually symptomatic of malicious behavior, including packet dropping or misinformation dissemination, results in a reduced value of trust. This value is critical as the dynamic logarithmic trust function used to form the basis of TITAN incorporates both the success rate and punishment-reward manipulations allowing an adaptive reflection of node action. In turn, the success rate will be used to differentiate between the unreliable and their reliable counterparts. This will help build trust in a consistent and long-term interaction, and thus avoid acute growth of trust that may lead to poor trust operations or may signify the exploitation of trust by rogue SNs. As an example, by examining Fig. 4, it is apparent that, at success rates of 10 and 20, TITAN triggers trust scores of 1.2 and 2.3 respectively, which is a gradual and clean rise compared to models that can take off. The TITAN model is particularly effective in Fig. 5, which represents an attack situation when compared to SDTS, DTMS, and DST -WOA. TITAN has a trust score of 1.01 at a 10 0 percent success rate, which is higher than SDTS (1.00), DTMS (0.759), and DST-WOA (0.616). These statistics highlight the superior position of TITAN to sustain high trust values even in unfavorable circumstances. An important factor that increases the reliability of TITAN is that it has used both an aging factor and a decay factor. The decay factor takes into consideration the duration of time (t) that a node has been without interaction; such that the trust is gradually lost to SNs that have not been involved in the network over a long period of time. This algorithm puts more emphasis on the latest behavior than the old data, hence a confirmation of the new information on the node performance that is actionable. With decay and aging, the trust ratings are dynamic and will constantly be adjusted to the current SN behavior keeping the ratings relevant and accurate. The aging factor also adds weight to recent interactions in comparison with older which guarantees that the scores of trust are presented by current activity and eliminates the impact of outdated or poorly utilized connections. In the end, the characteristics make TITAN more reactive and reliable to work in dynamic network conditions.

The results obtained by TITAN in terms of false-positive rate (FPR) are depicted as being lower and steadily lower when the sensor nodes (SNs) are malicious, thus showing

that TITAN is more efficient at recognizing benign and malicious behavior (Fig. 6). The FPR is determined as the ratio of false positives to the overall number of true negative cases in the dataset. False positive- A false positive happens when an SN that is legitimate is classified as untrustworthy. In turn, the FPR measures the number of times the suggested model produces a false alarm, which reflects the chances of inefficiency or excessively penalizing trust functions that are over-punitive and penalize legitimate SNs inappropriately. The FPR should be lower (greater detection accuracy and reliability), by which the valid SNs can remain operational without the possibility of being wrongly detected and isolated. The FPR of TITAN rises slowly with a higher percentage of malevolent SNs where FPR is 0.5 with 5% of malicious SNs and is 0.6 with 60%. In comparison, SDTS [23] scheme upholds an FPR of zero at lower ratios but then increases drastically in the future when the number of malicious SNs increases. DSM-woa [35] and DTMS-woa [36] have greater values of FPR in most of the ratios, which means they are more prone to false classification of benign SNs as malicious. This high performance is as a result of the combination of direct and indirect forms of communication trust measures, as they ensure sound evaluation through a combination of SN interactions into a total trust rating. In addition, data trust metric improves system reliability by ensuring that there is accuracy and integrity of data sent. The active logarithmic trust has a key role in tuning the rewards and penalties based on SN behavior so as to reduce false positives by increasing trust evaluation accuracy. Besides, the fitness score used in unequal clustering enhances network resilience by maximizing SN distribution and reducing misclassifications. The aging mechanisms are used to make sure that the trust information is relevant and up-to-date by avoiding old information and a damping factor is applied to smooth the sharp changes in score, resulting in more consistent decision-making. Combined, all of these strategies significantly increase the ability of TITAN to distinguish between legitimate and malicious SNs, reducing the FPR and demonstrating its capability in reducing aggressive actions within the IWSNs. Similarly, Fig. 7 compares the false-negative rate (FNR) of several models SDTS, DTMS, DST-WOA and the proposed TITAN in different proportions of malicious SNs. The findings indicate that TITAN always has less FNR compared to the other ones, especially when the ratio of harmful SNs increases. As an example, TITAN reaches an FNR of 0.7 at an SN ratio of 35, significantly lower than the 1.5 of DTMS and 9.3 of DSTWOA. This continues at an increased ratio where at 60% TITAN

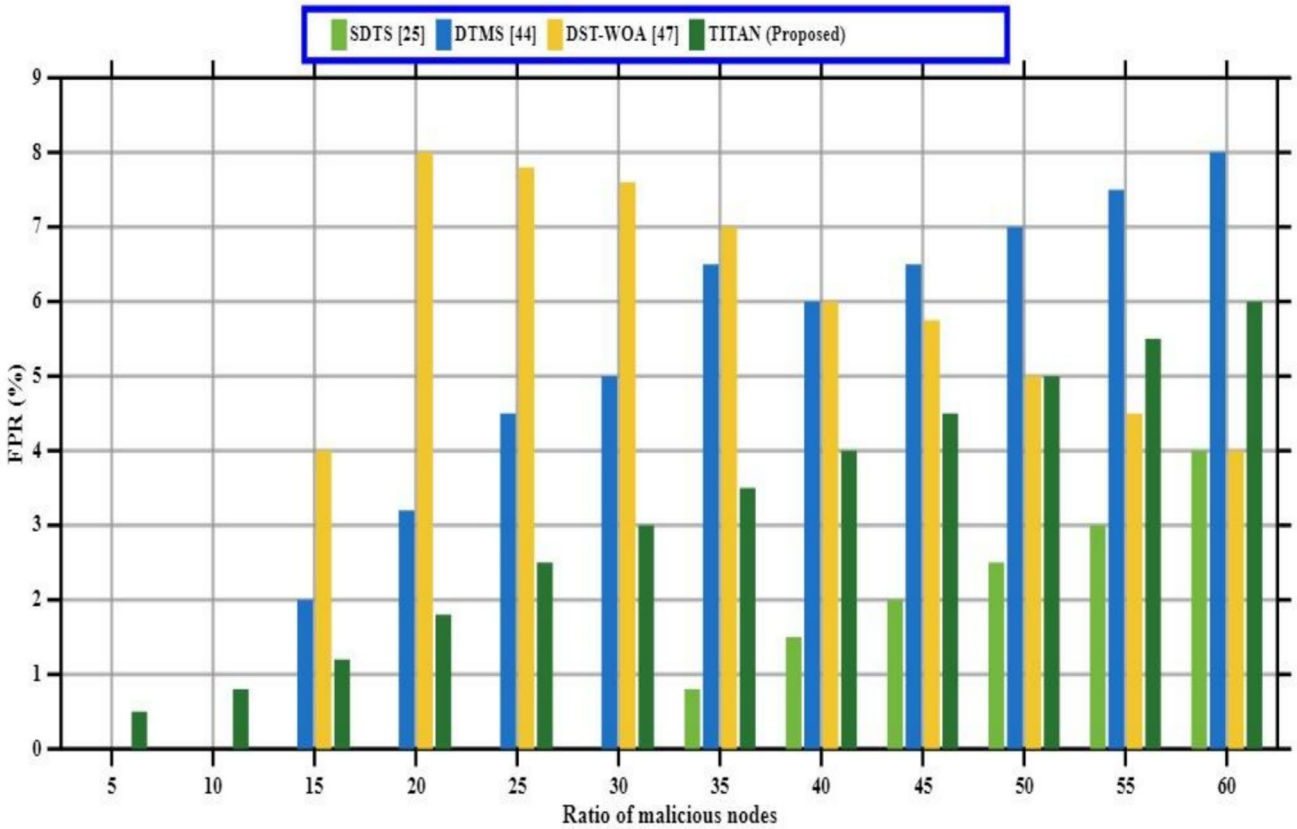

Fig. 6 Effect of malicious nodes on FPR

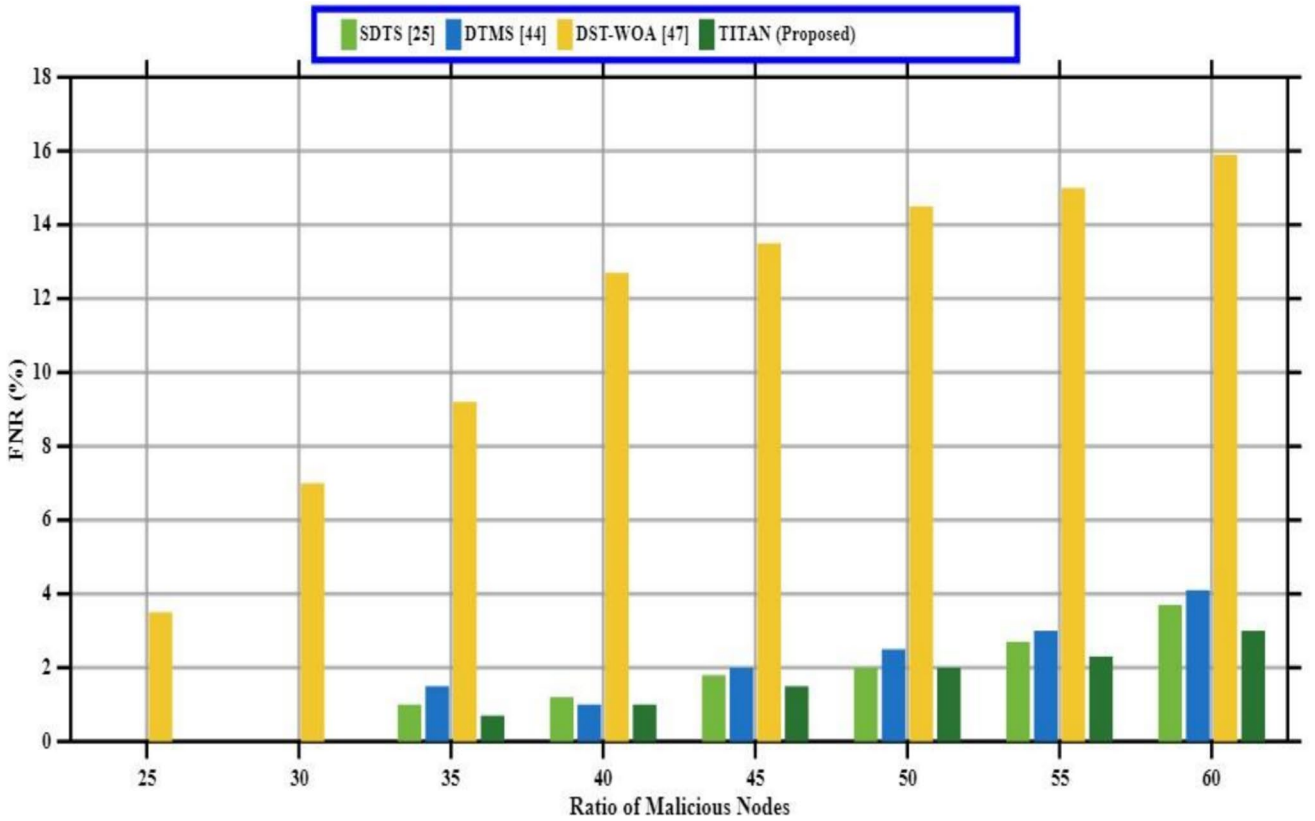

Fig. 7 Effect of malicious nodes on FNR

has an FNR of 2.9 whilst SDTS has a FNR of 3.5, DTMS has a FNR of 4.2 and DST-WOA has a FNR of 15.8. TITAN higher FNR performance is based on the inclusion of such main features as direct and indirect communication trust and data trust that enhance its ability to discriminate against malicious behavior. Flexible rewards and penalties are especially important to the dynamic logarithmic trust function to fine-tune the trust scores and eliminate false negatives. The aging factor will ensure that the outdated information does not contaminate the existing trust scores, whereas the damping factor will stabilize the trust updates, avoiding sudden and incorrect reclassification. The joint mechanisms enable TITAN to stay reflexive and accurate with trust judgments, which guarantees a reduction of FNR in different malicious conditions across the IWSNs.

The accuracy in detection of malicious activity with the existence of malicious SNs is shown in Fig. 8. We give evidence of the efficacy of the suggested strategy at different proportions of malicious SNs. The TITAN model that is proposed shows improved performance, particularly when there is an increased ratio of the malicious SNs. As an illustration, in the case of the 5% hostile SNs, TITAN achieves a perfect detection rate (100%), equivalent to SDTS and DTMS, but higher than that of DST -Woa (97%). With increase in the percentage of malicious SNs, TITAN has high accuracy compared to the other competing frameworks, with 95 percent accuracy in 35 percent malicious SNs, in comparison to SDTS, DTMS and DST-WOA, which reach 94 percent, 93 percent, and 80 percent, respectively. This trend continues to 60 percent of malevolent SNs, at which TITAN is 89 percent of detection, exceeding SDTS (85 percent) and DTMS (80 percent) and the DST-WOA (60 percent). A number of critical features is the main cause of this increase in the accuracy of detection. They consist in the use of TITAN of the interaction quality, sensitivity coefficient, delay, variable buffer threshold, interaction quality as well as the trust decay factor in its overall trust assessment. These variables make sure that the trust scores are up to date and they do not take a sudden spike in the wrong direction. These mechanisms together allow TITAN to better differentiate legitimate and malicious SNs thus providing better performance in detection.

Figure 9 presents the average energy consumption and thus shows how effectively the proposed model works at different ratios of malicious sensor nodes (SNs). The TITAN model always attains a low energy footprint, especially when the percentage of malicious SNs increases. To illustrate the point, when the malicious SN ratio is 5%

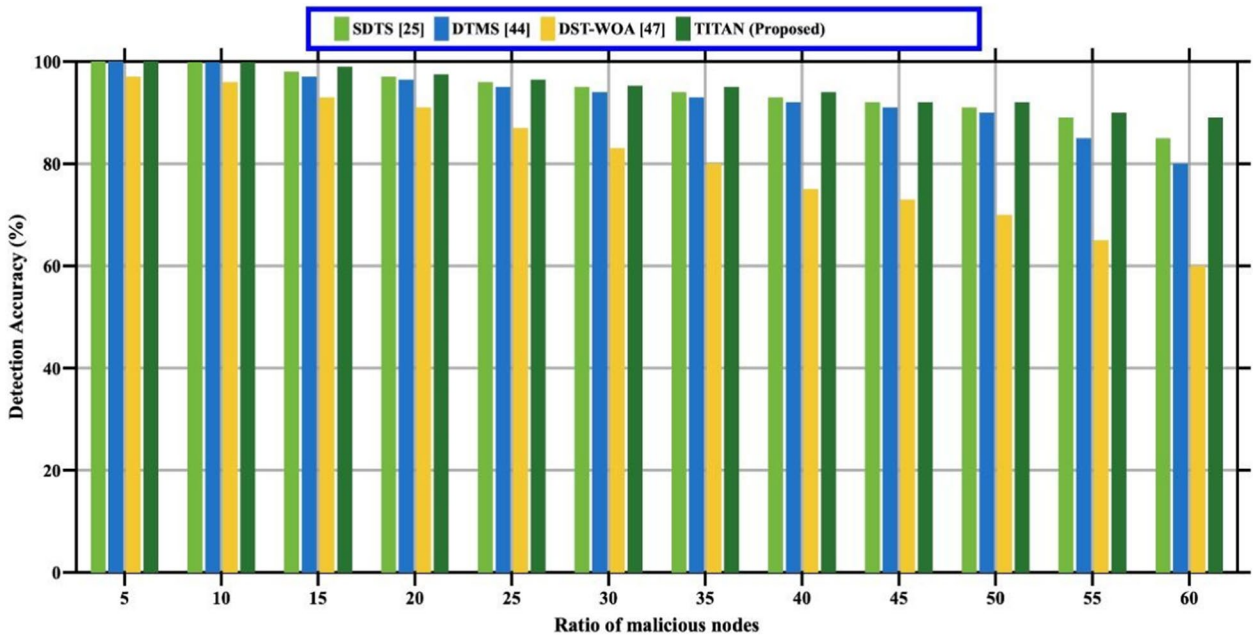

Fig. 8 Ration of malicious nodes vs. Detection accuracy

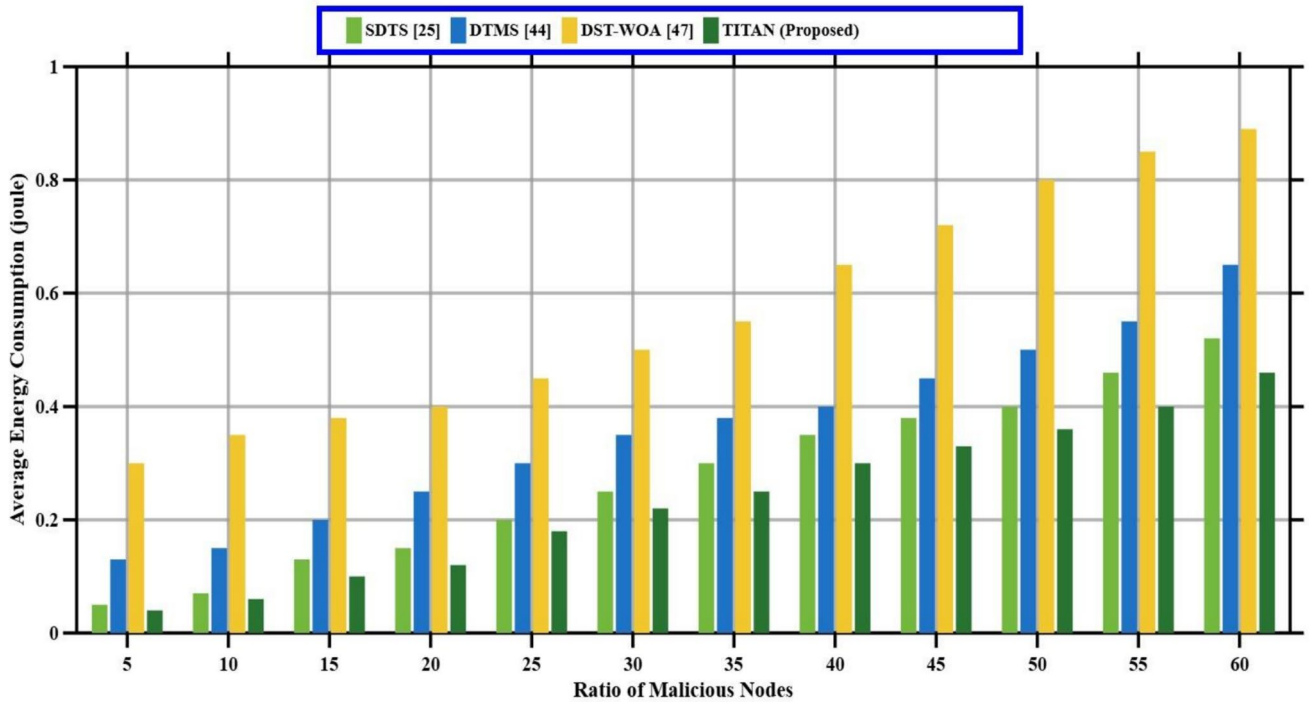

Fig. 9 Average energy consumption

the average energy consumption level recorded by TITAN stands at 0.04 J, which is significantly lower than SDTS (0.05 J), DTMS (0.13 J) and DST-WOA (0.30 J). This beneficial trend continues at higher malicious SN ratio with TITAN using less energy reaching 0.46 J at 60 malicious SNs and 0.65 J at 60 DTMS and 0.89 J at 60, respectively. The lowered power usage of TITAN may be explained by the fact that it has been carefully designed and its features contribute to its energy efficiency. The dynamic logarithm trust function enhances the efficiency in computation by attaching adaptive rewards and penalties based on SN behavior; such a dynamic system prevents unnecessary transmissions and calculations and thus reduces the total energy expenditure. Furthermore, the aging mechanism

of TITAN guarantees that outdated data on trust gradually expire and does not require unnecessary reconsideration of previous interactions and also conserves energy. The damping factor stabilizes the trust updates so that there is sudden recalibration and ensures that the energy is spent at a steady rate over time. By integrating successful direct and indirect communication trust with data trust, TITAN streamlines the use of energy in the trust assessment; direct trust applies to interactions that are recent whereas indirect trust offers additional verification thus reducing unnecessary data transfer. Lastly, the skill of TITAN in balancing fitness scores during uneven clustering also gives an equal distribution of energy consumed throughout the network, and no specific SNs gets their energy depleted in a short time.

The detection rates (%) of each proportion of malicious sensor node (SNs) are compared in Fig. 10. The TITAN model has always displayed high detection rates, which increases with the percentage of malicious SNs. TITAN has a 100,000-detection rate at low malicious SN rates (520, 520), equivalent to SDTS, DTMS and marginally greater than DST -WoA. At a malicious SN ratio of 25 per cent, TITAN has a 99 per cent detection rate, which is higher than DTMS (90 per cent) and DST-WOA (85 per cent) but slightly lower than SDTS (98 per cent). TITAN has a consistent detection rate of 95 98 between 30 45 0 per cent hostile SNs, consistently surpassing DTMS and DST -WOA. Interestingly, with 50 per cent adversarial SNs, TITAN has a 93 per cent detection rate, which is higher than DTMS (75 per cent) and DST-Woa (60 per cent). This tendency remains at greater ratios; 60 per cent hostile SNs, TITAN has an 87 per cent detection rate which is significantly higher in comparison with SDTS (75 per cent), DTMS (60 per cent), and DSTWOA (50 per cent). The performance of TITAN in the detection is outstanding because of the effective combination of direct and indirect communication credibility, dynamic credibility evaluating systems, and efficient data-validation processes. The model considers trust as a product of interaction quality, sensitivity coefficient, latency, variable buffer threshold, link quality and trust decay factors which allows the detection of malicious activity with high reliability as malicious SNs continue to grow. This analytic model shows the effectiveness of TITAN as a trust-management system, which is characterized by a high detection accuracy and the highest level of energy efficiency, which makes it beneficial to secure and sustainable inter-sensor wireless networks (IWSNs). Figure 11 represents the relative throughput (Kbps) of the different ratios of malicious SNs and throughput is determined by means of Eq. (13). The TITAN model has always demonstrated better throughput when compared to other techniques particularly when the malicious SN ratio increases. At such a low hostile SN level of 5 0, TITAN maintains a throughput of 285 0 Kbps as compared to SDTS (250 0 Kbps), DTMS (200 0 Kbps), and DST-WOA (170 0 Kbps). It means that the TITAN is able to sustain an efficient data transmission even under comparatively safe circumstances. At 10 and 15 percent malicious SN proportion, TITAN still provides the most impressive throughput rates of 260 and 245 Kbps, respectively, which is

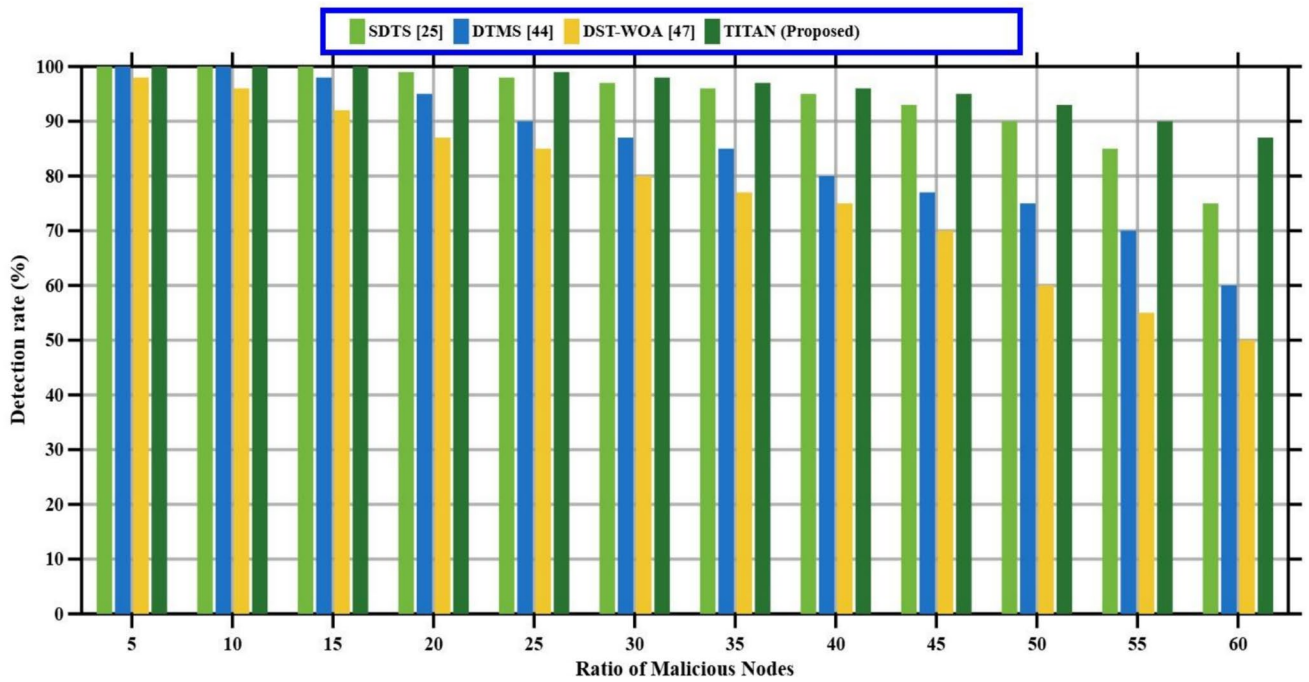

Fig. 10 Detection rate (%) in presence of malicious nodes

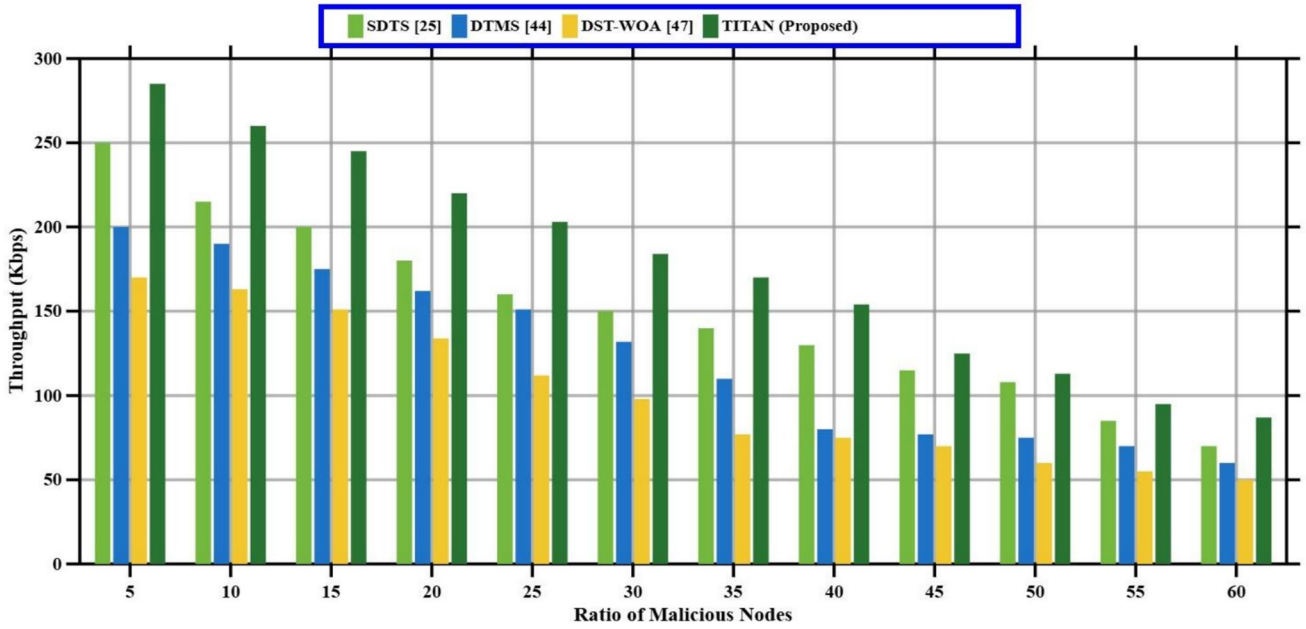

Fig. 11 Throughput in presence of malicious nodes

much higher than the deteriorating rates of the other models; SDTS, DTMS, and DST -WOA record 200, 175, and 151 Kbps, respectively. At malicious SNs of 25 and 30 percent, TITAN retains its lead, with throughputs of 203 and 184 Kbps, respectively, which is much higher than DTMS (151 and 132 Kbps) and DST-WOA (112 and 98 Kbps). TITAN also supports throughput at 125Kbps and 113Kbps, which is significantly higher than SDTS (115Kbps and 108Kbps), DTMS (77Kbps and 75Kbps), and DST-WOA (70Kbps and 60Kbps) at high SN ratios of 4550 of 50. TITAN has a throughput of 87 Kbps in extreme conditions with percentages of 60 per cent malicious SNs, and achieves greater throughput compared to SDTS (70 Kbps), DTMS (60 Kbps), and DSTWoa (50 Kbps). TITAN has achieved remarkable throughput performance due to the combination of adaptive comprehensive trust schemes, dynamic reward-penalty scheme, link-quality and trust decay factors along with successful strategic clustering. Collectively, these factors contribute to the improvement of the transmission of data by placing emphasis on reliable SNs and limiting the communication with potentially malicious SNs, which underscores TITAN capabilities of maintaining high network throughput in the situations of significant hostile conditions and offers effective, steady communication in the IWSNs

$$Throughput = \frac{Total\ data\ successfully\ received\ (in\ bits)}{Total\ time\ taken\ (in\ Seconds)} \tag{14}$$

Figure 12 shows the number of detected malicious sensor nodes with a different number of operating rounds. The TITAN model is always shown to have a better ability to detect malicious SNs more efficiently as compared to the comparative methods. TITAN detects three malicious SNs after ten rounds, which is more than SDTS and DTMS, each of which detects two, and DST-WOA, which detects one. This finding highlights early detection of threats at the early stages of network operation, which is strong at the beginning of operation of TITAN. On the twenty rounds, TITAN stays ahead by finding four malicious SNs, SDTS and DTMS find three and DST -WoA finds two. With the rounds going up to forty and sixty, TITAN still performs better and identifies five and six malicious SNs, respectively. In comparison, SDTS and DTMS identify four and 5.5 SNs, and DSTWOA is behind with three and four identifications. This trend is an indication of the effectiveness of TITAN in identifying the rising levels of malicious behavior with increased network activity. In installations of a minimum of eighty rounds, TITAN also outperforms in terms of detection having seven detections compared to DTMS 6.5, SDTS 6 and DST-WOA 5. TITAN identifies nine malicious SNs at one hundred rounds, and SDTS and DTMS identify only seven and DST- WOA identifies six. The increased sensing capability of TITAN is based on its dynamic trust evaluation schemes, the evaluation of its interaction quality as well as its latency, configurable buffer threshold, trust evaluation, gradual reduction of trust and its improved clustering features, which taken together contribute to the overall effectiveness of the model to detect the malicious SNs in the long-term network use. TITAN, therefore, improves the security and integrity of the network by managing any threat proactively as the adversarial activities evolve with time. With one hundred rounds, TITAN is still enjoying a

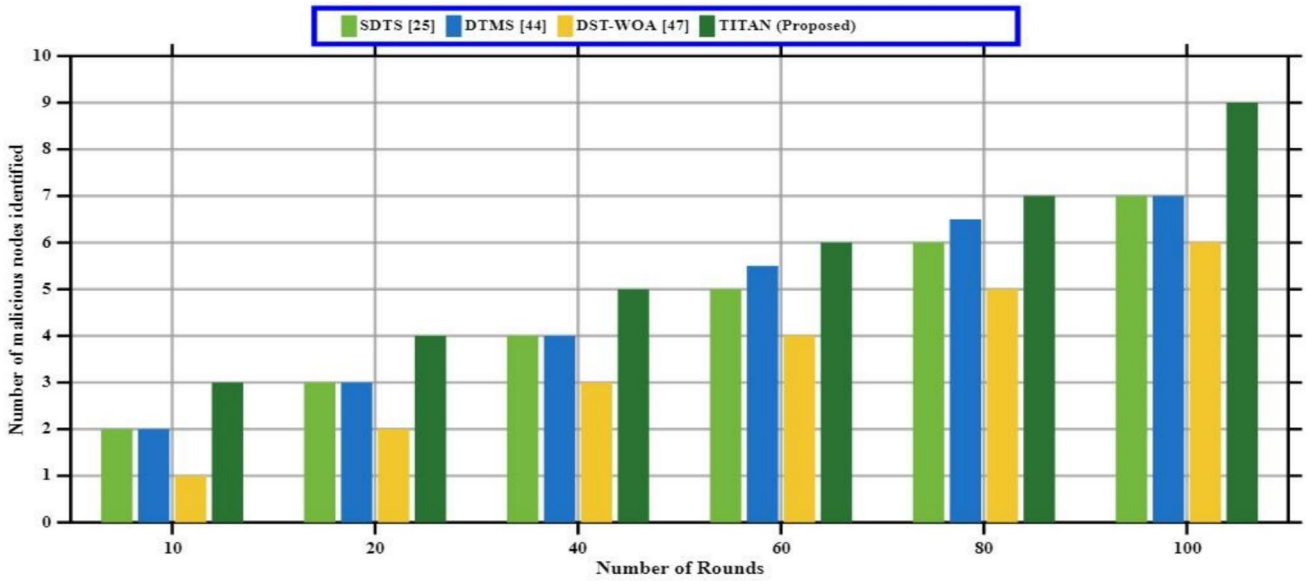

Fig. 12 Number of malicious nodes identified over different numbers of rounds

significant lead with a score of nine successful transmission detection, compared to SDTS and DTMS, which score seven each, and DST -WOA, which scores six. The adaptive clustering mechanism, dynamic trust assessment, and the effective use of resources makes TITAN have augmented network longevity and high round performance. Such synergetic factors reduce the use of energy and increase the collaboration of SN to the maximum, thus, allowing TITAN to maintain a long duration of functioning and transfer data through the large volumes with the best efficiency.

The Fig. 13 shows the packet-loss rate (%), which was incurred in consecutive rounds, of four different trust-management schemes, that is, SDTS, DTMS, DST-WOA, and the proposed TITAN model. The statistics show that the TITAN model always has a lower packet-loss rate than the others hence highlighting its high reliability in protecting the integrity of data during network operation. At the first stage, or after 10 rounds, TITAN has the lowest packet-loss rate of only 1% as compared to SDTS (2%), DTMS (5%), and DSTwoa (4%). This advantage will be realized at an early age and shows the effectiveness of TITAN in handling the primary network transmissions at a negligible rate of data loss. At 20 rounds, TITAN continues to dominate with a reported 4 per cent packet loss over SDTS 6 per cent, DTMS 10 per cent and DST-WOA 8 per cent, which proves it to be operating efficiently with its packets and delivering them on-demand. With higher rounds, TITAN proved to be better with packet-loss rates at 15 and 26 percent, which is significantly better than SDTS, which was 17 and 28 percent, DTMS, which was 22 and 45, and DST-WOA, which was 20 and 40. The findings support the ability of TITAN to support stress and transmission requirements in the network and reduce the loss of packets. After 80 rounds, the rate of packet-loss in TITAN is relatively lower at 34% compared to SDTS at 36% and DTMS at 60% and DST-WOA at 50%. Lastly, TITAN at 100 rounds offers a packet loss rate of 39 per cent, though, which is much more impressive compared to SDTS (47 per cent), DTMS (70 per cent) and DST-WOA (60 per cent). The improved resilience of TITAN to packet losses can be explained by the fact that the algorithm has been developed to take into account the clustering technology, packet routing through the use of trusted sensor nodes, and estimation of the link quality that result in maximum data flow and minimum loss during transmission. Therefore, TITAN provides reliable communication and data transfer in long network operation and in severe environment conditions.

Table 5 contains a summary of the attack-wise performance of the proposed TITAN framework, provided that 100 rounds of trust updates are performed, and. The periodic trust computations in the simulation configuration are associated with each round. In every case of an attack, both. The statistics of the malicious SNs in terms of numbers and percentage are clearly defined among the 500 nodes to make it clear and reproducible, in agreement with the findings of the paper. Such attacks as Sybil and Blackhole are rated at lesser malicious node ratios (10%, and 15% respectively) since even a few such structurally aggressive attackers will cause a drastic effect to identity management and packet forwarding. TITAN identifies them because they are in persistent and distinguishable manner, attack fewer trust rounds and can achieve a higher detection rate, very low packet loss and higher throughput values which are still nearly at the highest range reported in Fig. 11. Packet Dropping and Greyhole

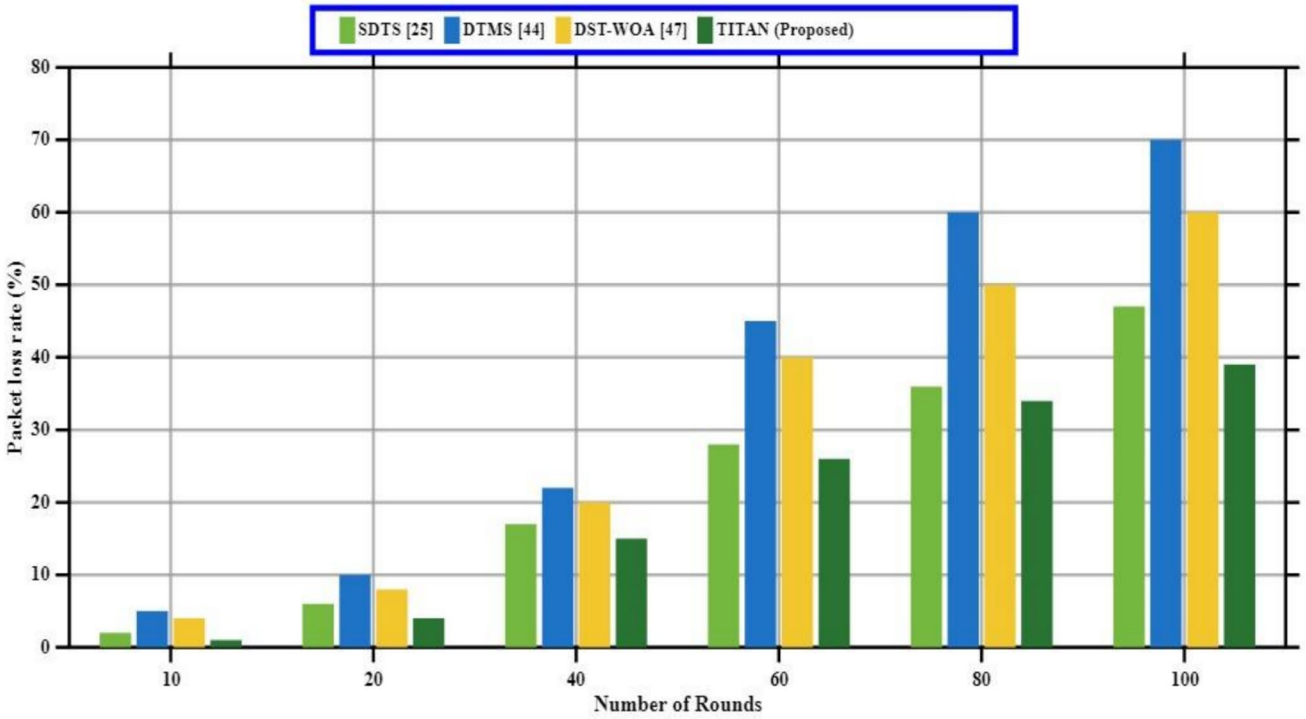

Fig. 13 Packet loss rate (%) over different number of rounds

Table 5 Attack-wise performance evaluation of TITAN

Attack type	Malicious SNs (No., %)	Detection rate (%)	Packet loss rate (%)	Throughput (Kbps)	Average energy consumption (J)
Packet dropping	100 (20%)	88.4	9.5	228	1.72
Misleading information dissemination	125 (25%)	86.9	10.6	215	1.75
Bad-mouthing	150 (30%)	85.7	11.1	208	1.77
Blackhole	75 (15%)	90.8	8.2	245	1.69
Greyhole	100 (20%)	88.1	10.0	220	1.73
Sybil	50 (10%)	92.6	7.0	260	1.66
On–Off	175 (35%)	84.8	11.6	198	1.80
Ballot-stuffing	200 (40%)	84.1	12.0	192	1.83

attacks, at moderate malicious ratio (20 percent) show balanced performance trends, as detection will be observed following a few rounds, causing controlled drop of packets, and stable throughput, as malicious forwarding behavior will be punished by the trust decay and reward-penalty provisions. Conversely, Bad-Mouthing, On–Off and Ballot-Stuffing attacks are tested at higher malicious ration (30–40) so that they are used by malicious nodes in a behavioral and collusive fashion, that is, malicious nodes manipulate trust feedback intermittently or as a collective. The behavior postpones convergence of trust and permits malicious nodes to engage in routing through more rounds of intermediates, which enhances loss of packets and raises effective throughput in the meantime before effective isolation is attained. Values of throughput in Table 5 thus reflect the attack-specific effective throughput averaged over all 100 rounds, and not peak global throughput, and are entirely consistent with the decreasing throughput curve of Fig. 11 as the fraction of malicious nodes rises. The average energy usage reported is the total per-node energy use relative to the total time spent on the simulation (100 rounds) and includes data transmission, trust computation, control messaging and cluster-head operations. Redundancy in energy consumption is witnessed when isolated and malicious nodes are detected early hence fewer retransmissions and control overheads are incurred, and increased energy consumption is incurred when attacks are intermittent and collusive since the monitoring cycle, updating trust and adjusting routes takes long.

6 Conclusion and future work

Our study presents an excellent and effective model known as the Trust-based Integrated Techniques of Anomaly in this research paper. Neutralization (TITAN) model of enhancing cooperation and security in large size IWSNs. TITAN leverages on an innovative strategic unequal clustering to optimize the energy consumption in terms of having smaller clusters placed near the sink and larger clusters placed farther away to balance energy distribution and also communication load. The suggested OCREA algorithm is one of the important aspects of dynamically choosing CHs. Using a fitness score, using the residual energy, quality of the link, signal strength and distance between the BS and the user. This systematic process enables TITAN to be resource efficient, and with longer network lifespan and using less energy. This makes TITAN particularly useful in resource-vary resource scarce IWSNs, where networks must be conserved of energy to be able to last longer and performance. More so, the logarithmic punishment by TITAN is efficient in isolating untrustworthy SNs, saving energy lost in messages to these untrustworthy SNs. Besides, TITAN also involves a distributed intra-cluster and centralized intercluster trust decision-making, which encompasses the multi-dimensional trust measures which include communication trust, data trust and energy trust. The components will provide proper and thorough assessment of trust and provide a trustworthy and dependable network climate. This is done by the introduction of dynamic logarithm trust operations where TITAN can provide due rewards and penalties on the behavior of the SNs, differentiating between honest and corrupt SNs. The dynamic aging and damping factors that are added to TITAN can guarantee that trustworthiness is gauged by the latest conduct. This eases the impact of outdated data and increasing the responsiveness to evolving network dynamics. The aging factor would make sure that by involving time, quality and intensity in the computation of the trust, this would guarantee that the trust was correct where obsolete or less crucial interactions hold are considered as having lesser impact on the value of trust. The trust model is permitted by this dynamic approach to give weight to the new and important interactions, more responsive and reliable trust assessment. Simulation results emphasize the fact that it is better in different metrics of performance. TITAN always groups in low in the assessment of packet loss rate percentages of lost packets, out of the schemes such as SDTS, DTMS and DST-WOA were out performing in all rounds. This demonstrates TITAN's capacity to ensure high integrity of data and quality communication even on long operation. Also, the superior of TITAN detection rate on various ratios of malicious SNs illustrates its ability to distinguish vertically adversarial SNs and isolate them. It has a high detection rate even in a more challenging environment of the network. For instance, even at a 60% malicious SN ratio, the detection rate with TITAN is 87, which is much higher than other models. The FPR and FNR further validate TITAN's precision. The suggested model is continually showing low values of FPR and FNR at different ratios of selfish. SNs with SDTS, DTMS, and DST-WOA, which puts a strong focus on its reliability in providing accurate classification of trustworthy and malevolent SNs. This will make sure that they do not wrongly flag benign SNs as threats by keeping operational efficiency intact deterrence of maliciousness. The dynamism of TITAN in adapting to the various network environments due to its multi-factor trust analysis and neighboring SNs feedback mechanism, improves its robustness and resiliency against typical and advanced ones attacks.

Further development of the TITAN model can be conducted on the areas that need to be improved to enhance its skills and effectiveness. Integrating advanced deep reinforcement learning models have the potential to increase real-time mitigation and anomaly detection as well preserving data privacy [51, 52]. TITAN will be able to support complex heterogeneous IWSNs by means of scalability improvements, dynamical distribution of resources. It is also possible to increase protection against multi-layered by introducing cross layer security measures attacks. Future studies may also look into adaptive trust measures, contextualized management and incorporation of edge calculating to more efficiency [53]. Lastly, the practical use will prove the efficiency of TITAN and will reveal usefulness challenges that simulations can help miss.

Authors contribution Khushboo Tripathi: Writing – original draft, Methodology. Shalu: Methodology, Software, Validation, Visualization, Conceptualization, Formal analysis, Investigation. Sheetal Kaushik: Conceptualization, Writing – review & editing, Methodology. Shubham Vyas: Conceptualization, Writing, Formal analysis, Investigation. Mohd Anas Khan: Supervision, Formal analysis, Investigation, Editing. Ali Ahmadian: Conceptualization, Methodology, Supervision.

Funding There is no funding for this research article to be declared.

Data availability The datasets generated and/or analyzed during the current study are available from the corresponding author on reasonable request.

Declarations

Competing interests The authors declare no competing interests. AI Usage Disclosure: Artificial intelligence tools (Grammarly, ChatGPT) were used solely for language refinement and grammatical correction. All scientific and technical content was developed and validated by the authors.

References

1. Zhang J et al (2010) A trust management architecture for hierarchical wireless sensor networks. IEEE Local computer network conference. IEEE
2. Li X, Zhou F, Du J (2013) LDTS: a lightweight and dependable trust system for clustered wireless sensor networks. IEEE Trans Inf For Secur 8(6):924–935
3. Talbi S et al (2017) Adaptive and dual data-communication trust scheme for clustered wireless sensor networks. Telecommun Syst 65(4):605–619
4. Singh M et al (2017) A lightweight trust mechanism and overhead analysis for clustered WSN. IETE J Res 63(3):297–308
5. Shaikh RA, Jameel H, d'Auriol BJ, Lee H, Lee S (2009) Group-based trust management scheme for clustered wireless sensor networks. IEEE Trans Parallel Distrib Syst 20(11):1698–1712
6. Kwon S, Jeong J, Shon T (2018) Toward security enhanced provisioning in industrial IoT systems. Sensors 18(12):4372
7. Kim T-H, Goyat R, Rai MK, Kumar G, Buchanan WJ, Saha R, Thomas R (2019) A novel trust evaluation process for secure localization using a decentralized blockchain in wireless sensor networks. IEEE Access 7:184133–184144
8. Smache M, Olivereau A, Franco-Rondisson T, Tria A (2019) Time synchronization attack scenarios and analysis of effective self-detection parameters in a distributed industrial wireless sensor network. In: 2019 17th International conference on privacy, security and trust (PST), IEEE, pp 1–5
9. 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. Wirel Netw 26:3169–3182
10. Yang L, Lu Y, Yang SX, Guo T, Liang Z (2020) A secure clustering protocol with fuzzy trust evaluation and outlier detection for industrial wireless sensor networks. IEEE Trans Ind Inform 17(7):4837–4847
11. Leng J, Ye S, Zhou M, Zhao JL, Liu Q, Guo W, Cao W, Fu L (2020) Blockchain-secured smart manufacturing in industry 4.0: A survey. IEEE Trans Syst, Man, Cybern: Syst 51(1):237–252
12. Wang J, Jing X, Yan Z, Fu Y, Pedrycz W, Yang LT (2020) A survey on trust evaluation based on machine learning. ACM Comput Surv (CSUR) 53(5):1–36
13. Saidi A, Benahmed K, Seddiki N (2020) Secure cluster head election algorithm and misbehavior detection approach based on trust management technique for clustered wireless sensor networks. Ad Hoc Networks 106:102215
14. Nancy P, Muthurajkumar S, Ganapathy S, Santhosh Kumar SVN, Selvi M, Arputharaj K (2020) Intrusion detection using dynamic feature selection and fuzzy temporal decision tree classification for wireless sensor networks. IET Commun 14(5):888–895
15. Demertzis K, Iliadis L, Tziritas N, Kikiras P (2020) Anomaly detection via blockchained deep learning smart contracts in industry 4.0. Neural Comput Appl 32(23):17361–17378
16. Leng J, Ruan G, Jiang P, Xu K, Liu Q, Zhou X, Liu C (2020) Blockchain-empowered sustainable manufacturing and product lifecycle management in industry 4.0: A survey. Renew Sustain Energy Rev 132:110112
17. Khan T, Singh K, Hasan MH, Ahmad K, Reddy GT, Mohan S, Ahmadian A (2021) ETERS: A comprehensive energy aware trust-based efficient routing scheme for adversarial WSNs. Futur Gener Comput Syst 125:921–943
18. Rathee G, Balasaraswathi M, Chandran KP, Gupta SD, Boopathi CS (2021) A secure WSN sensors communication in industry 4.0 using blockchain technology. J Ambient Intell Humaniz Comput 12(1):533–545
19. Yang L, Yang SX, Li Y, Lu Y, Guo T (2022) Generative adversarial learning for trusted and secure clustering in industrial wireless sensor networks. IEEE Trans Ind Electron 70(8):8377–8387
20. Roy PK, Bhattacharya A (2022) SDIWSN: A software-defined networking-based authentication protocol for real-time data transfer in industrial wireless sensor networks. IEEE Trans Netw Serv Manage 19(3):3465–3477
21. Kavitha V, Ganapathy K (2022) Galactic swarm optimized convolute network and cluster head elected energy-efficient routing protocol in WSN. Sustain Energy Technol Assess 52:102154
22. Anitha S, Saravanan S, Chandrasekar A (2023) Trust management based multidimensional secure cluster with RSA cryptography algorithm in WSN for secure data transmission. Measurement: Sensors 29:100889
23. Khan T, Singh K, Ahmad K, Bin Ahmad KA (2023) A secure and dependable trust assessment (SDTS) scheme for industrial communication networks. Sci Rep 13(1):1910
24. Kumar S, Chinthaginjala R, Ahmad S, Kim T (2025) Energy-efficient unequal multi-level clustering for underwater wireless sensor networks. Alex Eng J 111:33–46
25. Shafique T, Soliman A-H, Amjad A (2024) Data traffic based shape independent adaptive unequal clustering for heterogeneous wireless sensor networks. IEEE Access 12:46422–46443
26. Mir F, Meziane F (2024) Unequal-radius clustering in WSN-based IoT networks: energy optimization and load balancing in UDCOPA protocol. J Supercomput 80(19):26890–26921. https://link.springer.com/article/10.1007/s11227-024-06426-w
27. Srivastava G, Singh JN, Manjul M, Paul A (2024) Dyclust: A hybrid key management scheme for wireless sensor network. SN Computer Science, 5(2):269. https://link.springer.com/article/10.1007/s42979-023-02584-5
28. Vazhuthi PPI, Prasanth A, Manikandan SP, Devi Sowndarya KK (2023) A hybrid ANFIS reptile optimization algorithm for energy-efficient inter-cluster routing in internet of things-enabled wireless sensor networks. Peer-to-Peer Network Appl 16(2):1049–1068
29. Khan T, Singh K, Shariq M, Ahmad K, Savita KS, Ahmadian A, Salahshour S, Conti M (2023) An efficient trust-based decision-making approach for WSNs: Machine learning oriented approach. Comput Commun 209:217–229
30. Leontaris L, Mitsiaki A, Charalampous P, Dimitriou N, Leivaditou E, Karamanidis A, Margetis G et al (2023) A blockchain-enabled deep residual architecture for accountable, in-situ quality control in industry 4.0 with minimal latency. Comput Ind 149:103919
31. Wang C, Liu G, Jiang T (2024) Malicious node detection in wireless weak-link sensor networks using dynamic trust management. IEEE Trans Mobile Comput 12:12866–12877
32. Ravikumar P, Ganesh Kumar P (2024) A novel energy-efficient routing protocol for industrial WSN using hybrid COOT-LS algorithm with LSTM-based DOM prediction. Int J Commun Syst 37(3):e5656

33. Dinesh K, Svn SK (2024) GWO-SMSLO: Grey wolf optimization based clustering with secured modified Sea Lion optimization routing algorithm in wireless sensor networks. Peer-to-Peer Netw Appl 1–27
34. Khan T, Singh K (2023) RTM: realistic weight-based reliable trust model for large scale WSNs. Wirel Pers Commun 129(2):953–991
35. Khan T, Singh K (2024) DTMS: A dual trust-based multi-level sybil attack detection approach in WSNs. Wireless Person Commun 1–32
36. Singh S, Anand V, Yadav S (2024) Trust-based clustering and routing in WSNs using DST-WOA. Peer-to-Peer Network Appl 1–13
37 Khan MA, Shalu QN, Naveed AL, Kaushik S, Kumar S (2024) A multi-layered assessment system for trustworthiness enhancement and reliability for industrial wireless sensor networks. Wireless Person Commun 137(4):1997–2036
38. Singh H, Bala M, Bamber SS, Angurala M (2024) Detection of wormhole attack via bio-inspired ant colony optimization based trust model in WSN assisted IoT Network. Wireless Person Commun 1–22
39. Baharloo N, Bentahar J, Alwhishi G, Drawel N, Pedrycz W (2024) Verifying trust over IoT-ad hoc network-based applications under uncertainty. Ad Hoc Netw 154:103380
40. Kumar N, Sharma S (2024) PathGuard: Trustworthy routing for sustainable and secure IoT-WSN networks. Wireless Person Commun 1–19
41. Juwaied A, Jackowska-Strumillo L (2025) DL-HEED: a deep learning approach to energy-efficient clustering in heterogeneous wireless sensor networks. Appl Sci 15(16):8996
42. Juwaied A, Jackowska-Strumillo L (2025) Applying machine learning to DEEC protocol: improved cluster formation in wireless sensor networks. Network 5(3):26
43. Dinesh K, Santhosh Kumar SVN (2023) Energy-efficient trust-aware secured neuro-fuzzy clustering with sparrow search optimization in wireless sensor network. Int J Inf Sec 1–25
44. Bangali H, Rodrigues P, Pandimurugan V, Rajasoundaran S, Santhosh Kumar SVN, Selvi M, Kannan A (2023) Prediction of middle box-based attacks in Internet of Healthcare Things using ranking subsets and convolutional neural network. Wireless Netw 1–19
45. Santhosh Kumar SVN, Yesuraj R, Munuswamy S, Arputharaj K (2023) A comprehensive survey on certificate-less authentication schemes for vehicular ad hoc networks in intelligent transportation systems. Sensors 23(5):2682
46. Rajkumar Y, Santhosh Kumar SVN (2024) An elliptic curve cryptography based certificate-less sigTITAN aggregation scheme for efficient authentication in vehicular ad hoc networks. Wireless Netw 30(1):335–362
47. Rajasoundaran S, Santhosh Kumar SVN, Selvi M, Thangaramya K, Arputharaj K (2024) Secure and optimized intrusion detection scheme using LSTM-MAC principles for underwater wireless sensor networks. Wireless Netw 30(1):209–231
48. Jayashree S, Santhosh Kumar SVN (2024) LAPEP—Lightweight authentication protocol with enhanced privacy for effective secured communication in vehicular ad-hoc network. Wireless Netw 30(1):151–178
49. Sharma V, Beniwal R, Kumar V (2024) Multi-level trust-based secure and optimal IoT-WSN routing for environmental monitoring applications. J Supercomput 1–44
50. Gangwani P, Perez-Pons A, Upadhyay H (2024) Evaluating trust management frameworks for wireless sensor networks. Sensors 24(9):2852
51. Khan T, Singh K, Purohit KC (2020) ICMA: an efficient integrated congestion control approach. Recent Pat Eng 14(3):294–309
52. Khan T, Singh K, Gupta S, Manjul M (2022) Multi trust-based secure trust model for WSNs. J Inf Technol Manage 14(Special Issue: Security and Resource Management challenges for Internet of Things):147–158
53. Dohare I, Singh K, Khan T, Mohan Y, Alam I (2025) Coati optimization algorithm for node localization in sensor enabled-IoT. Cluster Comput 28(4):221

Authors and Affiliations

Khushboo Tripathi[1] · Shalu[2,8] · Sheetal Kaushik[3] · Shubham Vyas[4] · Mohd Anas Khan[5] · Ali Ahmadian[6,7]

✉ Ali Ahmadian
ahmadian.hosseini@gmail.com

Khushboo Tripathi
khushbootripathi.cse@gmail.com

Shalu
singhshalu2609@gmail.com

Sheetal Kaushik
sheetal.kaushik618@gmail.com

Shubham Vyas
r.shubhamvyas@gmail.com

Mohd Anas Khan
anas.cse786@gmail.com

[1] Department of Computer Science & Applications, Sharda University, Greater Noida, Uttar Pradesh, India

[2] London Metropolitan University, London, UK

[3] Department of Computer Applications, Shanti Business School, Ahmedabad, Gujarat 380058, India

[4] Amity Institute of Information Technology, Amity University Haryana, Gwaliar, Haryana 122413, India

[5] School of Engineering, Jawaharlal Nehru University, New Delhi 110067, India

[6] Institute of Visual Informatics, Universiti Kebangsaan Malaysia (UKM), Selangor 43600 Bangi, Malaysia

[7] Faculty of Engineering and Natural Sciences, Istanbul Okan University, Istanbul, Turkey

[8] Manav Rachna University Faridabad, Delhi, India