IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 16, 2019, accepted April 29, 2019, date of publication May 3, 2019, date of current version May 15, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2914769

A Novel and Comprehensive Trust Estimation Clustering Based Approach for Large Scale Wireless Sensor Networks

TAYYAB KHAN[1], KARAN SINGH[1], LE HOANG SON[2], MOHAMED ABDEL-BASSET[3], HOANG VIET LONG[4,5], SATYA P. SINGH[6], AND MANISHA MANJUL[7]

[1]School of Computer and Systems Sciences, Jawaharlal Nehru University, New Delhi 110067, India
[2]VNU Information Technology Institute, Vietnam National University, Hanoi 010000, Vietnam
[3]Department of Operations Research, Faculty of Computers and Informatics, Zagazig University, Zagazig 44519, Egypt
[4]Division of Computational Mathematics and Engineering, Institute for Computational Science, Ton Duc Thang University, Ho Chi Minh City 700000, Vietnam
[5]Faculty of Mathematics and Statistics, Ton Duc Thang University, Ho Chi Minh City, Vietnam
[6]School of Computer Science and Engineering, Nanyang Technological University, Singapore 639798
[7]CSE, G. B. Pant Government Engineering College, New Delhi 110020, India

Corresponding author: Hoang Viet Long (hoangvietlong@tdtu.edu.vn)

ABSTRACT With the wide applications of wireless sensor networks (WSNs) in various fields, such as environment monitoring, battlefield surveillance, healthcare, and intrusion detection, trust establishment among sensor nodes becomes a vital requirement to improve security, reliability, and successful cooperation. The existing trust management approaches for large-scale WSN are failed due to their low dependability (i.e., cooperation), higher communication, and memory overheads (i.e., resource inefficient). In this paper, we propose a novel and comprehensive trust estimation approach (LTS) for large-scale WSN that employs clustering to improve cooperation, trustworthiness, and security by detecting malicious (faulty or selfish) sensor nodes with reduced resource (memory and power) consumption. The proposed scheme (LTS) operates on two levels, namely, intra-cluster and inter-cluster along with distributed approach and centralized approach, respectively, to make accurate trust decision of sensor nodes with minimum overheads. LTS consists of unique features, such as robust trust estimation function, attack resistant, and efficient trust aggregation at the cluster, head to obtain the global feedback trust value. Data trust along with communication trust plays a significant role to cope with malicious nodes. In LTS, punishment and trust severity can be tuned according to the application requirement, which makes it an innovative LTS. Moreover, dishonest recommendations (outliers) are eliminated before aggregation at the base station by observing the statistical dispersion. The theoretical and mathematical validations along with simulation results exhibit the great performance of our proposed approach in terms of trust evaluation cost, prevention, and detection of malicious nodes as well as communication overhead.

INDEX TERMS Trust management, data trust, communication trust, attack mitigation.

I. INTRODUCTION

Wireless sensor networks (WSNs) are collections of small size, self-organized hundred to thousand low-cost resource constraint sensor nodes (SNs) and mainly deployed in the hazardous/ hostile area to monitor events and report continuous as well as discrete data. WSNs nodes communicate via radio links with limited available bandwidth and form a temporary network i.e. network without predefined infrastructure and without centralized network administration [1]–[3]. WSN uses a highly dynamic network topology where, any time, sensor nodes can leave-joins a network and change their locations. Due to the broadcast(deployment) nature of WSNs, SNs are less reliable, failure-prone and susceptible to several security attacks like on-off attack, Sybil attack, etc. [4]–[7]. Once a sensor node (SN) is compromised by adversary force, it misguides other SNs to misbehave (false feedbacks, false positive, etc.) therefore, erroneous data routing by malicious nodes will breakdown the entire network. In such cases, whenever WSN node itself becomes a malicious node and due

The associate editor coordinating the review of this manuscript and approving it for publication was Victor Hugo Albuquerque.

to resource constraints (limitation of WSNs) nodes, cryptographic techniques and authentication schemes cannot alone prevent from internal attacks [8], [9]. Thus, we need a different kind of robust security mechanism to prevent WSNs from internal and external attacks known as trust estimations mechanism in wireless sensor networks. Trust estimation methods are used to estimate the dependability, reliability, and trustworthiness of SNs by analyzing their behaviors to prevent them against malicious nodes for the survival of wireless sensor nodes [10], [11].

Security, trust, and reputation are the most frequently used terms regards to WSNs. Let's, very first we briefly define these terms. In WSNs or secure systems, the terms security and trust are used interchangeably. Trust and security have many key differences in terms of complexity and overhead. Security imposes overhead on the networks. Trust is less complex than security and used to improve the security and reliability of WSN [12], [13]. Reliability is defined as ''How long a sensor node can be trustworthy''. In WSN, Reputation is defined as the ''opinion of one sensor node about the other sensor nodes'' and ''Trust is a derivation of the reputation of an entity'' [14]–[16]. Both trust and reputation are used to make effective decisions to select relay nodes and analyzing sensed data coming from other neighboring nodes to classify it trustworthy and malicious [17], [18]. Trust establishment provides various advantages by resolving several issues and limitations [19] listed as follows:

1) Trust establishment (TE) analyze the behavior of sensor nodes to resolve the limitation of traditional security mechanism by providing corresponding access control.
2) Trust establishment (TE) detects selfish and malicious nodes to make a reliable and robust security mechanism.
3) Trust establishment (TE) solves the issue of finding a reliable routing path (or gateway nodes) by detecting all the malicious or faulty nodes of routing paths (especially in inter-cluster communication).
4) Trust establishment (TE) ensures that communication happens among trustworthy sensor nodes (SNs) during key management, authentication, and authorization.

We visualize that exiting clustering approaches [4], [7], [10], [11], [19]–[23] is far better than individual SNs for effective collaboration in order to collect, aggregate and forward accurate data to base station. Moreover clustering approaches improve network throughput, scalability and gives flexibility to choose a cluster head (a sensor node with strong computing power or selected by election process [25]–[32] that will be responsible for detecting selfish (malicious) nodes and provide reliable route to cluster members within cluster to send their data. Decision making considering only communication trust in an open and hostile WSN might deceive the entire network performance. A huge number of selfish nodes might provide a false recommendation about neighbor nodes which results in incorrect evaluation during aggregation at cluster heads and base station to obtain final trust value.

Unlike the above existing reported schemes, the proposed scheme consider data trust along with communication trust to mitigate untrustworthy nodes by eliminating false recommendation using an outlier filtering approach. With this proposed scheme, successful collaboration among all cluster heads during inter-cluster communication would be able to select a trusted and reliable global route to send trusted ''data to the base station (BS) without interruption.''

A. MOTIVATION

Unfortunately, the most fundamental requirements namely resource efficiency and dependability issues with TMS for WSN have not received much attention from researchers. Among the various existing trust management approaches for WSN [3], [7], [10], [19], [22]–[24], [20], [33]–[37], only the following researches in [10], [19], [22]–[24] were developed specifically for clustered WSNs that suffers from several limitations such as memory overhead, communication overhead and work under assumptions like dependency on specific platform or routing scheme that makes them unrealistic for large scale WSN [19]. To the best of our knowledge, only [10], [22], [23], [38] focused on both resource efficiency and dependability issues with TMS for WSN but still suffer from various issues like accuracy, attack resistant, convergence speed, complexity, and additional overheads. Moreover, in an open or hostile environment, malicious feedbacks can reduce the system dependability, availability and leads to incorrect trust decision.

B. OUR CONTRIBUTION

To remove the limitation of existing trust management schemes (TMS) [10], [19], [22], [23], we propose a novel and comprehensive TMS consisting the following unique features to improve cooperation among SNs in order to build a robust and reliable trust system.

1) Generate unique identity for each sensor node to make communication easier and secure from external attacks
2) Provide a robust and lightweight trust estimation scheme by employing clustering to improve cooperation among CMs and CHs. During intra-cluster trust evaluation, CH computes indirect communication and data trust to reduce the overhead of maintaining feedbacks at a CM (say i) of other CMs (say j). In the same way, the base station will be responsible to evaluate indirect trust during inter-cluster communication. This approach significantly reduces the transmission (communication) overhead and the possibility of malicious behavior (badmouthing and ballot stuffing attack) by malicious SNs.
3) Provide an efficient ''trust decision-making scheme at CH level to improve resource efficiency and cooperation among CHs by reducing the overhead of network communication.''

4) A simple averaging scheme is introduced to aggregate the trust values for cluster heads to overcome the limitations of existing TMS [8], [22].
5) Punishment and trust severity can be tuned according to the application requirement makes it an innovative LTS.
6) Platform independent and not affected by chosen of any specific routing scheme

The effectiveness and validation of the proposed scheme [LTS] are shown by mathematical foundation and simulation results. The remaining part of this paper is structured into five more sections. Section II discusses the related work with their research gaps and comparative analysis. Section III and IV provide the proposed TMS and their comprehensive validation respectively. Section V provides the comparative simulation analysis and exhibits the performance of the proposed scheme and finally, Section VI gives the conclusion and future work.

II. RELATED WORKS

There are various methods and approaches to model the trust like probability, fuzzy, weighted, Bayesian, game theory, neural network, entropy-based and miscellaneous trust computation methods. These trust models are generally categorized into two subcategories namely node and data trust models. Node trust models are further divided into two categories namely centralized and distributed trust model [4], [5], [10], [12], [18], [19], [22], [24].

In the centralized model, a trusted node (SN or BS) calculates the trust value of SNs but in the distributed model, each SN itself calculates their trust value. Many TMSs have been proposed recently in various fields like WSNs, peer-to-peer networks and e-commerce [39]–[44] that exhibit the significance of trust estimation. However, most of them suffer from various limitations such as resource constraint, dependability and vulnerable to attacks. This section provides the literature survey of the existing TMSs for distributed and clustered WSN. Desai *et al.* [54] proposed a novel trust evaluation known as ''MITE: Memory integrity based trust evaluation in Wireless Sensor Networks.'' The author believes that the trust scheme plays an important role to improve security over cryptographic techniques. The proposed scheme uses a metric known as ''integrity of the node-memory'' to evaluate trust and experimental results exhibit its great performance in terms of trust evaluation at both node-level and network-level. The advantages of this scheme ''are the elimination of persistent storage and inaccuracy due to second-hand information. The results obtained indicate that the change in hash value can be observed for tampered memory. If hash values are the same, time taken to compute hash at both ends is used to determine if the node is trustworthy'' or not.

According to Ishmanov *et al.* [9], a robust trust estimation scheme plays a vital role in WSN to improve security, reliability and successful cooperation. Authors believe that on-off attack is the most severe attack to degrade the performance of sensor network so they proposed a trust management scheme to mitigate persistent malicious behavior and on-off attacks. In addition, a misbehavior component along with forgetting factor is introduced to effectively deal with such types of attacks. Recommendation trust is computed by removing outliers from the available feedbacks from CMs. The authors state that it is lightweight and robust against badmouthing attack and persistent malicious behavior.

Kim *et al.* [6] proposed an accurate and dynamic trust model (TM) known as ''an efficient dynamic trust evaluation model (DTEM)'' for WSNs. This weight-based scheme considers the multi-trust (data, communication and energy trust) and dynamic approach to calculate the direct, indirect trust and in updating the trust respectively. DTEM uses Beta probability density function (BPDF) at the node level, regulating function, IOWA update mechanism enhance flexibility and punishment factor to achieve correct trust estimation results by analyzing the good and bad behavior of neighboring nodes. The BPDF used in this scheme can be represented as

$$f(x|\gamma,\beta) = \frac{1}{(\gamma,\beta)} x^{\gamma-1}(1-x)^{\beta-1} \tag{1}$$

where γ and β are two indexed parameters and $0 \leq x \leq 1, \gamma > 0, \beta > 0$:

$$\mathrm{E(x)} = \frac{\gamma}{\gamma+\beta} = \frac{\mathrm{a}+1}{\mathrm{a}+\mathrm{b}+2} \tag{2}$$

where the term E(x) is defined as the probability expectation value for BPDF. The symbol a denotes the number of successful interactions between nodes and b denotes the unsuccessful interactions between nodes. Although DTEM can effectively identify malicious behavior to improve security in WSN, it still suffers from communication overhead and high resource consumption that makes it an unrealistic approach because of limited resources (memory, processor, etc.) of sensor nodes.

Shaikh *et al.* [3] proposed energy aware, lightweight and attack resistant scheme for Clustered WSNs knows as GTMS that calculate trust at three levels (node, cluster head, and the base station) in order to identify various attacks by classifying trust values in trusted, untrusted and uncertain states. It uses the timing window concept to get information about successful and unsuccessful interactions between two nodes in trust computation. The information present in the timing window is used to evaluate the trust value of node y at node x according to (3) where $S_{x,y}$ and $U_{x,y}$ are defined in TABLE 3.

$$T_{x,y} = \left[100 \times \left(\frac{(S_{x,y})^2}{(S_{x,y} + U_{x,y})(S_{x,y} + 1)} \right) \right] \tag{3}$$

GTMS is attack resistant under an assumption that is $S_{x,y} \leq U_{x,y}$ that is not always true and it cannot effectively encounter on-off attack that makes it not suitable for real-time applications [8]–[10]. Zhang *et al.* [21] suggested two-tier architecture based lightweight and attack resistant trust management scheme (TMS) especially for secure medical SNs

known as "ReTrust" which is Similar to [3] with a newly proposed trust estimation equation (4) defined as follows:

$$T_{x,y} = \left[\alpha \times \left(\frac{\sum_{j=1}^{m} \beta_j \times (1-p_j)\times p_j}{\sum_{j=1}^{m} \beta_j \times (1-p_j)}\right)\right] \quad (4)$$

where α, m, β_j, and p_j represent the format and range of the trust values, "number of units in a window-based forgetting mechanism, aging-factor parameter, β_j," and successful interaction rate respectively. The term p_j in (4) is estimated by using the (5)

$$p_j = \frac{S_j + 1}{S_j + U_j + 2} \quad (5)$$

The author states that "ReTrust" is an efficient attack resistant, lightweight with effective malicious behavior detection that makes it highly suitable for medical sensor networks and can improve network performance by removing the weakness of TMS. Although it is said that this scheme is robust against bad- mouthing and on-off attack but without considering misbehavior rate along with frequency and persistency of misbehavior, a good on-off mitigating trust model (TM) is quite complicated to design [9]. Fang *et al.* [48] proposed novel healthcare –oriented TMS for healthcare WSN (HWSN) based on binomial distribution with higher detection and accuracy to resolve various security issues caused by internal attacks such as on-off attack and bad mouthing attack. The author states that BDTMS is secure and realistic and can rapidly and effectively detect an on-off attack and collusion attack but scalability, stability, and overhead issues are still there that makes it non-suitable for large HWSN.

Zhang *et al.* [49] proposed energy efficient, accurate and reliable improved Bayesian-based TMS for WSNs to detect and mitigate malicious nodes. The author introduced two new factors (reward, penalty) along with attenuation function (for updating trust values) to improve the performance and efficiency of proposed TMS. The proposed model is compared with the well-known trust model RFSN [33] through simulation on NS-2 and exhibit good performance than RFSN in terms of trust estimation, attack detection, and energy consumption. Feng *et al.* [7] proposed "A trust evaluation algorithm for wireless sensor networks based on node behaviors and DS evidence theory" known as NBBTE to identify compromised and malicious nodes. It employs a weighted and fuzzy approach depending on the number of malicious nodes. MATLAB is used to simulate the proposed work that exhibits the accuracy and efficiency in terms of nodes trustworthiness, uncertainty and fuzziness. The main drawback of NBBTE is higher communication overhead (resource consumption) and memory overhead that makes it non-realistic for large scale WSNs.

Górski and Turower [51] proposed a novel TMS employing a weighted, lightweight and energy efficient approach for data trust, behavior trust, and historical trust to ensure data credibility and reliability in WSNs. After analyzing the OMNET++ simulation results, Author claims that it is better than LDTS, DRBTS and TRM-IoT model in terms of abnormal behavior detection (monitoring) and resource consumption results in improved node's survival time in the sensor network. Only trusted nodes can participate in data fusion to reduce overheads and trust list is dynamically updated. The major drawbacks of this scheme are non-scalability, non-stability and not robust against on-off attack. Moreover, no mathematical validations are provided to prove the efficiency of the proposed scheme and no external security module is considered. Kim *et al.* [6] suggested a "fuzzy logic based trust model" for WSNs. In this work, only highly trusted nodes can participate in sharing their trust values in order to make safe and secure communication by choosing a trusted communication path "between the source node and the destination" node. The trust evaluation (trustworthiness (T) and untrustworthiness (U)) between two nodes i and j can be estimated by using (6) and (7) respectively

$$T = \left[\frac{avg\left(T_i, T_j\right)}{1 - \left(avg\left(T_i, U_j\right) + avg\left(T_j U_i\right)\right)}\right] \quad (6)$$

$$U = \left[\frac{avg\left(U_i, U_j\right)}{1 - \left(avg\left(T_i U_j\right) + avg\left(T_j U_i\right)\right)}\right] \quad (7)$$

Trust evaluation value between nodes i and $j = \frac{T}{T+U}$ The BS has the reputation value of each node, But the problem is in most cases WSN is either distributed or hierarchical in nature and they have not mentioned the way how BS evaluates the trust of a node. Moreover, it works only for static workload and not robust against various malicious attacks. Memory and communication overheads are not discussed.

Singh *et al.* [45] proposed a dynamic, adaptive and lightweight trust evaluation scheme for decentralized WSN. It calculates direct trust (using successful and unsuccessful interactions) and indirect trust (using reputation scheme) to quantize nodes as trusted or untrusted. trust value of node B at node A is computed by (8) as follows:

$$T_i^{A,B} = \left[\frac{S_i^{A,B}}{\left(S_i^{A,B} + F_i^{A,B}\right)}\right] \quad (8)$$

where S is successful and F is unsuccessful transactions. Direct & Indirect trust in this scheme is evaluated using (9) and (10) as follows

$$DT^{A,B} = C^{A,B} * \sum_{i=1}^{m} \left(W_i * T_i^{A,B}\right) \quad (9)$$

$$\&IT^{A,B} = \sum_{j=1}^{n} \left(W_{A,N_j} * DT^{NjB}\right) \quad (10)$$

Thus, Total Trust is

$$(TT^{A,B}) = W_a * DT^{A,B} + W_b * IT^{A,B}.$$

Here the distance trust is also incorporated as: $T_d = 1 - \frac{d_i}{\sum d_i}$ where d_i is the distance of the i^{th} neighbor. Although this method is suitable for clustered WSNs but it is not highly recommended because it is not robust against well-known on-off attack. Singh *et al.* [23] proposed "A lightweight trust mechanism (LWTS) and overhead analysis for clustered WSN."

In this work, the author try to resolve the weight allocation problems by applying a self-adaptive weight allocation method at the cluster head level for both direct trust and indirect trust using (11) and (12) respectively as follows:

$$W_1 = 1 - \left(\frac{S^{direct}_{ch_i,ch_j}}{S^{direct}_{ch_i,ch_j} + S^{indirect}_{BS,,ch_i}} \right) \tag{11}$$

$$W_2 = 1 - \left(\frac{S^{indirect}_{BS,ch_i}}{S^{direct}_{ch_i,ch_j} + S^{indirect}_{BS,,ch_i}} \right) \tag{12}$$

where W1 and W2 provide more weightage to direct trust and indirect trust respectively under the situations mentioned in [23] Where $S^{direct}_{ch_i,ch_j}$ and $S^{indirect}_{BS,ch_i}$ is the successful interaction between CH_i and CH_j and positive recommendations about CH_i collected by BS from other neighboring cluster head of CH_i . Moreover, in LWTS, each cluster member can directly communicate with the cluster head to reduce communication overhead leads to creation of more number of cluster for large WSNs that makes it unrealistic for large WSNs because in reality cluster member send trust values through other cluster members comes in the trusted shortest route selected by any shortest path algorithms [50], [58], [59], [60]. However, it has been proved that LWTS is better than LDTS [22] (due to specific topology) and GTMS [19] in terms of memory, communication overhead but scalability issue is not considered in this work.

Shakkira [38] proposed an advance trust system known as ALDTS to identify compromised, malicious and malevolent nodes in WSNs by providing node level protocol-based security. The author states that TMS should be highly dependable, energy efficient and secure along with low communication and memory (resource) overhead for the survival of WSNs. ALDTS uses SHA-256 to incorporate security and eliminate unnecessary communication overhead created by cluster members on the cluster head. ALDTS doesn't provide any mathematical, simulation proof against on-off, badmouthing, and various other external attacks. Moreover, ALDTS has not discussed about scalability issue, memory overhead issue, and dynamic that makes it unrealistic approach for WSNs.

Ishmanov *et al.* [9] proposed a simple, stable, attack- resistance and lightweight TMS known as ''A robust trust establishment scheme for wireless sensor networks'' to mitigate various internal attacks like on-off with high detection rate by incorporating a key component misbehavior frequency. The author states that security and cooperation improvement among sensor nodes (SNs) through TMS is vital for the survival of WSNs because external attack resiliency using various authentication and cryptographic techniques are fail to protect WSNs due to it open, remote and unattended nature of deployment. The author believes that TMS can also be vulnerable to on-off attack in which nodes periodically changes their behaviors to damage the WSN. Each parameter in all proposed equations is clearly defined with appropriate reasons in this work. By using the time window concept, rate and weight of misbehavior is computed respectively as follows:

$$\begin{cases} oif \dfrac{UJ}{UJ + SJ} \leq \theta \\ \dfrac{UJ}{UI + SI} \qquad \text{otherwise} \end{cases} \tag{13}$$

and $w^m_{tk} = \max(\alpha 1r1, \alpha 2r2, \alpha 3r3, \ldots\ldots \alpha jrj, \alpha LrL)$.

After computing weight of misbehavior at time tk $\left(\mathrm{w}^{\mathrm{m}}_{\mathrm{tk}}\right)$, trust is computed using (14) as follows

$$\mathrm{T_{tk}} = 1 - \mathrm{w}^{\mathrm{m}}_{\mathrm{tk}} \tag{14}$$

The concept of on and off period is used to measure the misbehavior frequency (15) as follows

$$f^m_{tk} = \frac{o_{tk}}{o_{tk} + p_{tk}} \tag{15}$$

In order to find the node status, misbehavior frequency component is used as follows

$$\mathrm{S}\left(\mathrm{f}^{\mathrm{m}}_{\mathrm{tk}}\right) = \left\{ \begin{array}{c|c} 1 & persistentmaliciousnode \\ (0;\theta) & legitimatenode \\ (\theta;1) & maliciousnode \end{array} \right\}. \tag{16}$$

Once node status is identified, final trust value is obtained by aggregating $w^m_{tk} and f^m_{tk}$ as follows

$$\mathrm{T_{tk}} = \begin{cases} \left(1 - \mathrm{w}^{\mathrm{m}}_{\mathrm{tk}}\right) & \mathrm{if w}^{\mathrm{m}}_{\mathrm{tk}} > \mathrm{f}^{\mathrm{m}}_{\mathrm{tk}} \\ \beta * \left(1 - \mathrm{f}^{\mathrm{m}}_{\mathrm{tk}}\right) + (1-\beta) * \left(1 - \mathrm{w}^{\mathrm{m}}_{\mathrm{tk}}\right) & \text{otherwise} \end{cases} \tag{17}$$

Although it has been proved that it is better than GTMS, LDTS, etc. [10], [23] but the major drawback of this trust model is sensitivity to false positive alarms and only specific to on-off attack that makes it suitable for specific situation because in reality collusion attack might degrade the performance of whole WSN. Almomani *et al.* [46] developed a ''specialized dataset for intrusion detection systems in wireless sensor networks'' that improves the speed and accuracy of intrusion (DoS attacks) detection process. LEACH, NS-2 simulator and WEKA toolbox are used for clustering, routing, simulation, and 10-fold cross validation respectively. The data obtained through NS-2 is collected for the training of the artificial neural network in order to detect and achieve higher classification accuracy rate for various DoS attacks. The main disadvantage of this intelligent intrusion detection and prevention mechanism that it is suitable only for DoS attacks and not able to mitigate on-off and collusion attacks.

Ishmanov *et al.* [8] proposed ''A secure trust establishment scheme for wireless sensor networks'' to detect and mitigate well known dangerous internal attack: on-off attack by introducing a misbehavior component along with current node status. Simulation results demonstrate good performance of this scheme in terms of misbehavior detection along with their persistency. The author claims that it is suitable for on-off attack mitigation but without employing the misbehavior frequency component, a robust on-off TMS is infeasible to design. Various attacks like collusion attacks,

blackhole attacks, etc are not considered that makes it unrealistic because collusion attacks can succeed to destroy the whole WSN. Labraoui *et al.* [47] proposed an ''application independent distributed trust model'' known as RaRtrust that combine the risk factor with the reputation to obtain a global trust value of a SN in order to mitigate the bad-mouthing attack and on-off attack. The author states that it is accurate and efficient TMS with high detection capability but it requires more resource consumptions compare to [10], [19], [22], [23].

Karthik and Ananthanarayana [24] proposed a communication and data trust based hybrid approach known as HTMS to detect faulty data based on data consistency using correlation (spatial, temporal) techniques. Decision-making is done on the basis of data trust score. HTMS employs provenance data, communication trust, and correlation metric to estimate the trust score of sensor nodes and sense data respectively. HTMS gives reward and punishment on the basis of the reliability of data by increasing and decreasing trust scores of WSN nodes. Moreover, HTMS uses metrics like self and peer data trust along with interdependency property, data provenance and communication competence to estimate the final trust score of the source node, intermediate node, and data item. Experimental results exhibit the robustness and effectiveness of HTMS in terms of detection and mitigation of malicious nodes and untrustworthy numeric data but it is not well suited for estimation of trust score of non- numeric data has been identified as a research gap. Górski *et al.* [52] provideWCT2M for clustered WSN to improve security and mitigate various cybersecurity threats. WCT2M uses validity history and deviation history along with direct (local assessment) and indirect (peer recommendation) trust and aggregate all to obtain final trust value. Its performance is evaluated under several attacks with multilayer WSN deployment that seems to be effective under various attacks scenarios but data trust is not considered to eliminate the bad recommendations. Trust decision based on considering only communication trust might be misled by various attacks like on-off attack, grey hole attack etc.

Gautam *et al.* [53] discussed a Scalable TM for WSN to detect and mitigate various security threats like bad-mouthing, collusion attacks and self-promoting. Direct trust is computed by using ''time lapses function based on forgetting curve'' and for indirect trust, reputation function is used. Trust updating mechanism is also employed. SNs are categorized as trusted or selfish (malicious) by considering a predefined threshold value. The author believes that this approach is lightweight under the constant environmental factor and robust against intrusion detection and various other security attacks. The author does not provide any information regarding communication overhead and not a valid mathematical proof for its robustness. Moreover, only communication trust is considered which is not sufficient to provide robust trust value because it might be a possibility that two or more nodes communicate very frequently but not giving correct data reports to each other.

Desai *et al.* [55] proposed a recent topology independent trust model based on the internal resource of SNs known as ''Node-Level Trust Evaluation in Wireless Sensor Networks.'' This model allows only trusted (reliable) nodes to partake in the WSN and later these trusted nodes can be communicated with peers using the proposed ''Self-Attestation and Self-Scrutiny'' algorithms. This model is implemented on real sensor nodes does not use second-hand information during trust evaluation. The author states that it is robust and provides consistent results. Ghugar *et al.* [56] proposed a novel trust scheme known as ''protocol layer trust-based intrusion detection system (LB-IDS)'' to protect WSN from various security threats. This scheme can efficiently detect attackers at each layer. Trust values are computed by using the concept of trust value deviation w.r.t. attack. Mainly three layers (physical, MAC and network layer) are considered for trustworthiness by taking key trust metrics of that particular layer. The status of the sensor node is determined by comparing the aggregated the individual trust values of each layer with some predefined threshold. This scheme implements three attacks namely jamming attack, ''back-off manipulation attack and sinkhole attack at physical, MAC and network layer'' respectively. The author proves that it is better than Wang's scheme in terms of detection and mitigation of defined attacks.

Reddy *et al.* [57] proposed ''Trust Computation Model Using Hysteresis Curve for Wireless Sensor Networks'' to protect the WSN from various security threats as well as wrongs decisions. This model uses a differential method for direct trust evaluation and hysteresis curve for indirect trust and compare it with cos function to measure its effectiveness. The proposed model is reliable and reduces the increased network traffic by drawing a better tradeoff between traffic and reliability.

Trust establishment in WSN has become an interesting and challenging issue for the research community because of its requirement in various fields [1]–[5]. Among the existing trust models, very few are comprehensive and focus on fundamental requirements of WSN but suffer from various limitations due to limited resource availability. The comparative analysis of these states of art trust models for clustered WSN is shown in Table 1.

III. PROPOSED TRUST SCHEME

This section presents a communication and data trust-based framework to prevent the WSN from various attacks. Proposed scheme (LTS) operates on two levels namely, intra-cluster and inter-cluster along with distributed approach and centralized approach respectively to make accurate trust decision of sensor nodes with minimum overheads. In the centralized model, a trusted node (CH or BS) calculates the trust value of SNs but in the distributed model, each and every sensor node itself calculate neighbors' trust value for decision making based on a defined threshold value. Table 2 shows a brief overview of the proposed scheme.

TABLE 1. Comparative analysis of various trust schemes.

Trust model	Key objectives (Purpose)	Basis of computation	Limitation	Complexity
ATRM [20]	Overhead reduction	Agent	Unrealistic (due to assumption made)	Proportional to packets and independent of number of nodes
HTCW[4]	Transaction data based reputation estimation	Classical beta binomial framework	Suitable for limited size clusters and CH can be easily compromised. Only Sybil and replication attack resilient	High delay with excess message overheads introduced by surveillance node
GTMS [19]	Communication and memory overhead reduction	Group	Low dependability and weak punishment coefficient	High (due to broadcast strategy)
TMA [21]	Multi-attribute based communication trust	Group, Decay function	Does not mitigate bad mouthing attack	Minimal
NBBTE [7]	Node behavior based Trust estimation	Weight (fuzzy theory and D-S evidence theory)	Communication and memory overhead varies with network density. Only on-off attack resilient	Higher (due to its excessive energy and memory requirement)
[62]	Global trust computation among routes	Percentage of successful communications	Not resilient against malicious feedbacks	Minimal
[63]	Data trust , communication trust and history collectively used to obtain reputation. Suitable for multi-hop routing	Bayes theorem	Data and communication trust aggregation method is not defined. Only bad mouthing and conflicting behavior attack resilient	Minimal
HTMP [11]	Security improvement	Geographic	Does not deal with Malicious feedbacks	Higher (due to complex trust estimation scheme)
LDTS [22]	Overheads reduction and security improvement	Weight	Static punishment coefficient so vulnerable to attacks	minimal (Calculation and communication overhead)
LWTM [23]	Design a realistic TMS with reduced overheads	Weight	Not robust against on-off attack	Minimal (Calculation and communication overhead)
HTMS [24]	An energy efficient attack resistant TMS	Weight	Not suitable for non-numeric data	Minimal

A. NETWORK TOPOLOGY AND ASSUMPTIONS

Figure 1 shows that a node in clustered WSN can be either a cluster member or cluster head. Cluster members can be communicated with their CH via single hop (directly) or via multi-hop communication. In the same way, CHs forward aggregated trust value to BS via single hop or through other cluster heads.

It is important to list the various assumptions considered in this work to make it transplantable [10], [19], [22], [23].

1) *Clustering:* clusters are formed by using well-known clustering scheme [63]–[66] and cluster heads are selected using proposed schemes [25]–[32] as it plays a vital role in trust computation and decision making. Cluster head (CH) within a cluster has a large communication range and power. The base station (BS) assigns initial trust values to sensor nodes and respond to the queries of CHs.
2) *Secure channel:* Key management scheme [22], [25], [31] is used to establish a secure communication channel to protect trust values.
3) *Domain of trust values:* To reduce memory overhead and transmission overhead, we take trust value range as an unsigned integer in [0 4] that saves 25% space compared to [10] and 70 % space than [22]. Although we can choose any range for trust values but in sensor networks, the range of trust values plays a

TABLE 2. Overview of LTS.

Trust levels	Trust Relationship	Working
Intra-cluster	CM to CM direct communication and data trust	Each cluster member estimates the trust values of other cluster members and forms a trust vector i.e. (communication trust vector and data trust vector).
	CH to CM indirect (feedback) communication and data trust	Cluster members send their trust vectors to CH. Indirect trust (IDT) of cluster member x is reported by cluster head to reduce communication overhead.
Inter-cluster	CH to CH direct communication and data trust	Each CH maintain the trust vectors of the past interactions in the same way as cluster members maintain within a cluster
	BS to CH indirect (feedback) communication and data trust	Indirect trust of a CH is computed by taking feedback from BS. BS maintains trust vector into a matrix by periodically sending a request message to CHs.

significant role in exchanging of trust values among sensor nodes results in less transmission and power overhead [19], [22], [23], [67], [68].

4) *Monitoring:* A timing window is used to record (observe) the number of successful and unsuccessful interactions within each time unit that add new experience and forget the earlier experience.
5) *Central command authority:* We assume that the base station (BS) has no resource constraint problem and cannot be compromised by'' attackers. BS can remove malicious nodes or replace it with good nodes for proper functioning and known as central command authority.

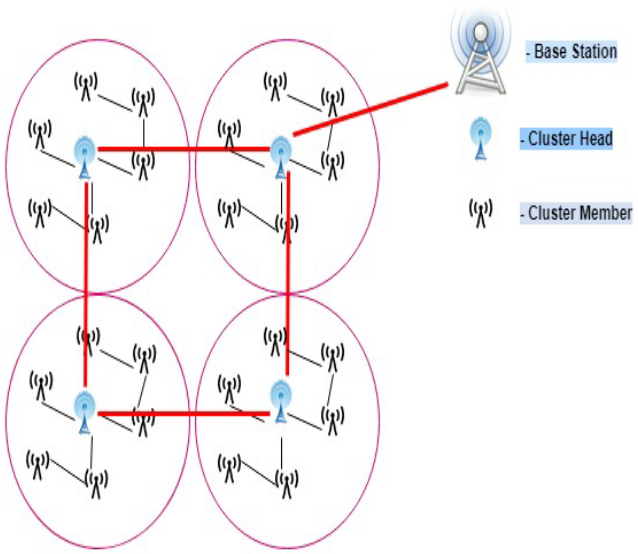

FIGURE 1. WSN Topology.

B. ASSIGNING UNIQUE IDENTITY TO CM

To improve the security of the system, we assign a unique identity (labels or hash values) to each node by employing modified SHA-1

$$UID = \left((K' + 1) \oplus RN \| H\left((K' + 1) \oplus ID \| RN\right)\right) \quad (18)$$

where K' is key required for hash function and ID and UID is a serial number and unique identity of each SN respectively. RN is a random number introduced by the base station. Labeling of SNs using this approach makes communication easy and prevents the system from various external attacks like spoofing attack. Refer to table 3 for the symbols used in the proposed work of this article.

C. TRUST DECISION AT INTRA-CLUSTER LEVEL

Based on the literature review refer to Table 1, we observe that very few schemes focus on application requirement [10], [23] and mostly uses static punishment [19], [22] or reward coefficient. Some trust functions even do not use any severity coefficient while computing successful interactions.

A good Trust function must provide some flexibility in terms of tuning the punishment and reward coefficient (according to the application requirement) along with good decision-making capability. The proposed scheme (LTS) uses a robust trust function in which severity coefficient can be tuned according to the application requirements with the help of parameters α *and* ψ. In addition, LTS incurs minimal communication overhead with high detection capability.

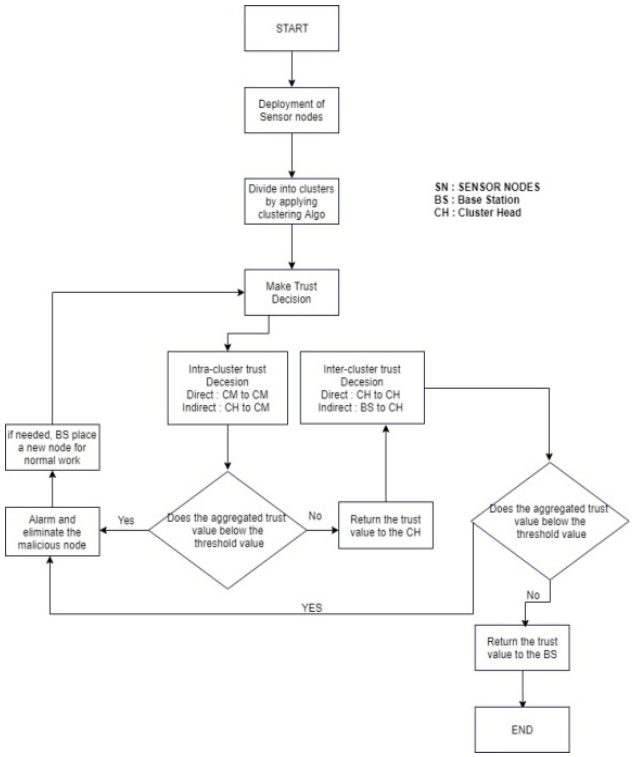

FIGURE 2. Flow Chart of proposed model.

1) CM TO CM COMMUNICATION TRUST CALCULATION

The Communication trust of node y at node x during $\Delta t T^{C}_{x,y}(\Delta t)$ at CM level is defined by (19)

$$T^{C}_{x,y}(\Delta t)) = \left[4 \times \left(\frac{S^{C}_{x,y}(\Delta t)}{\left(S^{C}_{x,y}(\Delta t) + U^{C}_{x,y}(\Delta t) \right)} \right) * \frac{1}{\psi^{U^{C}_{x,y}(\Delta t))}} * \left(\frac{S^{C}_{x,y}(\Delta t)}{S^{C}_{x,y}(\Delta t) + 1} \right)^{\alpha} \right] \quad (19)$$

where Δt is the time window consists of several time units (refer to figure 4) whose length can be changed depending on network scenario and with the time elapses it adds newer experiences and forget older experiences [8]. It is used to eliminate the effect of the time on trust values.

Superscript C denote communication interactions and [.] denotes greatest integer function. Meaning of all variables and parameters (such as $(S^{C}_{x,y}(\Delta t)$ and $U^{C}_{x,y}(\Delta t))$ used in the proposed work are listed in Table 3. Parameters ψ can be tuned according to application requirement to give punishment with the increase in unsuccessful interactions. The linear term $\frac{S^{C}_{x,y}(\Delta t)}{S^{C}_{x,y}(\Delta t)+1}$ slowly tends to 1 with increase in $S^{C}_{x,y}(\Delta t)$ indicates small alteration in trust value of node x for node y. Figure 3 illustrates the change in trust values (wrt. ψ and α) with the rise in successful interactions $(S^{C}_{x,y}(\Delta t))$. The exponent parameter $\alpha \geq 1$ in (19) gives the harshness to the trust function whose value can be adjusted according to network scenario and application requirement and plays a significant role to cope with untrustworthy (non-cooperative) nodes with greater values of α. Refer to table 4 to analyze the change in trust values according to $S^{C}_{x,y}(\Delta t)$.

Based on the value computed by (19), a node can be classified into three possible states (w.r.t. to CM only) as

TABLE 3. Notations (Symbols) used in LTS.

Symbol	Meaning
$S_{x,y}(\Delta t)$ or (S)	Successful Interactions (communications) of node x with node y during (Δt)
$U_{x,y}(\Delta t)$or (U)	Unsuccessful Interactions (communications) of node x with node y during (Δt)
RN	Random Number
UID	Unique Identity Number
ψ	Punishment Coefficient
α	Reward Coefficient
θ	Application Specific Trust Threshold Value
Δt	Time Window Consisting of 4 Time Units
$R^{D}_{i}(\Delta t)$	Data Reported By Sensor Node i at Time Δt
	Error Tolerance Parameter
$F^{C}_{x,y}$	Feedback Communication Trust
$F^{D}_{x,y}$	Feedback Data Trust
w	Weight
a and b	Amount of Positive and Negative Feedbacks
$GFT^{\Delta t}_{x,y}$	Global Feedback Trust at Time Δt
	Application Specific Threshold to Determine Dishonest Feedback
N	Total Number of Nodes in WSN
n	Size of Each Cluster
g	Number of Clusters

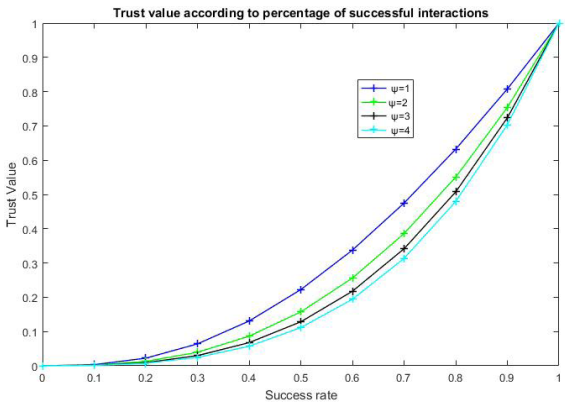

FIGURE 3. Successful interactions VS Trust Value (w.r.t $\alpha. = 2$).

follows:

$$S\left(\mathrm{T}^{\mathrm{C}}_{\mathrm{x,y}}(\Delta t)\right) = \left\{ \begin{array}{l|c} (3;4) & highlytrustednode \\ (0;\theta) & maliciousnode \\ (\theta;3) & legitimatenode \end{array} \right\} \quad (20)$$

where the parameter θ provide the flexibility whose value can be set according to application requirement and network scenario.

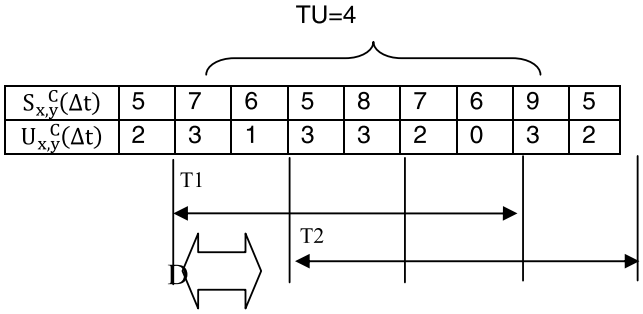

FIGURE 4. Behavior of nodes in Trust model.

Figure 4 illustrates a sample scenario of time window scheme that shows the number of successful and unsuccessful interactions recorded in each D time. Thus, the total time for a time window is 4D as there are 4-time units and each time unit requires D time. In the first time unit of the time window, the number of successful and unsuccessful interactions is 5 and 2 respectively. In the entire first time window, the number of successful and unsuccessful interactions are 23 and 9'' respectively. After each D time units, window slides to right and add new interaction while it forgets old (very first) experience. (Note that trust of an entity x wrt. entity y changes with time, so to monitor the past as well as present behavior we employed time window concept).

2) CM TO CM DATA TRUST CALCULATION

The Data trust of node y at node x during Δt $\left(\mathrm{T}^{\mathrm{D}}_{\mathrm{x,y}}(\Delta t)\right)$ at CM level is defined by (21) as follows

$$\mathrm{T}^{\mathrm{D}}_{\mathrm{x,y}}(\Delta t) = \left[4 \times \left(\frac{\mathrm{S}^{\mathrm{D}}_{\mathrm{x,y}}(\Delta t)}{\left(\mathrm{S}^{\mathrm{D}}_{\mathrm{x,y}}(\Delta t) + \mathrm{U}^{\mathrm{D}}_{\mathrm{x,y}}(\Delta t)\right)} \right) * \frac{1}{\psi^{\mathrm{U}^{\mathrm{D}}_{\mathrm{x,y}}(\Delta t))}} * \left(\frac{\mathrm{S}^{\mathrm{D}}_{\mathrm{x,y}}(\Delta t)}{\mathrm{S}^{\mathrm{D}}_{\mathrm{x,y}}(\Delta t) + 1} \right)^{\alpha} \right] \quad (21)$$

where Δt is the ''time window consists of several times unit'' whose length can be changed depending on network scenario and with the time elapses it adds newer reported data interactions and forget older reports. Superscript D denotes data interactions and [.] denotes greatest integer function. Parameter ψ can be tuned according to application requirement to give punishment with the increase in unsuccessful interactions.

The linear term $\frac{\mathrm{S}^{\mathrm{D}}_{\mathrm{x,y}}(\Delta t)}{\mathrm{S}^{\mathrm{D}}_{\mathrm{x,y}}(\Delta t)+1}$ slowly tends to 1 with increase in $\mathrm{S}^{\mathrm{D}}_{\mathrm{x,y}}(\Delta t)$ indicates small change in data trust value of node x for node y. The exponent parameter $\alpha \geq 1$ gives the harshness to the trust function whose value can be adjusted according to network scenario (application requirement) which plays a significant role to cope with untrustworthy nodes with greater values of α. Based on the value computed by (21), a node can be classified into three possible states (wrt to CM only) as follows:

$$S\left(\mathrm{T}^{\mathrm{D}}_{\mathrm{x,y}}(\Delta t)\right) = \left\{ \begin{array}{l|c} (3;4) & highlydatatrustednode \\ (0;\theta) & maliciousnode \\ (\theta;3) & legitimatenode \end{array} \right\} \quad (22)$$

where the parameter θ provide the flexibility whose value can be set according to application requirement and network scenario.

3) SUCCESSFUL DATA REPORT

A node j is said to be successfully report data to node i if and only if

$$|\mathrm{R}^{\mathrm{D}}_{\mathrm{i}}(\Delta t) - \mathrm{R}^{\mathrm{D}}_{\mathrm{j}}(\Delta t) \leq \rho| \quad (23)$$

where $\mathrm{R}^{\mathrm{D}}_{\mathrm{i}}(\Delta t)$ and $\mathrm{R}^{\mathrm{D}}_{\mathrm{j}}(\Delta \mathrm{t})$ ''are the reported data values by sensor node i and its neighbor j in the cluster'' at time Δt. ρ is defined as error tolerance parameter depends on error variance of sensor's sensing unit or network spatial correlation because data reported by the sensor nodes in the high density of deployment has a spatial correlation.

4) CH TO CM FEEDBACK COMMUNICATION TRUST ($\mathbf{F^{C}_{x,y}}$) AND DATA TRUST ($\mathbf{F^{D}_{x,y}}$) CALCULATION

Let us assume there are r (r ≤n-1) good members (excluding CH) among n members within a cluster. A cluster is said to be good if it is either a legitimate node or highly trusted node. Cluster head collect direct trust values of communication trust and data trust of r cluster members by periodically sending a request packet and store in a r∗ r matrix respectively as follows:

$$CH^{d} = \begin{bmatrix} T^{d}_{1,1} & T^{d}_{1,2} & \cdots & T^{d}_{1,n-1} \\ T^{d}_{2,1} & T^{d}_{2,2} & \cdots & T^{d}_{2,n-1} \\ \cdots & \cdots & \cdots & \cdots \\ T^{d}_{n-1,1} & T^{d}_{n-1,2} & \cdots & T^{d}_{n-1,n-1} \end{bmatrix}$$

$$CH^{C} = \begin{bmatrix} T^{c}_{1,1} & T^{c}_{1,2} & \cdots & T^{c}_{1,n-1} \\ T^{c}_{2,1} & T^{c}_{2,2} & \cdots & T^{c}_{2,n-1} \\ \cdots & \cdots & \cdots & \cdots \\ T^{c}_{n-1,1} & T^{c}_{n-1,2} & \cdots & T^{c}_{n-1,n-1} \end{bmatrix}$$

where $T^{c}_{x,y}$ and $T^{d}_{x,y}$ are the direct trust values (communication and data) of node x on node y. The idea of considering the direct trust values of good nodes reduce transmission overhead as well as improve the accuracy of the trust system. Moreover, CH discards $T^{c}_{i,i}$ and $T^{d}_{i,i}$ during feedback trust calculation to reduce the rating of a node towards itself. Inspired from the beta distribution function [6], [69], feedback trust can be estimated as follows

$$\mathrm{FT}^{\mathbf{c}}_{\mathbf{x,y}}(\boldsymbol{\Delta t})) = \frac{\mathrm{w}_1\left(4 * \frac{\mathrm{a}+1}{\mathrm{a}+\mathrm{b}+2}\right) + \mathrm{w}_2 * [\frac{\sum_{\mathrm{k}=1}^{\mathrm{a}+\mathrm{b}} \mathrm{T}^{\mathbf{c}}_{\mathbf{x,y}}(\boldsymbol{\Delta t})}{\mathrm{a}+\mathrm{b}}]}{2} \quad (24)$$

$$\mathbf{GFT}^{\Delta t}_{\mathbf{x,y}} = \text{ceil}\left[\mathbf{4}*\left(\frac{\mathbf{FT}^{\mathbf{c}}_{\mathbf{x,y}}(\boldsymbol{\Delta t})*\mathbf{FT}^{\mathbf{d}}_{\mathbf{x,y}}(\boldsymbol{\Delta t})}{\mathbf{T}^{\mathbf{c}}_{\mathbf{x,y}}(\boldsymbol{\Delta t})*\mathbf{FT}^{\mathbf{d}}_{\mathbf{x,y}}(\boldsymbol{\Delta t})+\left(\mathbf{4}-\mathbf{T}^{\mathbf{c}}_{\mathbf{x,y}}(\boldsymbol{\Delta t})\right)*(4-\boldsymbol{FT}^{\mathbf{d}}_{\mathbf{x,y}}(\boldsymbol{\Delta t}))}\right)\right] \tag{26}$$

$$\mathrm{CH}^{\mathrm{C}}_{\mathrm{i,j}}(\Delta t)) = \left[4\times\left(\frac{\mathrm{S}^{\mathrm{C}}_{\mathrm{i,j}}(\Delta t)}{\left(\mathrm{S}^{\mathrm{C}}_{\mathrm{i,j}}(\Delta t)+\mathrm{U}^{\mathrm{C}}_{\mathrm{i,j}}(\Delta t)\right)}\right)*\frac{1}{\psi^{\mathrm{U}^{\mathrm{C}}_{\mathrm{i,j}}(\Delta t))}}*\left(\frac{\mathrm{S}^{\mathrm{C}}_{\mathrm{i,j}}(\Delta t)}{\mathrm{S}^{\mathrm{C}}_{\mathrm{i,j}}(\Delta t)+1}\right)^{\alpha}\right] \tag{29}$$

$$\mathrm{FT}^{\mathbf{d}}_{\mathbf{x,y}}(\boldsymbol{\Delta t})) = \frac{\mathrm{w}_1\left(4*\frac{\mathrm{a}+1}{\mathrm{a}+\mathrm{b}+2}\right)+\mathrm{w}_2*[\frac{\sum_{\mathrm{k}=1}^{\mathrm{a}+\mathrm{b}}\mathrm{T}^{\mathbf{d}}_{\mathbf{x,y}}(\boldsymbol{\Delta t})}{\mathrm{a}+\mathrm{b}}]}{2} \tag{25}$$

where $T^{c}_{x,y}(\Delta t)$ *and* $T^{d}_{x,y}(\Delta t)$ is the feedback of node x towards node y. w_1 is the weight assigned to feedback provided by a single node and w_2 is the weight assigned to aggregated feedback from m (=a+b) members. Note that and $w_1 + w_2 = 1$. A feedbacks is said to be positive if and $T_{x,y}(\Delta t) \geq 2$ and negative if $T_{x,y}(\Delta t) < 2$. Now using (24) and (25), global feedback trust can be computed as follows

The Global feedback trust computed by (26), as shown at the top of this page, can easily detect malicious nodes in terms of communication if the neighboring nodes report incorrect measure, which improves the efficiency of the trust system. Final trust value $(f^{T}_{x,y}(\Delta t))$ is computed by simply aggregating (simple averaging performs better than complex averaging [22], [70]) as follows

$$(\mathrm{f}^{\mathrm{T}}_{\mathrm{x,y}}(\Delta \mathrm{t})) = \frac{\mathrm{T}_{\mathrm{x,y}}(\Delta t)+\mathrm{GFT}^{\Delta \mathrm{t}}_{\mathrm{x,y}}}{2} \tag{27}$$

where $T_{x,y}(\Delta t)$ is defined as the average value of data and communication (direct) trust of CH-to-CH. In order to find the node status, $(f^{T}_{x,y}(\Delta t))$ component is used as follows

$$S\left((f^{T}_{x,y}(\Delta t))\right) = \left\{\begin{array}{l|c}(3;4) & highlytrustednode\\ (0;\theta) & maliciousnode\\ (\theta;3) & legitimatenode\end{array}\right\} \tag{28}$$

The value of (or parameter) θ is application dependent i.e. its value can be tuned according to application requirements.

D. TRUST DECISION AT INTERCLUSTER LEVEL

Trust decision at inter-cluster level is also defined by direct (CH-to-CH) trust evaluation and indirect (BS to CH). For direct trust evaluation, we use the same trust computing function defined for CM level but during indirect trust calculation, base station discards the dishonest feedbacks and simply aggregate remaining feedbacks as simple averaging is always perform better than complex aggregation [70]. Trust decision at inter-cluster level considers only communication trust because adjacent CHs aggregate the data coming from clusters members and it will be difficult to find the false data report from the aggregated data.

1) CH TO CH COMMUNICATION TRUST CALCULATION

CH-to-CH communication trust at inter-cluster level is computed in the same way as CM computes in the intra-cluster level using (29), as shown at the top of this page, where $\mathrm{CH}^{\mathrm{C}}_{\mathrm{i,j}}(\Delta t))$ is defined as the communication trust maintained by CH (j) at CH (i) during Δt. The parameter α and ψ serve the same purpose defined at CM level. The superscript C indicate communication trust and [.] indication nearest integer function.

2) BS TO CH INDIRECT (FEEDBACK) TRUST CALCULATION

In feedback trust calculation, the BS excludes those feedbacks from CHs having high diversity around them to build trustworthy feedback for CHs. Note that the median absolute deviation is better than standard deviation [9], [19], [20]. Suppose there are g numbers of cluster heads in the WSN, and then BS collect all feedbacks from all CHs into the matrix B as follows:

$$B = \begin{bmatrix} C_{1,1} & C_{1,2} & \dots & C_{1,g} \\ C_{2,1} & C_{2,2} & \dots & C_{2,g} \\ \dots & \dots & \dots & \dots \\ C_{g,1} & C_{g,1} & \dots & C_{g,g} \end{bmatrix}$$

In order to determine the dishonest (untrustworthy) feedback, we use the following equation based on the median absolute deviation along with scaled constant β [71] $\frac{|F_i - median(f)|}{medianabsolutedeviation/\beta} > \delta$ where F_i denotes i^{th} feedback and $median\,(f)$ is the median of given feedbacks. δ is some threshold value used to determine dishonest feedbacks whose value can be decided anything depending on the network and application scenario as in some application like military application, the value of δ plays a vital role to identify dishonest recommendations to obtain more accurate trust values. Now the indirect trust is computed by taking the average of remaining recommendations.

IV. THEORETICAL ANALYSIS AND EVALUATION

This section describes the robust of proposed trust model against malicious behavior, the severity of trust function and communication overhead by some definitions, theorems, and proofs. We categorize sensor network nodes (SNs) into good (trustworthy) nodes, malicious (bad or untrustworthy) nodes and awful malicious nodes with the consideration that good nodes frequently and successfully interact with each other and submit true report (feedback or recommendation) and malicious nodes interact rarely or do unsuccessful interactions with false feedback report to ruin or boost the reputation of SNs. More clear definition of such nodes is defined below in the continuation of this section.

A. ANALYSIS AGAINST MALICIOUS BEHAVIOR

Firstly, we need to define the kinds of attacks (malicious behavior) on any clustered WSN as follows:

1) *Garnished attack:* Malicious (selfish) nodes behave good (trustworthy) and bad (untrustworthy) alternatively and attacks suddenly to damage the network with the aim of remain undetected.
2) *Bad mouthing attack:* It is one of the most straightforward attacks in which malicious nodes provide wrong (false or dishonest) feedback about peer nodes to boost or ruin their reputation.
3) *Blackhole and Greyhole attack:* In these attacks, malicious nodes try to convince its peer nodes to forward trust values via itself to disrupt communication by discarding true values of trust.
4) *Ballot-stuffing attack:* In this attack, good reputation (higher trust values) are strewn about malicious nodes to destroy the network.

Our model efficiently detects such types of attacks and prevent from malicious activities. Let us first give some definitions and then theorems with their theoretical validation to demonstrate the effectiveness and robustness of the proposed trust model.

Definition 1: A SN x is said to good (communication trusted and data trusted) for other node y if and only if x successfully interacts with some predefined threshold number of times with y during (Δt) and $S^{c,d}_{x,y}(\Delta t) > U^{c,d}_{x,y}(\Delta t)$ and $T^{c,d}_{x,y}(\Delta t) \geq 2$ where c and d denotes communication and data interactions.

Definition 2: A SN x is said to malicious for other node y if and only if x is interacted atleast once with y during (Δt) and $U^{c,d}_{x,y}(\Delta t) \geq S^{c,d}_{x,y}(\Delta t)$ or $T^{c,d}_{x,y}(\Delta t) < 2$ where c and d denotes communication and data interactions.

Definition 3: A node x is said to be deceived by malicious node y if and only if $T^{c,d}_{x,y}(\Delta t) \geq 2$.

Definition 4: A trust model is said to be robust against deception if and only if no malicious node can deceive another node

Definition 5: A SN x is said to an awful malicious for other node y if and only if x is interacted at least once with y during (Δt) and $U^{c,d}_{x,y}(\Delta t) > S^{c,d}_{x,y}(\Delta t)$ or $T^{c,d}_{x,y}(\Delta t) < 1$ where c and d denotes communication and data interactions.

Definition 6: A trust model is said to be robust against deception by awful malicious nodes if and only if no awful malicious node can deceive (mislead) another node.

Definition 7: A group of malicious or awful malicious nodes is said to be performing collaborating attack at intra-cluster level if they provide wrong feedback about a particular node to the CH.

Definition 8: A group of malicious or awful malicious nodes (say i) is said to be performed collaborating attack successfully (at intra-cluster level) if they provide wrong feedback about a particular node to the CH in the following way:

Case 1) $T^{c,d}_{ch,i}(\Delta t) \geq 2$. when number of positive recommendations (a) is less than number of negative recommendations (b) i.e. group of malicious nodes collaborate to lie about a malicious node. Here malicious nodes say about another malicious node (x) that x is trusted node.

Case 2) $T^{c,d}_{ch,i}(\Delta t) < 2$ when number of positive recommendations (a) is greater than number of negative recommendations (b).'' Here malicious nodes say about a trusted node (y) that y is an untrustworthy node. In both cases 1 and 2, a group of malicious nodes collaborates to lie about a trustworthy node.

Theorem 1: In cluster member (CM)-to-cluster member (CM) trust estimation and decision making, the proposed trust model is robust against the deceptive behavior of cluster members.

Proof (by contradiction): Suppose a CM (y) successfully deceived CM (x) then $U^{c,d}_{x,y}(\Delta t) \geq S^{c,d}_{x,y}(\Delta t) \& T^{c,d}_{x,y}(\Delta t) \geq 2$ (according to definition 1 and 2). There exist three cases for this deceptive behavior.

Case 1: if cluster members x and y are not interacted with each other i.e. $U^{c,d}_{x,y}(\Delta t) + S^{c,d}_{x,y}(\Delta t) = 0$ then CM x will rely on the feedback (recommendation) sent by CH towards y.

Case 2: If $S^{c,d}_{x,y}(\Delta t) = 0$ & $U^{c,d}_{x,y}(\Delta t) \geq 1$ then $T^{c,d}_{x,y}(\Delta t) = 0$ using (19) and (21).

Case 3: If cluster member (CM) x interact at least once with CM y within (Δt) i.e. $U^{c,d}_{x,y}(\Delta t) + S^{c,d}_{x,y}(\Delta t) > 1$ and $U^{c,d}_{x,y}(\Delta t) \geq S^{c,d}_{x,y}(\Delta t)$ then the term $\frac{S^{c,d}_{x,y}(\Delta t)}{\left(S^{c,d}_{x,y}(\Delta t) + U^{c,d}_{x,y}(\Delta t)\right)}$ will always be less than 50% (i.e. 0.5) and the value of $T^{c,d}_{x,y}(\Delta t)$ will be less than 2 for any value of α which contradict the hypothesis. Moreover, α provide the flexibility to the trust function in the sense that by setting a larger value of α, a CM will take a longer time to increase its trust value towards other cluster CM. Theorem 1 indicates that the proposed model can prevent from sudden attacks by providing strict punishment coefficient and meanwhile ''theorem 1 indirectly proves that the proposed model is robust against garnished attack.''

Theorem 2: In cluster head (CH) -to- cluster head (CH) trust estimation and decision making, the proposed trust model is robust against the deceptive behavior'' of cluster heads.

Proof: Similar to theorem 1.

Theorem 3: A group of malicious CMs cannot collaborate successfully against a CH towards another CM.

Proof (by contradiction): suppose a group of malicious CMs collaborate successfully against a CH towards another trusted CM then according to definition 7 and definition 8 then $T^{c,d}_{ch,i}(\Delta t) > 2$. Consider that a <b then the value of $\frac{w_1\left(4*\frac{a+1}{a+b+2}\right)+w_2*[\frac{\sum_{k=1}^{a+b} T^{c,d}_{x,y,(\Delta t)}}{a+b}]}{2}$ using (24) and (25) is always less than 2 which contradict the hypothesis. This situation covers the bad mouthing scenario and validate that our proposed model is robust against bad mouthing attack. For the

simplicity, we can assign equal value to w_1 and w_2 with the constraint that $w_1 + w_2 = 1$. In the same way, other implications can be proved.

Theorem 4: A group of malicious CHs cannot collaborate successfully against a BS towards another CH

Proof: Similar to theorem 3

B. SEVERITY ANALYSIS OF TRUST FUNCTION

This section provides a relative analysis of the some existing TMSs. For symbols and their meanings, refer to Table 3. Table 4 indicates trust functions along with some observations such as TMA is least severe and employ only linear trust function. GTMS [19] and LDTS [22] considered only communication trust and vulnerable to attack. Although ADCT [10] employs both communication and data trust to evaluate the trustworthiness of sensor nodes but punishment coefficient does not provide any flexibility as in our trust model, punishment coefficient is dependent on ψ whose value can be tuned according to application requirement and greater the values of α, larger the time required to change the trust value of a node (say x on another node (say y). Moreover, punishment coefficient of ADCT depends on successful, unsuccessful interactions and value of α but proposed model (LTS) depends on unsuccessful interactions only, which makes it simple and lightweight. LWTM [23] considers only communication trust, which may result in an incorrect trust decision. In addition, LWTM does not consider the multi-hop network model in the computation of communication overhead analysis. It is less adaptive and non-realistic than LTS because LWTM does not employ the parameters, which can be tuned according to application requirement.

TABLE 4. Comparison of WSN Trust functions.

Trust management Scheme	Observation	Trust function
TMA [21]	Only communication trust	$\left(\frac{S}{S+U}\right)$
GTMS [19]	Only communication trust	$\frac{S^2}{(S+U)*(s+1)}$
LDTS [22]	Only communication trust	$\left(\frac{S}{S+U}\right)*\frac{1}{\sqrt{U}}$
ADCT [10]	Communication and Data trust	$\left(\frac{S}{S+U}\right)^{(1-\frac{S}{S+U})\alpha}$
LWTM [23]	Only communication trust	$\frac{(S^{G1}+S^{G2})}{(S^{G1}+S^{G2}+U^{G1}+U^{G2})}*\frac{1}{\sqrt{P1*U^{G1}+P2*U^{G2}}}*\left(\frac{p1*S^{G1}+p2*S^{G2}}{1+p1*S^{G1}+p2*S^{G2}}\right)$
LTS	Communication and Data trust with flexible punishment coefficient	$\left(\frac{S}{S+U}\right)*\left(\frac{1}{\psi^U}\right)*\left(1\frac{S}{S+1}\right)^{\alpha}$ where α is exponent to $\frac{S}{S+1}$

C. COMMUNICATION OVERHEAD ANALYSIS

As we know, WSNs are collections of small size, self-organized hundred to thousand low-cost resource constraint sensor nodes and mainly deployed in the hazardous/ hostile area to monitor events and report continuous and discrete data. More number of communications among sensor nodes during trust estimation requires more power and transmission cost. By reducing the number of communication during trust evaluation, we can increase the lifetime of the sensor network. We consider the worst-case scenario in which the maximum number of nodes can communicate during trust evaluation according to the proposed model as CM to CM or CM to CH etc. Let us, we define the number of nodes in WSN is N and the number of clusters (groups/cluster heads) are g then size (n) of each cluster can be defined by (30) as follows

$$n = N/g \tag{30}$$

where size n represents the number of nodes (including CH) within the cluster. We divide the total communication overhead into intra-cluster communication overhead and inter-cluster communication overhead. In intra-cluster trust evaluation, node x sends and receive one CH feedback request to interact with node y i.e. total communication overhead of 2 request packets. In the worst case, if node x wants to interact with all (n-2) nodes then total communication overhead is 2 (n-2) request packets. If all CMs (except CH) wants to interact with each other than maximum communication overhead is 2 (n-2)(n-1). During intra-cluster feedback trust calculation, CH sends r requests to only direct trusted members and receive r response where ($r \leq$ n-1). The total communication overhead due to feedbacks by CH at CM level is 2$*$r request and response packets. Thus total communication overhead in intra-cluster trust computation $C_{intra} = 2$ (n-2)(n-1)+2r.

In intra-cluster trust evaluation, CH (i) sends and receive one BS feedback request to interact with CH (j) i.e. total communication overhead of 2 request packets. In the ''worst case, if CH (i) wants to interact with all (g-1) CHs then total communication overhead is 2 (g-1) request packets. If all CHs wants to interact with each other than maximum communication overhead is 2g(g-1). During BS to CH feedback trust calculation, BS send g requests and receive total g responses from all CHs leads to a total communication overhead of 2g packets. Thus total communication overhead in inter-cluster trust computation $C_{inter} = 2g(g-1)+ 2g$. Therefore, in the worst case, maximum communication overhead (Cmax) of the proposed scheme is:''

$$\begin{aligned} C_{\max} &= g^{*}C_{\mathrm{intra}} + C_{\mathrm{inter}} \\ &= g^{*}(2(n-2)(n-1)+2r)+2g(g-1)+2g \end{aligned} \tag{31}$$

If we consider an average case scenario where only 50% of the CMs are directly (peer to peer) trusted, then r = (n-1)/2. Substitute r value in the (31), we get

$$C_{\max} = g(n-1)(2n-1) + 2g^2 \tag{32}$$

In this report, the term direct trust nodes represent those nodes whose trust value is greater than or equal to two (2)

during CM-to-CM-direct trust evaluation. In the real scenario, all CMs might not be directly trusted and neither all CMs can be malicious so average case analysis can be considered as a real scenario where 50% to 70% nodes may be direct trusted and others are malicious. Table 5 indicates the communication overhead of various existing and proposed trust management schemes.

TABLE 5. Communication overhead analysis.

Trust management Scheme	Total Communication Overhead
RFSN [33]	2*g[n*(n-2)*(n-1)+(g-1)*(g-2)]
PLUS [35]	2*g[n $(n-1)^2 + (g-1)^2$]
ATRM [20]	4g[n(n-1)+ (g-1)]
TMA [21]	$constant\ i.e$ independent of n amd g
GTMS [19]	2g[n(n-1)*r+(n-1)]
LDTS [22]	2g[(n-2)(n-1)+n]+2 $(g-1)^2$ + 2g
ADCT [10]	2g $(n-1)^2$+2$(g)^2$
LWTM [23]	g[$(n)^2$(n-1)+g(g-1)]
LTS	g*(2 (n-2)(n-1)+ 2r)+2g(g-1)+ 2g

V. RESULT AND DISCUSSION

In this section, we exhibit the effectiveness of the proposed trust model (LTS) by doing various experiments on MATLAB. Although we have already provided theoretical validation of LTS by several theorems but experimental results along with theoretical analysis prove the feasibility of LTS for security enhancement in large scale WSN. We categorize the experimental results in three categories namely severity of LTS with the percentage of successful interactions, communication overhead, and malicious node detection. Emulation parameters are taken in the proportion of [22], [23] to analysis the performance of LTS.

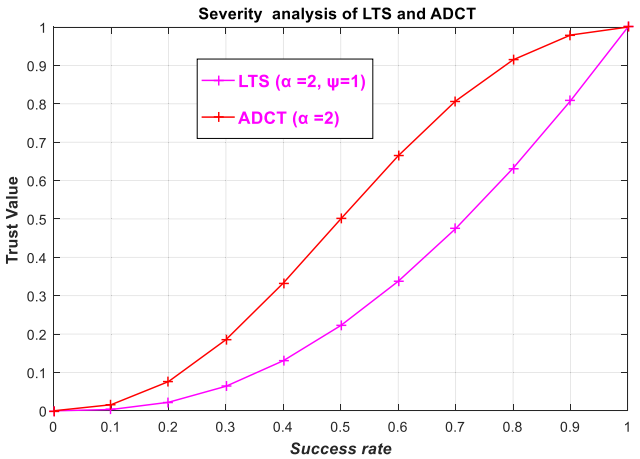

FIGURE 5. Severity analysis of LTS and ADCT.

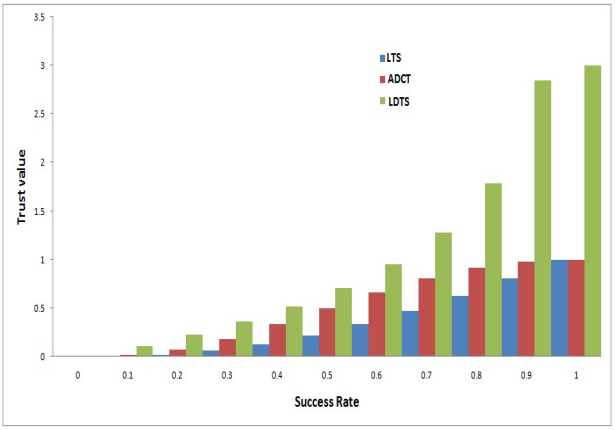

FIGURE 6. Severity analysis of LTS, LDTS and ADCT.

TABLE 6. Comparative analysis of change in trust values.

% of success rate	LTS (ψ =1&α = 2)	LTS (ψ =2 &α = 2)	LTS (ψ =3&α = 2)	ADCT (α = 2)	LDTS
0	0	0	0	0	0
0.1	**0.0033058**	**0.0017715**	**0.0012299**	**0.015 849**	**0.105 41**
0.2	0.022222	**0.012763**	0.0092276	0.076 146	0.223 61
0.3	0.063905	0.039338	**0.029618**	0.185 34	0.358 57
0.4	0.13061	0.086172	0.067563	**0.333 02**	0.516 4
0.5	0.22222	0.15713	0.1283	0.5	**0.707 11**
0.6	0.3375	0.25578	0.21748	0.664 54	0.948 68
0.7	0.47474	0.38561	0.34144	0.807 34	1.278
0.8	0.6321	0.55027	0.50741	0.914 61	1.788 9
0.9	0.80776	0.75366	0.72372	0.979 15	2.846
1	1	1	1	1	2.999

A. SEVERITY ANALYSIS OF LTS

The proposed trust model (LTS) can mitigate blackhole and greyhole attacks in any environment by providing suitable values of $\psi \& \alpha$ according to application requirements.

Figures 5 and 6 exhibit the severity of LTS and Table 6 provide the exact change in trust values with respect to change in percentage of successful interacts.

In addition, Table 6 indicate the effect of *change in* ψ value on the trust values. Although we have done several experiments for different values of $\psi \& \alpha$ but to provide comparative analysis we have considered $\alpha = 2$. In LTS, a nodes takes longer time to change its value (because of ψ and α) to deal with blackhole and greyhole attacks and several others. ψ and α values will be selected based on the application

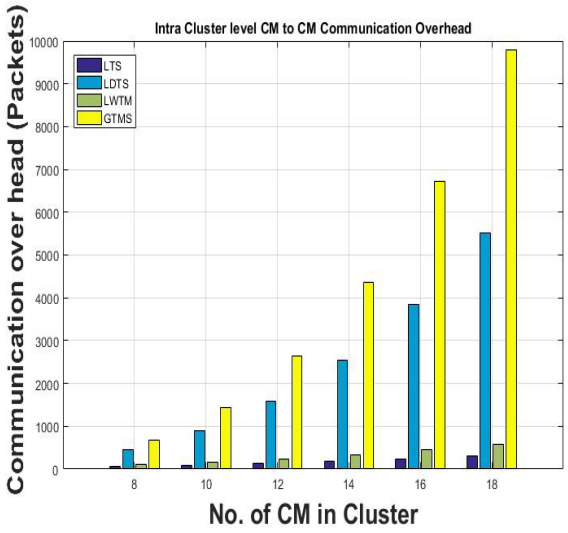

FIGURE 7. Intra-cluster communication overhead.

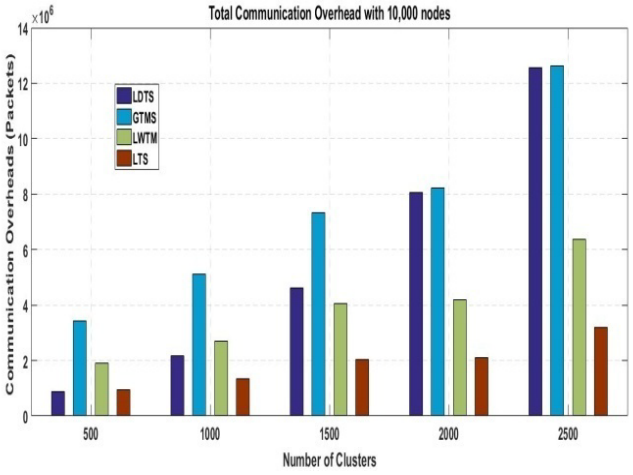

FIGURE 8. Worst-case analysis of communication overhead with 10,000 nodes.

requirement. For example, for defense applications, we need highly trusted reports so in such cases we can set $\psi \geq 3$ with $\alpha = 2$.

B. COMMUNICATION OVERHEAD

As we have discussed in subsection C of section IV, our LTS take minimal communication overhead. Figure7 represents maximum intra-cluster communication overhead in LTS is minimal than other TMS while figure 8 represents maximum communication overhead incurred by whole WSN. The experimental results exhibit that LTS impose minimal communication overhead on WSN by creating multiple scenarios, for example, as in figure 7, the number of cluster members is increasing while in figure 8 number of clusters are increasing.

C. MALICIOUS NODES DETECTION

In order to check the detection capability of LTS, we have injected 40% malicious nodes in a WSN scenario consisting of total 500 nodes.

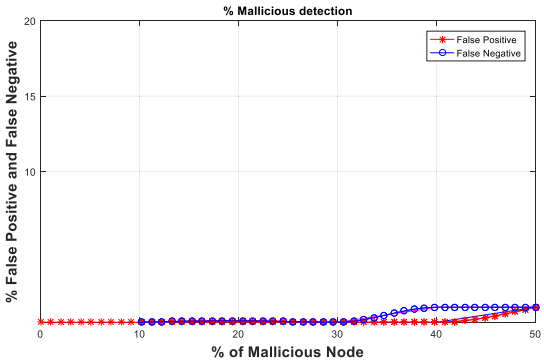

FIGURE 9. False positive and false negative alarms.

Figure 9 represents that approx 35% malicious nodes provide correct feedback report about neighbor nodes. To the best of our knowledge, LTS is the first severe trust model that detect approx. 35% malicious node.

Note: false positive means here that a malicious node gives positive feedback of untrustworthy node. In the false negative, a malicious node gives negative feedback of a trustworthy node.

VI. CONCLUSION AND FUTURE DIRECTIONS

In this paper, we proposed a novel and comprehensive trust estimation approach for large scale WSN employing clustering to improve cooperation, trustworthiness, and security by detecting malicious (faulty or selfish) sensor nodes with reduced resource consumption. Proposed scheme (LTS) consists of unique features like robust trust estimation function, attack resistant and simple trust aggregation at cluster heads. Data trust along with communication trust plays a significant role to cope with malicious nodes.

Initially, unique identities are assigned to each SN to make communication easier and secure from external attacks. Clusters are formed using well-known algorithms [63]–[66]. LTS operates on two levels namely, intracluster and intercluster along with distributed approach and centralized approach respectively to make accurate trust decision of sensor nodes with minimum overheads. A timing window mechanism is employed to monitor successful and unsuccessful interactions. The punishment to the malicious nodes and harshness of the trust function can be tuned according to application requirements, which is one of the interesting novelty about the proposed scheme. We introduce a simple averaging scheme to aggregate the trust values for cluster heads to overcome the limitations of existing TMS. In addition, dishonest recommendations (outliers) are eliminated before aggregation at the base station by observing statistical dispersion. LTS is Platform independent and not affected by chosen of any specific routing scheme.

Theoretical and mathematical validation along with experimental results exhibits that the proposed model is feasible for security enhancement by detecting and mitigating malicious nodes. The proposed work does not provide memory

overhead because we believe that with technical development storage problems is likely to be resolved in the future.

As in our work, we are not considering the weight and frequency of misbehavior, LTS is not highly recommended to mitigate on-off attacks and collusion attacks. The suitability of LTS for homogeneous WSN is seems to be another limitation.

In the future, we are planning to extend our work to detect and mitigate the on-off attack, DoS attacks and collusion attack along with minimal communication and storage overhead. We have planned to examine the scalability and convergence rate of LTS with optimal number of clusters. We are also planning to design a robust, risk-aware trust model for heterogeneous WSN and IoT using machine learning [72]–[111], [122]–[137].

CONFLICTS OF INTEREST

The authors declare that they have no competing interests.

REFERENCES

[1] T. Park and K. G. Shin, "LiSP: A lightweight security protocol for wireless sensor networks," *ACM Trans. Embedded Comput. Syst.*, vol. 3, no. 3, pp. 634–660, Aug. 2004.
[2] E. Shi and A. Perrig, "Designing secure sensor networks," *IEEE Wireless Commun.*, vol. 11, no. 6, pp. 38–43, Dec. 2004.
[3] R. A. Shaikh, H. Jameel, S. Lee, S. Rajput, and Y. J. Song, "Trust management problem in distributed wireless sensor networks," in *Proc. 12th IEEE Int. Conf. Embedded Real-Time Comput. Syst. Appl. (RTCSA)*, Aug. 2006, pp. 411–414.
[4] G. Han, J. Jiang, L. Shu, J. Niu, and H.-C. Chao, "Management and applications of trust in wireless sensor networks: A survey," *J. Comput. Syst. Sci.*, vol. 80, no. 3, pp. 602–617, May 2014.
[5] X. Chen, K. Makki, K. Yen, and N. Pissinou, "Sensor network security: A survey," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 2, pp. 52–73, 2nd Quart., 2009.
[6] T. Kyung and H. S. Seo, "A trust model using fuzzy logic in wireless sensor network," *World Acad. Sci., Eng. Technol.*, vol. 42, no. 6, pp. 63–66, Aug. 2008.
[7] R. Feng, X. Xu, X. Zhou, and J. Wan, "A trust evaluation algorithm for wireless sensor networks based on node behaviors and D-S evidence theory," *Sensors*, vol. 11, no. 2, pp. 1345–1360, Feb. 2011.
[8] F. Ishmanov, S. Kim, and S. Nam, "A secure trust establishment scheme for wireless sensor networks," *Sensors*, vol. 14, no. 1, pp. 1877–1897, Jan. 2014.
[9] F. Ishmanov, S. Kim, and S. Nam, "A robust trust establishment scheme for wireless sensor networks," *Sensors*, vol. 15, no. 3, pp. 7040–7061, Mar. 2015.
[10] S. Talbi, M. Koudil, A. Bouabdallah, and K. Benatchba, "Adaptive and dual data-communication trust scheme for clustered wireless sensor networks," *Telecommun. Syst.*, vol. 65, no. 4, pp. 605–619, Aug. 2017.
[11] F. Bao, I.-R. Chen, M. Chang, and J.-H. Cho, "Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection," *IEEE Trans. Netw. Service Manage.*, vol. 9, no. 2, pp. 169–183, Jun. 2012.
[12] M. Momani, "Trust models in wireless sensor networks: A survey," in *Proc. Int. Conf. Netw. Secur. Appl.* Berlin, Germany: Springer, Jul. 2010, pp. 37–46.
[13] T. Zahariadis, H. C. Leligou, P. Trakadas, and S. Voliotis, "Trust management in wireless sensor networks," *Eur. Trans. Telecommun.*, vol. 21, no. 4, pp. 386–395, Jun. 2010.
[14] Y. Yu, K. Li, W. Zhou, and P. Li, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures," *J. Netw. Comput. Appl.*, vol. 35, no. 3, pp. 867–880, 2012.
[15] F. Ishmanov, A. S. Malik, S. W. Kim, and B. Begalov, "Trust management system in wireless sensor networks: Design considerations and research challenges," *Trans. Emerg. Telecommun. Technol.*, vol. 26, no. 2, pp. 107–130, Feb. 2015.
[16] V. U. Rani, and K. S. Sundaram, "Review of trust models in wireless sensor networks," *Int. J. Comput. Inf. Syst. Control Eng.*, vol. 8, pp. 371–377, Apr. 2014.
[17] H. Fouchal, J. Biesa, E. Romero, A. Araujo, and O. N. Taladrez, "A security scheme for wireless sensor networks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2016, pp. 1–5.
[18] A. Ahmed, K. A. Bakar, M. I. Channa, K. Haseeb, and A. W. Khan, "A survey on trust based detection and isolation of malicious nodes in ad-hoc and sensor networks," *Frontiers Comput. Sci.*, vol. 9, no. 2, pp. 280–296, Apr. 2015.
[19] R. A. Shaikh, H. Jameel, B. J. d'Auriol, H. Lee, S. Lee, and Y.-J. Song, "Group-based trust management scheme for clustered wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 20, no. 11, pp. 1698–1712, Nov. 2009.
[20] A. Boukercha, L. Xu, and K. El-Khatib, "Trust-based security for wireless ad hoc and sensor networks," *Comput. Commun.*, vol. 30, nos. 11–12, pp. 2413–2427, 2007.
[21] J. Zhang, R. Shankaran, A. O. Mehmet, V. Varadharajan, and A. Sattar, "A trust management architecture for hierarchical wireless sensor networks," in *Proc. IEEE Local Comput. Netw. Conf.*, Oct. 2010, pp. 264–267.
[22] X. Li, F. Zhou, and J. Du, "LDTS: A lightweight and dependable trust system for clustered wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 6, pp. 924–935, Jun. 2013.
[23] M. Singh, A. R. Sardar, K. Majumder, and S. K. Sarkar, "A lightweight trust mechanism and overhead analysis for clustered WSN," *IETE J. Res.*, vol. 63, no. 3, pp. 297–308, May 2017.
[24] N. Karthik and V. S. Ananthanarayana, "A hybrid trust management scheme for wireless sensor networks," *Wireless Pers. Commun.*, vol. 97, no. 4, pp. 5137–5170, Dec. 2017.
[25] G. V. Crosby, N. Pissinou, and J. Gadze, "A framework for trust-based cluster head election in wireless sensor networks," in *Proc. 2nd IEEE Workshop Dependability Secur. Sensor Netw. Syst. (DSSNS)*, Apr. 2006, pp. 10–22.
[26] K.-W. Kim, K.-R. Kim, and S.-G. Min, "Distributed cluster head election algorithm using local energy estimation," in *Proc. Int. Conf. Hybrid Inf. Technol.*, Aug. 2009 pp. 256–259.
[27] K. Lee, J. Lee, M. Park, J. Kim, and Y. Shin, "EECHE: An energy-efficient cluster head election algorithm in sensor networks," in *Proc. Asia–Pacific Netw. Oper. Manage. Symp.*, Berlin, Germany: Springer, Sep. 2009, pp. 486–489.
[28] H. Taheri, P. Neamatollahi, M. H. Yaghmaee, and M. Naghibzadeh, "A local cluster head election algorithm in wireless sensor networks," in *Proc. CSI Int. Symp. Comput. Sci. Softw. Eng. (CSSE)*, Jun. 2011, pp. 38–43.
[29] M. Mehr, "Cluster head election using imperialist competitive algorithm (CHEI) for wireless sensor networks," *Int. J. Mobile Netw. Commun. Telematics*, vol. 4, no. 3, pp. 1–9, Jun. 2014.
[30] Y. M. Miao, "Cluster-head election algorithm for wireless sensor networks based on LEACH protocol," in *Appl. Mech. Mater., Trans. Tech. Publications*, vol. 738, pp. 19–22, Mar. 2015.
[31] A. Singh and K. Gupta, "Optimal cluster head election algorithm for mobile wireless sensor networks," in *Proc. 2nd Int. Conf. Inf. Commun. Technol. Competitive Strategies*, Mar. 2016, p. 132.
[32] W. Abidi and T. Ezzedine, "Fuzzy cluster head election algorithm based on LEACH protocol for wireless sensor networks," in *Proc. 13th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2017, pp. 993–997.
[33] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," *ACM Trans. Sensor Netw.*, vol. 4, no. 3, p. 15, May 2008.
[34] Z. Yao, D. Kim, and Y. Doh, "PLUS: Parameterized and localized trust management scheme for sensor networks security," in *Proc. IEEE Int. Conf. Mobile Ad Hoc Sensor Syst.*, Oct. 2006, pp. 437–446.
[35] M. Momani, S. Challa, and K. Aboura, "Modelling trust in wireless sensor networks from the sensor reliability prospective," in *Innovative Algorithms and Techniques in Automation, Industrial Electronics and Telecommunications*. Dordrecht, The Netherlands: Springer, Jun. 2007, pp. 317–321.
[36] K. Liu, N. Abu-Ghazaleh, and K.-D. Kang, "Location verification and trust management for resilient geographic routing," *J. Parallel Distrib. Comput.*, vol. 67, no. 2, pp. 215–228, 2007.
[37] H. Chen, H. Wu, X. Zhou, and C. Gao, "Reputation-based trust in wireless sensor networks," in *Proc. Int. Conf. Multimedia Ubiquitous Eng. (MUE)*, Apr. 2007, pp. 603–607.

[38] K. Shakkira, "Advanced lightweight, dependable and secure trust system for clustered wireless sensor networks," in *Proc. Int. Conf. Innov. Inf., Embedded Commun. Syst. (ICIIECS)*, Mar. 2015, pp. 1–4.

[39] G. Zhan, W. Shi, and J. Deng, "Design and implementation of TARF: A trust-aware routing framework for WSNs," *IEEE Trans. Dependable Secure Comput.*, vol. 9, no. 2, pp. 184–197, Mar. 2012.

[40] A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decision Support Syst.*, vol. 43, no. 2, pp. 618–644, Mar. 2007.

[41] F. Musau, G. Wang, S. Yu, and M. B. Abdullahi, "Securing recommendations in grouped P2P e-commerce trust model," *IEEE Trans. Netw. Service Manage.*, vol. 9, no. 4, pp. 407–420, Dec. 2012.

[42] L. Xiong and L. Liu, "Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities," *IEEE Trans. Knowl. Data Eng.*, vol. 16, no. 7, pp. 843–857, Jul. 2004.

[43] D. He, C. Chen, S. Chan, J. Bu, and A. V. Vasilakos, "A distributed trust evaluation model and its application scenarios for medical sensor networks," *IEEE Trans. Inf. Technol. Biomed.*, vol. 16, no. 6, pp. 1164–1175, Nov. 2012.

[44] D. He, C. Chen, S. Chan, J. Bu, and A. V. Vasilakos, "ReTrust: Attack-resistant and lightweight trust management for medical sensor networks," *IEEE Trans. Inf. Technol. Biomed.*, vol. 16, no. 4, pp. 623–632, Jul. 2012.

[45] M. Singh, A. R. Sardar, R. R. Sahoo, K. Majumder, S. Ray, and S. K. Sarkar, "Lightweight trust model for clustered WSN," in *Proc. 3rd Int. Conf. Frontiers Intell. Comput., Theory Appl. (FICTA)*. Cham, Switzerland: Springer, 2015, pp. 765–773.

[46] I. Almomani, B. Al-Kasasbeh, and M. Al-Akhras, "WSN-DS: A dataset for intrusion detection systems in wireless sensor networks," *J. Sensors*, vol. 2016, Aug. 2016, Art. no. 4731953.

[47] N. Labraoui, M. Gueroui, and L. Sekhri, "A risk-aware reputation-based trust management in wireless sensor networks," *Wireless Pers. Commun.*, vol. 87, no. 3, pp. 1037–1055, Apr. 2016.

[48] W. Fang, C. Zhu, W. Chen, W. Zhang, and J. J. P. C. Rodrigues, "BDTMS: Binomial distribution-based trust management scheme for healthcare-oriented wireless sensor network," in *Proc. 4th Int. Wireless Commun. Mobile Comput. Conf.*, Jun. 2018, pp. 382–387.

[49] M. Zhang, "Trust computation model based on improved Bayesian for wireless sensor networks," in *Proc. IEEE 17th Int. Conf. Commun. Technol. (ICCT)*, Oct. 2017, pp. 960–964.

[50] M. A. Youssef, F. A. Mohamed, and Y. K. Arisha, "A constrained shortest-path energy-aware routing algorithm for wireless sensor networks," in *Proc. IEEE Wireless Commun. Netw. Conf. Rec. (WCNC)*, vol. 2, Mar. 2002, pp. 794–799.

[51] Z. Chen, L. Tian, and C. Lin, "Trust model of wireless sensor networks and its application in data fusion," *Sensors*, vol. 17, no. 4, p. 703, Mar. 2017.

[52] J. Górski and A. Turower, "A method of trust management in wireless sensor networks," *Int. J. Secur., Privacy Trust Manage.*, vol. 7, no. 3, pp. 1–19, Nov. 2018.

[53] A. K. Gautam and R. Kumar, "A robust trust model for wireless sensor networks," in *Proc. 5th IEEE Uttar Pradesh Section Int. Conf. Electr., Electron. Comput. Eng. (UPCON)*, Nov. 2018, pp. 1–5.

[54] S. S. Desai and M. J. Nene, "MITE: Memory integrity based trust evaluation in wireless sensor networks," in *Proc. Int. Conf. Commun. Netw. (ICCN)*, Nov. 2015, pp. 202–208.

[55] S. S. Desai and M. J. Nene, "Node-level trust evaluation in wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, to be published.

[56] U. Ghugar, J. Pradhan, S. K. Bhoi, and R. R. Sahoo, "LB-IDS: Securing wireless sensor network using protocol layer trust-based intrusion detection system," *J. Comput. Netw. Commun.*, vol. 2019, Jan. 2019, Art. no. 2054298.

[57] V. B. Reddy, A. Negi, and S. Venkataraman, "Trust computation model using hysteresis curve for wireless sensor networks," in *Proc. IEEE SENSORS*, Oct. 2018, pp. 1–4.

[58] N. H. Ambreen, "Wireless sensor network through shortest path route," *Int. J. Emerg. Technol. Adv. Eng.*, vol. 3, no. 2, pp. 158–161, Feb. 2013.

[59] O. Yilmaz and K. Erciyes, "Distributed weighted node shortest path routing for wireless sensor networks," in *Proc. Int. Conf. Wireless Mobile Netw.* Berlin, Germany: Springer, Jun. 2010, pp. 304–314.

[60] O. Yilmaz, S. Demirci, Y. Kaymak, S. Ergun, and A. Yildirim, "Shortest hop multipath algorithm for wireless sensor networks," *Comput. Math. Appl.*, vol. 63, no. 1, pp. 48–59, Jan. 2012.

[61] D. Hao, A. Adhikari, and K. Sakurai, "Mixed-Strategy game based trust management for clustered wireless sensor networks," in *Proc. Int. Conf. Trusted Syst.* Berlin, Germany: Springer, Nov. 2011, pp. 239–257.

[62] Z. Liu, Z. Zhang, S. Liu, Y. Ke, and J. Chen, "A trust model based on Bayes theorem in WSNs," in *Proc. 7th Int. Conf. Wireless Commun., Netw. Mobile Comput.*, Sep. 2011, pp. 1–4.

[63] O. Younis and S. Fahmy, "HEED: A hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks," *IEEE Trans. Mobile Comput.*, vol. 4, no. 4, pp. 366–379, Oct./Dec. 2004.

[64] A. A. Abbasi and M. Younis, "A survey on clustering algorithms for wireless sensor networks," *Comput. Commun.*, vol. 30, nos. 14–15, pp. 2826–2841, Oct. 2007.

[65] B. Prabhu, R. Mahalakshmi, S. Nithya, P. D. Manivannan, and S. Sophia, "A review of energy efficient clustering algorithm for connecting wireless sensor network fields," *Int. J. Eng. Res. Technol.*, vol. 2, no. 4, pp. 477–481, Apr. 2013.

[66] P. Nayak and A. Devulapalli, "A fuzzy logic-based clustering algorithm for WSN to extend the network lifetime," *IEEE Sensors J.*, vol. 16, no. 1, pp. 137–144, Jan. 2016.

[67] Y. L. Sun, W. Yu, Z. Han, and K. J. R. Liu, "Information theoretic framework of trust modeling and evaluation for ad hoc networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 305–317, Feb. 2006.

[68] G. Theodorakopoulos and J. S. Baras, "On trust models and trust evaluation metrics for ad hoc networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 318–328, Feb. 2006.

[69] A. Whitby, A. Jøsang, and J. Indulska, "Filtering out unfair ratings in Bayesian reputation systems," in *Proc. 7th Int. Workshop Trust Agent Soc.*, vol. 6, Jul. 2004, pp. 106–117.

[70] L. Zhengqiang and S. Weisong, "Analysis of recommendations on trust inference in open environment," *J. Perform. Eval.*, vol. 65, no. 2, pp. 99–128, Apr. 2008.

[71] Y. S. Dodonov and A. Y. Dodonova, "Robust measures of central tendency: Weighting as a possible alternative to trimming in response-time data analysis," *Psikhologicheskie Issledovaniya*, vol. 5, no. 19, pp. 1–11, Oct. 2011.

[72] S. Jha, L. H. Son, R. Kumar, I. Priyadarshini, F. Smarandache, and H. V. Long, "Neutrosophic image segmentation with dice coefficients," *Measurement*, vol. 134, pp. 762–772, Feb. 2019.

[73] G. N. Nguyen, L. H. Son, A. S. Ashour, and N. Dey, "A survey of the state-of-the-arts on neutrosophic sets in biomedical diagnoses," *Int. J. Mach. Learn. Cybern.*, vol. 10, no. 1, pp. 1–13, Jan. 2019.

[74] R. Kapoor, R. Gupta, R. Kumar, L. H. Son, and S. Jha, "New scheme for underwater acoustically wireless transmission using direct sequence code division multiple access in MIMO systems," *Wireless Netw.*, pp. 1–13, 2019. doi: 10.1007/s11276-018-1750-z.

[75] L. H. Son, S. Jha, R. Kumar, J. M. Chatterjee, and M. Khari, "Collaborative handshaking approaches between Internet of Computing and Internet of Things towards a smart world: A review from 2009–2017," *Telecommun. Syst.*, vol. 70, no. 4, pp. 617–634, 2019. doi: 10.1007/s11235-018-0481-x.

[76] L. H. Son and H. Fujita, "Neural-fuzzy with representative sets for prediction of student performance," *Appl. Intell.*, vol. 49, no. 1, pp. 172–187, 2019.

[77] K. Saravanan, S. Aswini, R. Kumar, and L. H. Son, "How to prevent maritime border collision for fisheries?-A design of real-time automatic identification system," *Earth Sci. Inform.*, pp. 1–12, Nov. 2019. doi: 10.1007/s12145-018-0371-5.

[78] H. V. Long, M. Ali, L. H. Son, M. Khan, and D. N. Tu, "A novel approach for fuzzy clustering based on neutrosophic association matrix," *Comput., Ind. Eng.*, vol. 127, pp. 687–697, Jan. 2019. doi: 10.1016/j.cie.2018.11.007.

[79] Y. H. Robinson, E. G. Julie, K. Saravanan, R. Kumar, and L. H. Son, "FD-AOMDV: Fault-tolerant disjoint ad-hoc on-demand multipath distance vector routing algorithm in mobile ad-hoc networks," *J. Ambient Intell. Humanized Comput.*, pp. 1–18, Nov. 2019. doi: 10.1007/s12652-018-1126-3.

[80] N. Singh, L. H. Son, F. Chiclana, and J.-P. Magnot, "A new fusion of Salp swarm with sine cosine for optimization of non-linear functions," *Eng. Comput.*, pp. 1–28, Jan. 2019. doi: 10.1007/s00366-018-00696-8.

[81] S. Kaur *et al.*, "Mixed pixel decomposition based on extended fuzzy clustering for single spectral value remote sensing images," *J. Indian Soc. Remote Sens.*, vol. 47, no. 3, pp. 427–437, 2019. doi: 10.1007/s12524-019-00946-2.

[82] P. H. Son, L. H. Son, S. Jha, R. Kumar, and J. M. Chatterjee, "Governing mobile virtual network operators in developing countries," *Utilities Policy*, vol. 56, pp. 169–180, Feb. 2019.

[83] R. Garg, M. Mittal, and L. H. Son, "Reliability and energy efficient workflow scheduling in cloud environment," *Cluster Comput.*, pp. 1–15, Feb. 2019. doi: 10.1007/s10586-019-02911-7.
[84] R. Kapoor, R. Gupta, L. H. Son, S. Jha, and R. Kumar, "Adaptive technique with cross correlation for lowering signal-to-noise ratio wall in sensor networks," *Wireless Pers. Commun.*, vol. 105, no. 3, pp. 787–802, 2019. doi: 10.1007/s11277-019-06121-7.
[85] R. Kapoor, R. Gupta, L. H. Son, and R. Kumar, "Iris localization for direction and deformation independence based on polynomial curve fitting and singleton expansion," *Multimedia Tools Appl.*, pp. 1–25, Feb. 2019. doi: 10.1007/s11042-019-7314-0.
[86] L. H. Son *et al.*, "Dental diagnosis from X-ray images: An expert system based on fuzzy computing," *Biomed. Signal Process. Control*, vol. 39C, pp. 64–73, Jan. 2018.
[87] M. Ali, L. H. Son, M. Khan, and N. T. Tung, "Segmentation of dental X-ray images in medical imaging using neutrosophic orthogonal matrices," *Expert Syst. Appl.*, vol. 91, pp. 434–441, Jan. 2018.
[88] N. T. Tam, D. T. Hai, L. H. Son, and L. T. Vinh, "Improving lifetime and network connections of 3D wireless sensor networks based on fuzzy clustering and particle swarm optimization," *Wireless Netw.*, vol. 24, no. 5, pp. 1477–1490, 2018.
[89] R. T. Ngan, M. Ali, and L. H. Son, "Δ-equality of intuitionistic fuzzy sets: A new proximity measure and applications in medical diagnosis," *Appl. Intell.*, vol. 48, no. 2, pp. 499–525, 2018.
[90] M. Ali, L. Q. Dat, L. H. Son, and F. Smarandache, "Interval complex neutrosophic set: Formulation and applications in decision-making," *Int. J. Fuzzy Syst.*, vol. 20, no. 3, pp. 986–999, 2018.
[91] D. Jude Hemanth, J. Anitha, D. E. Popescu, and L. H. Son, "A modified genetic algorithm for performance improvement of transform based image steganography systems," *J. Intell., Fuzzy Syst.*, vol. 35, no. 1, pp. 197–209, 2018.
[92] M. Ali, L. H. Son, N. D. Thanh, and N. V. Minh, "A neutrosophic recommender system for medical diagnosis based on algebraic neutrosophic measures," *Appl. Soft Comput.*, vol. 71, pp. 1054–1071, Oct. 2018.
[93] C. N. Giap, L. H. Son, and F. Chiclana, "Dynamic structural neural network," *J. Intell. Fuzzy Syst.*, vol. 34, pp. 2479–2490, Jan. 2018.
[94] R. Kapoor, R. Gupta, L. H. Son, S. Jha, and R. Kumar, "Detection of power quality event using histogram of oriented gradients and support vector machine," *Measurement*, vol. 120, pp. 52–75, May 2018.
[95] K. Singh, K. Singh, L. H. Son, and A. Aziz, "Congestion control in wireless sensor networks by hybrid multi-objective optimization algorithm," *Comput. Netw.*, vol. 138, pp. 90–107, Jun. 2018.
[96] B. T. Pham, L. H. Son, T.-A. Hoang, D.-M. Nguyen, and D. T. Bui, "Prediction of shear strength of soft soil using machine learning methods," *Catena*, vol. 166, pp. 181–191, Jul. 2018.
[97] D. J. Hemanth, J. Anitha, and L. H. Son, "Brain signal based human emotion analysis by circular back propagation and deep Kohonen neural networks," *Comput. Elect. Eng.*, vol. 68, pp. 170–180, May 2018.
[98] R. T. Ngan, L. H. Son, B. C. Cuong, and M. Ali, "H-max distance measure of intuitionistic fuzzy sets in decision making," *Appl. Soft Comput.*, vol. 69, pp. 393–425, Aug. 2018.
[99] L. H. Son *et al.*, "ARM–AMO: An efficient association rule mining algorithm based on animal migration optimization," *Knowl.-Based Syst.*, vol. 154, pp. 68–80, Aug. 2018.
[100] R. Kapoor, R. Gupta, L. H. Son, S. Jha, and R. Kumar, "Boosting performance of power quality event identification with KL divergence measure and standard deviation," *Measurement*, vol. 126, pp. 134–142, Oct. 2018.
[101] T. Le, L. H. Son, M. T. Vo, M. Y. Lee, and S. W. Baik, "A cluster-based boosting algorithm for bankruptcy prediction in a highly imbalanced dataset," *Symmetry-Basel*, vol. 10, no. 7, pp. 250–262, 2018.
[102] M. Khan, L. H. Son, M. Ali, H. T. M. Chau, N. T. N. Na, and F. Smarandache, "Systematic review of decision making algorithms in extended neutrosophic sets," *Symmetry*, vol. 10, no. 8, pp. 314–342, 2018.
[103] K. Saravanan, E. Anusuya, R. Kumar, and L. H. Son, "Real-time water quality monitoring using Internet of Things in SCADA," *Environ. Monitor. Assessment*, vol. 190, pp. 556–572, Sep. 2018.
[104] A. Dey, L. H. Son, P. K. K. Kumar, G. Selvachandran, and S. G. Quek, "New concepts on vertex and edge coloring of simple vague graphs," *Symmetry-Basel*, vol. 10, no. 9, pp. 373–391, 2018.
[105] S. Doss *et al.*, "APD–JFAD: Accurate prevention and detection of jelly fish attack in MANET," *IEEE Access*, vol. 6, pp. 56954–56965, 2018.
[106] M. Ali, H. Khan, L. H. Son, F. Smarandache, and W. B. V. Kandasamy, "New soft set based class of linear algebraic codes," *Symmetry-Basel*, vol. 10, no. 10, pp. 510–520, 2018.
[107] D. J. Hemanth, J. Anitha, L. H. Son, and M. Mittal, "Diabetic retinopathy diagnosis from retinal images using modified hopfield neural network," *J. Med. Syst.*, vol. 42, pp. 247–253, Dec. 2018.
[108] T. T. Ngan *et al.*, "Logic connectives of complex fuzzy sets," *Romanian J. Inf. Sci. Technol.*, vol. 21, no. 4, pp. 344–358, 2018.
[109] R. Jain, N. Jain, S. Kapania, and L. H. Son, "Degree approximation-based fuzzy partitioning algorithm and applications in wheat production prediction," *Symmetry-Basel*, vol. 10, no. 2, pp. 768–791, 2018.
[110] D. J. Hemanth, J. Anitha, A. Naaji, O. Geman, D. E. Popescu, and L. H. Son, "A modified deep convolutional neural network for abnormal brain image classification," *IEEE Access*, vol. 7, pp. 4275–4283, 2018.
[111] L. H. Son and P. H. Thong, "Soft computing methods for WiMax network planning on 3D geographical information systems," *J. Comput. Syst. Sci.*, vol. 83, no. 1, pp. 159–179, 2017.
[112] P. H. Phong and L. H. Son, "Linguistic vector similarity measures and applications to linguistic information classification," *Int. J. Intell. Syst.*, vol. 32, no. 1, pp. 67–81, 2017.
[113] L. H. Son and P. H. Thong, "Some novel hybrid forecast methods based on picture fuzzy clustering for weather nowcasting from satellite image sequences," *Appl. Intell.*, vol. 46, no. 1, pp. 1–15, 2017.
[114] L. H. Son and T. M. Tuan, "Dental segmentation from X-ray images using semi-supervised fuzzy clustering with spatial constraints," *Eng. Appl. Artif. Intell.*, vol. 59, pp. 186–195, Mar. 2017.
[115] D. T. Hai, L. H. Son, and L. T. Vinh, "Novel fuzzy clustering scheme for 3D wireless sensor networks," *Appl. Soft Comput.*, vol. 54, pp. 141–149, May 2017.
[116] L. H. Son, P. van Viet, and P. van Hai, "Picture inference system: A new fuzzy inference system on picture fuzzy set," *Appl. Intell.*, vol. 46, no. 3, pp. 652–669, 2017.
[117] L. H. Son, "Measuring analogousness in picture fuzzy sets: From picture distance measures to picture association measures," *Fuzzy Optim. Decision Making*, vol. 16, no. 3, pp. 359–378, 2017.
[118] N. D. Thanh, M. Ali, and L. H. Son, "A novel clustering algorithm in a neutrosophic recommender system for medical diagnosis," *Cogn. Comput.*, vol. 9, no. 4, pp. 526–544, 2017.
[119] L. H. Son and N. D. Tien, "Tune up fuzzy C-means for big data: Some novel hybrid clustering algorithms based on initial selection and incremental clustering," *Int. J. Fuzzy Syst.*, vol. 19, no. 5, pp. 1585–1602, 2017.
[120] M. Ali, L. H. Son, I. Deli, and N. D. Tien, "Bipolar neutrosophic soft sets and applications in decision making," *J. Intell. Fuzzy Syst.*, vol. 33, no. 6, pp. 4077–4087, 2017.
[121] L. H. Son and T. M. Tuan, "A cooperative semi-supervised fuzzy clustering framework for dental X-ray image segmentation," *Expert Syst. Appl.*, vol. 46, pp. 380–393, Mar. 2016.
[122] L. H. Son, "Dealing with the new user cold-start problem in recommender systems: A comparative review," *Inf. Syst.*, vol. 58, pp. 87–104, Jun. 2016.
[123] A. W. Wijayanto, A. Purwarianti, and L. H. Son, "Fuzzy geographically weighted clustering using artificial bee colony: An efficient geo-demographic analysis algorithm and applications to the analysis of crime behavior in population," *Appl. Intell.*, vol. 44, no. 2, pp. 377–398, 2016.
[124] P. H. Thong and L. H. Son, "Picture fuzzy clustering: A new computational intelligence method," *Soft Comput.*, vol. 20, no. 9, pp. 3549–3562, 2016.
[125] L. H. Son and P. V. Hai, "A novel multiple fuzzy clustering method based on internal clustering validation measures with gradient descent," *Int. J. Fuzzy Syst.*, vol. 18, no. 5, pp. 894–903, 2016.
[126] T. M. Tuan, T. T. Ngan, and L. H. Son, "A novel semi-supervised fuzzy clustering method based on interactive fuzzy satisficing for dental X-ray image segmentation," *Appl. Intell.*, vol. 45, no. 2, pp. 402–428, 2016.
[127] L. H. Son and A. Louati, "Modeling municipal solid waste collection: A generalized vehicle routing model with multiple transfer stations, gather sites and inhomogeneous vehicles in time windows," *Waste Manage.*, vol. 52, pp. 34–49, Jun. 2016.
[128] L. H. Son and P. H. Phong, "On the performance evaluation of intuitionistic vector similarity measures for medical diagnosis," *J. Intell. Fuzzy Syst.*, vol. 31, no. 3, pp. 1597–1608, 2016.
[129] L. H. Son, "Generalized picture distance measure and applications to picture fuzzy clustering," *Appl. Soft Comput.*, vol. 46, pp. 284–295, Sep. 2016.
[130] P. H. Thong and L. H. Son, "A novel automatic picture fuzzy clustering method based on particle swarm optimization and picture composite cardinality," *Knowl.-Based Syst.*, vol. 109, pp. 48–60, Oct. 2016.

[131] P. H. Thong and L. H. Son, "Picture fuzzy clustering for complex data," *Eng. Appl. Artif. Intell.*, vol. 56, pp. 121–130, Nov. 2016.
[132] T. T. Ngan, T. M. Tuan, L. H. Son, N. H. Minh, and N. Dey, "Decision making based on fuzzy aggregation operators for medical diagnosis from dental X-ray images," *J. Med. Syst.*, vol. 40, no. 12, pp. 1–7, 2016.
[133] L. H. Son, "DPFCM: A novel distributed picture fuzzy clustering method on picture fuzzy sets," *Expert Syst. Appl.*, vol. 42, no. 1, pp. 51–66, 2015.
[134] L. H. Son and N. T. Thong, "Intuitionistic fuzzy recommender systems: An effective tool for medical diagnosis," *Knowl.-Based Syst.*, vol. 74, pp. 133–150, Jan. 2015.
[135] N. T. Thong and L. H. Son, "HIFCF: An effective hybrid model between picture fuzzy clustering and intuitionistic fuzzy recommender systems for medical diagnosis," *Expert Syst. Appl.*, vol. 42, no. 7, pp. 3682–3701, 2015.
[136] L. H. Son, "HU-FCF++: A novel hybrid method for the new user cold-start problem in recommender systems," *Eng. Appl. Artif. Intell.*, vol. 41, pp. 207–222, May 2015.
[137] L. H. Son, "A novel kernel fuzzy clustering algorithm for geo-demographic analysis," *Inf. Sci.*, vol. 317, pp. 202–223, Oct. 2015.

TAYYAB KHAN received the Engineering degree in computer science and engineering from Gautam Buddh Technical University, India, and the M.Tech. degree in computer science and engineering from the School of Computer and Systems Sciences, JNU, New Delhi, India, in 2016, where he is currently pursuing the Ph.D. degree in computer science. His primary research interests include wireless sensor networks, network security, and multicast communication.

KARAN SINGH received the Engineering degree from the Kamla Nehru Institute of Technology, Sultanpur, India, and the M.Tech. and Ph.D. degrees from the Motilal Nehru National Institute of Technology, India, all in computer science and engineering. He was with Gautam Buddha University, India. He is currently with the School of Computer and Systems Sciences, Jawaharlal Nehru University, New Delhi. He has published over 70 research papers in refereed journals and good conferences. His primary research interests include computer networks, network security, multicast communication, the IoT, and body area networks. He is also an Editorial Board Member of the *Journal of Communications and Networks* (CN), USA. He was the General Chair of the International Conference (Qshine 2013) at Gautam Buddha University. He is a supervisor of many researcher scholars. He is also a Reviewer of Springer, Taylor & Francis, Elsevier journals, and IEEE Transactions. He organized the workshops, conference sessions, and trainings. Recently, he organized the ICCCS 2018 conference at the Dronacharya College of Engineering, Gurgaon, and a special session at the 2nd ICGCET 2018, Denmark.

LE HOANG SON received the Ph.D. degree in mathematics (informatics) from the VNU University of Science, Vietnam National University (VNU), in 2013.

He was promoted to Associate Professor of information technology, in 2017. He was a Senior Researcher and the Vice Director with the Center for High Performance Computing, VNU University of Science, VNU, from 2007 to 2018. Since 2018, he has been the Head of the Department of Multimedia and Virtual Reality, VNU Information Technology Institute, VNU. His research interests include artificial intelligence, data mining, soft computing, fuzzy computing, fuzzy recommender systems, and geographic information systems. He is a member of the International Association of Computer Science and Information Technology (IACSIT), the Vietnam Society for Applications of Mathematics (Vietsam), and the Key Laboratory of Geotechnical Engineering and Artificial Intelligence, University of Transport Technology, Vietnam. He serves on the Editorial Board of *Applied Soft Computing* (ASOC, SCIE), *International Journal of Ambient Computing and Intelligence* (IJACI, SCOPUS), and *Vietnam Journal of Computer Science and Cybernetics* (JCC). He is also an Associate Editor of the *Journal of Intelligent & Fuzzy Systems* (JIFS, SCIE), IEEE Access (SCIE), *Neutrosophic Sets and Systems* (NSS), *Vietnam Research and Development on Information and Communication Technology* (RD-ICT), *VNU Journal of Science: Computer Science and Communication Engineering* (JCSCE), and *Frontiers in Artificial Intelligence*.

MOHAMED ABDEL-BASSET received the B.Sc., M.Sc., and Ph.D. degrees from the Faculty of Computers and Informatics, Zagazig University, Egypt. He has published more than 150 articles in international journals and conference proceedings. His current research interests include optimization, operations research, data mining, computational intelligence, applied statistics, decision support systems, robust optimization, engineering optimization, multi-objective optimization, swarm intelligence, evolutionary algorithms, and artificial neural networks. He is working on the application of multi-objective and robust meta-heuristic optimization techniques. He is also the Program Chair of many conferences in the fields of decision making analysis, big data, optimization, complexity, and the Internet of Things, as well as editorial collaboration in some high impact journals. He is also an/a Editor/Reviewer of different international journals and conferences.

HOANG VIET LONG received the Ph.D. degree in computer science from the Hanoi University of Science and Technology, in 2011, where he defended his thesis on the fuzzy and soft computing field. He is currently the Head of the Faculty of Information Technology, People's Police University of Technology and Logistics, Bac Ninh, Vietnam. He is also a Researcher with the Institute for Computational Science, Ton Duc Thang University, Ho Chi Minh City, Vietnam. He was promoted to Associate Professor of information technology, in 2017. He has published more than 20 papers in ISI-covered journals. His current research interests include cybersecurity, machine learning, bitcoin, and block chain.

SATYA P. SINGH received the bachelor's degree in electronics and telecommunication engineering from IETE, New Delhi, India, in 2007, the master's degree in electrical and electronics engineering from the YMCA University of Science and Technology, India, in 2010, and the Ph.D. degree in electrical engineering from Gautam Buddha University, India, in 2017. He is currently a Postdoctoral Research Fellow with the School of Computer Science and Engineering, Nanyang Technological University, Singapore. His research interests include artificial intelligence in healthcare and development of medical imaging algorithms for computer-aided diagnosis of life-threatening diseases. He is also interested in analyzing MRI, fMRI, and DTI modalities using artificial intelligence.

MANISHA MANJUL received the Engineering degree from KNIT, Sultanpur, India, the M.Tech. degree from NIT Jalandhar, India, and the Ph.D. degree from Gautam Buddha University, India, all in computer science and engineering. She was with Gautam Buddha University. She is currently with the Department of Computer Engineering, G. B. Pant Engineering Collage, New Delhi. Her primary research interests include computer networks, network security, multicast communication, and object-oriented programming. She is also a Life Member of CSI, India.