International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *25 August 2023* ***Revised:*** *05 October 2023* ***Accepted:*** *24 October 2023*

Communication and Content Trust Aware Routing For Clustered IoT Network

Mohammad Osman[1], Kaleem Fatima[2], P. Naveen Kumar[3]
[1]Research Scholar, Department of Electronics and Communication Engineering, Osmania University, Hyderabad, Telangana, India.
e-mail: adnan.aspect@gmail.com
[2]Professor, Muffakham Jah College of Engineering & Technology, Department of Electronics and Communication Engineering, Hyderabad, Telangana, India.
e-mail: kaleemfatima@mjcollege.ac.in
[3]Professor, Department of Electronics and Communication Engineering, Osmania University, Hyderabad, Telangana, India.
e-mail: naveen.gps@gmail.com

Abstract—Security has become a major concern in practical applications related to Internet of Things, a Trust Aware Routing is found as second line of defence. To ensure a secure and hassle-free communication in IoT, this paper proposes a new routing strategy called as Communication and Content Trust Aware Routing (CCTAR) for Clustered IoT network. CCTAR is applied on a clustered IoT network in which the entire nodes are clustered into different clusters. Distance, initial energy, transmission range, angle of overlap and the sensing range are the fur major metrics used to cluster the network into hierarchical clusters followed by Cluster Head Selection. Next, the Trust Aware routing computes three different trust metrics namely Nobility rust, bilateral trust and Data oriented trust to determine the trustworthiness of Cluster Heads. The experimental evaluation of the proposed mechanism shows its superiority in terms of malicious nodes identification, Storage overhead reduction and Network lifetime improvisation.

Keywords-Internet of Things, Trust sensing, Clustering, Data trust, bilateral trust, Network lifetime.

I. Introduction

Internet of Things (IoT) is the wide network where billions of daily objects are connected to each other and they have unique identification and pervasive intelligence in an internet [1]. IoT devices simplify tasks and add convenience to peoples' daily lives. With huge research and efforts, IoT is used in various applications like industrial, healthcare, agriculture, transportation, and automotive sector. Despite IoT's development, a lot of problems remain unresolved. The major challenge in an IoT network's deployment is security concerns which create several hurdles at data transmission [2]. The conventional security ensuring methods like cryptography and encryption algorithms cannot be directly applied in IoT networks for secure communication due to the several reasons like 1) Limited energy-based sensor nodes which makes it economically viable. 2) Sensor nodes are frequently placed in remote locations thereby increasing the possibility of physical attack. 3) IoT sensor devices interact closely with people and their environment which exacerbates security issues and 4) IoT is a heterogeneous network made up of several types of sensor nodes used for various applications.

The sensor nodes may or may not cooperate with each other due to the nature of heterogeneity [3]. For example, consider the example sensor node which believes the energy as a precious resource, it may or may not cooperate to other nodes to forward the data. Such selfish nature of node triggers some severe attacks and degrades the network's performance [4]. In addition, IoT is used in wide range of applications and it creates several security issues due to the openness of the transmission medium and deployed environment. Several attacks like tampering attacks, hijack attacks, selective forwarding attacks, DoS attacks, sinkhole attacks, and etc. [5] are possible to occur in IoT. So, trust evaluation is required to address the aforementioned problems due to its low computational complexity and significant resilience to various types of attacks. Hence, trust sensing is a crucial factor for sensor enabled IoT networks to ensure a secure and hassle-free communication.

In earlier, several strategies are developed to solve the security problems in IoT [6]. Recently, the Trust Aware Routing has been widely employed in IoT to determine the insider attacks [7], [8] and it is often employed for secure routing that determines a secure path based on the trustworthiness of neighbour nodes. The Trust Aware models are generally reputation-based methods and they can be used for the detection of malicious or adversary nodes in IoT. These methods analyse the reputation of nodes based on their communication paradigm which indicates the collaboration between sensor nodes. So trust aware routing considers the communication and data related attributes to detect the malicious nodes in IoT.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *25 August 2023* ***Revised:*** *05 October 2023* ***Accepted:*** *24 October 2023*

Next, the trust evaluation in clustered IoT networks is done by Cluster heads (CH) which are responsible for aggregating and collecting the trust values and sends it to the preferred cluster [9]. Since there exist low battery powered sensor nodes in IoT, the trust computation makes them to deplete quickly. Hence, trust evaluation responsibility is taken by CHs and Sink node which have rich resources like energy bandwidth etc. Moreover, the non-cooperative nature of nodes in IoT imbalances the energy consumption and makes the network to get compromised. Next, at the trust computation, most of the existing methods considered Communication behaviour as a reference scenario and least concentrated over other attributes like data acquired, transmitted etc. The malicious nodes may deliver false information and consequences to inaccurate computation of trust values when the data is accumulated by the CHs. Likewise, sink node also suffer from the same issue during the trust evaluation of CHs.

To address the aforementioned problems in IoT, this paper proposed a new method Called as Communication and Content Trust Aware Routing (CCTAR) for Clustered IoT network. CCTAR employs only CHs and Sink node to evaluate trust of nodes in IoT. Initially, the entire network is partitioned followed by clustered the entire network and then accomplishes CH selection. Then CHs mutually computes their communication trust and cooperates to transmit the data to sink node. Unlike, the content trust is measured at both CH and sinks nodes based on the data collected from clustered member and CHs respectively. The major contributions of this paper are outlined as follows:

- To lessen the energy consumption, this work proposes an adaptive clustering mechanism in which the nodes are clustered based on the distance and energy. Entire nodes are categorized as energy rich and energy poor nodes and clustered based on their communication range.
- To encounter the attacks related to content (ex. Data tampering attacks), this work introduced a new trust metric called as Content Trust which determine the trust of a node based on its data. CH and sink node uses this metric because they are collectors of data from multiple nodes.

Remaining paper is organized as follows; section 2 describes the related work of various computational techniques for clustered IoT network, section 3 explores detailed description of proposed methodology, section 4 explains simulation experiments and obtained results, finally section 5 discusses the conclusion of proposed work.

II. Related Work

Recently, research towards trust evaluation for IoT security has been increased. So many authors concentrated in his direction and proposed several methods to ensure a secure communication between nodes in IoT. Researchers tried to achieve a balance between the energy efficiency and security requirements in different deployed IoT environments. In this regard, this section explores the recent related works on trust evaluation in clustered IoT networks.

Fang et al. [10] addressed various trust evolution methods. These methods consist of collecting of trust values, storing, modelling, forwarding, and decision making. Initially, trust values are computed by considering the location of nodes, status, and information of the nodes. Then, they are stored and modelled to fight against different attacks. Later, the modelled trust values are forwarded towards the destination to take the decision by considering the trust values i.e., a node that has low trust value is considered as malicious node. However, this procedure increases computational complexity and memory requirement. H. Aldawsari et al. [11] proposed a trust evaluation method to reduce each node's malicious behaviour within the IoT network named as reliable lightweight trust evaluation method (RTE). Initially, they divided the entire network into few clusters and cluster members are categorised based on the residual energy in each cluster. Here, base station verifies each node's residual energy. If any node founds with less residual energy, then it is suspended until it regains the energy. The trust evaluation is handled by the CH based on its coverage and energy. However, their method is concentrated majorly on optimization of energy consumption than the trust computation.

Dass et al. [12] suggested a trust computation model for IoT based intelligent transport system. They computed trust using direct and indirect methods by considering each node's sensed data. Then the sensed data is updated in regular intervals of time to measure the trust. Their results show low false detection rate and high detection rate. However, the trust computations are done in the cloud server which leads to delay for trust assessment. Tao yang et al. [13] proposed a distributed trust computation model to defend against malicious attacks that are comes from internal nodes. They also proposed energy-optimised secure routing (EOSR) based on each nodes remaining energy, trust value, and route length. This strategy is used to identify and isolate the malicious nodes. Authors achieved good results by balancing the transmitted information and energy consumption among the trusted nodes. However, this method is not considered data related trust to compute trust.

To reduce the malicious effects from illegitimate nodes, R. Rani et al. [14] proposed a hierarchical based Energy Efficient Trust Evaluation (EETE) technique. EETE restricts the propagation of trust requests over the network to optimize the energy consumption in the clustered IoT

network. They divided the proposed work into three phases; they are i) optimal number of clusters formation ii) CH selection and iii) trust computation to identify the malicious activity. They considered only network-oriented trusts but not considered data related trust. F. A. M. Solomon et al. [15] developed a centralized trust model for clustered IoT network. Initially, clusters are formed based on their location. Next, CH is selected by considering the direct and indirect trust values. The trust values are measured based on the social trust properties and quality of service (QoS). The trust value is determined by analysing the intra and inters cluster behaviour. Even though data trust values are considered to compute the trust, their results show poor Malicious Detection Rate (MDR).

To optimise the energy utilisation and enhance the security of wireless sensor network, Kalidoss et al. [16] proposed a secured QoS aware energy efficient (SQEER) routing protocol. Both recommendation trust and directed trust are used for trust computation. Trust scores are computed by considering spatial and temporal parameters. CHs are elected based on trust scores and QoS metrics. Finally, they considered energy, hop-count, and path trust for efficient secure root establishment. Augustine et al. [17] proposed a taylor kernel fuzzy C-means clustering (TKFCC) algorithm for energy and trust aware CH selection. Initially, TKFCC algorithm is used to form the clusters. Later, CHs are selected by formulating one fitness function which includes metrics like maximum energy, maximum trust, and minimum distance. However, the weights considered for each metric are not very reasonable. It leads to equal opportunity that a malicious node with high energy and normal node with less energy can be a CH.

T. Khan et al. [18] proposed a trust estimation method named as large-scale trust estimation scheme (LTS). LTS concentrated on to improve the security and trustworthiness of a larger scale sensor network. Inter and inter clusters along with centralised and distributed approaches respectively are utilised to estimate the trust. Further, communication trust and the data trust are used to improve the trust computation. To balance the energy consumption and trust values, Gaber et al. [19] suggested a new trust evaluation method for clustered IoT network. Here, bat algorithm is used to select CH. This algorithm includes parameters like number of neighbours, remaining energy, and trust value. Direct mode of trust evaluation method is considered to compute the trust and observed that its MDR is less.

Das et al. [20] Introduced Multi Agent Weight based clustering Dynamic Trust Estimation (MWC-DTE) technique to improve the trusted communication with minimum energy consumption. Initially, CH is selected using weight-based clustering algorithm (WBCA) after partitioning entire nodes into few clusters. WBCA algorithm includes node battery, communication power, mobility, and the ideal node degree for CH selection. Next, DTE technique is implemented in four phases; they are direct trust, indirect trust, integrated trust, and update trust phase. Direct trust is computed based on the metrics such as energy trust, communication trust, and data trust. Further, third party recommendations are considered to evaluate indirect trust. Then, direct and indirect trusts are combined by adding weights to each metric to evaluate the integrated trust. Finally, all computed trust values are updated in regular intervals of time to evaluate the trust dynamically. Multimodal trust computation increases computational complexity and it leads to more energy consumption. To detect the malicious node, Ma Z et al. [21] suggested a new trust evaluation scheme named as Distributed Consensus-Based Trust Mechanism (DCONST). A new matrix called as Cognition matrix is formulated by measuring the reputation of each node. The base station evaluates the trust of each node and declares untrustworthy node as a malicious node. However, it is not consider the data trust for trust computation.

R. I. Sajan et al. [22] developed a Three-Level Weighted Trust evaluation-based Grey Wolf Optimization (3LWT-GWO) method to detect the malicious nodes and provides secure routing through trusted nodes. The proposed model is derived in three phases; i) cluster formation based on trust values ii) CH selection and iii) optimal secure data routing. Initially, all sensor nodes are categorized into several clusters by calculating Overall Trust Score (OTS) for each node. OTS is formulated by combining direct trust, indirect trust, long term neighbour recommendation trust, energy trust, link quality trust, and authentication trust. OTS is utilized to determine the unsafe node. After successful removal of unsafe nodes, clustering is performed. Next, fitness function is formulated that includes residual energy, trust, and distance for CHs selection. Then, one node is selected as CH that has highest weight. Finally, optimal route is established through most trusted nodes based on GWO algorithm. Even though the proposed method considers multiple metrics to evaluate the trust but not concentrated on aggregated data trust.

III. Proposed Methodology

This section explores the full details of proposed clustering mechanism along with trust aware routing. This section explores the network model, detailed description of hierarchical non- uniform clustering and finally the trust evaluation mechanism of cluster head.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *25 August 2023* ***Revised:*** *05 October 2023* ***Accepted:*** *24 October 2023*

3.1 Overview

Here, we assumed entire network consist of two types of sensor nodes and they are divided based on their initial energy, sensing range, and transmission range. Further, the network is divided into number of concentric circles followed by straight lines. This division reorganizes the network into non-uniform sized hierarchical clusters. In each cluster, one node is selected as a CH based on its residual energy, type, and distance from the centre of the cluster. Further, each CH's trust value is evaluated by the sink node directly or indirectly. Sink node computes the trust of one-hop neighbour CH directly and the trust of non-one-hop neighbour CH indirectly with the help of other CHs. Here, trust evaluation includes two types of trusts namely network related trust and content related trust. Further, network related trust is divided into two Sub trusts; they are bilateral trust and nobility trust whereas content related trust consists of data-oriented trust. Data-oriented trust concentrates majorly on multidimensional observing data at CH which is acquired from various sensors. To save the memory of sensors, we consider 10-scale integer representation [23] of trust. Here, the computed trust value is compared with integer scale of [0, 10], where '10' indicates highly trusted node, '0' indicates non-trusted node, and '5' indicates medium trusted node.

3.2 Network Model

Here, we consider an IoT network that consists of *N* number of static sensor nodes and one sink node. The following assumptions are made for this network; 1) all sensor nodes are location aware and deployed in circular shaped network. 2) Sink node is placed at the centre of the network and 3) Heterogeneous sensor nodes are considered i.e., initial energy, sensing range, and transmission range is different for each node.

3.3 Hierarchical Non-uniform Clustering

3.3.1 Cluster Formation

Here, circular network field is considered to form non-uniform sized clusters hierarchically. The entire circular network having the radius of *R* is divided into *m* number of concentric circles having the radius of $R_1, R_2, R_3, \ldots, R_m$. In this network field, two types of heterogeneous sensor nodes are deployed densely; they are S_h and S_l. The number of sensor nodes in the network $N = n_{S_h} + n_{S_l}$, where number of S_h and S_l nodes are represented with n_{S_h} and n_{S_l} respectively. All these nodes are heterogeneous in terms of their initial energy, transmission range, and the sensing range. Moreover, these sensors are capable of sensing different kind of parameters and forward it to the sink node. The Type-S_h and Type-S_l nodes are divided based on their initial energy i.e., the energy of Type-S_l node (E_{S_l}) is lower than the energy of Type-S_h node (E_{S_h}). Higher energy nodes are Type-S_h nodes and it has high communication and sensing ranges. Moreover, each sensor node's communication range is assumed as double the sensing range of corresponding sensor node. A virtual layered network structure is established where the width of each circular region is same as CR_{S_l} i.e., $R_i - R_{i-1} = CR_{S_l}$, where, $CR_{S_l}(\ll R)$ is the communication range of Type-S_l nodes. Further, consecutive circles radii is indicated as $R_1, 2R_1, 3R_1, \ldots, mR_1$ and they maintains equal distance i.e., $R_1 = R_2 - R_1 = R_3 - R_2 = \cdots = R_m - R_{m-1} = CR_{S_l}$.
Therefore, the total number of circles to be framed in the given network can be expressed as

$$N_c = \left[\frac{R}{CR_{S_l}}\right] \quad (1)$$

Further, N_l number of straight lines are intersected each other from the centre of the network field by dissecting each concentric circle. The number of lines are decided in such a way that Type-S_h sensor nodes in the adjacent clusters of the outermost ring region (k^{th} ring region) can communicate directly, i.e., the arc length of two clusters should be the maximum communication range of Type-S_h sensor nodes expressed as

$$CR_{S_h} = R_m \times 2\varphi \quad (2)$$

Where, CR_{S_h} is the communication range of Type-S_h nodes, φ is the angle between the two lines and $R_m = mR_1$. Therefore,

$$\varphi = \frac{CR_{S_h}}{2\times R_m} = \frac{CR_{S_h}}{2\times m\times R_1} \quad (3)$$

In general, the total number of lines needed to dissect the circular region is computed by

$$N_l = \frac{360}{2\times\varphi} \quad (4)$$

Then from Eq.(2) and (3), Eq.(4) can be reframed as

$$N_l = \frac{360}{2\times\frac{CR_{S_h}}{2\times m\times R_1}} = \frac{360\times m\times R_1}{CR_{S_h}} \quad (5)$$

Then the final representation of N_l is given as

$$N_l = \frac{2\pi m\left(CR_{S_l}\right)}{CR_{S_h}} \quad (6)$$

Further, zones are framed after dividing entire network into few concentric circles, and lines. These zones are called as clusters (indicated in fig. 1 (b)). Therefore, the number of clusters is given by the following expression

$$N_{clusters} = 2 \times N_c \times N_l \quad (6)$$

The communication range of Type-S_l nodes (CR_{S_l}) is used to determine the number of concentric circles whereas the communication range of Type-S_h nodes (CR_{S_h}) is used to

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *25 August 2023* ***Revised:*** *05 October 2023* ***Accepted:*** *24 October 2023*

determine the number of straight lines. Here, CR_{S_h} is considered in such a way that to partition the network into N_l lines where Cluster Heads (CH) of each adjacent clusters can directly communicate each other. This partitioning show that the framed clusters have different sizes and the size of cluster increases as we move away from the sink node.

3.3.2 Cluster Head Selection

After forming entire network into few clusters, one node is selected CH for each cluster. Here, CH is selected based on sensor nodes' residual energy, type, and the distance from centre of the cluster. Further, the responsibility of CH changes in each round to balance the energy consumption and enhance the network lifetime. In each cluster, each node must have the information about all remaining nodes. After successful retrieval of information about all nodes, the probability of each node is calculated for getting selected as a CH. Therefore, the probability of each node in the cluster getting selected as a CH in k^{th} round is expressed as

$$P_{ij}(k) = \begin{cases} \frac{E_i^R(k)}{\sum_{t=1}^{n_{S_l}} E_t^R(k)} D_{SN_i}^C, & if\ SN_i\ is\ a\ \text{Type} - S_l\ sensor\ node \\ \frac{E_i^R(k)}{\sum_{t=1}^{n_{S_h}} E_t^R(k)} D_{SN_i}^C, & if\ SN_i\ is\ a\ \text{Type} - S_h\ sensor\ node \end{cases} \quad (7)$$

Where, $P_{ij}(k)$ is the probability of node *i* getting selected as a CH of cluster *j* in k^{th} round, $E_i^R(k)$ represents residual energy of i^{th} sensor node in k^{th} round, $D_{SN_i}^C$ represents the distance from the sensor node i (SN_i) to the centre of cluster *j*, $\widehat{D_{SN_i}^C}$ indicates the normalized value [24] of $D_{SN_i}^C$, n_{S_l} and n_{S_h} represents the number of Type-S_l and Type-S_h sensor nodes respectively. Using Eq. (7) every cluster member computes the probability in each round for each other cluster member in cluster *j*. After computing the probability of each cluster member, one node which has maximum probability is selected as a CH in the cluster *j* for k^{th}round and it is expressed as

$$CH_j(k) = \max_{\forall i} P_{ij}(k) \quad (8)$$

Once the CH selection is completed, the trust value is computed by the sink node at each CH. After computing trust value, the CH sends its accumulated data towards the sink node through the most trusted nodes. The next sub-section describes the trust value computation of CH.

3.4 Trust Computation

Here, trust value of CH is computed in the clustered IoT network. The trust of CH is evaluated by the sink node based on three individual trusts namely bilateral trust, nobility trust, and the data-oriented trust. Bilateral and nobility trusts are evaluated by sink node to its one-hop neighbour CHs and non-one-hop neighbour CHs or feedback from one-hop neighbour CHs of sink node. Further, the data-oriented trust of CH is computed by considering the deviation between the gathered observing data and average observing data of sensor nodes in its cluster by sink node.

3.4.1 Bilateral Trust

Bilateral trust is computed by considering the number of interactions between the nodes. Here, the interaction can be defined as a node transmitting or receiving a request/packet to or from its neighbour nodes. Higher degree of interaction between the nodes results in greater the trust and vice versa. Mostly, this trust is evaluated directly or indirectly by the sink node. Sink node evaluates the trust of one-hop neighbour CHs directly whereas it evaluates the trust of non-one hop neighbour CHs indirectly through other CHs based on the type of feedback. The type of feedback may be positive or negative. For positive feedback the trust value is assumed as ≥ 5 and < 5 for negative feedback. The bilateral trust is computed by the sink node of one-hop neighbour CHs is given by

$$BT_{ij} = \begin{cases} \lfloor 10 \times x_{ij} / \max(x_{ij}) \rfloor & x_{ij} \leq \alpha\beta; \\ \lfloor 10 \times \exp(-|x_{ij} - \beta|/\gamma \rfloor & x_{ij} \leq \alpha\beta; \end{cases} \quad (9)$$

Where, BT_{ij} bilateral trust of one-hop neighbour CHs, i is one-hop-neighbours of j, and here, j is assumed as sink node,$\lfloor y \rfloor$ represents the largest integer i.e., $\leq y$, x_{ij} denotes the number of interactions between the nodes i and j, α denotes the upper limit of normal interaction, β denotes the mean value of x_{ij}, γ is a special factor and its values are 1, 10, and 100 when x_{ij} is a single, tens, and hundred digit respectively and so on. Further, bilateral trust is evaluated for non-one-hop neighbour CHs of sink node. It is computed by sink node based on the type of feedback from their one-hop neighbour CHs. Initially, one-hop-neighbour CHs trust value is calculated by each CH using Eq. (9). Later, sink node computes bilateral trust based on the type of feedback.

$$FBT_i = \lfloor 10 \times (P_f + 1)/(P_f + N_f + 2) \rfloor \quad (10)$$

Where, FBT_i is bilateral trust of feedback from one-hop neighbour CHs, destination CH is denoted with i, P_f and N_f denotes number of instances for positive and negative feedback respectively. To improve the quality of feedback, sink node considers only the feedback of CH *i*'s one-hop neighbours whose trust value is ≥ 5. If there is no such type of neighbour CHs then it is consider as 5. Hence, the bilateral trust of CH i is computed by sink node S is denoted with CBT_{iS} and it is given by

$$CBT_{iS} = \begin{cases} BT_{ij}, & i\ \text{is one} - \text{hop neighbor of}\ S \\ FBT_i, & i\ \text{is non} - \text{one} - \text{hop neighbor of}\ S \end{cases} \quad (11)$$

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *25 August 2023* ***Revised:*** *05 October 2023* ***Accepted:*** *24 October 2023*

3.4.2 Nobility Trust

Nobility trust is computed based on the successful and failure interactions between the sensor nodes. Higher the number of successful interactions represents the higher degree of nobility trust. Nobility trust computation is similar to the bilateral trust computation. Nobility trust is evaluated based on the number of successful and failure interactions between the CHs or CH and sink node. It is computed by sink node to the one-hop neighbour CHs and feedback from one-hop neighbours of CHs. The number of successful and failure interactions between the CH to CH and CH to sink node is represented with I_s and I_f. Therefore, the nobility trust of one-hop neighbour CHs is computed by the sink node is denoted with NT_{ij} and it is expressed as

$$NT_{ij} = \begin{cases} \lfloor 10 \times (I_s + 1)/(I_s + I_f + 2) \rfloor, & when\ I_f = 0 \\ \lfloor 10 \times (I_s + 1)/(I_s + I_f + 2) \times {I_f}^{-1/2} \rfloor, & when\ I_f \neq 0 \end{cases} \quad (12)$$

Where, *i* and *j* denotes one-hop-neighbour CH and sink node respectively. If CH *i* send a packet through the node *k* to *j* and overhears the behaviour of *k*, if *k* is not willing to send a packet in predefined interval or sends to another node which is not listed in the routing table then that interaction is said to be failed (not- noble) otherwise the interaction is considered as successful (noble). Further, non-one-hop neighbour CHs nobility trust is evaluated indirectly by sink node based on the type of feedback and that is given by

$$FNT_i = \lfloor 10 \times (P_f + 1)/(P_f + N_f + 2) \rfloor \quad (13)$$

Where FNT_i nobility trust of feedback from one-hop neighbor CHs, destination CH is denoted with *i*, P_f and N_f denotes number of instances for positive and negative feedback respectively. To improve the quality of feedback, sink node considers only the feedback of CH *i*'s one-hop neighbours whose trust value is ≥ 5. If there is no such type of neighbour CHs then it is consider as 5. Hence, the nobility trust is computed by sink node is denoted with CNT_{iS} and expressed as

$$CNT_{iS} = \begin{cases} NT_{ij}, & i \text{ is one} - \text{hop neighbor of } S \\ FNT_i, & i \text{ is non} - \text{one} - \text{hop neighbor of } S \end{cases} \quad (14)$$

3.4.3 Data-Oriented Trust

All IoT networks are data-centric networks and heterogeneous sensors are connected to each other in this network. Mostly, these sensors collect various types of data and this multi-dimensional observing data is gathered at CH. Finally, the gathered data is transferred to sink node directly or indirectly. By observing the gathered multi-dimensional data, the data-oriented trust is evaluated by the sink node. Moreover, it is evaluated at sink node by considering the difference between multi-dimensional gathered observing data and average of multi-dimensional observing data at CH. Lesser deviation indicates higher data-oriented trust of the node. So, in order to compute the data-oriented trust, the CH needs to send the gathered multi-dimensional observing data and average of multi-dimensional observing data to the sink node. Hence, the data-oriented trust of CH *i* is computed by sink node *S* indicated with DOT_{iS} , expressed as

$$DOT_{iS} = \lfloor 10 \times exp^{-D_{di}} \rfloor \quad (15)$$

Where D_{di} represents the deviation between the average of multi-dimensional observing data at CH *i* and gathered multi-dimensional observing data at CH *i* and it is given by

$$D_{di} = \left(\sum_{p=1}^{d_n} \left(d_{ip} - d_{imp} \right)^2 \right)^{1/2} \quad (16)$$

Where, d_n represents dimension of observing data, d_{ip} and d_{imp} indicates the average of p^{th}- dimension observing data computed by CH *i* and gathered p^{th}- dimension observing data of CH *i* respectively.

3.4.4 Composite Trust

The trust of each CH for every cluster is computed by the sink node by combining the bilateral trust, nobility trust, and data-oriented trust. Therefore, the composite trust of CH *i* is evaluated by sink node *S* is represented with CT_{iS} and it is given by

$$CT_{iS} = \lfloor a_1 \times CBT_{iS} + a_2 \times CNT_{iS} + (1 - a_1 - a_2) \times DOT_{iS} \rfloor \quad (17)$$

Where, a_1 and a_2 are the weights of each sub-trust and $a_1, a_2 \in [0,1]$. Here, we considered as equal priority for each sub-trust i.e. $a_1 = a_2 = 1/3$. The trust of CH i is evaluated using Eq. (16) and if it is less than 5 then that node is considered as compromised or malicious.

IV Simulation Results and Discussions

This section explores the performance evaluation of proposed method by conducting various simulation experiments. Initially this section discusses the details of experimental setup and then explains the details of simulation results. The results are explored through the performance metrics.

4.3.1 Simulation Setup

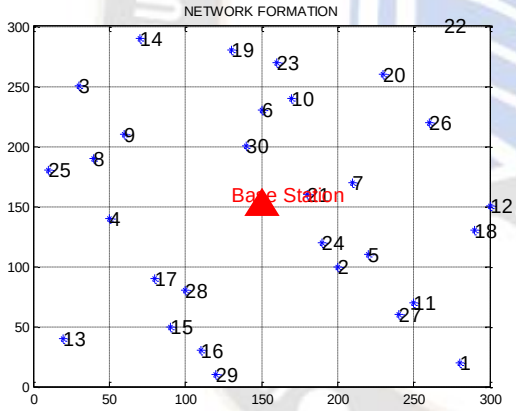
Under experimental setup, create a random network with varying node count and the radius of network is mentioned as 1000. For experimental validation, MATLAB software is used. Figure.1 shows an example network with 30 nodes with sink node at center and its clustered version. The entire nodes are assumed as stationary and they don't have mobility. For each and every node, the communication range is kept as constant and it is approximately specified as $1/10^{th}$

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *25 August 2023* ***Revised:*** *05 October 2023* ***Accepted:*** *24 October 2023*

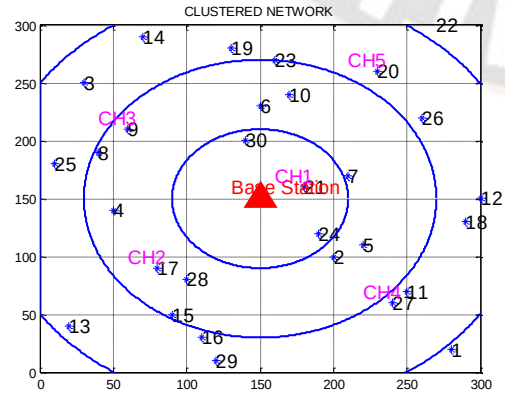
of total network width or length. For the realization of random nature, the node positions are changed at every simulation instance. To check the robustness, the simulation is done by varying rounds and at every instance the performance analysis is done. The simulation is done by keeping the BS at the centre of network. In this network, two types of sensor nodes such as Type-S_l and Type-S_h are deployed. The required simulation parameters are tabulated in Table.1.

Table.1 Simulation Setup

Parameter	Value
Node count (N)	100
Radius of the network	$1000m$
Data packet size	512 bytes
Nodes placement	Random
Percentage of Malicious nodes	0-40% of Nodes
Initial Energy of Type-S_l node (E_{S_l})	1J
Initial Energy of Type-S_h node (E_{S_h})	2J
Communication range of Type-S_l node (CR_{S_l})	100m
Communication range of Type-S_h node (CR_{S_h})	200m
Number of Simulation Rounds	2000



(a)



(b)

Figure.1 Random network with Base station at center and clustered network

4.3.2 Results

To analyse the performance of proposed work, we consider the metrics such as Malicious Detection Rate (MDR), False Positive Rate (FPR), False Negative Rate (FNR), Maximum Communication Overhead (MCO), and network lifetime to evaluate the performance. These metrics are computed at various malicious node count. To assess the performance of proposed work, compared it with existing methods such as MWC-DTE [20], 3LWT-GWO [22].

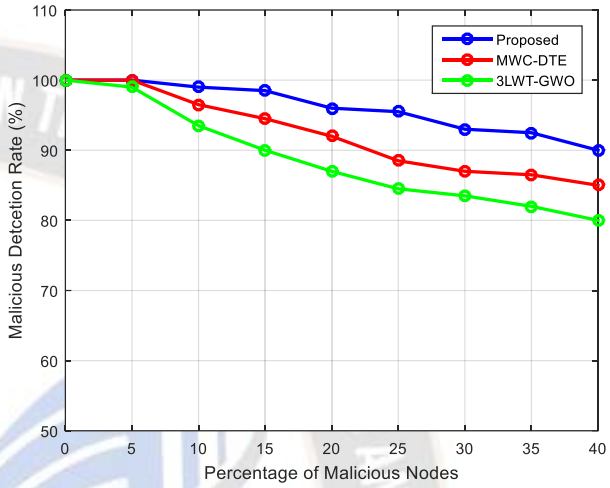


Fig.2 Malicious detection rate for various malicious node count

Figure.2 shows the MDR for varying malicious node count. From the figure, we observe that as malicious nodes are increasing then MDR is decreasing for all three methods. The proposed method achieved larger MDR than the existing methods MWC-DTE, 3LWT-GWO. Since the proposed method considered three different trusts, it can detect maximum number of malicious nodes effectively than the existing methods. Here, we considered malicious node count is varying from 5% to 40%. The average MDR of proposed work, MWC-DTE and 3LWT-GWO is approximately 96.05%, 92.22%, and 88.83% respectively. Further, FPR and FNR indexes are used to assess the malicious activity that is shown in the Figure.3 and Figure.4 respectively. FPR indicates normal nodes are declared as malicious nodes. From figure 4, we observe that as malicious node count increases then FPR increases due to the dynamic trust evaluation mechanism. As shown in the Figure.3, average FPR for proposed work is approximately 8.38%, and for MWC-DTE, and 3LWT-GWO is approximately 9.5%, and 11.33% respectively. From the results, we observed that FPR of proposed method is less than the state-of-the-art methods.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
Article Received: *25 August 2023* ***Revised:*** *05 October 2023* ***Accepted:*** *24 October 2023*

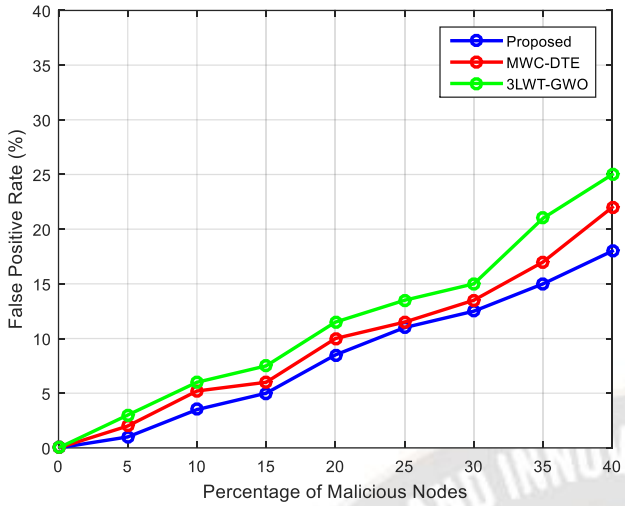


Fig. 3 False positive rate for various malicious node count

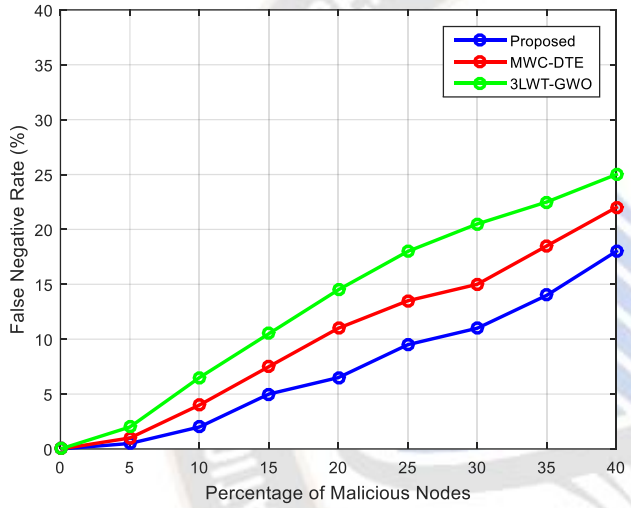


Figure.4 False negative rate for various malicious node count

Figure.4 shows the FNR for various malicious node count. The characteristics of FNR are similar to the FPR as observed in the Figure.3. FNR indicates malicious nodes are declared as normal nodes. From Figure.4, we observe that as malicious node count increases FNR increases due to the detection of malicious nodes in multiple aspects. From results, average FNR for proposed work is approximately 7.38%, and for MWC-DTE, and 3LWT-GWO is approximately 10.27%, and 13.27% respectively. From the results, we observed that FNR of proposed method is less i.e., less number of false negatives than existing methods.

Figure.5 shows the storage overhead at different cluster count. From the Figure.5, we observe that as cluster density increases, the storage overhead decreases. Since the presence of more number of clusters in the network shares the data forwarding responsibility, the storage overhead reduces. Moreover, as the number of clusters is more, the number of nodes being clustered into a cluster is less. Hence, the overall storage overhead is less. Here, direct and indirect communication for non 1-hop neighbour CHs is observed. The storage overhead includes sensor node with CH, CH with CH, and CH with sink node. Further, as node density increases the number clusters increases and communication between the nodes also increases. It leads to high energy consumption in the network. Compared with existing methods, the proposed method has an innovative clustering strategy which initially separates high energy and low energy nodes, the additional burden on low energy nodes are less. From the results, the average storage overhead for proposed work, MWC-DTE, and 3LWT-GWO is observed as 1860, 2500, and 3000 bytes respectively. From the results, we observe that the proposed method faced a less storage overhead than the state-of-the methods.

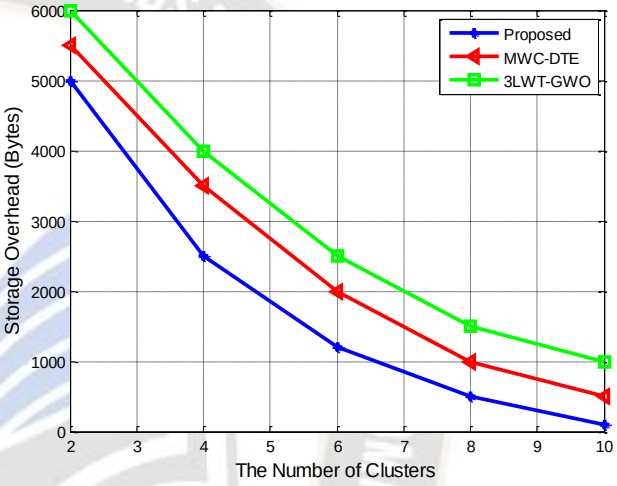


Figure.5 Storage overhead (bytes) for varying number of clusters

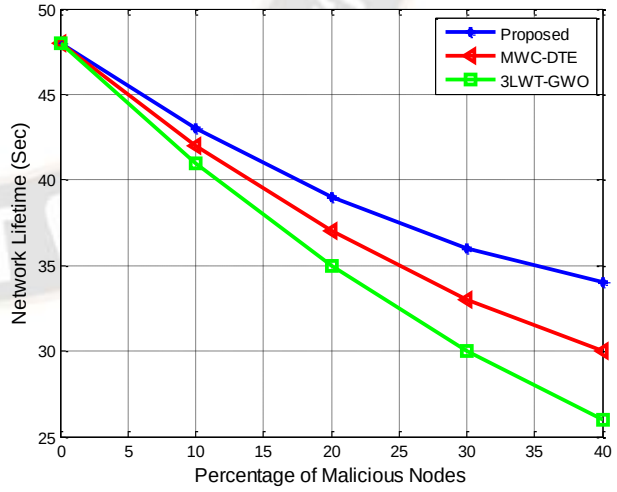


Figure.6 Network lifetime (Sec) for varying malicious node count

Network lifetime has an inverse relation with the malicious nature of network. As the number of malicious node count increases, different types of attacks are probable to get

launched. Due to these reasons, the nodes get depleted quickly and results in lowering of network lifetime, as shown in Figure.6. From the results, we can see that the proposed approach has attained more network lifetime than the conventional methods. Since the proposed approach has applied data related trust which has superiority in the detection of attacks such as data tampering, data manipulation etc. whereas the existing methods didn't concentrated on the data attributes. Due to these reasons, they experienced less network lifetime than the proposed method. The average network lifetime of proposed approach is noticed as 40 seconds while the existing methods had experienced only 32 seconds and 28 seconds at MWC-DTE and 3LWT-GWO respectively.

V. Conclusion

In this paper, we proposed hierarchical non-uniform cluster based trust evaluation mechanism called as Communication and Content Trust Aware Routing (CCTAR) for Clustered IoT network. Initially, the entire network is divided into few clusters non-uniformly through concentric circles and straight lines. Next, trust is computed by sink node directly through 1-hop neighbour CHs and indirectly through non-1-hop neighbour CHs at each CH. Here, two network oriented trust metrics such as bilateral trust and nobility trust, and one data-oriented trust metric are used to compute the trust of CH. Finally, all trusts are combined by incorporating individual weights to each trust metric. The performance of proposed method is examined by conducting several simulation experiments at different malicious node count and proved that the proposed method can achieve best results compared to state-of-the art methods.

References

[1] Čolaković, A., & Hadžialić, M., "Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues", Computer Networks, Vol. 144, pp.17–39, 2018.

[2] I. Butun, S. D. Morgera, and R. Sankar, "A survey of intrusion detection systems in wireless sensor networks", IEEE Commun. Surveys Tuts.,Vol. 16, No. 1, pp. 234-241, 1st Quart., 2014.

[3] Rani, R. and Katti, C.P "End-to-End Security in Delay Tolerant Mobile Social Network." International Conference on Application of Computing and Communication Technologies, Springer, Singapore, pp. 45-54, 2018.

[4] Ishaq, Zeba, Seongjin Park, and Younghwan Yoo. "A security framework for Cluster-based Wireless Sensor Networks against the selfishness problem" 2015 Seventh International Conference on Ubiquitous and Future Networks. IEEE, 2015.

[5] 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, May 2012.

[6] Aya Ayadi, Oussama Ghorbel, Abdulfattah M. Obei, Mohamed Abid, "Outlier detection approaches for wireless sensor networks: A survey", Computer Networks 129 (2017) 319–333.

[7] Saleh, A.; Joshi, P.; Rathore, R.S.; Sengar, S.S. Trust-Aware Routing Mechanism through an Edge Node for IoT-Enabled Sensor Networks. Sensors **2022**, 22, 7820

[8] Kumar, D.P.; Amgoth, T.; Annavarapu, C.S.R. Machine learning algorithms for wireless sensor networks: A survey. Inf. Fusion **2019**, 49, 1–25.

[9] Zhihua Zhang, Hongliang Zhu, Shoushan Luo, Yang Xin, And Xiaoming Liu, "Intrusion Detection Based on State Context and Hierarchical Trust in Wireless Sensor Networks", IEEE Access, Volume 5, 2017, pp.12088- 12102.

[10] Weidong Fang, Wuxiong Zhang, Wei Chen, Tao Pan, Yepeng Ni, Yinxuan Yang, "Trust-Based Attack and Defense in Wireless Sensor Networks: A Survey", Wireless Communications and Mobile Computing, Vol. 2020, pp. 1-20, 2020.

[11] Hamad Aldawsari and Abdel Monim Artoli, "A Reliable Lightweight Trust Evaluation Scheme for IoT Security" International Journal of Advanced Computer Science and Applications(IJACSA), Vol. 12, No. 11, pp. 723-731, 2021.

[12] Dass, P.; Misra, S.; Roy, C. "T-safe: Trustworthy service provisioning for IoT-based intelligent transport systems", IEEE Transactions on Vehicular Technology, Vol. 69, No. 9, pp. 9509-9517, 2020.

[13] Tao Yang, Xu Xiangyang, Li Peng, Li Tonghui, Pan Leina, "A secure routing of wireless sensor networks based on trust evaluation model", Procedia Computer Science, Vol. 131, pp. 1156-1163, 2018.

[14] R. Rani, S. Kumar and U. Dohare, "Trust Evaluation for Light Weight Security in Sensor Enabled Internet of Things: Game Theory Oriented Approach" in IEEE Internet of Things Journal, Vol. 6, No. 5, pp. 8421-8432, 2019.

[15] Feslin Anish Mon Solomon and S. Godfrey Winster and Ram Ramesh, "Trust Model for IoT Using Cluster Analysis: A Centralized Approach", Wirel. Pers. Commun, Vol. 127, pp. 715-736, 2021.

[16] T. Kalidoss, L. Rajasekaran, K. Kanagasabai, G. Sannasi, and A. Kannan, "QoS Aware Trust Based Routing Algorithm for Wireless Sensor Networks", Wireless Pers. Commun., Vol. 110, No. 4, pp. 1637-1658, Feb.2020.

[17] S. Augustine, and J. P. Ananth, "Taylor kernel fuzzy C-means clustering algorithm for trust and energy-aware cluster head selection in wireless sensor networks," Wireless Netw., Vol. 26, pp. 5113–5132, Jun. 2020.

[18] Khan T, Singh K, Abdel-Basset M, Long HV, Singh SP, Manjul M, "A Novel and Comprehensive Trust Estimation Clustering Based Approach for Large Scale Wireless Sensor Networks", IEEE Access, Vol. 7, pp. 58221-58240, 2019.

[19] T. Gaber, S. Abdelwahab, M. Elhoseny, and A. E. Hassanien, "Trust-based secure clustering in WSN-based intelligent transportation systems", Comput. Netw., Vol. 146, pp. 151–158, 2018.

[20] Das, R., Dwivedi, M., "Multi agent dynamic weight based cluster trust estimation for hierarchical wireless sensor networks", Peer-to-Peer Netw. Appl. , Vol. 15, pp. 1505–1520, 2022.

[21] Ma Z, Liu L, Meng W, "DCONST: Detection of multiple mix-attack malicious nodes using consensus-based trust in IoT networks", Australasian Conference on Information Security and Privacy, Springer, Vol. 12248, pp. 247–267, 2020.

[22] Sajan, R.I., Christopher, V.B., Kavitha, M.J., "An energy aware secure three-level weighted trust evaluation and grey wolf optimization based routing in wireless ad hoc sensor network", Wireless Netw , Vol. 28, pp. 1439–1455, 2022.

[23] 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.

[24] Perera, C., Zaslavsky, A., Liu, C. H., Compton, M., Christen, P.,& Georgakopoulos, D., "Sensor search techniques for sensing as a service architecture for the internet of things", IEEE Sensors Journal, Vol. 14, No. 2, pp. 406–420, 2013.