Multi-Level Fuzzy Cluster Based Trust Estimation for Hierarchical Wireless Sensor Networks

Rahul Das and Mona Dwivedi
Mansarovar Global University, Madhya Pradesh, India

In Hierarchical Wireless Sensor Network (HWSN), the energy transmission of data packets belongs to the distance between source and destination, vulnerable to various malicious attacks. Thus clustering of HWSN reduces energy consumption, achieves scalability, and reduces network traffic. Therefore in this paper, a Multi-level Fuzzy Cluster Trust Estimation (MFCTE) logic model is used for clustering nodes and select trustworthy Cluster Head (CH) from clustered nodes. For this, the proposed method uses five attributes to become a trust-based CH. The following attributes given as input to fuzzy are Density of the other sensor nodes near to CH, Compaction of the surrounding nodes, Distance from the base station, Residual energy of the sensor nodes, and Packet integrity. MFCTE detects malicious nodes and ensures security in CH by automatically adjusting a load of direct trust, indirect trust, and parameters of update mechanism. The simulation results indicate that the proposed technique is energy efficient in terms of energy consumption, network lifetime for different network sizes, and better at defining malicious attacks.

Keywords: Trust estimation, Cluster head, Fuzzy model, Multi-level Clustering, and Wireless Sensor Network.

1. INTRODUCTION

Wireless Sensor Network (WSN) consists of various sensors (infrared, thermal, magnetic, and visual sensors) with distributed sensor nodes for tracking and gathering information via wireless link from the field. Hence, it be used in various applications include health care monitoring, battlefield operations, smart city surveillance, and intrusion detection (Qiu, T et al 2016). Using of clustering algorithm in WSN, the Sensor Nodes (SN) are grouped into clusters, and high energy power Cluster Node (CN) are nominated as Cluster Head (CH). This formation of CHs forms a strong backbone on network named as cluster-based WSN environment. But the openness behavior of the WSN are vulnerable to various types of security attacks like Sybil, on-off, collusion, bad mouthing, data hardening, Denial of Service (DoS) attacks etc. (He, J., and Xiong, N. 2018; Han, G et al 2014; Talbi, S et al2017). Above of all these attacks helps adversaries to intercept private information on impersonating nodes. This destroy the security, non-reputation, and usability of WSN. There also present some other factors may create problem in SNs. To that, some complicated encryption algorithm are used in WSN, it become unfit because of restricted capabilities of low cost nodes. Hence a symmetric cryptographic method is adopted, but this method be unable to identify the threads of detecting the malicious nodes. As the malicious node are not be identified at a right time in network, the secret information be revealed (Ishmanov, F et al 2017; Fang, W et al 2016). To overcome the security issues, trust assessment is necessary to be act as a protect mechanism to collects data from the intermediate node by monitoring the sensor network to be send to the base station (BS). Therefore, an efficient mechanism is necessary to identify the malicious node and minimize the loss in network by selecting proper CH. The trustworthy communication between the clustered nodes belong to the integrity and reliability of collected information (Liu, X.et al 2018) Some malicious sensor nodes may illegally drop the data packets and disturb network communication. Hence, internal networks attacks of malicious nodes becoming a challenging research topic under on its trust and security

solutions for WSN (Prabha, V. R., and Latha, P. 2017). Trust management is one of the way to identify the malicious node which be authenticated. However, the reality of sensor nodes has special character and limited resources, which makes trust approach more challenge and significant (Zawaideh, F., and Salamah, M. 2019). Thus the present research focus on trust on nodes in HWSN of presenting trust evaluation to improve security and robustness. Applying already exist security solutions such as hash function, authentication, and cryptography only present security upto certain extent. But finding of malicious nodes has large complexity in computation and energy consumption. Thus trust-based mechanism is introduced which is better than traditional cryptographic techniques in term of reliability and efficient of detecting the malicious nodes (Gomathy, V et al 2020; Prabha, V. R., and Latha, P. 2017). The trust-based approaches like Bayesian approach employs Bayes rule as a criterion for computing trust rating, thus the SN can verify the position of neighbor nodes information by cross checking the neighbor nodes (Zhang, T et al 2018; Yang, Het al 2020; Zawaideh, F et al 2017) Distributed reputation-based framework for sensor network (RFSN) consider the trust value of sensor node by direct trust, but ignore the recommendation trust (Cheng, X et al 2018), Then Group based Trust Management Scheme (GTMS) calculate the trust value based on indirect and direct trust value observations (Labraoui, N. 2015). Node Behavioral strategies banding belief theory of the trust evaluation method (NBBTE) interact among two neighbor nodes and values of trust are measured by fuzzy set theory (Dhakne, A. R., and Chatur, P. N. 2015). Trust joined light probe-based defense mechanism sent probe message sent to the trust nodes identifying the malicious nodes (Jaint, B et al 2018) Trust management and evaluation has several issues due to un-unique features of WSN. As the nodes increases, the complexity of monitoring the node behavior, evaluation and management of trust increase non-linearly. Therefore, performing the trust estimation and management by node is a greater challenge to neighbor nodes. Moreover, an exchanging the trust value between nodes are limited due to high energy consumption and limited bandwidth due to congestion (Rehman, E et al 2017). The trust establishment mechanism analyzes the sensor node behavior to recover the limitation of security mechanism, key management, authorization, and authentication process (Kulkarni, S. B., Yuvaraju, B. N. 2017; Liu, Let al 2019). Till now, enormous amount of research done in managing trust which consider the communication interaction among nodes, identifies and protect against the malicious attack. However, the techniques had various problems such as minimum network lifetime, packet loss and poor quality links of sensor node causes high energy utilization. Furthermore, the earlier models decreases the detection rate of nodes, reduce memory space and increases the routing overhead. Hence to facilitate all those issues, an efficient trust based mechanism is necessary for sending data to the destination node with high trust value, and to isolate the malicious node and thereby ensure the security and enhances the lifetime of sensor network (Singh, O et al 2018; Manoranjini, J et al 2019)

2. RELATED WORK

Some of the recent works carried out in trust node estimation scheme and its drawbacks are discussed as follows: Desai, S. S., and Nene, M. J. (2019), discussed a Software-based node-level trust evaluation method (SNTEM) that aims the trust at node level by using the available internal resources without non-cryptographic technique and lesser energy overheads in the network. This model consists of two stages which include the challenge-response (CR) model and node-level trust evaluation task. In the first stage, the destination node is trusted by performing a comparison between the response and the challenge estimated at the source node. The second stage is categorized under three levels where node Conditioning is performed based on the lookup table and Immutable Response. Next, the Self-scrutiny algorithm deployed node by Sequential boot check method. Finally, a Self-attestation algorithm enables the communication among source and destination within its range in peer-peer mode. However, two nodes with the same node memory are trusted otherwise it was not trustworthy. Xia et al. (2016), developed Beta and Link Quality Indicator based Trust Model (BLTM) that calculate the trust relationship between the sensor

nodes. This model consists of five modules such as Link Quality Indicator (LQI) analysis, direct trust, recommendation trust, integrated trust, and trust update-modules. Firstly, the source node collects LQI data within the destination node and its link quality is good to continue the trust calculation. The three metrics such as energy, communication, and data trust which are used to calculate direct trust value and combine the value of two nodes. Next, the integrated trust was calculated by the weight of direct trust and recommendation trust. Finally, the trust values are updated by using a sliding time window. Although it reduces poor quality links this method could not defend DOS and Data tampering attacks. Raja et al. (2019), suggested Belief based Trust Evaluation Mechanism (BTEM) detach the malicious node and protect against On-off and Bad-mouthing attacks. This mechanism has three modules such as the Traffic Monitoring module, Trust Evaluation module, and Decision Maker. At first, the source node with a transmission range forward data to the destination node, and it was monitored by a traffic profile to identify the malicious node. The three metrics are traffic receiver, direct trust, and indirect trust evaluate trust nodes in communication range receive packet tuned on the same channel by Bayesian Estimation approach. Finally, the Decision Maker module compares the threshold value ranges with the probability of each node. However, to identify the malicious nodes are a challenging task due to computation complexity, large memory requirements, and high energy consumption. Jin et al. (2019), recommended an Exponential based Trust and Reputation Evaluation System (ETRES) which estimates the distributed trust node. This model consists of three models consists of Trust and Reputation modeling, Trust and Reputation Estimation Modelling, and Exponential based trust modeling. According to the relationship between beta distribution and exponential distribution, the nodes calculate their trust value based on the time interval between the adjacent nodes. Then the entropy-based confidence factor saves the computing node power to consume low energy. Finally, trust value calculated by an interaction between the nodes. However, selective forwarding, on-off, slander, and collusion attack reduce the lifetime of the network. Tayyab et al. (2019), proposed Light Weight Estimation Trust Scheme (LTS) to improve the trust of clustering and security to defend a malicious attack. This model operated in two phases such as intra-cluster trust level, inter-cluster trust level along with centralized and distributed approaches where the unique identifier is given to each sensor node to communicate with the destination node. First, the trust level occurs at minimum communication overhead with high capability detection and monitor the sensor node by its intermediate node. Next, consider the communication trust and evaluate the indirect trust by a base station and examine scalability and convergence rate of LTS to optimize the cluster. However, the storage memory is low due to on-off and collusion attacks. Karthik and Anantha (Karthik, N., Ananthanarayana, V. S. 2017). proposed a Hybrid Trust Mechanism Scheme (HTMS) to detect data fault used by spatial and temporal relationships and recover the untrusted data. This model depends upon three phases such as data trust evaluation, node trust evaluation, and trust score adjustment. Initially, data item sent to the sink node through its intermediate node and then allot the data trust score calculated by self-data trust, peer- data trust. Then, node trust value was evaluated by the sliding window. Finally, trust score adjustment based on provenance based trust done by a sink node to detect data fault. This approach destroys the information of sensor nodes due to on-off, bad-mouthing attacks. Dan et al. (2017), proposed Trust Sensing based Secure Routing Mechanism (TSSRM) to handle network attacks. This model consists of three phases such as Network initialization process, route construction process, and route maintenance method. At first, the cluster head was selected by monitoring the node with its neighbor node and exchange its trust degree. Next, construct the transmission link which controls the transmission range and direct trust, indirect trust, and incentive factor detect the nodes with the attack. Finally, new nodes are joined due to route update and handle the route repair initiated by node movement. This approach was difficult to ensure the multi-hop information transmission security. Xian et al. (2017), proposed Multi-agent trust-based Intrusion Detection Scheme (MTIDS) to detect the node intrusion and trusted value of the node. First, the attributes of the node to assigned and check whether attributes

are normal by Mahalanobis distance theory. According to the combination of beta distribution and a tolerance factor the sensor, the node transmits data to cluster head calculate and update the reputation distribution of node trust. The tolerance factor detects the false rate of the node. Finally, compare the trust value with the threshold value to detect node intrusion. However, the multiple types of intrusion occur then decrease the detection rate of the node. A review on the popular trust mechanisms and trust approaches are discussed in Table 1.

3. PROPOSED METHODOLOGY

In this research, we design a framework of Multi-level Fuzzy Cluster Trust Estimation (MFCTE) system model to provide trustworthy data transmission which can handle various malicious attacks in nodes with minimum energy consumption.

3.1 **System Model** The type of network used for the proposed trustworthy system model is Hierarchical Wireless Sensor Network (HWSN) contains Senor Nodes (SNs), Cluster Heads (CHs), and Base Station (BS). Here, the HWSN used is a cluster-based. In cluster-based hierarchical WSN, the sensors are organized into the form of clusters, and while transmission go via CHs. The type of transmission held between the SN to CH is single hop, and CH to BS by single or Multi-hop. The consideration of trust is performed between the Intra-cluster and Inter-cluster levels.

3.1.1 **Multi-level Fuzzy Cluster Trust Estimation model design procedure** The different factors influence CH selection are flawed assumptions, signal overhead, and accuracy. Therefore Multi-level fuzzy clustering mechanism is presented to combine all input parameters to reflect the influence of effectiveness in CH selection. The four linguistic attribute variable consider to form trust over malicious nodes by our proposed system are Residual Energy Value (REV), Packet Integrity Value (PIV), Density Value (DV), Compaction degree Value (CdV), and Distance Value (DiV) with a different degree of membership such as Very Large , Large, Medium, Very small, and Small.

i) **Initialization Phase:** Initially the nodes are placed randomly in a square area without mobility, and clusters are not formed in the beginning itself. Every node has a trust value given randomly at the initial stage in between the range

ii) **Cluster Head formation phase:** CH selection is done by the node having higher initial trust degree (Higher energy, longer node lifetime). Each nodes exchanges its trust value to its neighboring nodes by sending a Trust Request Packet (TRP) message to select the CH with high degree trust. The information of the TRP carries the ID of node, Threshold trust value, Hop count of TRP list and Serial number of TRP.

iii) **Trust is calculated based on the direct and indirect trust evaluation:** The trust is computed based on communication trust, energy trust, and data trust. The total trust estimation is performed in CH and BS. The operation on the CH and BS is performed using a fuzzy decision making process to detect good, bad and uncertain nodes. In the intra-cluster level, the direct trust is estimated by Cluster Member (CM) to CM within the cluster and CH estimates the trust of CM of its cluster for indirect trust calculation. In inter-cluster level, the direct trust is estimated between CH -CH and the indirect trust evaluation is performed by the BS based on the trust information calculated by the CH. Trust model is one of the mathematical model gives opinion to one node to another at the way of transmission of information or data over the network. The trust values also cause some uncertainty while taking decision based on the behavior of nodes. Thus Multi-level fuzzy model is used of its easy nature and of capturing the expert knowledge. The four level of operation performed are Fuzzification, Fuzzy rules creation, Fuzzy interference system, and Defuzzification. In the first level of fuzzification, a conversion of multiple input trust attributes into fuzzy sets are performed. Then creation of fuzzy rules are made to map the input trust attributes to present trust output. Degree of the trust value on sensor nodes are decided by the factor of trust

Table I: Comparison of existing Trust and clustering model

Trust models	**Trust mechanism**	**Attack**	**Parameters**	**Trust Evaluation**	**Merits**	**Demerits**
BLTM (Wu, X et al 2019)	LQI mechanism	Selective forwarding attack, DoS attack, Tampering Attack	Normal data sequence (a), Tampered data sequence (b)	Direct Trust and Recommendation Trust	LQI data detect external node intrusion	Does not properly defend DOS and Data tempering attacks.
BTEM (Anwar, R. W et al 2019)	Bayesian Estimation	On-off, Badmouth, Dos	Packet received evaluation (PRE), Transit packet evaluation (TPE), and Packet sending evaluation (PSE).	Direct Trust and Indirect Trust	Increase network lifetime	High computation complexity, large memory requirements
ETRES (Zhao, J et al 2019)	Exponential-based trust	Selective forwarding attack, Slander attack, on-off attack and collusion attack	Number of successive interactive behavior (a), and Number of Unsuccessful interactive behavior (b) of the node	Direct Trust and Indirect Trust	Save computing power, low energy consumption	Prone to Selective forwarding, on-off, slander and collusion attack which increases the lifetime of the network.
LTS (Khan, T et al 2019)	Distributed and centralized approach	Garnished attack, Badmouth attack, Blackhole attack, and Ballot-Stuffing attack	Reward coefficient, and Punishment coefficient	Communication Trust, Indirect Trust	Improve security and reliability of the node	Problem in storage memory due to on-off and collision attacks
HTMS (Karthik, N., 2017)	Efficient distributed trust model	DoS attack, Bad mouthing attack, on-off attack, Conflicting Behavior attack, Attack on data, Sybil attack, Replication attack and Collusion attack	Aging factor	Direct Trust, Indirect Trust, Trust score, Self-data Trust, Peer data Trust, Provenance based trust, punish and reward	Recover untrusted data, provide attack residence degree	Destroy the information of sensor nodes due to on-off, bad-mouthing attacks.
TSSRM (Qin, D et al 2017)	Analytical Hierarchy process	Grayhole, Tampering, on-off, and bad mouthing attacks	Energy	Direct Trust and Indirect Trust	Efficient and reliable data transmission	Reduce routing overhead

classification. Communication Behavior Trust (CBT) value is mentioned to detect malicious nodes. For that message success rate and interval time among transmission and reception are denoted as Qos variables. The self-adaptive weights of direct trust value calculated at CH level and indirect trust value at BS level are used to aggregate trust values at BS. Our trust model is able to effectively detect the malicious or compromised nodes between dealing nodes and it also proves to be resilient against different attacks by Fuzzy model. Formation and clustering of HWSN structure is shown in Figure 1.

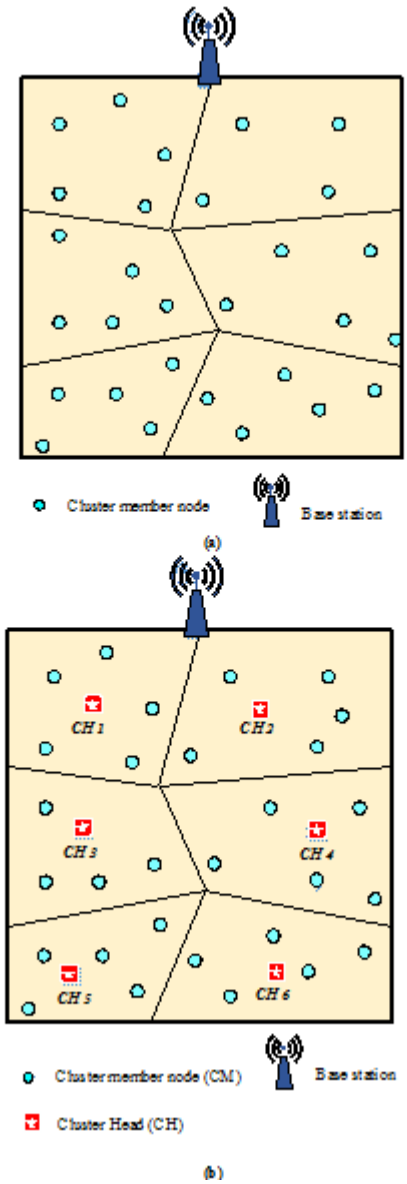

Figure 1. Formation of cluster-based HWSN

3.2 Trust Evaluation Module (TEM)

TEM is responsible for evaluating trustworthiness value of each communicating node through its packet forwarding, receiving and transit packet behavior and estimates the probability of

a node whether it is malicious or trustworthy. A node is declared as trustworthy if it forwards all the data to intend destination node and these informations are monitored which is then shared with other neighbouring nodes as directly or indirectly. Similarly, node is considered as malicious if it intentionally drops some or all the packets and record wrong information in the traffic profile by indicating correct number of received and forwarded packets. The structure of routing path of inter and intra clustering is shown in Figure 2.

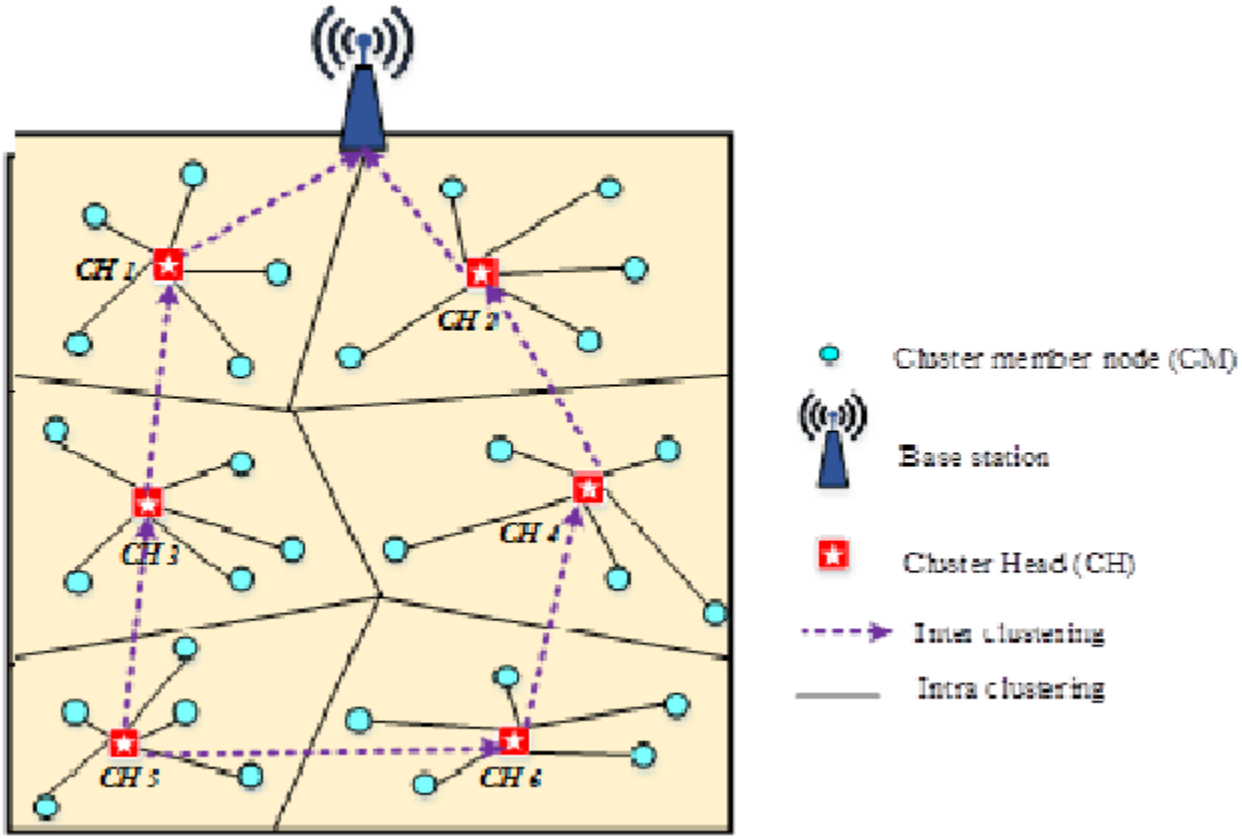

Figure 2. Routing path of inter-intra clustering

(i) **Trust metrics** The highest degree of important features of trust management strategy is the process of data collection for direct trust computation. The trust value of a neighboring node can be computed by using number of successful and unsuccessful interaction on different trust metrics. Trust metrics is nothing, but the various Quality of Services (QoS) characteristics of nodes are threshold of the trust, timestamp, serial number of the TRP and hop counter. Here the trust metrics are divided in to two priority groups. These priority groups are used for rewarding and penalizing trust value of the sensor nodes. The structure of WSN Clustering based trust estimation is illustrate in Figure 3.

3.2.1 **Intra Cluster trust evaluation in CM-CM Direct Trust Calculation** In this phase we consider real time scenario and calculates two events (successful and unsuccessful) in every small time stamp (δ_t) . Here, the successful interaction event between the node a and

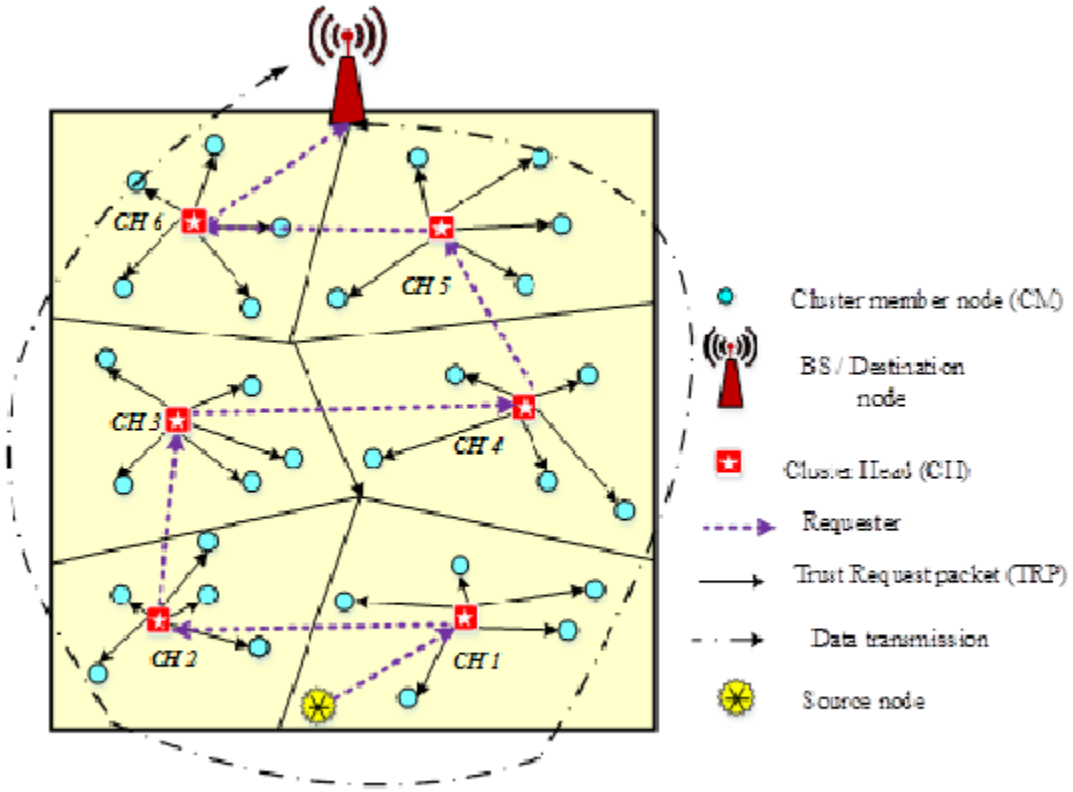

Figure 3.Structure of WSN Clustering based trust estimation

b is represented by $\zeta_{ab}^{c_i}(\delta_t)$ and the successful interaction event between the node a and b is represented by $\vartheta_{ab}^{c_i}(\delta_t)$

The evaluation equation of CM-CM Direct Trust Calculation is given below,

$$Tr_{ab}^{dir}(\delta_t) = \left[\begin{array}{c} \left(10 * \frac{\zeta_{ab}^{c1}(\delta_t)+\zeta_{ab}^{c2}(\delta_t)}{\zeta_{ab}^{c1}(\delta_t)+\zeta_{ab}^{c2}(\delta_t)+\vartheta_{ab}^{c1}(\delta_t)+\upsilon_{ab}^{c2}(\delta_t)}\right) \times \\ \left(\frac{P_1*\zeta_{ab}^{c1}(\delta_t)+P_2*\zeta_{ab}^{c2}(\delta_t)}{1+P_1*\zeta_{ab}^{c1}(\delta_t)+P_2*\zeta_{ab}^{c2}(\delta_t)+\zeta_{ab}^{c1}(\delta_t)+\upsilon_{ab}^{c2}(\delta_t)}\right) \times \left(\frac{1}{\sqrt{P_1*\zeta_{ab}^{c1}(\delta_t)+P_2*\zeta_{ab}^{c2}(\delta_t)}}\right) \end{array} \right] \quad (1)$$

The factors of above equation, the first stage is the proposition of successful interaction between the node a and b for the particular time stamp. it is based on the event belonging to the cluster trust metrics. The second stage represents the reward factor, then the third stage denotes the stringent penalty for the unsuccessful interaction between a and b, P represents the priority and [] denotes the matrix function, to find the nearest unsigned integer value of the direct trust.

3.2.2 **Intra Cluster trust evaluation in CH-CM Indirect Trust Calculation** The indirect trust in CH-CM is evaluated with trust circulation. In the trust proliferation, trust transits through third parties. Assume, the node a tries to set up indirect trust on b (When there is no direct trust of node an on b). The node b needs to request the direct trust of neighbours Xi on hub b. Here, the Master Node (MN) periodically collects the direct trust value of its cluster member node to maintain the trust matrix (Tr) .

$$Tr = \begin{bmatrix} Tr_{11} & Tr_{12} & Tr_1, n-1 \\ Tr_{21} & Tr_{22} & Tr_2, n-1 \\ \cdots & \cdots & \cdots \\ Tr_{n-1} & Tr_{n-1,2} & Tr_{n-1,n-1} \end{bmatrix} \tag{2}$$

For the evaluation of indirect trust in CH-CM, we considered the neighboring trusted node and average trusted nodes. Hence, the trust value of the recommendation of a given by CH is,

$$Tr^{indir}_{MN,a}(\delta_t) = \frac{\sum_{i \varepsilon m} \sqrt{Tr_{i,a} \times ave_{j \varepsilon n}(Tr_{j,i})}}{|m|} \tag{3}$$

where, m denotes the set of all trusted neighbors of node a , and n denotes the set of neighbor nodes of each trusted node set m.

3.2.3 Inter Cluster trust evaluation in CH-CH Direct Trust Calculation

The inter cluster evaluation contain two data sources: CH-to-CH direct trust and BS-to-CH indirect recommended trust. As per the qualities of bunched WSNs, the two CMs and CHs become resource-constrained nodes, and BSs have expanded figuring and storage capacity limit with no asset constrained nodes. Energy preservation in this remains stays a fundamental requirement for trust evaluation at CHs. Each CH record their past interactions with other nearest CHs for direct trust evaluation of CH to CH and the trust value is evaluated in the same way as the direct trust evaluation of CM to another CMs. Whenever there is at any one interaction between the (CH_i) and (CH_j) within the time stamp (δ_t), the direct trust of two CH will calculated by using the below equation.

$$Tr_{CH_i, CH_j}^{indir}(\delta_t) = \left[\begin{array}{c} \left(\frac{\zeta_{ij}^{c1}(\delta_t) + \zeta_{ij}^{c2}(\delta_t)}{\zeta_{ij}^{c1}(\delta_t) + \zeta_{ij}^{c2}(\delta_t) + \vartheta_{ij}^{c1}(\delta_t) + \upsilon_{ij}^{c2}(\delta_t)} \right) \times \\ \left(\frac{P_1 * \zeta_{ij}^{c1}(\delta_t) + P_2 * \zeta_{ij}^{c2}(\delta_t)}{1 + P_1 * \zeta_{ij}^{c1}(\delta_t) + P_2 * \zeta_{ij}^{c2}(\delta_t) + \zeta_{ij}^{c1}(\delta_t) + \upsilon_{ij}^{c2}(\delta_t)} \right) \times \left(\frac{1}{\sqrt{P_1 * \vartheta_{ij}^{c1}(\delta_t) + P_2 * \zeta_{ij}^{c2}(\delta_t)}} \right) \end{array} \right] \tag{4}$$

3.2.3 Intra Cluster trust evaluation in BS-CH Indirect Trust Calculation

In intra clustering, the indirect trust evaluation of CH is depend on the feedbacks which are received from the BS. During the communication between CH CH, when CH want to interact with neighbour CH, it sends a feedback request to its BS. Then the response message from the CH, therefore the communication overhead has two packets. In this model may significantly reduce the network communication overhead and consequently develop the system efficiency resource. The request packet to each CHs is periodically multicast from the BS. When the request packet received from the BS, each CH send its trust values to another CHs (direct trust between CHs) to BS. BS also maintains all the collected direct trust values in a matrix 2.

$$Tr_{Bs}^{indir} = \begin{bmatrix} Tr_{CH_1CH_1} & Tr_{CH_1CH_2} & Tr_{CH_1CH_{n-1}} \\ Tr_{CH_2CH_1} & Tr_{CH_1CH_2} & Tr_{CH_1CH_{n-1}} \\ \cdots & \cdots & \cdots \\ Tr_{CH_{n-1}CH_1} & Tr_{CH_{n-1}CH_2} & Tr_{CH_{n-1}CH_{n-1}} \end{bmatrix} \tag{5}$$

3.3 Selection of transmission link

A secure path is selected based on the Total Trust (TT), Density, Residual energy, and Distance. To calculate the Final Trust Value (FTV) of CH node. The five parameters taken into consideration as input to the fuzzy logic system are REV, PIV, DV, CdV and DiV. Based on this five parameters the FTV of the node is calculated and the following timeout value to change the malicious CH node are assigned. The merits of the proposed trust mechanism creates a Final Trust Table (FTT) in form of four characteristics such as Trust value, Trust Timeout, Trust type and Node ID. If any one of the trust value of the node gets expired or

Table II: Fuzzy Membership with Trust values

S.No	Fuzzy Membership levels	Trust values for each fuzzy levels	Semantics
1	Very Large (VL)	0.8-1	Trust
2	Large(L)	0.6-0.8	Trust
3	Medium(M)	0.4-0.6	Trust
4	Small(S)	0.2-0.4	Untrust
5	Very small(SM)	0-0.2	Untrust

malicious, the CH request the proposed trust mechanism to compute new trust value. Each of the CH nodes maintains the FTT and update the table as per the requirement of trust value. In Equation (1), the calculation of the FTV are given as follows

$$FTV = REV + PIV + DV + CdV + DiV \tag{6}$$

3.3.1 CH Selection by Multi-Level Fuzzy Clusterin

In CH selection, nodes with Maximum trust value is selected to adequately perform a data exchange between the next nodes. The CH nodes perform an evaluation among Requester Node (RN) trust value to the trust value on FTT. Based on the issued trust values, two terms of operation are performed. The trusted nodes are consider for secure data transmission and nodes with malicious attacks are removed from the WSN. The Trust are issued as per the node within a timeout value. Once the timeout value is exceed a new CH is renewed by replacing the untrusted node. Therefore, any nodes with a highest trust value are been selected as cluster head in WSN.

3.3.2 Multi-Level Fuzzy Clustering Analyzer for Secure Transmission and Malicious Detection

Representing of trust value by Fuzzy logic handle the uncertainty and imprecision behavior on nodes to provide reliability and scalability performance. The fuzzy logic for trust evaluation is performed to calculate the trust values of the nodes under computation based on REV, PIV, DV, CdV and DiV to produce FTV. These five input are treated as input fuzzy variables and following rules are generated to mark the nodes as to be either malicious node or trusted node. This process will be performed at the time of RN request the CH node to exchange the data information or packets. Table 2, clearly represent the fuzzy discrimination used for trust evaluation.

(i) **Fuzzy rules for Trust and Malicious Node Determination** For classifying the trust levels on nodes, a fuzzy inference rules are used. The following fuzzy rules are mentioned as follows. 1. IF the trust value is Very Large : THEN node is Trusted 2. IF the trust value is Large : THEN node is Trusted 3. IF the trust value is Medium : THEN node is Trusted 4. IF the trust value is Small : THEN node is Malicious 5. IF the trust value is Very Small : THEN node is Malicious

Figure 4, shows the input and output of proposed method. If the RN request CH node to perform data exchange. The trust based fuzzy analyzer first verifies the RN trust value and look performance over fuzzy table for the FTV. The performance of the fuzzy analyzer works under the complete control of CH node. If the CH node define a RN as malicious an alert message is been generated to define the malicious node to all the trusted nodes being in its range. This makes the network more secure on detecting and removing the malicious node and prevent from various attacks of performing any illegal activity in its range. The proposed scheme is said to be secure of incorporating trust values and Fuzzy analyzer for CH selection. For secure transmission, the fuzzy rules as in the membership name of VL, L, and M for Trusted node and malicious node as S and VS.

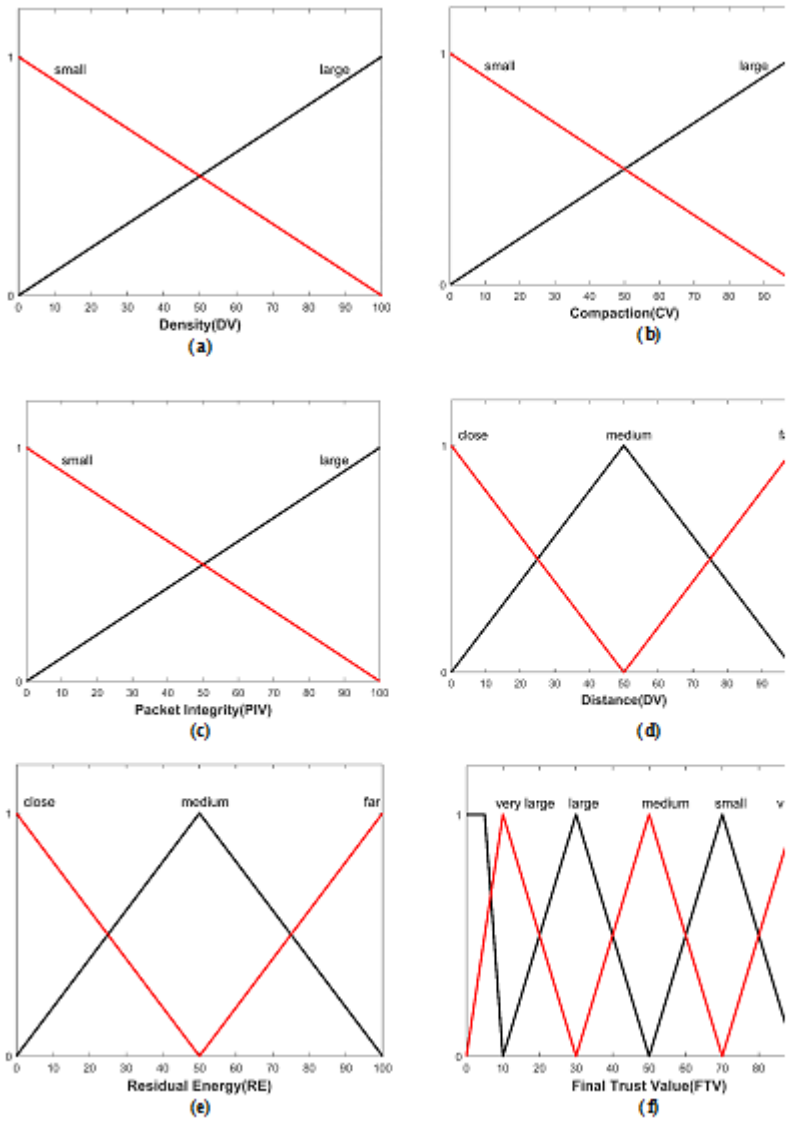

Figure 4. (a-f): Input and output of fuzzy

4. SIMULATION ANALYSIS AND RESULTS

In simulation, the performance of the proposed system is implemented and analyzed in MATLAB. The detection of the malicious nodes and trust node are defined based on the computed trust values. Malicious nodes can be of Denial of Service (DoS) attack, Bad-mouthing attack, on-off attack, collusion attack, Sybil attack and replication attack. The following evaluation metrics used to evaluate the trust of each node in WSN are detection accuracy and energy consumption. The experimental simulation are based on this parameters and the nodes are marked as Malicious and trusted according to the threshold value. The parameter taken into consideration are given in Table 3.

(i) **DoS attack:** The malicious node forwards many information to waste huge amount of resources in the environment. This attack can be handled by keep tracking the residual energy of node and comparing with others energy in the network.

Table III: Parameter Setting

Parameter	Value
Filed Size	500*500m^2
Node Department	Random
Simulation time	500ms
Traffic type	UDP
Packet Size	128bytes
Physical Standard	IEEE 802.15.4
Traffic loard	CBR
No of sensor Nodes	100
Type of nodes	Normal node N, Malicious Node M
Communication speed (kbps)	250
Detection time interval	60s
Transmission power	1mW
Communication Distance	40m
Message Interval	5s
Initial energy	1000J
Energy threshold	400J

(ii) **Bad-mouthing:**The malicious node spread wrong recommendation about neighbors in the network. This attack can be addressed by getting multiple recommendations from the nodes or having a direct transaction with target node instead of going for recommendation trust. 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.

(iii) **On-off or selective forwarding attack:** The malicious node behave well for some time and suddenly start to act abnormal in the network. This can be addressed by using trust decay factor where the trust score made long ago carries less weight than late trust scores. The use of dynamic sliding window also useful in detecting and overcoming this attack.

(iv) **Collusion attack:** Two or more malicious nodes are work together to give wrong recommendation about nodes in the network. This attack is known to be most destructive attack than above said attacks. This can be handled by having direct observation of each and every nodes in the network

(v) **Sybil Attack:** The malicious nodes can produce many false ID and tries to imitate as different nodes at different time in the network. This can be addressed by identification of ID by powerful node like base station or centralized server in the network.

(vi) **Replication Attack:** If an enemy seize a node and pull out its credentials, it is possible for an enemy to produce many number of replicas with same identity and deploy at different locations. This is called replication attack. Like Sybil attack, this also can be handled by base station.

Figure 5, illustrate the impact of malicious node on trust calculation. It is demonstrated from figure that our proposed trust calculation conspire lies underneath LDTS (Das, R et al 2017), GATE (Das, R et al 2017), and GTMS (Das, R et al 2017). The calculation trust esteems are a lot stricter than related plans in light of the fact that HTMS considers the credit point dissemination and penalty policies. Figure 6, illustrate the comparison of network lifetime using the proposed method with four existing methods. The data for certain specific number of rounds was extracted when some of the nodes died, and the percentage of the node death after each interval was plotted to visualize the performance comparison of the four algorithms more intuitively. This analysis of the dead no.de is compared with FML, SPFL and ESRAD methods (Razzaq, M., and Shin, S. 2019) Figure 7 illustrate the comparison of network energy consumption as for increasing number of nodes in the WSN. It very well may be seen from the graph that when network size is increased from 100 nodes to 500 nodes, the differents between the measures of energy consumption for FML (Razzaq, M., and Shin, S. 2019)., SPFL (Razzaq, M., and Shin, S. 2019)., ESRAD (Razzaq, M.,

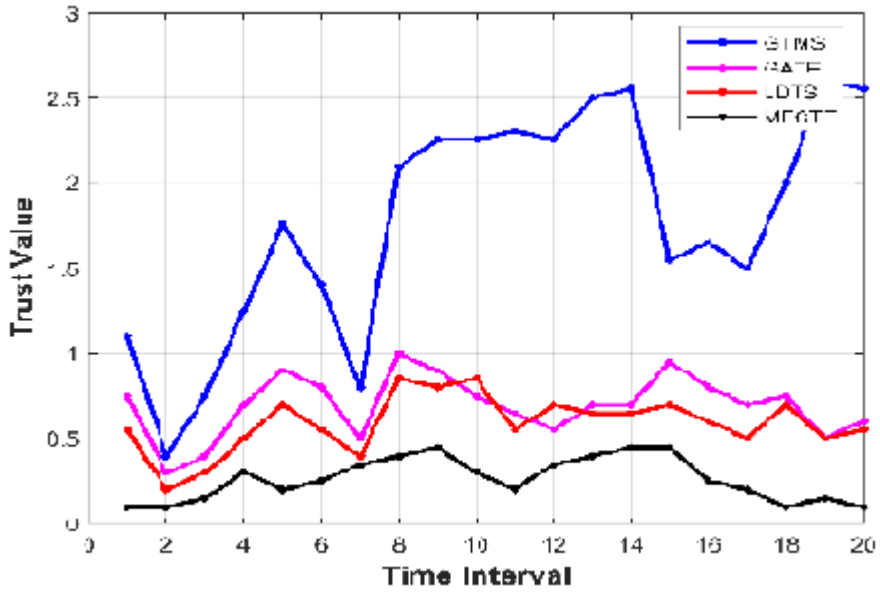

Figure 5. Effect of malicious node on the trust evaluation in MFCTE and other existing schemes

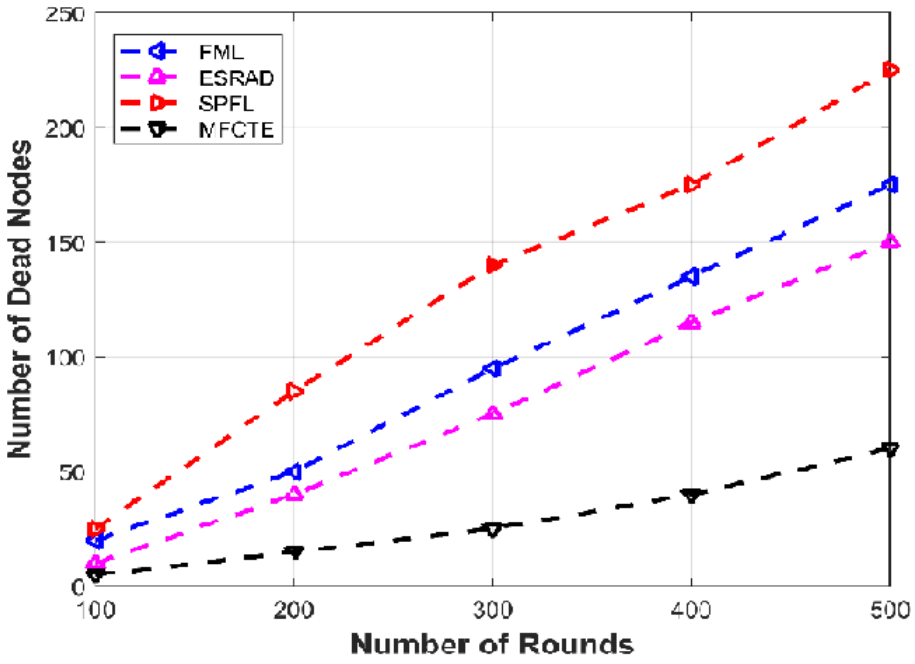

Figure 6.Evaluation of dead nodes with respect to number of rounds

and Shin, S. 2019) and proposed MFCTE is about 0.001 J though SPFL shows vitality utilization of 0.1 J which is 1 parentage of nodes absolute initial energy. In this result, we can see that the proposed method can provide best performance owing to the inclusion of residual energy and intra-cluster communication cost in the weight function while selecting the next node for data transmission. Figure 8, shows the results of detection accuracy of proposed MFCTE with existing SLT-POR (Rajesh, A et al 2016) and CAST (Rajesh, A et al 2016) methods. The detection

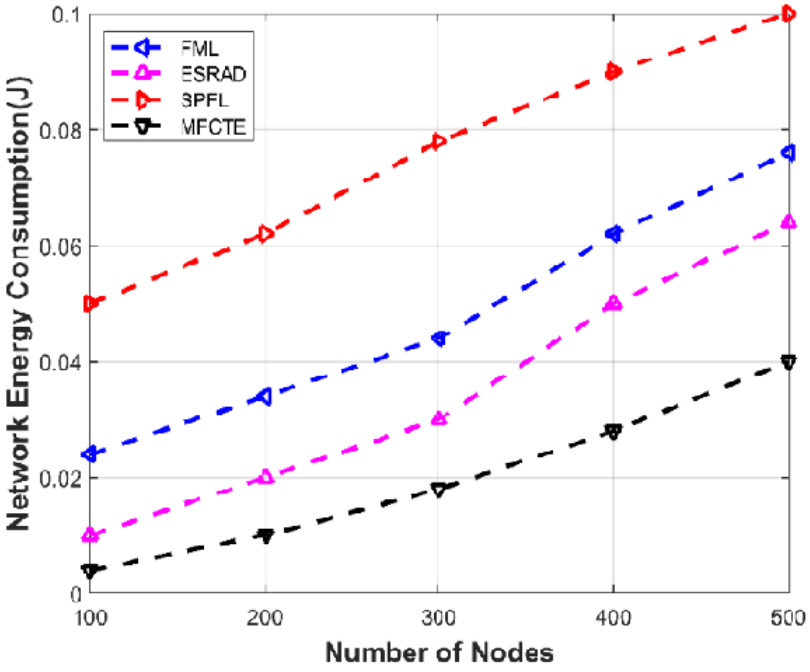

Figure 7. Network energy consumption of network nodes

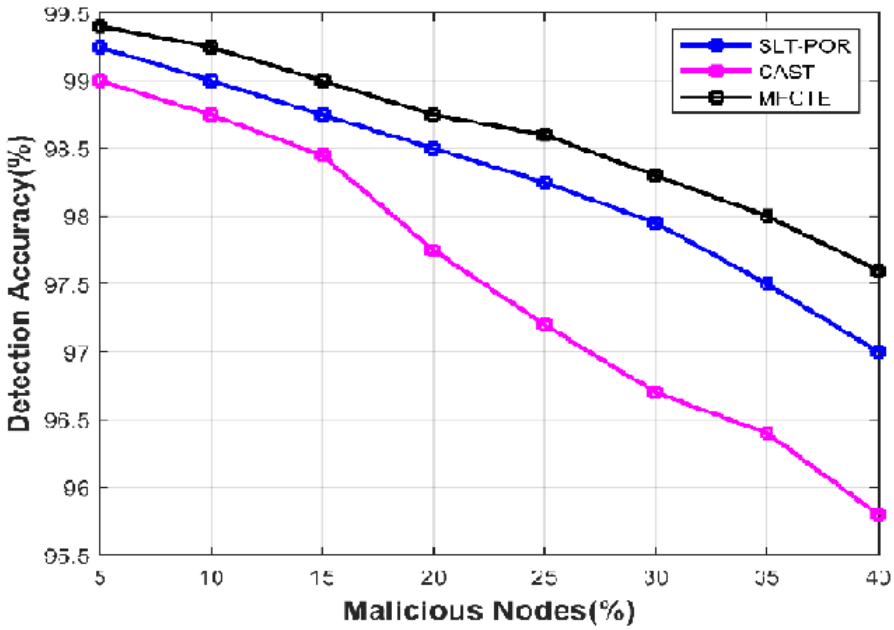

Figure 8. Analysis of Malicious node and Detection accuracy

accuracy the proposed model is higher than the SLT-POR and CAST as it accurately evaluates the trustworthiness of a node by exploiting subjective logic evidence fusion. In this analysis the detection accuracy of MFCTE is 98.7 percentage and the SLT-POR is 97.05 percentage and CAST is 95.8 percentage respectively when the percentage of malicious nodes is 40.

5. CONCLUSION

The selection of trust-based CH and detecting malicious nodes in HWSN is a promising approach. Hence, the MFCTE model for WSN based on minimum separation Distance enforcement between CHs is proposed which defects against malicious nodes. Here, the fuzzy-based decision logic is used for finding the behavioral changes of cluster nodes to distinguish the malicious node and trust node from a set of deployed nodes. The simulation results show the proposed method helps to take decision more accurately than the other applicable approaches used in WSN. Finally, our approach decreases in becoming a malicious node as a cluster head.

References

ANWAR, R. W., ZAINAL, A., OUTAY, F., YASAR, A., IQBAL, S. (2019). BTEM: Belief based trust evaluation mechanism for Wireless Sensor Networks. Future Generation Computer Systems, 96, 605-616.

CHENG, X., LUO, Y., GUI, Q. (2018, October). Research on trust management model of wireless sensor networks. In 2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC) (pp. 1397-1400). IEEE.

DAS, R., DASH, D., AND SARKAR, M. K. (2020). HTMS: Fuzzy Based Hierarchical Trust Management Scheme in WSN. Wireless Personal Communications, 1-34.

Desai, S. S., Nene, M. J. (2019). Node-level trust evaluation in wireless sensor networks. IEEE Transactions on Information Forensics and Security, 14(8), 2139-2152.

DHAKNE, A. R., CHATUR, P. N. (2015, November). Distributed trust based intrusion detection approach in wireless sensor network. In 2015 Communication, Control and Intelligent Systems (CCIS) (pp. 96-101). IEEE.

FANG, W., ZHANG, C., SHI, Z., ZHAO, Q., AND SHAN, L. (2016). BTRES: Beta-based Trust and Reputation Evaluation System for wireless sensor networks. Journal of Network and Computer Applications, 59, 88-94.

GOMATHY, V., PADHY, N., SAMANTA, D., SIVARAM, M., JAIN, V., AND AMIRI, I. S. (2020). Malicious node detection using heterogeneous cluster based secure routing protocol (HCBS) in wireless adhoc sensor networks. Journal of Ambient Intelligence and Humanized Computing, 1-7.

HAN, G., JIANG, J., SHU, L., NIU, J., AND CHAO, H. C. (2014). Management and applications of trust in Wireless Sensor Networks: A survey. Journal of Computer and System Sciences, 80(3), 602-617.

HE, J., AND XIONG, N. (2018). An effective information detection method for social big data. Multimedia Tools and Applications, vol.77, no. 9, pp.11277-11305.

ISHMANOV, F., MALIK, A. S., KIM, S. W., AND BEGALOV, B. (2015). Trust management system in wireless sensor networks: design considerations and research challenges. Transactions on Emerging Telecommunications Technologies, 26(2), 107-130.

JAINT, B., SINGH, V., TANWAR, L. K., INDU, S., PANDEY, N. (2018, October). An Efficient Weighted Trust Method for Malicious Node Detection in Clustered Wireless Sensor Networks. In 2018 2nd IEEE International Conference on Power Electronics, Intelligent Control and Energy Systems (ICPEICES) (pp. 1183-1187). IEEE.

JIN, X., LIANG, J., TONG, W., LU, L., LI, Z. (2017). Multi-agent trust-based intrusion detection scheme for wireless sensor networks. Computers and Electrical Engineering, 59, 262-273.

KARTHIK, N., ANANTHANARAYANA, V. S. (2017). A hybrid trust management scheme for wireless sensor networks. Wireless Personal Communications, 97(4), 5137-5170.

KHAN, T., SINGH, K., ABDEL-BASSET, M., LONG, H. V., SINGH, S. P., MANJUL, M. (2019). A novel and comprehensive trust estimation clustering based approach for large scale wireless sensor networks. IEEE Access, 7, 58221-58240.

KULKARNI, S. B., YUVARAJU, B. N. (2017, January). Challenge evaluation algorithm to

identify malicious node in MANET. In 2017 IEEE 7th International Advance Computing Conference (IACC) (pp. 297-302). IEEE.

LABRAOUI, N. (2015, April). A reliable trust management scheme in wireless sensor networks. In 2015 12th International Symposium on Programming and Systems (ISPS) (pp. 1-6). IEEE. LIU, L., MA, Z., MENG, W. (2019). Detection of multiple-mix-attack malicious nodes using perceptron-based trust in IoT networks. Future Generation Computer Systems, 101, 865-879.

LIU, X., LIU, Y., LIU, A., AND YANG, L. T. (2018). Defending ONOFF attacks using light probing messages in smart sensors for industrial communication systems. IEEE Transactions on Industrial Informatics, 14(9), 3801-3811.

Ma, Z., Liu, L., Meng, W. (2020, November). DCONST: Detection of Multiple-Mix-Attack Malicious Nodes Using Consensus-Based Trust in IoT Networks. In Australasian Conference on Information Security and Privacy (pp. 247-267). Springer, Cham. MANORANJINI, J., CHANDRASEKAR, A., JOTHI, S. (2019). Improved QoS and avoidance of black hole attacks in MANET using trust detection framework. Automatika, 60(3), 274-284.

PRABHA, V. R., AND LATHA, P. (2017). Enhanced multi-attribute trust protocol for malicious node detection in wireless sensor networks. Sdhan, 42(2), 143-151.

PRABHA, V. R., AND LATHA, P. (2017). Fuzzy trust protocol for malicious node detection in wireless sensor networks. Wireless Personal Communications, 94(4), 2549-2559.

QIN, D., YANG, S., JIA, S., ZHANG, Y., MA, J., DING, Q. (2017). Research on trust sensing based secure routing mechanism for wireless sensor network. IEEE Access, 5, 9599-9609.

QIU, T., LIU, X., FENG, L., ZHOU, Y., AND ZHENG, K. (2016). An efficient tree-based self-organiz ing protocol for internet of things. Ieee Access, Vol.4, pp.3535-3546.

RAJESH, A., RAJI, V., KUMAR, N. M. (2016). Subjective logic based trust model for geographic routing in mobile ad hoc networks. Tehniki vjesnik, 23(5), 1357-1364

RAZZAQ, M., SHIN, S. (2019). Fuzzy-logic dijkstra-based energy-efficient algorithm for data transmission in WSNs. Sensors, 19(5), 1040.

REHMAN, E., SHER, M., NAQVI, S. H. A., BADAR KHAN, K., ULLAH, K. (2017). Energy efficient secure trust based clustering algorithm for mobile wireless sensor network. Journal of Computer Networks and Communications, 2017.

SINGH, O., SINGH, J., SINGH, R. (2018). Multi-level trust based intelligence intrusion detection system to detect the malicious nodes using elliptic curve cryptography in MANET. Cluster Computing, 21(1), 51-63.

TALBI, S., KOUDIL, M., BOUABDALLAH, A., AND BENATCHBA, K. (2017). Adaptive and dual data-communication trust scheme for clustered wireless sensor networks. Telecommunication Systems, 65(4), 605-619.

WU, X., HUANG, J., LING, J., SHU, L. (2019). BLTM: beta and LQI based trust model for wireless sensor networks. IEEE Access, 7, 43679-43690.

YANG, H., ZHANG, X., AND CHENG, F. (2020). A Novel Algorithm for Improving Malicious Node Detection Effect in Wireless Sensor Networks. Mobile Networks and Applications, 1-10.

Zawaideh, F., and Salamah, M. (2019). An efficient weighted trustbased malicious node detection scheme for wireless sensor networks. International Journal of Communication Systems, 32(3), e3878.

Zawaideh, F., Salamah, M., and Al-Bahadili, H. (2017, December). A fair trust-based malicious node detection and isolation scheme for WSNs. In 2017 2nd International Conference on the Applications of Information Technology in Developing Renewable Energy Processes Systems (IT-DREPS) (pp. 1-6). IEEE.

ZHANG, T., YAN, L., AND YANG, Y. (2018). Trust evaluation method for clustered wireless sensor networks based on cloud model. Wireless Networks, 24(3), 777-797.

ZHAO, J., HUANG, J., XIONG, N. (2019). An effective exponential-based trust and reputation

evaluation system in wireless sensor networks. IEEE Access, 7, 33859-33869..

Mr.Rahul Das is a Research Scholar in Computer Science Department, Mansarovar Global University. Billkisganj, Sehore, Madhya Pradesh-466001.He is currently working as a teacher in the Department of Computer Science, Raja Narendralal Khan Womens college, Paschim Medinipur, West Bengal. He has received BCA degree in 2005 and Masters (MCA) under Vidyasagar University,2009 and B. Ed degree. He has 10 Years of teaching Experience in College. His research interest Security in Wireless Sensor Network.

Dr. Mona Dwivedi is currently working as an Assistant Professor in the Department of Computer Science at Mansarovar Global University, Billkisganj, Sehore, Madhya Pradesh, India. She received her M.Sc. and M.Phil. degree from Barkatullah University, Bhopal, M.P., India. Dr Dwivedi received her Ph.D. degree from Maulana Azad National Institute of Technology, Bhopal, India. Her research interest includes Green Computing, High Per-formance Computing, Wireless Sensor Networks, Numerical Analysis and Computational Modeling.