www.czasopisma.pan.pl PAN www.journals.pan.pl

jet INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2022, VOL. 68, NO. 1, PP. 5-12
Manuscript received January 14, 2022; revised January, 2022. DOI: 10.24425/ijet.2022.139841

Light Weight Clustered Trust Sensing Mechanism for Internet of Things Network

Rajendra Prasad M, and Krishna Reddy D

***Abstract*—Internet of Things (IoT) is the new research paradigm which has gained a great significance due to its widespread applicability in diverse fields. Due to the open nature of communication and control, the IoT network is more susceptible to several security threats. Hence the IoT network requires a trust aware mechanism which can identify and isolate the malicious nodes. Trust Sensing has been playing a significant role in dealing with security issue in IoT. A novel a Light Weight Clustered Trust Sensing (LWCTS) model is developed which ensures a secured and qualitative data transmission in the IoT network. Simulation experiments are conducted over the proposed model and the performance is compared with existing models. The obtained results prove the effectiveness when compared with existing approaches.**

***Keywords*—internet of things; trust sensing; clustering; mobility; packet forwarding factor; malicious detection rate packet delivery ratio**

I. Introduction

RECENTLY, the internet-based communication and control has gained a great significance due to its flexibility and availability. Based on this strategy of control and communication, a new paradigm called Internet of Things (IoT) has been evolved and it has penetrated its widespread applicability in different applications like Agricultural production, industrial manufacturing, climate control, medical care etc [1]. According to the general structure of IoT network, the IoT is able to connect any device with the help of different devices like infrared sensors, code recognition devices, Radio Frequency Identification Devices (RFIDs),Global Positioning Systems (GPSs), and laser scanners [2,3]. However, with an increased flexibility of allowing different devices to connect to the network, they can exchange information which do not have any security which is the major concern [4]. Since the information being exchanges between the IoT devices is carried out in an open environment, it can be said that it is at great risk of being manipulated or stolen. Hence our major focus is kept on the provision of security in IoT [5]. Since the IoT is an infrastructure less networks, for a long distance communication, the IoT nodes seeks the help of other nodes for an effective communication and information transfer. Due to this co-operative nature, the IoT network come across with many inherent constraints such as fully distributed architecture, continuously varying topology, makes these networks vulnerable to different attacks by misbehaving nodes. Any node compromised with any of the attack, it misbehaves like not co-operating to the data transmission to save the resources, dropping the packets intentionally, propagating false information into the network, manipulating the packets received from other nodes etc. To distinguish and to isolate such type of nodes, many benchmark algorithms were developed earlier [6]. Among the available different kind of security provision strategies, Trust Sensing (TS) is one of the effective strategy[7]. In the TS concept, the source node which have information, preliminarily does some sort of operations to measure the trustworthiness of the nodes through which it was willing to forward the data or signal to destination or another IoT controlled devices. In this paper, new method called as Light Weight Clustered Trust Sensing Mechanism for IoT (LWCTS_IoT) is proposed for the provision of secure and qualitative data transmission in IoT network. The trustworthiness of every IoT node is linked with mobility where the trust evaluating node will get clarity about the evaluated node's trustworthiness.

II. Literature Review

Various trust sensing schemes were developed earlier to ensure the trust based routing in IoT network. In the trust evaluation process, the parameter considered to define the trustworthiness of a node plays a vital role in the security provision. If these parameters are more in number, then the node selected is said to be more trustworthy and also robust. Considering this multi parameter strategy, Chen et al. [8] proposed a new trust and reputation model TRM-IoT based on fuzzy reputation and the parameters considered for trust evaluation are packet delivery ratio (PDR), energy consumption, and end-to-end packet forwarding ratio. However, this method did not focus over the resource constraints. Focusing over only trust and reputation reduces the network lifetime. As only few nodes are more trustworthy in the network, considering every time them only results in the node death followed by the reduced network lifetime. Further, a new method proposed by Bao and Chen [9] considered the community-interest, co-cooperativeness and honesty for trust evaluation. In the same year, a new strategy called, "Social Internet of Things (SIoT)" was proposed by Atzori et al. [10] in which the trust evaluation is developed based on the social network aspects. Further, Nitti et al. [11] developed two trust models, Objective evaluation model and subjective evaluation model for trust management. Here the trust value of every node is measured based on the social behavior of a node towards its neighbor nodes. The trust is measured in an indirect way, i.e., the opinion of neighbor nodes decides the trustworthiness of every node. Similar to this method, a new technique was proposed by Kogias et al. [12] which provides a Trust and Reputation Model for IoT (TRMS-IoT). It combines the Peer-to-Peer and MANETs adapting then on IoT protocols and according to this method each thing can compute the trustworthiness of anything in the network based

Rajendra Prasad M is with Vidya Jyothi Institute of Technology, India (email: rajendraresearch@gmail.com).

Krishna Reddy D is with Chaitanya Bharathi Institute of Technology, India (email: dkreddy@cbit.ac.in).

on its own experience of referring to its friends or the platform. Next, the method proposed by Bernabe et al. [13] provides a flexible access control system for trust management in IoT network, called TAC-IoT. Gai et al. [14] proposed multi-dimensional trust evaluation model for anomaly detection in IoT. This trust model considered the multi-dimensional trust elements such as Social Relationship, Quality of Service and Reputation. However, all these methods did not focus over the energy reservation which is most important in the resource constraint IoT network. Though some approaches considered the energy consumption as a parameter during the trust evaluation, it has not a sufficient impact over the energy preservation. Further due to the consideration of energy consumption, the node will know only the amount of energy consumed but would not preserve energy. To do this, some approaches are proposed by assigning the maximum responsibility of communication and trust evaluation to only few nodes which are rich is resources, called as "Cluster based Trust Management in IoT' [15]. Recently, a Fuzzy C-Means Clustering based cluster head selection was accomplished to cluster the nodes in IoT by P. K. Reddy and R. S. Babu [16]. An optimal Secure and 'Energy Aware Protocol (OSEAP)' and an 'Improved Bacterial Foraging Optimization (IBFO)' [17] algorithm were accomplished here. However, the FCM algorithm will not suit for clustering of nodes. Because, in the FCM, the nodes are clustered based on their significance but in actual the nodes needs to be clustered with respect to their distance from other nodes. Furthermore, the IBFO results in an extra computational burden over the route establishment process when the source node wants to send information to destination nodes. There is no discussion about the node selection strategy, i.e., there is no mechanism which measures the trust degree of nodes. In [18], a self-organized cluster based energy efficient trust management scheme is proposed through which the authors tried to achieve an energy preservative secure communication between nodes in IoT. In this paper, the trust model is derived based on the time identity to punish the malicious nodes. This method cluster the nodes based on their energy requirements and the trust model considers the PDR only as a reference metric, which is not sufficient. Recently, a 'Clustering-Driven Intelligent Trust Management Methodology for the Internet of Things (CITM-IoT)' is proposed by Alshehri et al. [19] which addresses the scalability and provides a solution for countering the bad mouthing attacks. This approach considered the memory as a reference resource to evaluate the trustworthiness of a node. Further, a clustering strategy is also developed in which the entire node set is categorized as Super Nodes (SNs), Master Nodes (MNs) and Cluster Nodes (CNs). But, this approach did not discuss about the energy preservation and also accomplished as cooperative communication between the cluster nodes by which the energy consumption will increase greatly. Recently, G. Sowmya and N. Venkatram proposed a Multi-Context Trust Aware Routing (MCTAR) for IoT [20]. This is a secure and composite routing which considered multiple factors for trust evaluation. MCTAR considered the communication trust and energy trust to detect and identify the malicious nodes.

III. PROPOSED APPROACH - LIGHT WEIGHT CLUSTERED TRUST SENSING (LWCTS)

A. *Overview*

In this paper a new trust sensing mechanism called as Light Weight Clustered Trust Sensing Mechanism for IoT (LWCTS_IoT) is proposed. Initially, the proposed model employs clustering mechanism to group up the nodes in IoT. The clustering is accomplished by the computation of Euclidean distances between IoT nodes. Among the clustered nodes one node is selected as Cluster Head (CH) which has an availability of huge resources. Further, the trust sensing is explained through which the CH senses the trustworthiness of other CHs for forwarding the data to destination. In IoT the destination lies very far away from the source. Hence even the CH needs additional nodes to forward the data to destination. For this purpose, the CH senses the trustworthiness of other CHs and selects one CH for forwarding the data.

B. *Clustering of IoT Nodes*

In IoT network, the nodes have limited energy, bandwidth, memory and processing capabilities. Hence if the entire nodes are engaged to execute the tasks, then they will show a huge impact on the network lifetime. Moreover the IoT nodes process data which are of larger in size, the additional processing tasks make the nodes to die quickly. Hence to reduce this additional burden, the IoT nodes are clustered into groups and the major processing task is assigned to the CH. To execute the major processing task the CH must have greater resources. Hence CH is selected based on the energy means among the cluster nodes the node which are rich in resources are selected as CH's. Here the normal nodes (cluster nodes) execute the simple task data transfer while the CH executes the data collection from multiple IoT nodes and forwards for further CH or destination. The IoT node is only responsible to send their data after sensing. Once the data from each cluster node are received at CH, then it finds and forwards the received data to destination or next CH (if destination lies far from the CH, then it seek the help of other CHs). The CH only sends the data to destination in multiple hops if required otherwise it will send directly if it lies within the communication range of destination. Consider an IoT network with N number of nodes connected and let it be $n_1, n_2, n_3, \ldots, n_N$, the clustering is implemented based on the following expression;

$$Ed(n_i, n_j) = \sqrt{(x_j - x_i)^2 + (y_j - y_i)^2} \quad (1)$$

Where $d(n_i, n_j)$ is Euclidean distance between node n_i and n_j. (x_i, y_i) is the location coordinates of n_i, (x_j, y_j) is the location of coordinates of node n_j.In this manner the Euclidian distance is measured from every node to every node and it constructed a distance matrix as follows

$$\mathrm{Ed} = \begin{bmatrix} \mathrm{Ed}_{11} & \mathrm{Ed}_{12} & \cdots & \mathrm{dE}_{1N} \\ \mathrm{Ed}_{21} & \mathrm{Ed}_{12} & \cdots & \mathrm{Ed}_{1N} \\ \vdots & \vdots & \cdots & \vdots \\ \mathrm{Ed}_{N1} & \mathrm{Ed}_{N2} & \cdots & \mathrm{Ed}_{NN} \end{bmatrix} \quad (2)$$

Where Ed_{ij} is the Euclidian distance two nodes n_i and n_j, where i and j varies from1 to N. After the construction of distance matrix then compute the neighbor nodes for every node based on the following expression;

$$\mathrm{Nd}_i = \mathrm{find}\left(\mathrm{d}_{ij} \le \mathrm{C}_i(\mathrm{n}_i)\right) \quad (3)$$

Where $C_i(n_i)$ is the communication range of node n_i and Nd_i is the neighbor nodes of node n_i whose distance with node n_i is less than the communication range R_i of node n_i. Once the neighbor nodes are measured for every node, one node is selected as CH which has huge resources availability. At this situation it can be concentrated on the selection of non-common nodes as CH's. Since there is a chance of a single node getting selected as CH for multiple clusters, to mitigate this problem. If it is observed a common CH for two groups then they are merged and formulated into a single cluster with only one CH selected which has higher resource availability.

C. *Trust Sensing*

LWCTS-IoT considers two simple factors for trust sensing; they are Interaction Trust (IT) factor and Nobleness Trust (NT) factor. Again the IT is evaluated in two phases; Forward Interaction Trust (FIT) and Recommended Interaction Trust (RIT). Next, the Nobleness trust is measured based on the packets forwarded by next hop neighbor node. Finally, a composite factor called as Trust Sensing Factor (TSF) is computed by combining these two factors. Further, it can be included the mobility factor to alleviate the effect of mobility in the IoT. For a node in IoT network which needs to transmit its information, it determines a best path towards the node to which the information has to transmit, through most trustworthy nodes those can ensure reduced energy consumption and secure data transmission. Initially, the source node forwards the data to its respective cluster head followed by destination. During this process, the CH finds an optimal path to the destination by the computation of TSF for very next hop cluster head.

D. *Interactive Trust*

The computation of interactive trust is implemented according to the past communication interactions those were among the nodes in network. Here considered all possible communication interactions like the interactions during the packet transmission, packet receptions, control packets transmission and control packets receptions etc. For a given node pair, the greater rate of interactive trust indicates a good trust and smaller value of interactive trust signifies lesser trust. However, as this interaction between nodes increases, it also has a drawback which resemblances the Denial of Service (DoS) attack. In the case of DoS attack, the attacker tries to deplete the resources of compromised nodes by sending the packets continuously. Continuous transmission of packets results in larger number of interactions and at this condition, the node which was trying the trustworthiness of another node may misunderstand that the receptive node is trustworthy due to the presence of larger IT. Hence it is defined as a interactions threshold means for a given node pair, if they have interaction within the threshold range, then only it is considered as trustworthy otherwise malicious and can be declared it as malicious. The IT is measured in two phases; Forward Interaction Trust and Recommended Interaction Trust.

E. *Forward Interaction Trust (FIT)*

In IoT, the nodes behavior is supervised through the nodes those lie in its communication range or simply called as neighbor nodes. FIT is an observation regarding the nature of packet forwarding nature of nodes in network. A simple and light weight trust computation is proposed here for the calculation of FIT. Consider p and q be the IoT nodes, the FIT between them is computed as

$$FIT_p^q = \alpha \times FIT_{P(b)}(p,q) + \beta \times FIT_{N(b)}(p,q) \quad (4)$$

Where $\mathrm{FIT}_{\mathrm{P(b)}}(\mathrm{p},\mathrm{q})$ is the forward interaction trust of node q for node p with respect to the positive attitude of q observed from the earlier communication interactions; $\mathrm{FIT}_{\mathrm{N(b)}}(\mathrm{p},\mathrm{q})$ is the forward interaction trust of node q for node p with respect to the negative attitude of node q observed from the earlier communication interactions.

Here P(b)signifies the positive attitude of nodes or it also denotes the good attitude, i.e., for any interaction request kept by any node in the network, if q was answered within the given instance of time period, then it is treated as positive attitude of node q. At this situation, the request may be a RREQ for route discovery or data packet for further forwarding. For any kind of request, the node needs to give a positive response and then only it will get added to its positive behavior. For a data packet sent from node p to node q, if the node q didn't responded (either giving acknowledgment or further forwarding to next hop node) within the specific time interval, then its positive behavior will get depreciated. Next, N(b) denotes the negative attitude of node or simple it can be called as bad behavior, means for any communication request put by any node p in the network, if the node q has not replied properly within the instance of time given, then it would be treated as negative attitude [21]. This may happen due to so many reasons and hence for a single instance of negative behavior, cannot conclude that node has become malicious. Hence, the node p keeps on monitoring the node q for particular instances, and then only decides whether it was malicious or not. Next, the two constants (α and β) are used to signify the weightage of positive and negative attitudes of node respectively. At forwarding stage, depending on the of $\mathrm{FIT}(\mathrm{p},\mathrm{q})$ value, the sensed node decides whether the receiving node is trustworthy or not.

In the case of positive and negative behavior calculation process it is considered the response as main reference parameter to judge the attitude of node. At this instant, the packet forwarding factor is considered to assess these two behaviors. For example, if an intermediate node is there at which the packet has been received, it does not work out anything with the packet if it was trustworthy. It checks for the next hop ID and forwards to the respective next hop neighbor node simply. Hence the packet forwarding factor is considered as one more reference parameter for the assessment of trustworthiness of nodes. Mathematically, the expression for packet forwarding factor F^{P} is expressed as

$$F^{P}(t) = \frac{C_{f(0,t-1)}}{T_{f(0,t-1)}} \quad (5)$$

Where $C_{f(0,t-1)}$ is the total number correctly forwarded packets from the starting time o to earlier time instance t-1, and $T_{f(0,t-1)}$ is the total packets count Forwarded actually from node p to q from starting time 0 to earlier time instance t-1. The both values $C_{f(0,t-1)}$ and $T_{f(0,t-1)}$ are the cumulative values from time 0 to t. Here correct forwarding means the forwarder node not only forwarding the packets to its next hop node but also forwarding correctly. At this instant, there is a possibility to introduce the malicious information into the packets by forwarding nodes which makes the packet to reach to malicious parties of some other part of the network. For instance, if a malicious node forwards a packet after tampering with data it is not considered as correct forwarding. If the sender notices this illegal notification, then the $C_{f(0,t-1)}$ value is decreased. Based on these two reference parameters, the forward interaction trust is measured as

$$FIT_{P(b)}(p,q) = F^{P}(t) * P(b) \quad (6)$$

And

$$FIT_{N(b)}(p,q) = F^{P}(t) * N(b) \quad (7)$$

Based on these expressions, the FIT of a node q is measured by node p before every packet transmission. For example, consider the on-off attack which is the common significant attack that occurs in Ad-Hoc networks at which the weight parameters behaves in self-adaptive manner. These two weights are linked to the time with an exponential relation. Depending over the lapses time period, the weights are measured as $\alpha = 1/e^{\sigma_1(t_c-(t_c-1))}$ and $\beta = 1/e^{\sigma_2(t_c-(t_c-1))}$, where t_c is the current time of interaction and $t_c - 1$ is the time instance at which the nodes has communicated previously. Next σ_1 and σ_2 signifythe positive and negative behavior's strength decay in exponential manner respectively, where $t_p > t_p - 1 \geq 0$ and $\sigma_1 > \sigma_2 \geq 0$. From a generalized analysis, it can be understood that with an increase in the time elapsed, the FIT declines. This illustration explore that the current communication interactions incurred between nodes is much significant than the communication interactions incurred between nodes. As the value of time elapsing increase, the two weight parameters follows an inverse relation, i.e., as the α values increase, the β value decrease and vice versa. This denotes that the node has more memory about the bad attitude of other nodes.

F. Recommended Interactive Trust (RIT)

RIT is the trust providing by other nodes those are common neighbors for two communicating nodes. In RIT, for a specific IoT node in the network, the trust is assessed that depends over the beliefs of it's surrounding IoT nodes. The RIT is an accumulated form of opinions obtained from different neighbor nodes of two nodes p and q. Here the p is trust evaluator node and node q is trust evaluated node. For a given two IoT nodes p and q, the RIT is computed as

$$RIT_p^q = FIT_p^r * FIT_r^q \quad (8)$$

Where FIT_p^r is the FIT between node p and node r, and FIT_r^q is the FIT between node r and node q. Here node r is a common neighbor node of p and q which has a direct link with them. Since the node has a direct link with both nodes, it can have its own FIT value with the respective node. Hence, it is formulated the RIT as the product of two FITs for a single common neighbor node. For the presence of more number of common neighbor node, the above expression changes as

$$RIT_p^q = \frac{1}{C}\sum_{c=1}^{C} FIT_p^c * FIT_c^q \quad (9)$$

Where C is total number of common neighbor nodes between the node p and node q. The major advantage of RIT is;

(1) Lower convergence time and speedy process.

(2) Earlier detection and isolation of malicious nodes.

(3) RIT ensures the IoT node that does not prosper in monitoring the nature of their neighbor nodes because of limitation constraints on resource availability.

G. Total Trust

The overall trust is measured by combining the Direct Trust and Recommended Trust. Mathematically the Total Trust is represented by integrating the Forwarding Interactive Trust and Recommended interactive trust as;

$$T_p^q = FIT_p^q + RIT_p^q \quad (10)$$

Where T_p^q is the total trust between two node p and q, FIT_p^q is the forward interactive trust obtained from the direct observations of node p on he behavior of node q, and RIT_p^q is the recommended interactive trust attained by node p from the common neighbor nodes of node q. The total trust computation and the trust node *p* and node *q* is evaluated as;

$$.T_p^q = FIT_p^q + \sum_{c\in s,u,r,t} RIT_{c_p}^{\ q} \quad (11)$$

$$T_p^q = FIT_p^q + \frac{1}{4}(RIT_{s_p}^{\ q} + RIT_{u_p}^{\ q} + RIT_{r_p}^{\ q} + RIT_{t_p}^{\ q}) \quad (12)$$

$$T_p^q = FIT_p^q + \frac{1}{4}\Big((FIT_p^s * FIT_s^q) + (FIT_p^u * FIT_u^q) + (FIT_p^r * FIT_r^q) + (FIT_p^t * FIT_t^q)\Big) \quad (13)$$

H. Mobility Factor

In most of the earlier developed trust models, the trust evaluation is implemented based on forward and recommended trusts only. However most of them neglect that different time periods of interactions have different impact on the trust evaluations. For instance, the packet loss occurred in the previous time interval has high impact on the trust values than that is the earlier intervals [97-98]. The main reason behind this issue is mobility of nodes in IoT. Due to the mobility of nodes, they move away from the nodes which cause to lose the overhearing of nodes retransmission. For a sender node which sent the packet to its next hop nodes, it has to make sure to overhear the retransmission of that packet to its next hop node in promiscuous mode. A successful overhearing only reveals the successful packet delivery to intend destination. If the sender node overhears the packet forwarding from the next hop node, then only it is treated as successful interaction or else it is declared as malicious behavior. In some cases where the sender is not able to overhear the retransmission of its packet even though it happened or a destination node is at the unreachable position due to the wrong information regarding its routing, then the forwarding node is declared as malicious node. Due to this reason, mobility is an important factor which needs to be considered during the trust computation. A node can evaluate

TABLE I
SIMULATION PARAMETERS

Parameter	Value
Number of node	50
Network area	1000*1000 m2
Node deployment	Random
Communication Range (R)	¼ of network area
Traffic type	Constant Bit rate
Packet size	512 bytes
Trust Threshold	0.6
Simulation time	100 seconds
Pause time	5 seconds
Resource Allocation	Random
% of Malicious Behavior	0-50% of total nodes
α, β	$0 \leq \alpha, \beta \leq 1$
Mobility Model	Random way point

the mobility of its neighbor node by measuring the rate of link changes in the neighborhood [21]. Such link change rate is used to examine reasons of packet loss. The rate of link changes at node n_a is mathematically determined as

$$\rho(q) = \alpha(q) + \beta(q) \tag{14}$$

Where ρ(q) is rate of link changes at node q, α(q) is the link arrival rate and β(q) is the link breakage rate experienced by node q [22].Consider α(q)max is maximum link arrival rate β(q)max is the maximum link breakage rate, based on results shown in the link change rate is formulated as

$$\alpha(q)max + \beta(q)max = 2.\sigma(q) \tag{15}$$

Then the rate of link changes can be expressed as

$$\rho = \frac{\alpha(q)+\beta(q)}{2.\sigma(q)} \tag{16}$$

Based on Eq.(12), the probability of successful packet forwarding with respect to rate of link changes is formulated as

$$p(q) = 1 - \rho \tag{17}$$

Based on Eq.(13) we can determine that the higher rate of link changes indicate more dynamic nature and consequence to less probability of successful packet forwarding. Finally node n_a computes the node $q's$ trustworthiness according to the mobility rate of link changed the overall trust is modified as

$$T_p^q = T_p^q * p(q) \tag{18}$$

Here the final T_p^q signifies the trustworthiness of node q with respect to its neighbor node's rate of link changes. The main advantage with the involvement of mobility factor in trust computation are to ensure an accurate identification of malicious nodes. For instance if packet was dropped at node q and node p is not able to overhear its retransmission, then it will check for mobility or ρat node q. Based on the probability of successful packet forwarding linked with ρthe node p decides whether the packet was dropped due to malicious activity or not. If probability of successful packet forwarding is less and ρ is high then the node p declares that node q is not malicious and retransmits the packet to it again.

Here the final T_p^q signifies the trustworthiness of node q with respect to its neighbor node's rate of link changes. The main advantages with the involvement of mobility factor in trust computation is to ensure a an accurate identification of malicious nodes. For instance if packet was dropped at node q and node $p$is not able to overhear its retransmission, then it will check for mobility or rate of link change at node q. Based on the probability of successful packet forwarding linked with rate of link changes the node p decides whether the packet was dropped due to malicious activity or not. If probability of successful packet forwarding is less and rate of link changes is high then the node p declares that node q is not malicious and retransmits the packet to it again.

IV. SIMULATION RESULT

A. Simulation Setup

For simulation purpose, a network is created which has N nodes with heterogeneous characteristics like different memory, energy and processing capabilities. The entire network area is confined in a range of 1000*1000 m2. For the purpose of clustering, it can utilize the concept of Euclidean distance and for this purpose utilized the horizontal and vertical coordinates of nodes are deployed in the network. For every node in the network, it is the fixed communication range as 1/4th of entire network area, means each node can communicate with the other nodes those are in its communication range. The nodes with which the node is able to communicate are called as neighbor nodes. After the completion of clustering, the CH selection is employed based on the availability of resources of clustered nodes. For every cluster one node is chosen as CH which has higher resources availability. At this phase, it can be concentrated on the cluster merging. In this merging, first find the common CH, i.e., if any node is selected as a common CH for more than one cluster, then all those clusters are merged and only one CH is selected as final CH. Due to the random energies of nodes, the prediction of CH is also random in nature and for every simulation, the CH varies. Further for the computation of interactions between nodes, enabled a variable with incrementing and decrementing in nature. For a packet sent from one CH to its next CH, the variable is increased by one if the sent node successfully overhears the packet's further transmission; otherwise, the variable is decremented by one. The packet size is considered as 512 bytes and the simulation time is considered as 100 seconds with a pause time of 5 seconds. At the trust sensing, it can be observed that the values in the range of 0 to 1, hence it has a fixed trust threshold to decide whether the respective node is malicious or not. The details of simulation parameters are shown in Table.I.

B. Results & Discussion

In this section, it can be discussed the details of performance metrics such as Malicious Detection Rate (MDR), False Positive Rate (FPR), False Negative Rate (FNR), Average Energy Consumption (AEC) and Packet Delivery Ratio (PDR). For every performance metric, the proposed method is compared with existing methods such as MCTAR-IOT [20], and CITM-IOT [19].

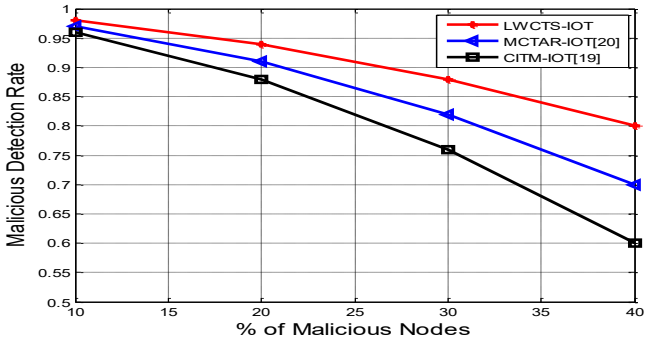

Fig.1. Malicious Detection Rate variations with varying malicious nature

Figure 1 shows the MDR variations with varying malicious nature. As the number of malicious nodes in the network increases, there is a possibility to launch different kinds of attacks on the IoT nodes. Hence the detection becomes complex and results in poor detection rate. Moreover, the IoT is an open network which provides a flexibility to join and leave the network, the probability of node compromise is more. Hence the MDR is high for larger malicious node count. Further it can be observed that the proposed LWCTS-IoT is gained a higher MDR when compared with the traditional methods such as MCCTAR-IoT and CITM-IoT. As the proposed approach concentrated on the overhearing, the sender node can analyze the behavior of its neighbor nodes much accurately. Even though the MCCTAR-IoT concentrated on the involvement of direct and recommended trusts, they considered only communication which means they are able to solve only resource depletion attacks like DoS. On an average, the proposed approach has gained a MDR of 90.2356% while for existing approaches, it is noticed as 85.4612% and 81.2234% for MCCTAR-IoT and CITM-IoT respectively.

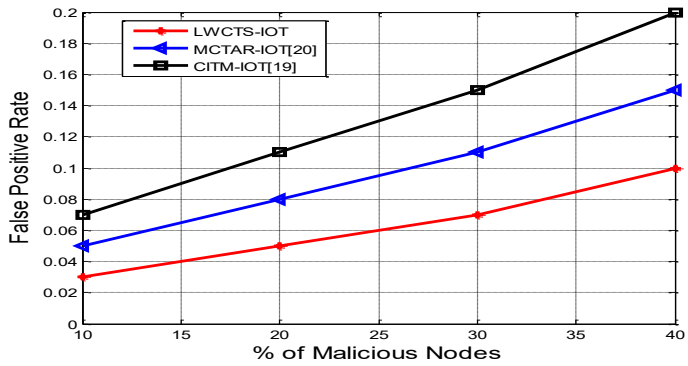

Fig.2 False Positive Rate variations with varying malicious nature

FPR and FNR are the two performance parameters which explores the information about negative performance or bad performance in the detection applications. These two parameters exactly follow opposite characteristics with MDR. Means, as the MDR rises, the FPR and FNR decreases and vice versa. The FNR is the one metric which measures the negatively detected nodes (for a given malicious node, the system is detected as non-malicious node). Similarly, the FPR is the one metric which measures the negatively detected nodes (for a given non-malicious node, the system is detected as malicious node). In the proposed approach, it is included the mobility factor to reduce the false positives count, i.e., reduction of wrongly detected number of nodes. In the IoT network, due to the possibility of mobility existence for IoT nodes, they may drop the packets if they move out of communication range of a sender node. At such kind of situation, the sender node may misunderstand and may declare the respective node became malicious. This is a wrong declaration because actually the packet is dropped due to mobility but not due to the attacks. If the sender node declares the receiver node as malicious, the negative behavior of receiver node increase and the remaining nodes in network also follows the same opinion which consequences to a great loss. This kind of situation increases the FPR and to solve this problem, it can be linked with the trust of a node with its mobility. Hence the FPR of proposed LWCTS-IoT is less when compared to the existing methods. From figure.2 and, on an average, the FPR of proposed approach is noticed as 8.2353%, while for existing methods, it is noticed as 12.7548% and 16.2554% for MCCTAR-IoT and CITM-IoT respectively. Similarly, from Figure.4, on an average, the FNR of proposed approach is noticed as 7.3789%, while for existing approaches, it is noticed as 8.8791% and 13.3122% for MCCTAR-IoT and CITM-IoT respectively.

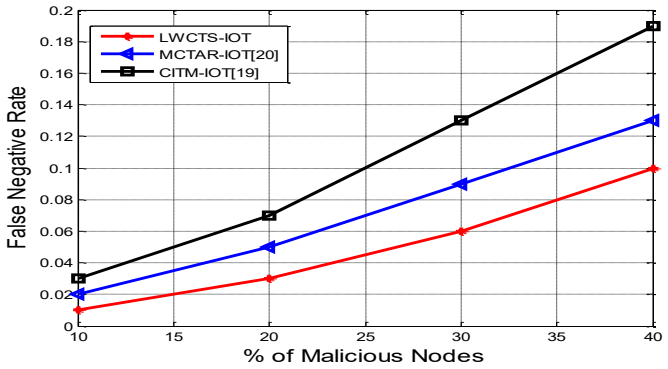

Fig.3 False Negative Rate variations with varying malicious nature

In the secure network, the data transmits happened in a secure way and successfully delivers at the intended destination. This kind of successful transmission results in a great packet delivery ratio. But with the increment in the malicious nature, the nodes will not cooperate for data forwarding and hence the packet delivery decreases, as shown in Figure.3. As the malicious nature increases, there is a possibility to launch more and different kinds of attacks which results in more packet drops. Some attacks are there like sink hole, black hole, and packet forwarding which mainly aims at the packet drop. If such kinds of attacks are launched on more nodes sink the network, the packet never reaches to the destination. Hence the packet delivery ratio always follows an inverse relation with malicious nature. From the figure 4, it can be noticed that the proposed LWCTS-IoT has gained a good PDR when compared with the conventional methods. Due to the involvement of packet forwarding factor as a trust reference metric, the sender node will get to know whether the packet was forwarded to next hop node or not. If the sender node finds that its next hop node has become malicious then it will stop sending information and broadcasts a control messages to the network regarding its maliciousness. However, the conventional MCCTAR-IoT only followed interactions which cannot explore the malicious nature perfectly. On an average, the PDR of LWCTS-IoT is noticed as 92.8367% while for existing approaches, it is noticed as 88.6467% and 84.6078% for MCCTAR-IoT and CITM-IoT respectively.

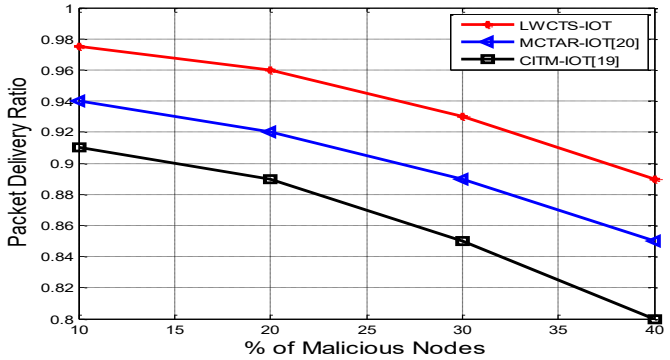

Fig.4 Packet Delivery Ratio with varying malicious nature

The nodes in IoT are energy constrained and if they are subjected to more processing tasks, then their energy will get depleted quickly and they will die. Hence the energy preservation is more important in IoT networks. Here the energy consumption has a direct link with malicious activities.

For example consider the DoS attack, the compromised node tries to send the packets continuously into the network thereby its energy depletes more quickly. Hence the involvement of malicious activity in the network raises the energy consumption and effects on the entire network lifetime.

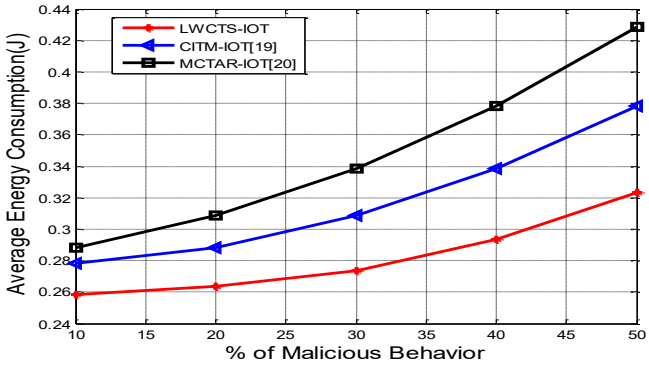

Fig.5 Average Energy Consumption with varying malicious nature

To solve this problem, clustering is the best solution in which only few nodes are subjected to new processing tasks. Here it is proposed that a new clustering concept in which the CH has the energy availability and it executes the computationally intensive tasks. Hence the AEC of proposed LWCTS-IoT is less. From the Figure.5 on an average, the AEC of suggested approach is observed as 0.3730 Joules while for the existing methods, it is observed as 0.4048 Joules and 0.4332 Joules for CITM-IoT and MCTAR-IoT respectively. Here it can be observed that the CITM-IoT has less energy consumption when compared with MCTAR-IoT because the CITM-IoT has followed a clustering mechanism while MCTAR-IoT has not.

V. Conclusion

Trust aware data transmission is a prime concern in IoT because the Internet is an open source that allows different devices to join and leave the network in a random fashion. Due to this open nature, the Devices connected to network can suffer from serious threats. To ensure a secure data transmission in IoT network a light weight clustered trust sensing mode which can provide better security along with a better Quality of Service to the network. The newly proposed clustering mechanism is able to provide the network a greater network lifetime by reducing the energy consumption at norm al nodes. Simultaneously, the proposed trust sensing model helps in the identification and isolation of malicious nodes from the network. For experimental validation it is realized this concept through an extensive simulation by varying the malicious nature of the network. The obtained results had proven that the proposed LWCTS-IoT is effective in the provision of QoS as well security comparatively MCTAR-IoT and CITM-IoT.

Acknowledgements

We would like to thank Director and Principal of Vidya Jyothi Institute of Technology for their continuous support in publishing this paper.

References

[1] Qiu T, Liu X, Li K, et al, “Community-aware data propagation with small world feature for internet of vehicles”, IEEE Communication Magazine 56(1), 86–91, 2018. http://doi.org/10.1109/MCOM.2018.1700511

[2] Liu X, Li K, Guo S, et al, “Top-k queries for categorized RFID systems”, IEEE ACM T Network, 25(5), 2587–2600, 2017. http://doi.org/10.1109/TNET.2017.2722480

[3] Atzori L, Iera A and Morabito G, “The Internet of Things: a survey”, ComputNetw, 54(15), 2787–2805, 2010. http://doi.org/10.1016/j.comnet.2010.05.010

[4] Raja S P, Rajkumar T D, and Raj V P, “Internet of Things: challenges, issues and applications”, J Circuit Syst Comp, 27(12), 1830007, 2018. http://doi.org/10.1142/S0218126618300076

[5] Liang Y, Cai Z, Yu J, et al, “Deep learning based inference of private information using embedded sensors in smart devices”, IEEE Netw Mag, 32, 8–14, 2018. http://doi.org/10.1109/MNET.2018.1700349

[6] K.-D. Chang and J.-L. Chen, “A survey of trust management in WSNs, internet of things and future internet,” KSII Transactions on Internet and Information Systems, vol. 6, no. 1, pp. 5–23, 2012. http://doi.org/10.3837/tiis.2012.01.001

[7] Z. Yan, P. Zhang, and A. V. Vasilakos, “A survey on trust management for Internet of Things,” Journal of Network and Computer Applications, vol. 42, pp. 120–134, 2014. https://doi.org/10.1016/j.jnca.2014.01.014

[8] D. Chen, G. Chang, D. Sun, J. Li, J. Jia, and X. Wang, “TRM-IoT: A trust management model based on fuzzy reputation for internet of things”, Computer Science and Information Systems, Vol. 8, No.4, pp. 1207-1228, 2011. https://doi.org/10.2298/CSIS110303056C

[9] F. Bao and I.-R. Chen, “Dynamic trust management for internet of things applications”, In: Proc. of international workshop on Self-aware internet of things, California, USA, pp.1-6, 2012. https://doi.org/10.1145/2378023.2378025

[10] Atzori, L., Iera, A., Morabito, G., Nitti, M., “The Social Internet of Things (SIoT) - when social networks meet the Internet of Things: concept, architecture and network characterization”, Comput. Netw,56(16), 3594–3608, 2012. https://doi.org/10.1016/j.comnet.2012.07.010

[11] Nitti, M., Girau, R., Atzori, L., “Trustworthiness management in the Social Internet of Things”, IEEE Trans. Knowl. Data Eng, 26(5), 1253–1266, 2014. https://doi.org/10.1109/TKDE.2013.105

[12] Kokoris Kogias E, Voutyras O, Varvarigou T., “TRM-SIoT: A scalable hybrid trust & reputation model for the social internet of things”, In: 2016 IEEE 21st international conference on emerging technologies and factory automation (ETFA), 1–9, 2016. https://doi.org/10.1109/ETFA.2016.7733612

[13] Bernabe, J. B., Ramos, J. L. H., Gomez, A.F.S., “TAC-IoT: multidimensional trust aware access control system for the Internet of Things”, Soft Comput.20(5), 1–17, 2016.

[14] Fangyu Gai, Jiexin Zhang, Peidong Zhu, and Xinwen Jiang, “Multidimensional Trust-Based Anomaly Detection System in Internet of Things”, Springer International Publishing, pp. 302–313, 2017 https://doi.org/10.1007/978-3-319-60033-8_27

[15] H. Xia, Z. Jia, L. Ju, Y. Zhu, Trust management model for mobile ad hocnetwork based on analytic hierarchy process and fuzzy theory, IET Wireless Sensor Systems 1 (4),248–266, 2011. https://doi.org/10.1049/iet-wss.2011.0042

[16] P. K. Reddy, R.S. Babu, “An Evolutionary Secure Energy Efficient Routing Protocol in Internet of Things”, International Journal of Intelligent Engineering and Systems, Vol.10, No.3, pp.337-346, 2017. https://doi.org/10.22266/ijies2017.0630.38

[17] Rajagopal, A., “Soft computing based cluster head selection in wireless sensor network using bacterial foraging algorithm”, Int. J. Electron. Commun.Eng. 9(3), 379-384, 2015.

[18] Reena Varghese, Dr. T. Chithralekha, CarynthiaKharkongor, “Self-organized Cluster Based Energy efficient Meta Trust model for Internet of Things”, 2nd IEEE International Conference on Engineering and Technology (ICETECH), Coimbatore, India, 2016.

[19] Mohammad Dahman Alshehri, Farookh Khadeer Hussain, Omar Khadeer Hussain, “Clustering-Driven Intelligent Trust Management Methodology for the Internet of Things (CITM-IoT)”, Mobile Networks and Applications, Volume 23 Issue 3, pp. 419-431, June 2018. https://doi.org/10.1007/s11036-018-1017-z

[20] Sowmya.G.,and Venkatram.N., “Multi-Context Trust Aware Routing for Internet of Things”, International Journal of Intelligent Engineering and Systems, Vol.12, No.1, 2019, pp.189-200.

[21] L. Qin and T. Kunz, ``Mobility metrics to enable adaptive routing inMANETs," in Proc. IEEE Int. Conf. Wireless Mobile Comput.Netw.Commun., pp. 1-8, 2006. https://doi.org/10.1109/WIMOB.2006.1696350

[22] P. Samar and S. B. Wicker, ``On the behavior of communication links ofa node in a multi-hop mobile environment," in Proc. 5th ACM Int. Symp.Mobile Ad Hoc Netw.Comput., pp. 145-156, 2004. https://doi.org/10.1145/989459.989478