Multi-Context Cluster Based Trust Aware Routing For Internet of Things

Sowmya Gali¹* Venkatram N²

¹,²Department of Electronics and Communication Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India

*Corresponding author’s Email: sowmya1046@gmail.com

http://doi.org/10.26782/jmcms.2019.10.00029

Abstract

Due to openness of the deployed environment and transmission medium (Internet), Internet of Things (IoT) suffers from various types of security attacks including Denial of service, Sinkhole, Tampering etc. Securing IoT is achieved a greater research interest and this paper proposes a new secure routing strategy for IoT based on trust model. In this model, initially the nodes of the network are formulated as clusters and the IoT nodes which are more prominent in trustworthiness and energy are only chosen as Cluster Heads. Further a trust evaluation mechanism was accomplished for every Cluster Node at Cluster Head to build a secure route for data transmission from source node to destination node. The trust evaluation is a composition of the communication trust, nobility trust and data trust. Simulation experiments are conducted over the proposed approach and the performance is analyzed through the performance metrics such as Packet Delivery Rate, Network Lifetime, and Malicious Detection Rate. The obtained performance metrics shows the outstanding performance of proposed method even in the increased malicious behavior of network.

Keywords: Internet of Things; Trust Management; Clustering; Communication Trust; Malicious Detection Rate; Network Lifetime

I. Introduction

In recent years, the rapid growth in the development of Internet of things (IoT) makes it to penetrate its widespread applicability into various fields including medical care, climate monitoring, industrial manufacturing and agricultural production. This can also be seen in daily life like smart home and internet of vehicles (IoV) [XXIII]. The IoT is a very flexible network that can accomplish multiple aspects such as tracking, identification, monitoring and management. According to the generalized nature of IoT, any device can be connected to the internet through various devices such as laser scanners, Global Positioning Systems (GPSs), Radio Frequency Identification Devices (RFIDs) [XVIII], code recognition devices and infrared sensors etc., to exchange the information as well as to
communicate [I]. Taking the advantage of IoT, different devices can be connected to
the internet and they can communicate with each other and also can exchange
information, which had given a great convenience in the daily lives. But as the
number of devices connected to internet increases, the information exchange also
increases which don’t have any guarantee about the security [XXIV]. Since the
devices are connected to the internet, the information exchanged is at great risk of
being stolen and modified. For example, a person’s location can be easily tracked and
based on the location, the travel time, and his/her feelings can be acquired easily. This
type of an unsecure communication between the IoT devices make the network secure
deficient. Hence the issue of security ensuring in IoT is getting more and more
attention [XVII].

Due to the open environment and the flexible transmission medium, the IoT nodes
may get compromised through various attacks like tampering, hijack, sinkhole,
Selective Forwarding (SF), DoS etc. To prevent the nodes getting compromised from
these attacks, a trust management scheme needs to develop through which the every
IoT node chooses a secure and trustworthy node before transmitting the information
to it. The secure and trust management scheme can be accomplished by providing a
continuous monitoring over the behavior of IoT nodes. During the monitoring, if any
suspicious is observed in the behavior of nodes, it can be notified as malicious and
can be discarded from the network. Hence, monitoring or detecting the node’s
behavior is an effective method. By developing a trust model and evaluating the
node’s trust value, the trustworthiness of a node can be evaluated. In this manner, the
trust managementscheme enhances the security by providing a continuous monitoring
over the behavior of node, measuring the trustworthiness of nodes and discovering
trustworthy nodes to collaborate with.

Towards this, a novel trust management scheme is developed in this paper
considering the communication scenario, nobility between nodes and the data
processing through the nodes. Consideration of more parameters for authenticity
makes the network more resilient towards all possible attacks and the nodes which
were compromised by any type of attacks can be detected more easily. Furthermore,
to achieve energy efficient and to increase the network lifetime, a novel clustering
mechanism is proposed in which only few nodes are chosen to process the trust
evaluation. An extensive simulations done over the proposed mechanism shows its
effectiveness in the detection of compromised nodes and also in the improvisation of
network lifetime.

Remaining paper is summarized as follows. The details of earlier developed security
strategies for IoT network are mentioned in section II. The details of network
considered in this paper are modeled section III. Section IV discusses the details of
trust evaluation mechanism which is composed of three different aspects. Section V
depicts the routing process details. Experimental investigations are discussed in
Section VI and the final concluding remarks are demonstrated in the section VII.

II. Literature Survey

In IoT network, the trust is a widespread topic of study, which is being used
to calculate the trustworthiness nodes [XXXIII]. For a node, the trustworthiness is
depicted based on its behavior in the network towards its neighbor nodes.
Confidentiality, integrity, reliability, and dependability are the most important
parameters which defines the trustworthiness of IoT nodes. These values are combined to depict the behavior of a node as a weight value representing the trust rating of a node. This rating defines the reputation of node, which explores a computational range of values as an indicator of the negative or positive capabilities of a node’s behavior to its neighbor nodes which are connected directly or indirectly to it.

Trust Management (TM) been developed for IoT network as a significant aspect to develop a secure and stable configuration of IoT. TM can be used to enhance the security of the nodes particularly when the node count increases to that extent such that the central administrator is not able to handle or when the communicating media among the nodes is navigate network media. Indirectly the trustworthiness of a node reflects the behavior of node to the Quality of Service (QoS). QoS like supporting in decision making results a secure process and also an optimal decisions in routing [IX]. Provision of security in the network through cryptographic solutions makes the nodes resource constraint, making them susceptible to compromise. Contrary to these strategies, the TM schemes do not composed of much complex encryptions and hashing as like the cryptographic approaches. This makes the TM a feasible option to enhance the security in the IoT network. Furthermore, the TM also provides a constant monitoring and observation of the performance and behavior of nodes, assess the trustworthiness and determine only the nodes which are more trustworthy to collaborate with.

Various trust management schemes are developed in earlier to ensure the trust based routing in IoT network. In the trust evaluation process, the parameters considered to define the trustworthiness of a nodes 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 at al. [IV] 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 didn’t 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 [VII] 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. [II] in which the trust evaluation is done based on the social network aspects. Further, Nitti et al. [XXI] 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. [XV] 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 on its own experience of referring to its friends or the platform. Next, the method proposed by Bernabe et al. [III] provides a flexible access control system for trust management in
IoT network, called TAC-IoT. Gai et al. [VI] 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 didn’t 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 won’t 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 in resources, called as “Cluster based Trust Management in IoT” [XIX]. 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 [XXII]. An optimal Secure and ‘Energy Aware Protocol (OSEAP)” and an ‘Improved Bacterial Foraging Optimization (IBFO)’ [XXV] algorithm were accomplished here. However, the FCM algorithm won’t 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 [XXVI], 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. [XX] 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 didn’t discuss about the energy preservation and also accomplished as cooperative communication between the cluster nodes by which the energy consumption will increases greatly.

Other than the above specified works on clustering, a new methodology is also there in which there has been a significant research work was accomplished, called ‘Bio-Inspired Clustering (BIC)’ [XXX, XVI, XXXIV]. The main motivation behind this BIC is the self-organizing nature of nodes in the network. Based on simple rules, totally local decisions, with less number of broadcasted messages, the nodes in the network can decide their roles as either CHs or CNs [XII]. In this regard, the most popular Bio-inspired Meta heuristic algorithm, ‘Particle Swarm Optimization (PSO)’ was used in many approaches [V, XIII]. Some more approaches accomplished the ‘Artificial Bee Colony (ABC)’ algorithm [XVI, X, XIV] and Firefly based clustering [XXVII, XXVIII, XXIX]. A recent BIC method proposed by Jabeur et al. [XI] towards
an adaptive spatial clustering for IoT is also based on the Firefly Algorithm. In their approach, the authors developed a protocol in which the data regarding the trust relationship is stored at nodes. Further a convergence based trust relationship evaluation is proposed in this work to establish the trust for the nodes which are in the process. However this approach got failed in addressing the critical issues like energy preservation and storage requirements. Due to the heterogeneous nature of devices connected to internet, all devices won’t have equal space capacities. And also due to the convergence algorithm at every time, the energy of nodes will get drain up and makes the nodes to die quickly.

Though the approaches based on BIC are effective in the CH selection in a periodic fashion, the computational complexity is very high due to the convergence process. For every instant and at every node, the BIC based trust evaluation constitutes more energy consumption, which becomes the node to die quickly and makes the network lifetime very less.

### III. Network Model

This approach considers the IoT network as a cluster based network and the nodes in the network are categorized into Cluster Heads (CHs) and Cluster Nodes (CNs). In every cluster, the CH consists of more energy than CNs, and all the CNs will communicate with CH directly. Further the CH will communicate with another CH to further forward the information form source to destination. Each and every CN has unique identity and it can belong to more than one clusters.

Initially, among the all available nodes of a network, the nodes which have more energy and more trustworthiness are selected as cluster heads. Next, the clusters are formulated based on the Euclidean distance evaluation between the CHs and remaining nodes. For every CH, the Cluster nodes are decided based on the neighboring distance between the CH and nodes. The nodes which falls in the communication range of every CH is considered as its CNs and the range is defined as the average distance between the CH and remaining nodes. A sample architecture of cluster based IoT network are depicted in figure.1.

![Figure 1: The network model of Cluster based IoT network](image)

*Copyright reserved © J. Mech. Cont.& Math. Sci.*

*Sowmya Gali et al*
As show in the above figure.1, the network consists of CHs and CNs. Here the clusters are formulated based on the Euclidean distance. There exist some overlapping clusters and the nodes which falls in the overlapping region can connect to any of the CHs to which they have. Based on this aspect, the connections between nodes and CHs are categorized as Strictly Connected Nodes (SN) and Volatile Connected Nodes (VN). Except the CH to which the nodes are connecting every time, remaining all the characteristics is same for SN and VN. Different types of representation are considered for these nodes, as shown in Figure.1. The Strictly connected nodes means, that node is purely in the communication range of only one CH and the Volatile Connected Node means, it can be connected to any CH it have. Depends on the distance between the VN and the CHs, the VN connects to the CH to which it is close to and also the CH for which the highest trustworthiness exists. Because, as the distance between nodes increases, the power needed to communicate with nodes also increases, and hence to preserve the energy, the VNs will connected to the CHs to which they have less distance. In the case of equal distances for all CHs, the VN can connect to any of the CHs. This paper makes the following assumptions;

1. The IoT network is cluster based, and the communication between CH and the respective CNs is in a direct fashion whereas the communication between CHs in a free manner.
2. Each IoT node has only one unique ID and can be belongs to single cluster or multiple clusters, and the energy of CHs energy than CNs.
3. The propagating data in the IoT network is hybrid in nature, i.e., it can be a continuous and event-driven.

IV. Trust Evaluation Scheme

Based on the network model described in the earlier section, here a novel trust evaluation mechanism is introduced. After clustering the nodes into different clusters, the trust evaluation is accomplished to measure the trustworthiness of CNs and this responsibility is completely taken by CH. For a particular cluster, the communication between the CNs and CH should be in a uniform format. Hence the trust evaluation between CH and CNs consists of direct trust and indirect trust. The trust evaluation is done in a periodic fashion such that the malicious nodes can be detected at any time.

The proposed trust evaluation mechanism considers multi-dimensional trust. It is composed of two different trusts namely, data related trust and network related trust. To make the network resilient from all possible attacks, this work considered the trust evaluation in multi-dimensional fashion. The innovative trust considered here is the data related trust. Since some attacks types are there which compromise the network by tampering the data transferring through the network, this approach considered the trust evaluation through data also. In the network related trust, the trust evaluation is carried based on the communication and nobility of CNs. So the final composite routing metrics considers totally three parameters for decision making towards the malicious nature of nodes.
Communication Trust

The communication trust is assessed by measuring the number of communication interactions happened between the CH and CN. According the trust evaluation methodology described in [XXXII], the communication trust between two nodes is in the both direct and indirect form. In this paper, the CH takes the responsibility of trust evaluation. Since the CH has more energy, it can compute the trustworthiness of nodes in that particular cluster. Here the direct trust means the self-experience of CH towards a CN, \( j \) and indirect trust means the neighbor nodes experience towards that CN, \( j \). Since there exists \( 'p' \) number of neighbor nodes, the indirect trust is obtained by averaging the trust values of all neighboring nodes of that CN, \( j \). The mathematical Representation of total trust between the CH \( i \) and CN\( j \) is formulated as follows;

\[
TT_{i,j} = w_1 \times DT_{i,j} + w_2 \times \sum_{p=1}^{N_p} \frac{IT_{i,j}}{N_p}
\]

(1)

Where \( DT_{i,j} \) denotes the Direct trust between CH,\( j \) and CN,\( j \). \( IT_{i,j} \) is the indirect trust acquired by the CH,\( j \) from the neighboring node \( p \) of node \( j \). \( N_p \) is the total number of neighbors of node \( j \). The indirect trust \( IT_{p,j} \) is determined using Eq. 2.

\[
\sum_{k \in N_k \neq j} IT_{p,j} = \sum_{k \in N_k \neq j} DT_{i,p} \times DT_{p,j}
\]

(2)

Where \( DT_{i,p} \) represents the direct trust between the CH,\( j \) and its one of the CN,\( p \), which is a neighbor node of CN,\( j \) and \( DT_{p,j} \) represents the direct trust between the CN,\( j \) and its neighboring CN,\( p \).

In this paper, the communication trust refers all types of communication interactions including receiving and sending of route request (RREQ) packets Route Reply (RREP) packets and data packets. As of [VIII], the greater number of interactions between nodes reflects higher trust value. But in IoT network, if the total communication interactions count exceeds a predefined interactions threshold, the trust value will get decrease because there may be the communication interactions due to the attackers that send a huge number of packets to the node die up quickly. Hence this paper considered communication trust between node and CH to define the trust value. Based on the statistics of probability density function (PDF), which has a normalized range of \([0 1] \) to measure the communication trust is accomplished when the communication interactions count surpasses the predefined interactions threshold. The communication trust value of CN \( j \) evaluated by CH,\( i \) in the time interval can be formulated as [XXXV]

\[
CT_{i,j}(t) = \left\{ \begin{array}{ll}
10 \times \frac{DT_{i,j}}{\mu} & \text{if } TT \leq Th_{int} \\
[10 \times \exp (-|DT_{i,j} - \mu|/\theta)] & \text{if } TT > Th_{int}
\end{array} \right.
\]

(3)

Where \( DT_{i,j} \) defines the total number of direct communication interactions between CH,\( j \) and CN,\( j \), \( \mu \) is the average number of communication interactions between the CH,\( j \) and the all CNs in that cluster. \([z]\) represents the largest integer that is equal to or less than \( z \). \( Th_{int} \) is the threshold of communication interactions and it is formulated as the product of an arbitrary, \( \omega \) constant and \( \mu \), \( \omega \times \mu \). The value of \( \omega \) varies.
depending on the commutation paradigm and it defines the upper limit of communication interactions. \( \theta \) is an arbitrary constant and accomplished here to obtained the values range in the range of \([0, 10]\) to make the uniformity. This values is varied as 1, 10, 100 depends on the total number of communication interactions. For a single digit number of interactions, the \( \theta \) is 1 and it is 10 for ten digit and it is 100 for hundred digit number.

**Nobility Trust**

The nobility trust is measured with respect to the Packet Forwarding Probability (PFP) of a node. The PFP is directly related to the number of successful and unsuccessful interactions. In the IoT network, the CH, \( i \) overhears the CN \( j \), if CN \( j \) does not deliver the packet in the predefined time interval or transmit the packet to another node that is not in the routing table. For example assume that each node broadcasts a probe packet for every second up to 10 seconds. For instance, node A has received 7 packets from node B. At the same time, the node B found that it has received 9 probe packet form node A. Then the Packet Loss Rate (PLR) is 0.3 and the Packet Success Rate (PSR) is 0.7. But the PLR from node B to node A is 0.1 only. Hence the probability that a data packet can be successfully transmitted form node A to node B in a predefined time interval is 0.7. Here the overhearing is done through the HELLO packets instead of separate packets. This reduces the addition energy consumption and overhead incurred at CH in the network.

Based on this concept, the nobility trust is derived and is formulated with the accumulation of number of received packets to the total number of expected packets. If the CN, \( j \) received the packet from CH,\( i \) or it has forwarded that data packet received from CH, then it send a probe packet to the CH and it is treated as successful interaction otherwise it is treated as an unsuccessful interaction. For instance, if a CN is compromised due to the selective forwarding attack, then only some portion of the packets will reach to the CH or to other cluster nodes. Then the CH or other nodes can’t send the probe packets which are very less in number. This indicates some malicious activity in the cluster. The higher the ratios of number of successful interactions to the total number of interactions, higher the trust value. This paper accomplished the following formula to measure the nobility trust between CH,\( i \) and CN,\( j \).

\[
NT_{ij}(t) = \left[10 \times \frac{P_{\text{received}}(t_{i-1}, t_i)}{P_{\text{expected}}(t_{i-1}, t_i)}\right]
\]

Where \( P_{\text{received}}(t_{i-1}, t_i) \) the total number of HELLO packets is received at CH,\( i \) from CN,\( j \) and it represents the total number of successful interactions. Next, \( P_{\text{expected}}(t_{i-1}, t_i) \) is the total number of expected packets to receive at CH,\( i \) from CN,\( j \) in the predefined interval \((t_{i-1}, t_i)\).

The highest value of nobility trust of CN,\( j \) towards its CH denotes more trustworthiness and a less value indicates that the CN is malicious. The maximum value of NT is 10 and minimum value is 0 which denotes the CN is more trustworthy and CN is malicious respectively. A medium value of NT =5 denotes the medium trust of CN, \( j \) to the CH.
Data Related Trust

The data trust is measured by the CH node by observing the data propagating in the network. Attacks like data tampering can be detected through this analysis. Since the IoT is a data centric network and the data observed is the factor of most concern of applications. In IoT network, the nodes will transmit multi-dimensional data to Cluster Head. An observation in any deviations in the data can be regarded as abnormality. The deviation between observed data and the effective average of observed data governs the data related trust. Since the data is transmitted in numerical format and to find the deviation, Euclidean distance is considered as a reference metric. Let’s consider \( \mu_k \) and \( \sigma_k \) as the mean and standard deviation of \( k \)-th dimensional data, the effective average of observing data can be obtained as \( [\mu_k - \sigma_k, \mu_k + \sigma_k] \). The minimum value of observed data cannot be less than the lower limit \( [\mu_k - \sigma_k] \) of effective of observing data and also should not be greater than the higher limit \( [\mu_k + \sigma_k] \). Furthermore, if the node density is high in the IoT network, then all nodes have approximately same type of data and it is difficult for any node to spot the dissimilar data, unless it is attacked or compromised. The mathematical formulation of data related trust evaluated between CH, \( i \) and CN, \( j \) is represented as [XXV]

\[
AT_{i,j}(t) = [10 \times \exp (-D_{i,j})]
\]  

Where

\[
D_{i,j} = \sqrt{\sum_{k=1}^{K} (x_{ik} - x_{jk})^2}
\]

Overall Trust

The overall trust of CN, \( j \) measured by CH, \( i \), which is a combined form of communication trust \( (CT_{i,j}(t)) \), nobility trust \( (NT_{i,j}(t)) \) and data trust \( (AT_{i,j}(t)) \) and it is formulated as follows;

\[
OT_{i,j}(t) = \alpha \times CT_{i,j}(t) + \beta \times NT_{i,j}(t) + (1 - \alpha - \beta) \times AT_{i,j}(t)
\]  

Where, \( \alpha \) and \( \beta \) are two arbitrary constants, having the range of \([0\ 1]\). These two constants are considered to signify the priority of all three trusts with respect to their values. These two constants are weights for each sub trust value, a greater value defines more importance and less value signifies the less importance. For example, if \( \alpha = 0.5 \), \( \beta = 0.3 \) and \( (1 - \alpha - \beta) = 0.2 \), then the CH concentrates on the communication trust mostly. In such a case, the decision is most favored to the decision of communication trust. The result about the node’s trustworthiness revealed at communication trust is almost finalized at overall trust also. Further values of these two arbitrary constants vary depends on the environment.
V. Routing Process

A Multi-Context Cluster based Trust Aware Routing (MCCTAR) scheme is proposed in this paper according to the proposed routing metrics (discussed in section III) and the optimal algorithm for path selection.

Network Model Establishment

In this paper, initially, the nodes with higher energy and higher trust are selected as CHs. To obtain a stable cluster structure along with efficient network lifetime, the nodes with higher trust only has to select and the nodes which has higher energy will give better results with respect to network lifetime. A simple example demonstrating about the cluster selection process is depicted in figure 2.

![Figure 2: Selection of Cluster Head](image-url)
In the network model establishment, figure 2 (a) shows an initial state of IoT nodes, i.e., a random network with non-clustered nodes with initial trustworthiness which satisfies the condition $0.5 \leq TT \leq 1.0$. Every node in the network monitors the neighbor node’s behavior by exchanging their initial trust values with each other to choose a CH with reference to the methodology specified in the earlier section. Figure 2(b) shows the Initial trust values of all nodes in the network, which were shared to a node having the initial trust a value of 0.8. The trust values are received from totally six neighboring nodes and they are sequentially 0.7, 0.4, 0.6, 0.9, 0.6 and 0.5. From the received trust values, the node can be chosen the neighbor node with higher trust value is the node whose Initial Trust is 0.9 by comparison, so the node with Initial Trust = 0.8 considers the node with Initial Trust = 0.9 as cluster head node and treats itself as a member of that cluster. Considering the possible network deployment coverage area, the cluster heads are selected with highest trust values, in adjacent nodes after a finite number of comparisons and the formulated cluster is shown in Figure 2(c).

**Route Selection**

Once the network model is constructed and the cluster formulation is also completed based on the exchange of initial trust values, then the optimal path is need to be established from the available and possible routes for a given source and destination node pair. In general, the proposed trust evaluation model does not know about the routing process used in the network to accomplish the route selection. Once the nodes completed the route discovery according to the adopted routing protocol, it won’t enter into the data transmission phase but measures the Overall Trust of nodes initially. Once the source node is decided, the trust value of destination node is defined to 1 since it is no significant to determine the trust value. Hence, the trust value ($T$) of a hop link-$r$ between node $x$ and its downstream nod $y$ is formulated as

$$T(r) = \prod_{(x,y) \in r} T(x,y)$$

(8)

In general, there exists so many links for any source and destination node pair and the source node need to choose an optimal and secure path by measuring the trust of all the links. This process is depicted in figure 3, where $n_s$ is the source node and $n_d$ is the destination node.

**Table 1:** Possible routes and their Total Trust

| Route     | Total Trust |
|-----------|-------------|
| $R_1 = n_s \rightarrow n_1 \rightarrow n_2 \rightarrow n_d$ | $T(R_1) = 1 \times 0.9 \times 1 = 0.90$ |
| $R_2 = n_s \rightarrow n_1 \rightarrow n_3 \rightarrow n_2 \rightarrow n_d$ | $T(R_2) = 1 \times 0.7 \times 0.8 \times 1 = 0.56$ |
| $R_3 = n_s \rightarrow n_4 \rightarrow n_5 \rightarrow n_d$ | $T(R_3) = 1 \times 0.7 \times 1 = 0.70$ |
| $R_4 = n_s \rightarrow n_4 \rightarrow n_3 \rightarrow n_5 \rightarrow n_d$ | $T(R_4) = 1 \times 0.8 \times 0.6 \times 1 = 0.48$ |
| $R_5 = n_s \rightarrow n_1 \rightarrow n_3 \rightarrow n_5 \rightarrow n_d$ | $T(R_5) = 1 \times 0.7 \times 0.6 \times 1 = 0.42$ |
| $R_6 = n_s \rightarrow n_4 \rightarrow n_3 \rightarrow n_2 \rightarrow n_d$ | $T(R_6) = 1 \times 0.8 \times 0.8 \times 1 = 0.64$ |
According to the figure 3 (a), there are six possible routes from source node to
destination node and their total trust values are tabulated in the table 1. From the
values observed in table 1, the most credible route is $R_1 = n_s \rightarrow n_1 \rightarrow n_2 \rightarrow n_d$. In
this fashion, the trust ensured most secure route is established between any nodes of
IoT network and the trust evaluation is also accomplished in periodic fashion. At any
instant if any node is observed to be malicious, that node is discarded from the
network and an update is propagated in the network such that no node will select that
node for communication.

VI. Experimental Evaluation

This section describes the details of simulation experiments performed over
the proposed trust management mechanism and the obtained performance results
including the Malicious Detection rate (MDR), False Positive Rate (FPR), False
Negative Rate (FNR), Average Packet Delivery Ratio (APDR), and Storage Overhead. All these metrics are measured with varying number of malicious nodes. To simulate the proposed approach, an IoT network is created with $P$ number of nodes of an area of $MN$, where $N$ represents the width and $M$ represents the length of the network. The parameters considered for simulation are listed in Table 2.

**Simulation Setup**

| Parameter          | Value                                      |
|--------------------|--------------------------------------------|
| Number of nodes    | 20-60                                      |
| Area               | $1000 \times 1000$ m$^2$                  |
| Packet Size        | 512 Bytes                                  |
| Traffic Source     | CBR                                        |
| Node placement     | Random                                     |
| Malicious Nature   | 0-40% of total nodes                      |
| Simulation Time    | 50 Sec                                     |
| $\alpha, \beta$    | $0 \leq \alpha, \beta \leq 1$             |
| $\lambda$          | 1, 2, 3, and 4                             |
| $w_1, w_2$         | $0 \leq w_1, w_2 \leq 1$                  |

Initially, considering $P$ as a node count, a random network is created as shown in Figure 4. Further, the nodes on the created network are clustered based on the methodology specified in earlier sections. The clustered network is depicted in Figure 5. The number of clusters is defined manually and here the total number of clusters considered is five. Once the CHs are obtained, the CNs are obtained by evaluating the Euclidean distance between the CHs and remaining nodes in the network.

![Network Formation](image)

*Figure 4 Initial random network with 30 nodes*
Performance Metrics

**Malicious Detection Rate (MDR):** MDR is defined as the total number of nodes detected as malicious when they are malicious. In the simulation experiments, some nodes are defined as malicious from the overall nodes and if they are detected as malicious by the developed trust framework, then the MDR value will increase. Higher MDR indicates the good performance and lower MDR indicates bad performance.

**False Positive Rate (FPR):** FPR is defined as the total number of nodes detected as normal when they are malicious. Higher FPR indicates the bad performance and lower FPR indicates good performance.

**False Negative Rate (FPR):** FNR is defined as the total number of nodes detected as malicious when they are normal. Higher FNR also indicates a bad performance and lower FPR indicates good performance.

**Average Packet Delivery Ratio (APDR):** APDR is defined as a ratio of the total number of packets delivered to the total number of packets transmitted. The higher value of APDR indicates the good performance and lower value indicates the bad performance.

**Storage Overhead:** Storage Overhead is defined as the amount of additional storage belongs to the CNs stored at CH. A less value of this additional Storage overhead represents the better performance and higher value indicates bad performance.

Simulation Results

Under the simulation results, the performance metrics are measured over the network deployed with above simulation parameters depicted in table.2. Initially a network with \( N \) number of node is created and the proposed methodology is accomplished.
over that network. At every simulation, the portion of malicious nodes is varied and the performance metrics namely, MDR, FPR, FNR, APDR, and Storage Overhead are measured. The obtained performance metrics of proposed method are compared with the values of existing methods and the observed results are described in the following figures;

Figure 6: MDR for varying malicious number of nodes

Figure 6 illustrates the varying details of malicious detection rate with varying number of malicious nodes. From figure 6, it can be noticed that the MDR had shown a falling nature with an increment in the % of malicious nodes. But, the MDR of MCCTAR-IoT is observed to be high compared to the MDR of existing methods. For a particular % of malicious nodes, the MDR of MCCTAR-IoT is greater than the conventional approaches, ASC-IOT and CITM-IOT. Since the proposed MCCTAR-IoT considered the trust assessment in multiple orientations, the obtained trust value of a node will represent all compromising possibilities and hence the any node which was compromised with any type of attack was detected easily. This detection boosts up the MDR because the MDR is a ratio of total nodes detected as malicious to the total original malicious nodes. Furthermore, the conventional approaches considered only memory requirement as a main reference parameter for trust evaluation, which is not sufficient to detect all possible compromised nodes due to various attacks. On an average, the MDR of proposed approach is obtained as 92% and for the conventional approaches; it is approximately 88% and 84% for ASC-IOT and CITM-IOT respectively.
FPR is a metric which has an inverse relationship with MDR. As MDR increases, the FPR decreases and vice versa. Since the FPR is determined as a ratio of total nodes detected as normal when they are malicious, it has opposite relationship with MDR. Here the main objective of the proposed MCCTAR-IOT is to detect the malicious nodes and the nodes which are detected as normal when they are malicious, falls under False Positives (FPs). As the number of FPs increases, FPR also increases. FPR has increasing characteristics with increasing the malicious nature, as shown in figure.7. However the proposed MCCTAR-IOT has less FPR compared to the conventional approaches. The main reason behind this less FPR is the composition of multiple factors in the trust evaluation of every IoT node. Due to the evaluation of trustworthiness of nodes in an updated manner, the all malicious nodes can be detected at least one time, results in a less FPR. On an average, the FPR of proposed approach is obtained as 5% and for the conventional approaches; it is approximately 7% and 10% for ASC-IOT and CITM-IOT respectively.

FNR is a one more metric, similar to the FPR and it is also having inverse relationship with MDR. FPR considers the false positives whereas FNR considers he false negatives. In the proposed aspect, the FN is defined as the node which is detected as malicious node when it is normal node. For an approach, the FNR also should be less and that characteristics are shown in figure.8.
As it can be seen from figure 8, the FNR follows increasing characteristics with increasing malicious nature. However, compared to the existing methods, the FNR of proposed MCCTAR-IoT is observed to be less and it is due to the consideration of trust evaluation in multiples aspects. On an average, the FNR of proposed approach is obtained as 4% and for the conventional approaches; it is approximately 5% and 8% for ASC-IOT and CITM-IOT respectively.

Figure 9 represents the details of APDR for varying malicious nodes. As the number of % of malicious nature increase, the malicious nodes won’t cooperate to the general communication process due to which the packets cannot reach to the destination and results in a less packet delivery ratio. From the figure 9, it can be noticed that the APDR follows a declined characteristics with the increasing nature of maliciousness. But the APDR of proposed MCCTAR-IoT is obtained as high compared to the existing methods. Since the proposed approach considered a novel clustering mechanism and also an efficient multi-facet trust evaluation strategy, the nodes which
are compromised are detected and removed from the network. Next, an alternative path is allocated to the source node immediately through which the packets can move more successfully towards the destination node. This constitutes an increased APDR and it is better even in the case of increasing malicious nodes. Furthermore, the conventional approaches formulated only a single reference metric to define the trustworthiness of nodes but the attackers have so many options to compromise the node. On an average, the APDR of proposed approach is obtained as 95% and for the conventional approaches; it is approximately 91% and 88% for ASC-IOT and CITM-IOT respectively.

Storage overhead defines the amount of extra storage burden occurred at the node. In the developed mechanism, the trust evaluation is accomplished only at the CH, and to do this, the CH should have the knowledge about the CNs information like Number of interactions, energy, data observing etc. To store all this information, the CH should have more storage capacity otherwise; the CHs must be more in number. As the number of clusters increases, the storage overhead at a single CH will decrease and it is shown in the figure.10.

The proposed clustering mechanism is dynamic in nature and the number of clusters need to formulate are depends on the total number of nodes and network area. Hence, the storage overhead of MCCTAR-IOT is observed as less compared to the existing methods. On an average, the Storage Overhead of proposed approach is obtained as 1720 and for the conventional approaches; it is approximately 2500 and 3000 for ASC-IOT and CITM-IOT respectively.

![Figure.10 Storage Overhead for varying malicious number of Clusters](image_url)

The proposed clustering mechanism is dynamic in nature and the number of clusters need to formulate are depends on the total number of nodes and network area. Hence, the storage overhead of MCCTAR-IOT is observed as less compared to the existing methods. On an average, the Storage Overhead of proposed approach is obtained as 1720 and for the conventional approaches; it is approximately 2500 and 3000 for ASC-IOT and CITM-IOT respectively.
The network lifetime of any network is directly concerned with the energy consumption of nodes. With an increase in the % of malicious nodes, the more number of nodes are said to be compromised and in such situation, detection of a promiscuous node for forwarding the information is a time taking process and also consumes more energy. Excess energy consumption has a direct effect over the lifetime of node which also has impact on the network lifetime. The decreasing characteristics of network lifetime with increasing malicious nature are depicted in figure.11. However, the proposed MCCTAR-IOT is observed to have a better lifetime compared to the existing methods. Due to the accomplishment of a dynamic clustering technique, the nodes which have more energy are selected as CHs and the entire trust evaluation process is accomplished at CH only to preserve the energy of nodes which in turn increased the overall network lifetime.

On an average, the Network lifetime of proposed approach is obtained as 40 Sec and for the conventional approaches; it is approximately 38 Sec and 36 Sec for ASC-IOT and CITM-IOT respectively.

Figure 11 Network Lifetime for varying malicious nodes

Figure 12 Average Trust Value for Normal nodes and Malicious Nodes

Copyright reserved © J. Mech. Cont.& Math. Sci.
Sowmya Gali et al
The average trust value of normal nodes and malicious nodes is evaluated at every simulation experiment. Figure 12 illustrates the average trust value and trust threshold of normal nodes and malicious nodes in totally ten experiments. From figure 12, it can be observed that the approximate trust value of normal nodes and malicious nodes is 8.5 and 4 respectively and the dynamic trust threshold is varying in every experiment. Due to the consideration of three types of trusts such as communication trust, nobility trust and data trust the average trust value of both normal and malicious nodes is don’t have a sharp decrement or sharp increment.

VII. Conclusion

Security is the most important concern in the IoT network due to its widespread connectivity of different devices to the internet. To achieve a secure and energy efficient data transmission between IoT devices, this paper proposed a novel trust management scheme along with an effective clustering scheme. Due to the consideration of multiple factors in the trust evaluation, this approach ensures the secure data transmission with less power consumption. Simulation experiments conducted with different malicious nodes had shown the performance effectiveness with respect to the MDR, APDR and Network Lifetime. The performance enhancement is also shown by comparing the obtained APDR, MDR, and Network Lifetime through the proposed MCCTAR with the conventional approaches. The comparative analysis had shown that the proposed approach outperforms the conventional approach in all aspects. On an average the proposed MCCTAR gained an improvement of 4% and 8% in the MDR from conventional approaches ASC-IOT and CITM-IOT respectively. Furthermore, the reduction in the FPR is observed as 2% and 5% from the conventional ASC-IOT and CITM-IOT respectively. Among with FPR, the proposed approach also has gained a reduced FNR when it was compared to the conventional approaches and it is approximately 1% and 4% from ASC-IOT and CITM-IOT respectively. These improvements of proposed approach have proven that the proposed approach is effective in the detection of all possible malicious nodes in the IT network.

Next, focusing over the Quality enhancement, the improvement in APDR is observed as 4% and 7% from ASC-IOT and CITM-IOT respectively. Along with sufficient quality improvement, the proposed approach also gained an increased network lifetime and it is approximately 2 Sec and 4 Sec when compared with ASC-IOT and CITM-IOT respectively. From these observations, it can be concluded that the proposed approach is more resilient to various network attacks and provides a secure and reliable data transmission with less resources.

One important thing needs to analyzed during the malicious node detection is packet loss and this packet loss may be occurs due to various reasons and every lost packet is not of due to the malicious behavior of nodes. Due to this blind assumption, an innocent node may get punished and to overcome such types of problems a fine analysis over the packet loss must be done. In future, this work extends the trust evaluation by considering the packet loss reasons to find the malicious and selfish nodes in the IoT network.
References

I. Atzori L, Iera A and Morabito G. The Internet of Things: a survey, ComputNetw 2010; 54(15): 2787–2805  
II. 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 2012; 56(16):3594–3608.  
III. 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. 2016;20(5):1–17.  
IV. 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. 2011; 8(4):1207-1228.  
V. Dong J, Qi M.A new clustering algorithm based on PSO with the jumping mechanism of SA. In Proceedings of the 3rd International Conference on Intelligent Information Technology Application, NJ, USA, 21–22, 61–64.  
VI. Fangyu Gai, Jiexin Zhang, Peidong Zhu, and Xinwen Jiang. Multi-dimensional Trust-Based Anomaly Detection System in Internet of Things. Springer International Publishing 2017; pp. 302–313.  
VII. 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 2012; California, USA, pp.1-6.  
VIII. F. Hao, G. Min, M. Lin, C. Luo, and L. Yang. Mobi-FuzzyTrust: An efficient fuzzy trust inference mechanism in mobile social network. IEEE Trans. Parallel Distrib. Syst., 2014; 25(11): 2944-2955.  
IX. F. Ishmanov, A.S. Malik, S.W. Kim, B. Begalov. Trust management system in wireless sensor networks: design considerations and research challenges. Trans. Emerg. Telecommun. Technol 2015; 26:107–130.  
X. Hasnat MA, Akbar M, Iqbal Z, Khan ZA, QasimU, JavaidN. Bio inspired distributed energy efficient clustering for Wireless Sensor Networks, Information Technology: Towards New Smart World (NSITNSW). 5th National Symposium on, Riyadh 2015; pp. 1-7.  
XI. Jabeur N, Yasar AUH, Shakshuki E, Haddad H. Towards bio-inspired adaptive spatial clustering approach for IoT applications. Future Generation Computer Systems: May 2017.  
XII. Jacobsen R. H, Zhang Q, Toftegaard T. S.Bio-inspired Principles for Large-Scale Networked Sensor Systems: An Overview. Sensors 2011; 11(4): 4137–4151.  
XIII. Jin Wang, Yiquan Cao, Bin Li. Particle swarm optimization based clustering algorithm with mobile sink for WSNs. Journal of Future Generation Computer Systems. 2017; 76©: 452-457.  
XIV. Karaboga D, Oktan S, OzturkC. Cluster based wireless sensor network routing using artificial bee colony algorithm. International Journal of Wireless Networks:2012;7(18): 847-860.  
XV. Kokoris Kogias E, Voutyras O, Varvarigou T. TRM-SIoT: A scalable hybrid trust & reputation model for the social internet of things. In: Proc., of IEEE 21st international conference on emerging technologies and factory automation (ETFA); 2016:1–9.
XVI. KrishnaveniV, Arumugam G.A novel enhanced bio-inspired harmony search algorithm for clustering. *International Conference on Recent Advances in Computing and Software Systems (RACSS)*. 2012; 7-12.

XVII. Liang Y, Cai Z, Yu J, Han Q, Li Y. Deep learning based inference of private information using embedded sensors in smart devices. *IEEE Netw Mag* 2018; 32: 8–14.

XVIII. Liu X, Li K, Guo S and Liu A. Top-k queries for categorized RFID systems. *IEEE ACM T Network* 2017; 25(5): 2587–2600.

XIX. López T. S., Brintrup A., Isenberg, M A. and Mansfeld J. Resource Management in the Internet of Things: Clustering, Synchronization and Software Agents. In: Harrison, Mark, Uckelman, D and Michahelles, F, (eds.) *Architecting the Internet of Things*. Springer-Verlag. 2011; ISBN978-3-642-19156-5.

XX. 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*. 2018; 23(3): 419-431.

XXI. Nitti, M., Girau, R., Atzori, L. Trustworthiness management in the Social Internet of Things. *IEEE Trans. Knowl. Data Eng*. 2014; 26(5): 1253–1266.

XXII. P. K. Reddy, R.S. Babu. An Evolutionary Secure Energy Efficient Routing Protocol in Internet of Things. *International Journal of Intelligent Engineering and Systems*. 2017; 10(3): 337-346.

XXIII. Qiu T, Liu X, Li K and Hu Q. Community-aware data propagation with small world feature for internet of vehicles. *IEEE Commun Mag* 2018; 56(1): 86-91.

XXIV. Raja SP, Rajkumar TD, and Raj VP. Internet of Things: challenges, issues and applications. *J Circuit Syst Comp* 2018; 27(12).

XXV. Rajagopal, A. Soft computing based cluster head selection in wireless sensor network using bacterial foraging algorithm. *Int. J. Electron. Commun. Eng* 2015; 9(3): 379-384.

XXVI. Reena Varghese, Dr. T. Chithralekha, Carynthia Kharkongor. Self-organized Cluster Based Energy efficient MetaTrust model for Internet of Things. 2nd *IEEE International Conference on Engineering and Technology (ICETECH)*, Coimbatore, 2016.

XXVII. Sandeep K.E., Kusuma S.M., Kumar V.B.P. Fire-LEACH: A Novel Clustering Protocol for Wireless Sensor Networks Based on Firefly Algorithm. *International Journal of Computer Science Theory and Application*. 2014: 1(1): 12-17.

XXVIII. Sarma N.V.S.N, and Gopi M. Implementation of Energy Efficient Clustering Using Firefly Algorithm in Wireless Sensor Networks. *1st International Congress on Computer, Electronics, Electrical, and Communication Engineering (ICCEEECE2014)*, IACSIT Press, Singapore, 2014: 59.

XXIX. Sarobin V.R, Ganesan R. Bio-Inspired Cluster-Based Deterministic Node Deployment in Wireless Sensor Networks. *International Journal of Technology*. 2016; 4: 673-682.

XXX. Sarobin V.R, Ganesan R. Bio-Inspired Cluster-Based Deterministic Node Deployment in Wireless Sensor Networks. *International Journal of Technology*. 2016; 6: 673-682.

XXXI. Senthilnath J, Omkar S.N, Mani V. Clustering using firefly algorithm: performance study. *Swarm and Evolutionary Computation*. 2011: 1(3): 164–171.
XXXII. Sowmya Gali, and Venkatram Nidumolu. Multi-Context Trust Aware Routing For Internet of Things. *International Journal of Intelligent Engineering and System*. 2019;12(1): 189-200.

XXXIII. Z. Yan, P. Zhang, and A.V. Vasilakos,. A survey on trust management for Internet of Things. *J. Netw. Comput. Appl*. 2014; 42:120–134.

XXXIV. Zhang Q, Jacobsen RH, Toftegaard T. S.Bio-inspired low-complexity clustering in large-scale dense wireless sensor networks. *Global Communications Conference (GLOBECOM)*, Anaheim, CA. 2012;658-663.

XXXV. Zhihua Zhang, Hongliang Zhu, Shoushan Luo, Yang Xin, and Xiaoming Liu. Intrusion Detection Based on State Context and Hierarchical Trust in Wireless Sensor Network. *IEEE Access*, 2017; 5: 12088-12102.