Received: October 11, 2018

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Multi-Context Trust Aware Routing For Internet of Things

Sowmya Gali[1]* **Venkatram Nidumolu[1]**

[1]*Department of Electronics and Communication Engineering,*
Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India
* Corresponding author's Email: sowmya1046@gmail.com

Abstract: Security is a more important aspect in the IoT based communications due to the vast heterogeneity of devices used in the network. Considering the challenges in the provision of security in the IoT network, this paper proposes a new trust ensuring mechanism with multi contextual aspects including the interactions between the IoT nodes and their energy levels. Furthermore, a minimum hop count mechanism is also proposed to select a path with less processing delay. Combining all these multi facets, a composite routing metric is derived in this paper to define the trustworthiness of IoT node before choosing it as a next hop communicating node. An extensive simulations are carried out over the proposed approach by varying the network parameters and the performance is measured through the performance metrics namely, packet deliver ratio, malicious detection rate, network life time etc. The obtained Malicious detection rate and network life time of proposed approach outperforms the conventional approaches.

Keywords: IoT, Security, Communication trust, Energy trust, Packet delivery ratio, Malicious detection rate.

1. Introduction

In recent years, the Internet of Things (IoT) has gained a lot of interest due to its accomplishment in various areas including embedded systems, wireless sensor networks, automation, and micro-electromechanical systems (MEMS) etc. Actually the initial concept and implementation of IoT was started in the 1980s and became popular in 1990s [1]. Due to the vast development in the technology, the IoT also attained an accelerated evolution [2, 3]. In the present days, the applications of IoT exist nearly in every field and are playing an important role in the daily life [4] (e.g., environmental monitoring, home and building automation, health care systems, smart transportation systems, energy management, and infrastructure management). According to the survey carried out by Federal Trade Commission (FTC), the total number of IoT devices has already exceeded the number of working people in the working station [5, 6]. Further, it is approximated that by the year 2020, the total counts will be approximately 26 billion in number and also will be a greatly exceeds hub devices, including Personal Computers and smart phones etc. As a result, the IoT is trying to connect the real world to the virtual world by connecting the wide variety of non-traditional computing devices. However, connecting such stand-alone IoT devices with internet may bring so many challenges, like naming, scalability, inter-operability, mobility, resource constraints, privacy and security.

Various IoT architectures are developed to sort out these challenges and still some more problems are arising due to the typical natured devices (e.g. Heterogeneity) those connected to IoT. Expect the security and privacy the reaming challenges are solvable by changing the architectures of IoT. But, security is one major hurdle facing by IoT architectures. According to the standard definition of IoT [5], it is defined as "the connectivity between the internet and everyday objects and the ability to exchange the data between them". Due to this, potential security and privacy risks exist in broad manner, ranging from internet to the physical world and there is a possibility to harm to people. For example, a compromised IoT node may lead to attack on the other systems. Furthermore, depends

on the attack type, the compromised node also facilitates the leakage and misuse of personal information. A rupture in the internet may feedback to the real world and can create risks and threats to the physical safety of people.

Trust management is one of the security ensuring strategies to provide data protection and also the confidentiality of user's personal information [7]. Trust based security provision involves the evaluation of trustworthiness of devices which are in the IoT network and asks for help by other devices. The device which seeks the help measures the trustworthiness of its neighbor devices before forwarding data through it. A main problem with approaches towards defining the trust is that they do not lend themselves to the establishment of metrics and evaluation methodologies. Moreover, the satisfaction or trust requirements are strictly related to the identity management and access control issues.

This paper proposes a new trust aware routing framework for IoT network considering the multi-facet strategy to evaluate the trustworthiness. This multi-facet strategy considered the communication trust and energy trust to define the trustworthiness of a node in IoT network. Further, based on the hop count, one final path is selected for a given source and destination node pair.Due to the consideration of Multiple factors in the selection of forwarding node, the proposed approach is robust to both resource constraint and also for security constraints. Whereas, the conventional approaches only focused on single aspect either on energy or on security.Simulation experiments are carried out and the proposed approach is compared with conventional approaches.

Reminder of the paper is organized as follows: section II describes the literature survey details. Section III describes the proposed approach details. Simulation experiments are described in section IV and finally the conclusions are given in section V.

2. Literature survey

Various approaches are proposed in earlier to ensure the trust between the nodes communicating in the IoT network. A dynamic trust management mechanism was proposed by F. Bao and I. R. Chen [8] for a community-based social IoT environment by considering multiple social relationships among device owners. The three social relationships namely, Honesty, cooperativeness, and the community interest are considered to found the trustworthiness of nodes. Mainly [8] focused to make the network resilient to the Self-promoting attacks, good-mouthing and bad-mouthing attacks, but not focused on the energy efficinecy.

Recognizing that the smart objects in IoT are most likely human-carried or human-operated devices, B. Fenye and C. Ing-Ray [9] proposed a scalable trust management protocol for IoT, with the emphasis on social relationships. Each node performs trust evaluation towards a limited set of devices of its interest only. The trust management protocol is event-driven upon the occurrence of a social encounter or interaction event, and trust is aggregated using both direct observations and indirect recommendations. However, it can be argued against the weighting factor design in [8, 9] that estimating a node's trustworthiness when providing reports basing on its trustworthiness score when assisting in a service may lead to inaccuracies. An honest low-resource node can indeed be untrusted for providing assistance for cooperative services because of its resource constraints while still being able to provide good recommendations about other nodes assisting it.

A trust system based on behavior detection was proposed by Liu et.al. [10], which takes direct trust, recommended trust as well as history statistical trust into trust evaluation periodically and in communication. Recommended trust and history statistical trust were calculated by evidence combination and Bayes respectively [24].However, the main drawback of this method no node clustering.

A new distributed trust management mechanism for IoT is established by Wang et.al. [11] Firstly, it extracts three basic elements- service, decision-making and self-organizing, of trust management from the investigated trust solutions. Then, based on a service model, a trust management framework was established for the layered IoT, which is decomposed into three layers: sensor layer, core layer and application layer. Finally, the fuzzy set theory and formal semantics-based language were utilized to perform the layered trust mechanism. This process of trust evaluation constitutes an extra complexity and it is three times higher than the complexity of proposed approach.

Further, a new distributed trust evaluation model is proposed by Carolina et al. [12] to identify malicious behavior of nodes and prevent possible On-Off attacks to a multiservice IoT. The proposed trust management model uses direct information generated from direct communication with the nodes to evaluate trust between nodes. This distributed approach allows nodes to be completely autonomous in making decisions about the behavior of other

nodes.Furthermore, an indirect trust is also mandatory by which the security enhances.

Ben Saied et.al., [13] Proposed a novel trust management system (TMS) for the IoT that is able to induce from nodes past behaviors in distinct cooperative services how much trust can be put into a node for accomplishing a required task. Eventually, only the best partners with respect to a sought cooperative service are proposed to a requesting node.However, this work is not adaptive for IoT due to the dynamic environments such as varying attacks, varying malicious nodes ratio etc.

In [14], a formal trust management control mechanism was developed based on architecture modeling of IoT. Initially it decomposes the IoT into three layers, which are sensor layer, core layer and application layer, from aspects of network composition of IoT. Each layer is controlled by trust management for special purpose: self-organized, affective routing and multi-service respectively. And the final decision-making is performed by service requester according to the collected trust information as well as requester' policy. Finally, a formal semantics-based and fuzzy set theory is used to realize all above trust mechanism.Though this achieved good results at every layer, the network lifetime is observed to be less due to the non-focus over the energy constraints.

In the case of access models, the traditional access control model is not suitable to the nomadic, decentralized and dynamic scenarios in the IoT where identities are not known in advance. Mahalle et al., [15] proposed a Fuzzy approach to the Trust Based Access Control (FBAC) with the notion of trust levels for identity management. The presented fuzzy approach for trust calculations deals with the linguistic information of devices to address access control in the IoT.A trust and reputation model [17] is recognized as an important approach to defend a large distributed sensor networks in IoT against malicious node attacks, since trust establishment mechanisms can stimulate collaboration among distributed computing and communication entities, facilitate the detection of untrustworthy entities, and assist decision-making process of various protocols.This approach is effective in the provision of security for IoT devices but the IoT devices with limited resources, the network lifetime is very less due to the selection of only a single node every time.

In [16], based on in-depth understanding of trust establishment process and quantitative comparison among trust establishment methods, a trust and reputation model TRM-IoT was developed to enforce the cooperation between things in a network of IoT based on their behaviors. Further the TRM-IoT accomplished the fuzzy set theory to execute the proposed trust and reputation model. 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 an adaptive security model was proposed in [18] considering three basic facts such as recommendations, observations and experiences. It focused on the reduction of energy consumption in the mobile Adhoc Network. A clustering based trust mechanism proposed in [19] addresses the security problems in IoT. It finds the similarity of interest in every cluster through the Kalman filter to estimate the trust value in advance.

A trustworthy and secure sensing scheme is proposed in [20] based on the real alert policy. In this scheme, the trust evaluation considers the anomalous data and contextual information which represents the environment from which the anomalous data was acquired. The policy rues defines the trust evaluation mechanism under different situations. For an outdated policy, a new device or a new normal observation is considered as an attacker or malicious.

A multidimensional trust evaluation model is suggested in [21] in which the direct trust value is measured form the network communication. Under multidimensional trust, the delay, consistency of packet content, repetition rate, packet forwarding capacity, and integrity rate are measured through the D-S theory. However as the number of devices increases, the evaluation of multidimensional trust at every node results in more delay and continuously streaming data is complex to manage with conventional network communication analysis methods.

A trust relationship based trust evaluation is proposed for clustered WSN in [22]. The trust relationship considers the message, communication, energy factors for each trust factor to detect the attacks. A low-cost and lightweight algorithm is proposed in [23] to detect selective forwarding attack [25] in the Internet of things based on packet ID check. Namely, any cluster head will compare the received packet ID with its local record, and update local recorded ID, the result of inspection is used to decide if any suspicious node exists or not. The cluster head will send a warning packet to the base station to report a suspicious node. The base station judges malicious nodes by the reported suspicious times.

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 [26]. An optimal Secure and Energy Aware Protocol (OSEAP) and an Improved Bacterial Foraging Optimization (IBFO) algorithm were accomplished here. However, the FCM algorithm won't suits 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.

3. Multi-context trust aware routing (MCTAR)

This section describes the details of proposed Multi Context Trust Aware Routing (MCTAR). Under the multi context concept, this approach considered the trustworthiness, energy and hop count in the selection of route. Since the energy is also an important factor, this approach focused to reduce the overall energy consumption also. Furthermore, the delay also plays a significant role in the success of data transmission, this approach considered the hop count in the establishment of an optimal route. Three different factors are allocated for each context to signify the effect of that particular aspect.

3.1 Trust evaluation

In this paper, a new trust evaluation mechanism is proposed for IoT framework to detect the malicious nodes, which considers the Communication Trust. Meanwhile it reduces the possibility of misleading by malicious nodes in the process of trust evaluation through network related issues such as number of communication instances and the probability of successful data delivery. Here the communication trust is evaluated both directly and indirectly.

3.1.1. Communication trust

The Communication Trust evaluates the trustworthiness of neighbor nodes by overhearing their transmission in promiscuous mode and dynamically identifies misbehaving nodes. Here the Communication Trust is evaluated by the number of successful and unsuccessful interactions between the nodes. The node overhears the neighbor node if it doesnot deliver a packet or transmits the packet is the predefined time interval. The acknowledgement about the success of packet delivery can be notified to the source node. If the packet sent by a node reaches to any other node within its transmission range within a predefined time interval, it is considered as successful communication otherwise it is considered as unsuccessful communication.

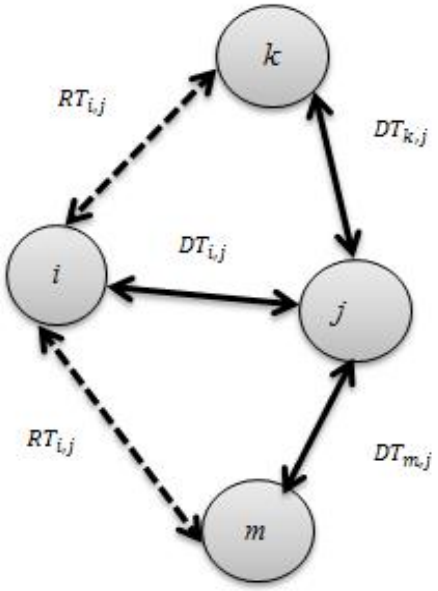
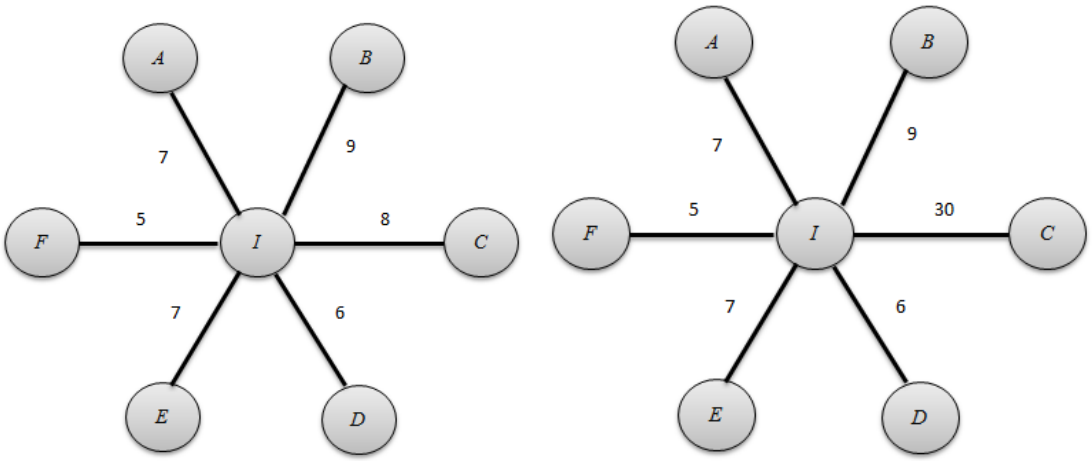


Figure. 1 Direct and recommended trust evaluation

For instance, if an IoT node is attacked by an attacker and a selective forwarding attack or black hole attack was launched over it, then only a partial set of packets are forwarded from that node to its next hop node. A ratio between the total numbers of successful communications to the total number of communications declares the degree of trustworthiness. A higher value indicates the higher trust degree and a lower indicates the malicious behavior. Based on this ratio, every node evaluates the trustworthiness of all of its neighbor nodes. Here the communication trust is measured in two directions, one is direct evaluation and another is recommended evaluation. In case of direct trust evaluation, the IoT node measures the total number of successful communications happened between them. In the case of recommended trust evaluation, the trustworthiness of an IoT node is evaluated through the neighboring nodes of that IoT node. A simple schematic representing the direct and recommended trust is shown in Fig.1.

For every IoT node, the recommended trust is evaluated through the set of neighbor nodes within



(a) (b)

Figure. 2 The sample graph showing communication interactions between nodes in the network

the transmission range. The communication trust $CT_{i,j}$ can be defined as a weighted aggregated sum of two components.

$$CT_{i,j} = w_1 \times DT_{i,j} + w_2 \times \sum_{k=1}^{K} \frac{RT_{k,j}^{i}}{N_k} \quad (1)$$

$DT_{i,j}(t)$ denotes the degree of direct trust between node i and node j, based on the node i's observation of packet forwarding behavior for node j. $RT_{k,j}^{i}$ is the indirect/recommended trust gained by the node i through the neighboring node k of node j. N_k represents a set consisting of neighbors for node j. The weight factors w_1 and w_2 are assigned to $DT_{i,j}$ and $RT_{k,j}$ respectively, such that $w_1 + w_2 = 1$, whereas $0 \leq w_1 \leq 1$ and $0 \leq w_2 \leq 1$. An indirect trust is determined from the observations gained through interactions with neighbors who notifies about their own direct observation for particular node. The indirect trust $RT_{k,j}(t)$ is determined using Eq. (2).

$$\sum_{k \in N_k, k \neq j} RT_{k,j}^{i} = \sum_{k \in N_k, k \neq j} DT_{i,k} \times DT_{k,j} \quad (2)$$

Where $DT_{i,k}$ represents the direct trust between the node i and neighboring node k of node j and $DT_{k,j}$ represents the direct trust between the node j and neighboring node k. Since there existsN_k number of neighboring nodes for every node, the summation is used in the Eq. (2). The evaluated recommended trust is exchanged as a part of recommendation with node k. Trust estimation involving trust degree of each node using indirect trust information brings several benefits. First, it speeds-up the convergence of trust evaluating process. Second, a node can detect and isolate misbehaving nodes at earliest. Third, neighbors' recommendation information enables the nodes that do not succeed in observing behavior of their neighbors due to resource limitations.

Table 1. Communication trust results of Fig. 2

Nodes	Evaluated result of 2.(a)	Evaluated result of 2.(b)
A	7	7
B	9	9
C	8	30
D	6	6
E	7	7
F	5	5

Two example graphs are shown in Fig. 2 (a) and (b). In the graph, G, a set of IoT nodes, {A,B,C,D,E,F} are considered which interacted with node {I} and the values marked on the edges between Node {I} and remaining nodes is considered as number of interactions happened between them. As it can be observed from the Table.1, the evaluated results at first cycle t are represented in Fig. 2 (a) and in the Table 1, it is shown in the second column. Further the number of communication interactions happened after the cycle $t+1$ are shown in Fig. 2 (b) and in the third column of Table 1.

Form the Table.1, it can be observed that, except the number of interaction between node I and node C, the interaction of node I with remaining nodes is constant for both cycles t and $t+1$. The difference between the interaction happened at cycle t and at cycle t+1 between node I and node C are observed

to be very high. Hence the node C can be declared as a malicious node in the context of communication trust.

3.1.2. Energy trust

The nodes in the IoT network will choose the nodes with high trust degree as next hop node for forwarding information in the conventional approaches developed for security model, which aggravates the energy consumption of nodes with higher trust degree, thus resulting in an uneven network load or even network segmentation. Hence there is a need to consider the energy also as a significant factor in the trust evaluation. Since the energy is a necessary thing for both reception and transmission of data form every IoT node, this approach considers both contexts including the reception and transmission states for energy trust evaluation. The mathematical representations for the energy cost for reception and transmission are represented as

$$RC(k,d) = E_{elec} \times k \quad (3)$$

$$TC(k,d) = E_{elec} \times k + E_{amp} \times k \times d^2 \quad (4)$$

Where RC is receiving Cost, TC is transmitting cost, k is the number of message bits, d is the distance between node i and node j.E_{elec}represents the unit energy consumption for transmitting the message at node j, and E_{amp} represent the unit energy consumption for achieving particular SNR during transmission. The total energy consumption cost at node j can be estimated as the sum of receiving energy and transmitting energy and it is obtained as;

$$TEC = 2 \times E_{elec} \times k + E_{amp} \times k \times d^2 \quad (5)$$

If the initial energy of a node is EB, the remaining energy ES of node j is measured as

$$ES = EB - TEC \quad (6)$$

Based on the above equation, a capability of a node will be decided whether it is able to cooperate with other nodes or not in the data transmission. The remaining energy ES of a node is compared with a predefined threshold, E_{th} and if it is greater that the threshold E_{th}, then that particular node is said to be capable otherwise it cannot participate in the data transmission. Though the node is observed as high trustworthy, if its ES is less than the threshold, it cannot participate in the data transmission. Based on these, the trust degree of node j with respect to the energy is defined as

$$ET_y = \begin{cases} 1, & ES \geq E_{th} \\ 0, & ES < E_{th} \end{cases} \quad (7)$$

In this manner, based on the energy levels of node, it can be selected as next hop node for forwarding data if it has sufficient energy trust degree. Similar to the Communication trust evaluation, the energy trust also measured both in direct fashion and recommended fashion. The total energy trust between node *i* and node *j* can be measured as

$$ET_{i,j} = w_1 \times DET_{i,j} + w_2 \times \sum_{k=1}^{K} \frac{RET_{k,j}^{i}}{N_k} \quad (8)$$

$DET_{i,j}$ denotes the degree of direct energy trust between node *i* and node *j*, based on the node *i*'s observation for node *j*. $RET_{k,j}^{i}$ is the indirect/recommended energy trust gained by the node *i* through the neighboring node *k* of node *j*. Similar to the illustration given in the communication trust evaluation, the recommended trust is an average trust of *k* neighboring node of node *i.* The recommended energy trust $RET_{k,j}(t)$ is determined using Eq. (9).

$$\sum_{k \in N_k, k \neq j} RET_{k,j}^{i} = \sum_{k \in N_k, k \neq j} DET_{i,k} \times DET_{k,j} \quad (9)$$

Where $DET_{i,k}$ represents the direct energy trust between the node *i* and neighboring node *k* of node *j* and $DET_{k,j}$ represents the direct trust between the node *j* and neighboring node *k*.

3.2 Hop count

Along with communication trust and energy trust, the proposed approach also considered hop count also during trust evaluation. In an IoT network, achievement of more secure path is an important but the path would not lead to be an excessive delay in the data transmission. A secure path may be long or may be short. In the case of short and secure path, the data transmission won't get effected but in the case of longer and secure path, the data will not deliver in the correct time. This process leads to an excessive delay. Furthermore, based on the characteristics of paths, there is a possibility to attack on the IoT. Hence, the path needs to change every time and it also should be a short length path. Hence, this paper considered the hop count also as an important factor in the evaluation of trustworthiness.

In the proposed MCTAR scheme, the path length is measured in terms of hop count. The path with minimum hops is selected as optimal path. The main problem arisen here is the selection criterion to choose a path with minimum delay. There is a possibility of a path with minimum number of hops may have longer hop lengths by which the security tolerance will be decreases. To overcome this issue, here a new process of path length evaluation is proposed which combines the hop length along with hop count. Here the path selection is not only based on the hop count but also considers the length of every hop. The path with minimum hops and with minimum hop lengths is selected as an optimal path. This is includes at the stage of path selection. Here the basic Euclidean distance metric is used for the path length evaluation.

3.3 Composite route metric (CRM)

Based on the above trust evaluations, a new routing metric is evaluated which defines the degree of trustworthiness of IoT nodes. The combined routing metric, CRM is defined as the summation of Communication trust, the Energy trust and hop count, represented as

$$CRM_{i,j} = \alpha \times CT_{i,j}(t) + \beta \times ET_{i,j} + \gamma \times HC \quad (10)$$

Where α, β and γ are the three arbitrary constants which determine the weightage of communication rust and energy trust and hop count respectively and has to satisfy $\alpha + \beta + \gamma = 1, s.t. 0 \leq \alpha \leq 1, 0 \leq \beta \leq 1$ and $0 \leq \gamma \leq 1$. HC represents the Hop Count. The higher the weight, the more importance to that sub trust to the overall trust and vice versa. In the case of higher α, the overall trust constitutes with communication trust and in the case of higher β value, the energy trust is more consistent to total trust. Since this method is mainly focused on the trust and secure path, prior importance is given for first two arbitrary constants. The third constant, γ is only to signify the effect of hop count only. Initially, the two arbitrary constants α, and β are chosen and the γ is measured as $\gamma = 1 - (\alpha + \beta)$.

4. Simulation results

This section describes the details of simulation experiments performed over the proposed trust mechanism and the obtained performance results including the average packet delivery ratio, End-to-End Delay, Packet Loss Ratio, Malicious Detection rate, False Positive Rate, and Network lifetime. All these metrics are measured with varying number of malicious nodes. To simulate the proposed framework, an IoT network with P number of nodes is created with an area of M×N, where M is the length and N is the width of the network. The simulation parameters are listed in Table.2.

Table 2. Simulation parameters

Parameter	Value
Number of nodes	30-100
Area	1000*1000 m^2
Mac	IEEE 802.11
Simulation Time	50 Sec
% Malicious behavior	0-50% of total nodes
Traffic Source	CBR
Transmission Range	250 m
Node placement	Random
Packet size	512 bytes
Trust threshold	0.6
α, β, γ	$0 \leq \alpha, \beta, \gamma \leq 1$

4.1 Simulation Setup

Table 2 shows the simulation parameters.

4.2 Performance metrics

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.

Average Packet loss Ratio (APLR):APLR is defined as the total number of packets lost to the total number of packets received at the respective node. The higher value of APLR indicates the bad performance and the lower value indicates the good performance.

End-to-End Delay (E2ED): E2ED is defined as the total time taken by the data to transfer from source node to destination node. For any routing approach, the E2ED must be less. A lesser value of E2ED indicates the good performance and higher value indicates the bad performance.

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 malicious when they are not malicious and vice versa. Higher FPR indicates the bad performance and lower FPR indicates good performance.

Network Lifetime (NL): NL is defined as the maximum extent of timespan up to which the network can withstand without any route failures. Due to the occurrence of attacks and more energy consumption, the network lifetime decrease. Higher NL indicates the good performance and lower NL indicates bad performance.

4.3 Results

In the simulation study, the performance evaluation is carried out by measuring the performance metrics, APDR, APLR, E2ED, MDR, NL and FPR for varying number of malicious nodes. Since the proposed approach focused on the trust awareness, at every node the trust evaluation, the trustworthiness evaluation is accomplished with the surrounding neighbor nodes and based on the obtained trust values, one node is selected for further communication. This process is repeated at the other nodes also if the destination is too far in which the multi-hop communication will come into picture. In the simulation study, the performance is evaluated by varying the % of malicious nodes as 5, 10, 15, 20 and 25. For example, if N = 100 nodes are there in the network, only 5 nodes are considered as malicious at 5% maliciousness. In this manner, the malicious of IoT network is increased and at every stage, the performance is measured through the performance metrics through the proposed and conventional approaches. The obtained results are depicted in the following figures.

When the maliciousness increases in the network, the attacked/compromised node won't help to the other nodes in the data transmission. And also they try to drop the packets intentionally. When the packets are dropped at intermediate node due to their maliciousness, the packet won't reach to the destination by which the packet delivery ratio decreases. This PDR will reach to higher levels with an increase in the malicious nature. It can be seen from Fig. 3 that the APDR is decreasing with increment the in the % of malicious nodes. However the APDR of proposed is observed to be high when compared to the conventional approaches. Due to the non-consideration of information trust in TRM-IOT, the overall trust is just related to the communication trust which reveals only the number of interactions. This process is not able to find the malicious nodes which are compromised through the data processing through them. Hence the conventional approaches can't provide sufficient APDR. Next, the recent conventional approach OSEAP-IOT [26] not effective due to its simplicity in the trust evaluation strategy. The optimality of OSEAP-IOT only helpful in the selection of optimal node but not optimal trustworthy nodes. Furthermore, this approach is not able to track the malicious nodes effectively due to no such mechanism proposed in [26].

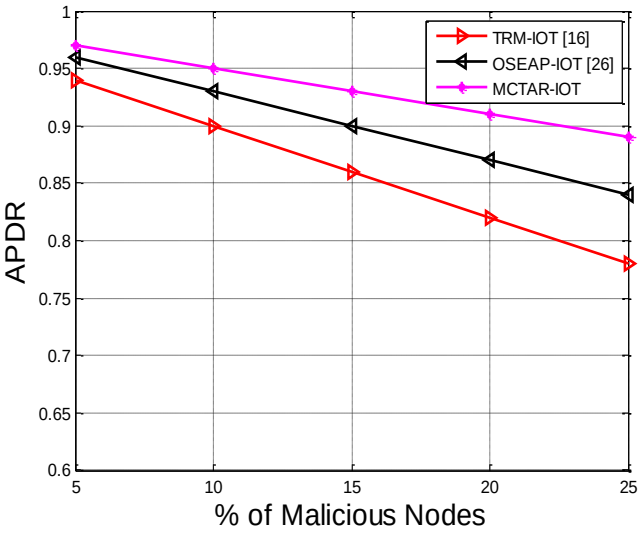


Figure. 3 Average packet delivery ratio for varying malicious behavior

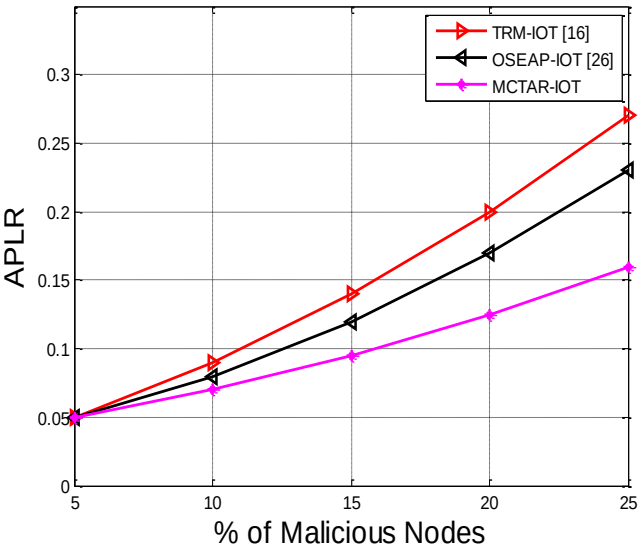


Figure. 4 Average Packet Loss Ratio for varying malicious behavior

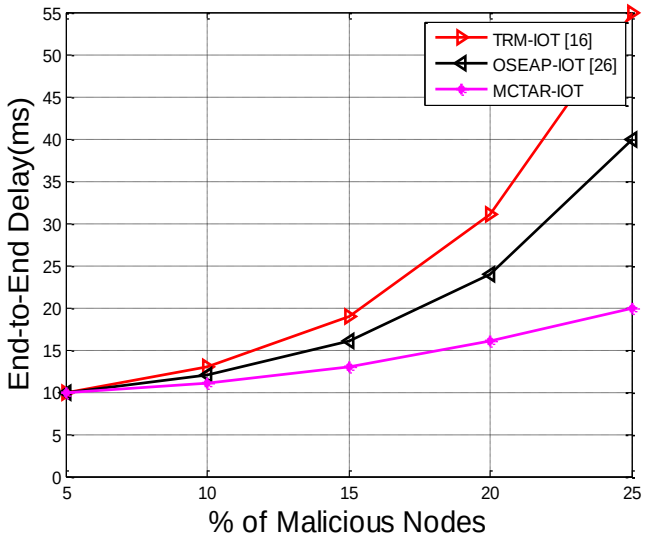


Figure. 5 End-to-End Delay (msec) for varying malicious behavior

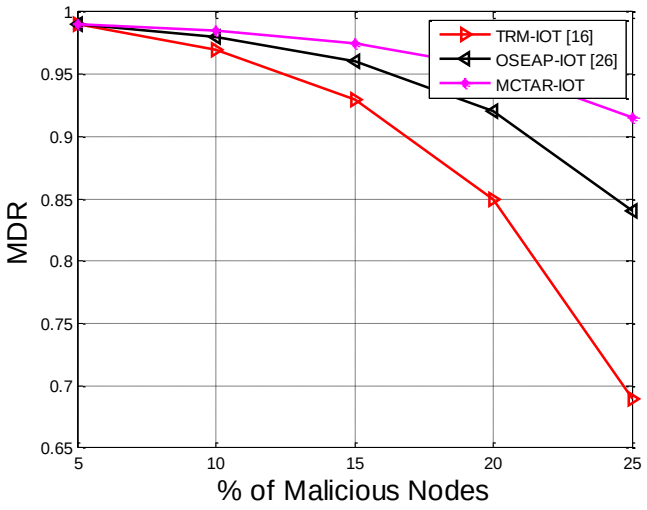


Figure. 6 Malicious detection rate for varying malicious behavior

As shown in the Fig. 4, the obtained average packet loss ratio, when the proposed approach is accomplished over the Network, is observed as increasing in nature with increment the number of malicious nodes. As the % of malicious behavior increases, the number of malicious nodes also increases and makes the network to compromise more and forces the adversary nodes to drop the packets instead of forwarding them. However, the PLR of proposed approach is less compared to the conventional approaches. Since the proposed approach accomplishes the trust evaluation with respect to both the communication interactions and energy acquired at every node, the packets transmitted from source to destination will reach more effectively and only few packers will get lost, whereas in the TRM-IOT and OSEAP-IOT, the security evaluation mechanism didn't considered the multi-dimensional trust (CT and ET) which effects the packets transmission and forces the nodes to drop the packets. Both of the conventional approaches are not proposed a strict method trust evaluation at node level which results in an inappropriate ode selection as a forwarding node.

As the number of malicious nodes increase, the End-to-End Delay also increases, because, the malicious node won't send any notification about the packet forwarding or packet reception to the pre-hop node. The pre-hop nodes wait for TTL and reroutes the packet if it was not received any update from its next hop time. This rerouting process results in an increased delay and it is too much with increase in the malicious nature. As it can be seen from the Fig. 5, the End-to-End Delay of proposed approach is less even though there is an increment in the % of malicious nodes, because of the accomplishment of multi-context trust evaluation in the selection of next hop node. Though there is an increment in the End-to-End Delay, the increment due to the proposed MCTAR-IOT is observed to be less due to the provision of alternative routes in the case of over maliciousness and energy drain. However, in the conventional approaches there is no provision of multiple routes for data transmission. This results in a new route establishment process which produces an excessive delay.

To realize the proposed trust aware routing mechanism, initially a random network is created with some set of nodes. In the run time, out of complete set of nodes, few nodes are declared as malicious nodes to check the performance. Since the proposed approach is developed to detect the malicious node and to skip that particular malicious node through which the path is going on. Here the performance is evaluated by counting the total number of nodes detected as malicious when they are really malicious. The ratio of these two values gives the metric called malicious detection rate. As it can be seen form the Fig. 6, the MDR of proposed MCTAR-IOT is more compared to the conventional approaches, TRM-IOT and OSEAP-IOT. Because, the MCTAR-IOT is proposed to select a path between two nodes based on the both communication and energy trust values. This phenomenon helps in the detection of malicious nodes more accurately. This is the mai drawback of conventional approaches.

Similarly, the one more metric, false positive rate is also evaluated to check the performance of proposed MCTAR-IOT mechanism in the detection of malicious nodes. The obtained FPR results for varying malicious nodes are depicted through Fig. 7

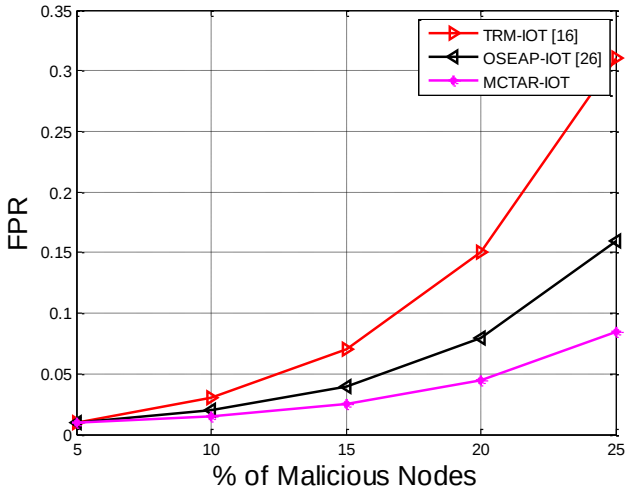


Figure. 7 False positive rate for varying malicious behavior

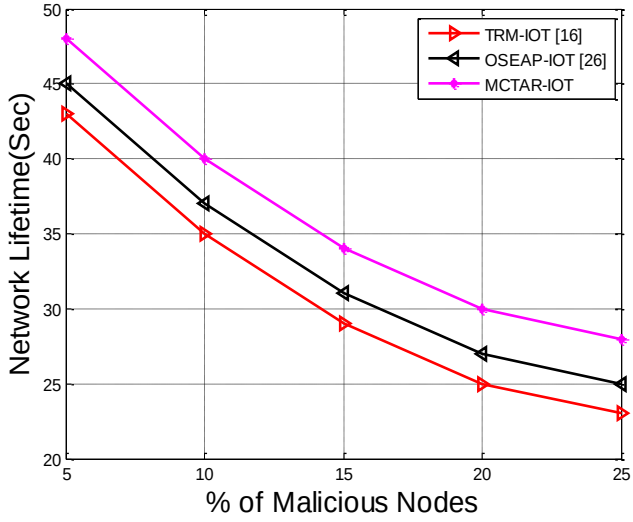


Figure. 8 Network lifetime (Sec) for varying malicious behavior

and the FPR of proposed approach is observed to be less compared to the conventional approaches. Here the FPR is simply referred as opposite to the MDR. As the MDR increases, the FPR decreases and vice versa.

For the conventional approaches, the MDR is lowand FPR is high due to the non-effective strategy for secure and energy efficient node selection which ensures the secure transmission of data in IOT network.

Due to the accomplishment of smart and resource constraint natured devices in the IoT based applications, they need to utilize in an organized way by which the overall network lifetime increases. The network lifetime is directly related to the energy consumed at every IoT node. As the malicious nature increases in the network, the reliable nodes needs to search for route establishment again and again which results in an excessive power consumption. As the energy of nodes losses, the nodes will get die and the overall network lifetime also affected. As it can be seen from Fig. 8, the graph of Network Lifetime is decreasing with increasing the number of malicious nodes. But, it is observed to be high when the network lifetime of TRM-IOT and OSEAP-IOT is compared with proposed MCTAR-IOT. Since the propose routing methodology is effective in the selection of most trustworthy node, the information reached at that node won't get lost and the extra burden occurs due to the rerouting will be avoided.

5. Conclusion and Future Scope

To ensure the secure communications between nodes of an IoT network, all possible directions like communication, energy, resource etc., are need to be considered by which a more efficient results will be obtained in the detection of malicious nodes which tries to compromise the network in different ways. This paper developed a new multi-context trust aware routing by considering the energy behavior and communication behavior of IoT nodes as a main context. Further to ensure a secure and less delay path, this mechanism also approached to the minimum hop count path, i.e., shortest path. Provision of a multiple aspects in the route establishment has achieved an effective performance and it is revealed through the simulation conducted over the developed mechanism. The performance enhancement is also shown by comparing the obtained APDR, MDR, network lifetime through the proposed MCTAR 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 approach obtained an increased APDR of 7% and 3% from the TRM-IOT and OSEAP respectively. Next, the increment in the MDR through the proposed MCTAR is observed as 7.8112% and 2.6341% from the TRM-IOT and OSEAP respectively. Next, the increased network lifetime is observed as 10% and 8% from the conventional approaches.

To further achieve an increased security for IoT, this work can be extended by designing the trust evaluation model for Cluster Heads also. It can design under the state context and following a hierarchical trust between the CH and nodes will improve the secure and effective communications in IoT.

References

[1] K. Ashton, "That Internet of Things", *RFID Journal*, Vol. 22, No. 6, pp.97-114, 2009.

[2] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A Survey", *Computer Networks*, Vol.54, No.15, pp.2787-2805, 2010.

[3] D. Giusto, A. Lera, G. Morabito, and L. Atzori, "The Internet of Things: 20th Tyrrhenian Workshop on Digital Communications", *eBook*, Springer, New York City, NY, USA, 2010.

[4] Y. Kawamoto, H. Nishiyama, M. Fadlullah, and N. Kato, "Effective Data Collection Via Satellite- Routed Sensor System (SRSS) to Realize Global- Scaled Internet of Things", *IEEE Sensors Journal*, Vol.13, No.10, pp.3645-3654, 2013.

[5] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: vision, applications and research challenges," *AdHoc Networks*, Vol. 10, no. 7, pp. 1497–1516, 2012.

[6] R. Roman, P. Najera, and J. Lopez, "Securing the internet of things", *Computer*, Vol. 44, No. 9, pp. 51–58, 2011.

[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, No.6, pp. 120-134, 2014.

[8] F. Bao and I.-R. Chen, "Dynamic trust management for internet of things applications", In: *Proc. of the International Workshop on Self-aware Internet of Things*, pp.1-6, 2012.

[9] B. Fenye and C. I. Ray, "Trust management for the internet of things and its application to service composition", In: *Proc. of IEEE International Symposium on World of Wireless, Mobile and Multimedia Networks*, pp.1-6, 2012.

[10] Y. B. Liu, X. H. Gong, and Y. F. Feng, "Trust system based on node behavior detection in Internet of Things", *Tongxin Xuebao Journal on Communications*, Vol. 35, No.5, pp. 8-15, 2014.

[11] J. P. Wang, S. Bin, Y. Yu, and X. X. Niu, "Distributed Trust Management Mechanism for the Internet of Things", *Applied Mechanics and Materials*, Vol. 347, No.8, pp. 2463-2467, 2013.

[12] V. L. M. Carolina and H. K. João, "Mitigating On-Off Attacks in the Internet of Things Using a Distributed Trust Management Scheme", *International Journal of Distributed Sensor Networks*, Vol. 2015, No.11, pp.1-8, 2015.

[13] Y. BenSaied, A. Olivereau, D. Zeghlache, and M. Laurent, "Trustmanagement system design for the Internet of Things: A context-awareand multi-service approach", *Computers & Security*, Vol. 39, No.2, pp.351-365, 2013.

[14] L. Gu, J. Wang, and B. Sun, "Trust management mechanism for Internetof Things", *China Communications*, Vol. 11, No.2, pp. 148-156, 2014.

[15] P. N. Mahalle, P. A. Thakre, N. R. Prasad, and R. Prasad, "A fuzzy approach to trust based access control in internet of things", In: *Proc. of International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems*, pp. 1-5, 2013.

[16] D. Chen, G. Chang, D. Sun, J. Li, J. Jia, and X. Wang, "TRM-IoT: Atrust management model based on fuzzy reputation for internet of things", *Computer Science and Information Systems*, Vol. 8, No.4, pp. 1207-1228, 2011.

[17] A. Boukercha, L. Xua, K. EL-Khatibb, "Trust-based security for wireless ad hoc and sensor networks", *Computer Communications*, Vol. 30, No. 11-12, pp. 2413- 2427, 2007.

[18] H. Hellaoui, A. Bouabdallah, and M. Koudil, "TAS-IoT: Trust-Based Adaptive Security in the IoT", In: *Proc. of the 41st IEEE Conference on Local Computer Networks*, pp.599–602, 2016.

[19] O. Ben Abderrahim, M. H. Elhdhili, and L. Saidane, "TMCoIS-IOT: A trust management system based on communities of interest for the social internet of things," In *Proc. of the 13th IEEE International Wireless Communications and Mobile Computing Conference*, pp. 747–752, 2017.

[20] W. Li, H. Song, and F. Zeng, "Policy-based secure and trustworthy sensing for internet of things in smart cities", *IEEE Internet of Things Journal*, Vol. PP, no. 99, pp. 1-1, 2017.

[21] Y. Yu, Z. Jia, W. Tao, B. Xue, and C. Lee, "An efficient trust evaluation scheme for node behavior detection in the internet of things", *Wireless Personal Communications*, Vol. 93, No. 2, pp. 571–587, 2017.

[22] T. Zhang, L. Yan, and Y. Yang, "Trust evaluation method for clustered wireless sensor networks based on cloud model," *Wireless Networks*, Vol.24, No.3, pp.777-797, 2018.

[23] H.U. Xiang-dong, Y.U. Peng-qin, and W. Qin-fang,, "Detection of Selective forwarding attack in internet of Things", *Journal of Chongqing university of posts and telecommunications*, Vol.24, No.2, pp. 148-152, 2012.

[24] T. Liu, Y. Xiong, W. Huang, L. U. Qiwe, and X. Gong, "Node behavior and identity based trust authentication in wireless sensor networks",

Journal of Computer Applications, Vol. 33, No. 7, 99.1842-1845, 2013.

[25] B. Xiao, B. Yu, and C. Gao, "CHEMAS: identify suspect nodes in selective forwarding attacks", *Journal of Parallel and Distributed. Computing*, Vol. 67, No. 11, pp. 1218-1230, 2007.

[26] P. K. Reddy and 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.