Journal of Science and Technology

ISSN: 2456-5660 Volume 9, Issue 4 (April -2024)

DOI:https://doi.org/10.46243/jst.2024.v9.i4.pp74-83

Trusted Net: A Lightweight Cluster-Based Trust Sensing System for IoT Networks

[1] G. Rajesh Babu, [2] K. Vaishali, [3] K. Hema Madhuri, [4] E. Deepika, [5] K. Kedharnath Chowdary.

[1] [2] [3] [4][5] Department of Electronics and Communication Engineering, Usha Rama College of Engineering and Technology, Telaprolu, Unguturu, India.

A. To Cite this Article

G. Rajesh Babu, K. Vaishali, K. Hema Madhuri, E. Deepika, K. Kedharnath Chowdary. " Trusted Net: A Lightweight Cluster-Based Trust Sensing System for IoT Networks." ***Journal of Science and Technology, Vol. 09, Issue 04 - April 2024, pp74-83***

B. Article Info

Received: 29-02-2023 Revised: 01 -03-2024 Accepted: 27-03-2024 Published: 16-04-2024

Abstract— The Internet of Things is founded on the premise that objects in the human living environment can be connected to the Internet. Adoption of the Internet of Things cannot be permitted until security issues are addressed. Security solutions for the Internet of Things can be built on unique designs such as partitioning a mobile network into clusters managed by a cluster head, often known as clustering. However, without any security considerations, the clustering process is vulnerable to a variety of security-related internal attacks. A trust management system, which has proven its security efficiency and friability in mobile networks, might be used to defend the IoT against rogue nodes within it. In this research, we provide a trust-based clustering technique for the Internet of Things. Trust Sensing has played an important part in dealing with security concerns. A novel Light Weight Clustered Trust Sensing (LWCTS) Mechanism has been created with the primary goal of reducing The amount of energy that IoT nodes use. The LWCTS first clusters the network and chooses highly resourced Cluster Heads. Additionally, two components are considered in the proposed trust model: the mobility component for trust sensing and the interactive trust factor. The primary purpose of mobility factor inclusion in the network is to reduce the number of false positives.

Index Terms: Clustering, Light Weight Clustered Trust Sensing, Internet of things, Wireless Sensor Network.

I.INTRODUCTION

The Internet of Things (IoT) was first proposed in 1998 [1] as an extension of the current Internet, allowing items to communicate directly or indirectly with Internet-connected electrical devices. IoT can be defined as a collection of independent systems that operate with their own infrastructures, which are built in part on the current Internet infrastructure. It includes three types of communication that can take place in restricted areas : person-to- person, object-to-object, and machine-to-machine. Using a variety of technologies, including RFID and sensor networks, items will be remotely found, identified, monitored, and controlled. This will result in a global and pervasive network that will help to construct intelligent and low-consumption cities for residents. Furthermore, the connecting of physical items with the Internet should amplify the already enormous network communications impact on society on a wide scale, gradually resulting in a genuine paradigm shift [2]. The IoT architecture is typically separated into three tiers [3]: the perception layer (context aware tier), the network layer, and the application layer. The perceptual layer is an important layer that collects heterogeneous information using physical

ISSN: 2456-5660 Volume 9, Issue 4 (April -2024)

DOI:https://doi.org/10.46243/jst.2024.v9.i4.pp74-83

equipment such as RFID readers, GPS devices, and sensors. The second level is the network layer, which forms the heart of the IoT. It integrates numerous wired and wireless networks to accurately communicate information. It ensures that information is reliably transmitted from the perceptual layer to the application layer. Finally, the application layer delivers personalised services based on the needs of a mobile device.

Security in this network should be included into all layers. However, this cannot be accomplished until Iot security concerns are addressed by developing new protocols tailored to Iot characteristics and limits, as security methods employed on the Internet are not appropriate for the IoT. Furthermore, IoT encompasses a diverse range of objects from multiple contexts, including human surroundings, sensor networks, mobile communications, and the Internet. Thus, security solutions should consider heterogeneity and privacy. Traditional security measures, such as encryption and key management, are successful against external attacks but useless against internal attacks because rogue nodes in a network can act appropriately in some situations but wrongly in others. Thus, establishing a trust management system could be useful in mitigating these malevolent behaviours. The Internet of Things (IoT) enables bright articles and savvy frameworks to collect and share information globally, allowing for smart climate [1]. There is a growing interest in the application of remote detection technologies in many IoT scenarios. Given the rapid development of objects and their applications, acquiring and analysing their item information is becoming one of the most difficult challenges. Sensor hubs are powered by batteries, so energy-efficient activities are essential. Thus, it is alluring for the sensor centre point to de-duplicate the data got from the connecting centre points before conveying the last data to the central station. Data amassing [2,3] is one of the strong systems to clear out data unmistakable dullness and further foster energy efficiency; extending the lifetime of distant sensor associations (WSNs). A troublesome issue for information the executives is really convey information to important clients. It utilizes practical strategies, for example, proficient stream circulation frameworks for IoT [4]. The framework gathers incorporated information streams created from various authorities and communicates applicable information to pertinent clients in light of client questions went into the framework [5]. Make two new information designs to meet the prerequisites of high proficiency information stream engendering in two circumstances, for example, highlight point frameworks and stream proliferation in remote transmission frameworks. Evaluation of approaches utilizing genuine world datasets demonstrates the way that they can communicate associated information streams more productively than current innovation [6]. In IoT progresses, various information arrangements are suggested for proficient information handling and negligible information recuperation. This incorporates putting away brought together information, like the cloud framework, on neighbouring circulation frameworks. Savvy urban communities are the useful execution of IoT, which plans to furnish individuals with productive, solid and secure applications, for example, water, power and transportation through sane administration [7].

II. METHODOLOGY

A. LIGHT-WEIGHT CLUSTERED TRUST SENSING (LWCTS)

In this paper a new trust sensing mechanism called Light- Weight Clustered Trust Sensing Mechanism for IoT (LWCTS_IoT) is proposed. Initially, the proposed model employs a clustering mechanism to group up the nodes in IoT. Euclidean distances between IoT nodes are computed in order to perform the grouping. Among the clustered nodes one node is selected as the cluster head which has huge resources. Furthermore, trust sensing is implemented through which the CH senses the trustworthiness of other CHs for forwarding the data to the destination. In IoT, the destination lies very far away from the source. Hence even the CH needs additional nodes to forward the data to the destination. For this purpose, the CH senses the trust worthiness of other CHs and selects one CH for forwarding the data. In the phase of trust sensing, the CH nodes measure the interactive trust and mobility factors to find a more secure and trustworthy node that can ensure a great QoS and data security.

B. Clustering

In an IoT network, the nodes have limited energy, bandwidth, memory, and processing capabilities. Hence if the entire nodes are engaged to execute the tasks, then they will show a huge impact on the network lifetime. Moreover, the IoT nodes process data that are larger, and the additional processing tasks make the nodes die quickly. The CH is tasked with doing the majority of the processing work, and the IoT nodes are grouped together to lessen this extra load. The CH needs more resources in order to complete the significant processing task. Hence CH is selected based on the energy means among the cluster nodes the nodes which are rich in resources are

ISSN: 2456-5660 Volume 9, Issue 4 (April -2024)

DOI:https://doi.org/10.46243/jst.2024.v9.i4.pp74-83

selected as CHs. Here the normal nodes (cluster nodes) execute the simple task data transfer, while the CH executes the data collection from multiple IoT nodes and forwards for further CH or destination. The IoT node is only responsible to send its data after sensing. Once the data from each cluster node are received at CH, then it finds and forwards the received data to the destination or next CH (if the destination lies far from the CH, then it seek the help of other CHs). If the data is within the destination's communication range, the CH will send it immediately; otherwise, it will send it in numerous hops as needed [21–23]. Think of an Internet of Things network that has N connected nodes. let it be *n*1, *n*2, *n*3, ..., *nN*, the clustering is implemented based on the following expression

Ed*(ni, nj)* = $\sqrt{(xj - xi)^2 + (yj - yi)^2}$ where *d(ni, nj)* is the Euclidean distance between the node *ni* and *nj*. *(xi, yi)* is the location coordinates of *ni*, *(xj, yj)* is the location of coordinates of the node *nj*. In this manner, the Euclidian distance is measured from one node to another node and we construct a distance matrix as follows

$$Ed = \begin{bmatrix} Ed11 & Ed11 & \dots & Ed11 \\ Ed11 & Ed11 & \dots & Ed11 \\ \vdots & \vdots & & \vdots \\ Ed11 & Ed11 & \dots & Ed11 \end{bmatrix}$$

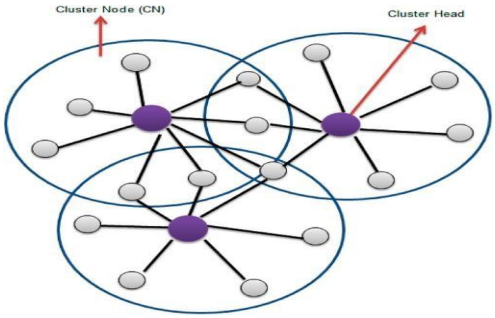

Figure1: Simple clustered IoT network

where Ed*ij* is the Euclidian distance between two nodes *ni* and *nj*, where *i* and *j* vary from 1 to N. After the construction of the distance matrix, we compute the neighbor nodes for every node based on the following expression: Nd*i* = find *(dij* ≤ *Ci(ni))* (3) where *Ci(ni)* is the communication range of the node *ni* and Nd*i* is the neighbor nodes of the node *ni* whose distance with the node *ni* is less than the communication range *Ri* of the node *ni*. Once the neighbor nodes are measured for every node, one node is selected as CH which has huge resource availability. In this situation, it can be concentrated on the selection of non-common nodes as CHs. There is a chance of a single node getting selected as CH for multiple clusters, to mitigate this problem. If it is observed a common CH for two groups then they are merged and formulated into a single cluster with only one CH selected which has higher resource availability.

C. Trust Sensing

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

ISSN: 2456-5660 Volume 9, Issue 4 (April -2024)

DOI:https://doi.org/10.46243/jst.2024.v9.i4.pp74-83

During this process, the CH finds an optimized path to the destination node by the computation of TSF for the very next hop cluster head.

D. Interactive Trust

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

E. Forward Interaction Trust (FIT)

In IoT, the node's behaviour is supervised through the nodes that lie in its communication range or are simply called neighbor nodes. FIT is an observation regarding the nature of packet forwarding nature of nodes in the network. A simple and lightweight trust computation is proposed here for the calculation of FIT. Consider *p* and *q* to be the IoT nodes, the FIT between them is computed as

$$FIT_p{}^q = \alpha \times \text{FITP(b)(p, q)} + \beta \times \text{FITN(b)(p, q)}$$

where FIT*P(b)(p*, *q)* is the Forward interaction trust of node *q* for node *p* according to the positive behaviour of node *q* observed in the past interactions; FIT*N(b)(p*, *q)* is the Forward interaction trust of node *q* for node *p* according to the negative behaviour of node *q* observed from the earlier interactions. Here *P(b)* signifies the positive attitude of nodes or it also denotes the good attitude, *i.e.* for any interaction request kept by any node in the network, if q was answered within the given instance of period, then it is treated as the positive attitude of node *q*. In this situation, the request may be an RREQ for route discovery or a data packet for further forwarding. For any kind of request, the node needs to give a positive response, and then only it will get added to its positive behaviour. For a data packet sent from node *p* to node *q*, if node q didn't

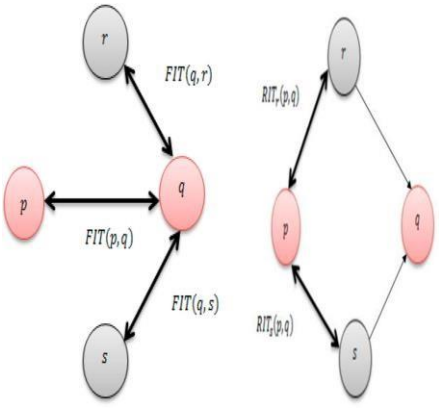

Figure2: (a) FIT,(b) RIT

If it does not reply within the allotted time frame (by acknowledging or by forwarding to the next hop node), then its good behavior will be diminished. Next, *N(b)* denotes the negative attitude of the node or simple it can be called bad behaviour, means for any communication request put by any node *p* in the network, if the node *q* has not replied properly within the instance of time given, then it would be treated as negative attitude. This may

ISSN: 2456-5660 Volume 9, Issue 4 (April -2024)

DOI:https://doi.org/10.46243/jst.2024.v9.i4.pp74-83

happen due to so many reasons and hence for a single instance of negative behaviour, cannot conclude that the node has become malicious. Hence, node p keeps on monitoring node q for particular instances, and this only decides whether it was malicious or not. Next, the two constants (α and β) are used to signify the weightage of positive and negative attitudes of nodes, respectively. At the forwarding stage, depending on the FIT(p, q) value, the sensed node in the IoT network decides whether the receiving node is trustworthy or not. In the case of the positive and negative behaviour calculation process, it is considered the response as the main reference parameter to judge the attitude of the node. At this instant, the packet forwarding factor is considered to assess these two behaviours. For example, if an intermediate node is there at which the packet has been received, it does not work out anything with the packet if it was trustworthy. It checks for the next hop ID and forwards it to the respective next hop neighbor node simply. As a result, the packet forwarding factor is taken into consideration as an additional reference parameter for determining a node's reliability. Mathematically, the expression for packet forwarding factor FP is expressed as

$$F_p(t) = \frac{Cf(0,t-1)}{Tf(0,t-1)}$$

where $Cf(0,t-1)$ the total number is correctly forwarded packet from the starting time o to earlier time instance $t-1$ and $Tf(0,t-1)$ is the total number of packets Forwarded actually from node p to q from starting time 0 to earlier time instance $t-1$. Both values $Cf(0,t-1)$ and $Tf(0,t-1)$ are the cumulative values from time 0 to t. Here correct forwarding means the forwarder node forwards the packets to its next hop node correctly (no modification). In the case of modification, the packet sent node may not receive the acknowledgment within the specific time interval). At this instant, there is a possibility to introduce the malicious information into the packets by forwarding nodes which makes the packet reach malicious parties of some other part of the network. For instance, if a malicious node forwards a packet after tampering with data it is not considered correct forwarding. If the sender notices this illegal notification, then the $Cf(0,t-1)$ value is decreased. Based on these two reference parameters, the forward interaction trust is measured as

$$\text{FITP(b)(p, q)} = F^p(t) * \text{P(b) and}$$

$$\text{FITP(b)(p, q)} = F^p(t) * \text{P(b)}$$

Based on these expressions, the FIT of the node q is measured by the node p before every packet transmission. For example, consider the on–off attack which is the common significant attack that occurs in Ad-Hoc networks in which the weight parameters behave in a self-adaptive manner. These two weights are linked to time with an exponential relation. Depending on the lapse's period, the weights are measured as $\alpha = 1/e\sigma 1(tc-(tc-1))$ and $\beta = 1/e\sigma 2(tc-(tc-1))$, where tc is the current time of interaction and $tc - 1$ is the time instance at which the nodes have communicated previously. Next $\sigma 1$ and $\sigma 2$ signify the positive and negative behaviour's strength decay exponentially, respectively, where $tp > tp - 1 \geq 0$ and $\sigma 1 > \sigma 2 \geq 0$. From a generalized analysis, it can be understood that with an increase in the time elapsed, the FIT declines. This illustration explores that the current communication interactions incurred between nodes are much more significant than the communication interactions incurred between nodes. As the value of time elapsing increases, the two weight parameters follow an inverse relation, *i.e.* as α values increase, β values decrease, and vice versa. This denotes that the node has more memory about the bad attitude of other nodes.

F. Recommended Interactive Trust (RIT)

RIT is the trust provided by other nodes which are common neighbours for two communicating nodes. In RIT, for a specific IoT node in the network, the trust is assessed that depends on the beliefs of its surrounding IoT nodes. The RIT is an accumulated form of opinions obtained from different neighbor nodes of two nodes p and q. Here p is the trust evaluator node and node q is the trust evaluated node. For a given two IoT nodes p and q, the RIT is computed as

$$RIT_p{}^q = FIT_p{}^r * FIT_r{}^q$$

Journal of Science and Technology

ISSN: 2456-5660 Volume 9, Issue 4 (April -2024)

DOI:https://doi.org/10.46243/jst.2024.v9.i4.pp74-83

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

$$RIT_p{}^q = \frac{1}{} + \sum_{C}{}^{c}{}_{c=1} FIT_p{}^c * FIT_p{}^c$$

where C is the total number of common neighbor nodes between the node p and the node q. The major advantage of RIT is (1) lower convergence time and speedy process. (2) Early identification and removal of rogue nodes. RIT enables the nodes that do not succeed in observing the behaviour of their neighbor nodes due to the limited resource constraints.

G. Total Trust

The overall trust is measured by combining Direct Trust and Recommended Trust.

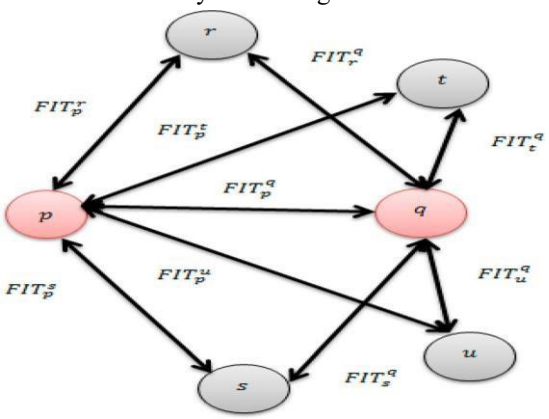

Figure3: Total trust evaluation

Mathematically the Total Trust is represented by integrating the Forwarding Interactive Trust and Recommended interactive trust as

$$T_p{}^q = FIT_p{}^q * RIT_p{}^q$$

Where $T_p{}^q$ is the total trust between the nodes p and q $FIT_r{}^q$ is the forward interactive trust obtained from the direct observations of the node p on the behaviour of the node q and $RIT_p{}^q$ is the recommended interactive trust gained by the node p from the common neighbor nodes of the node q. Figure shows the computation of total trust evaluation. As shown in Figure, the trust nodes p and q are evaluated as

$$T_p^q = FIT_p{}^q + \sum_{c \in s,u,r,t} RIT_p{}^q$$

$$T_{pq} = FIT_{pq} + 14\,(RIT_{spq} + RIT_{upq} + RIT_{rpq} + RIT_{tpq})$$

$$T_p{}^q = FIT_p{}^{q+1}{}_4((RIT_p{}^s * RIT_s{}^q) + (RIT_p{}^u * RIT_u{}^q) + (RIT_p{}^r * RIT_r{}^q) + (RIT_p{}^t * RIT_t{}^q))$$

H. Mobility Factor

In most of the earlier developed trust models, the trust evaluation is implemented based on forward and recommended trusts only. However, most of them neglect that different periods of interactions have different impacts on trust evaluations. For instance, the packet loss that occurred in the previous time interval has a high impact on the trust values than that in the earlier intervals. The main reason behind this issue is the mobility of

ISSN: 2456-5660 Volume 9, Issue 4 (April -2024)

DOI:https://doi.org/10.46243/jst.2024.v9.i4.pp74-83

nodes in IoT. Due to the mobility of nodes, they move away from the nodes which cause lose the overhearing of nodes' retransmission. For a sender node that sent the packet to its next hop nodes, it has to make sure to overhear the retransmission of that particular packet to its next hop node in a promiscuous mode of operation in the IoT network. A successful overhearing only reveals the successful packet delivery to the intended destination. If the sender node overhears the packet forwarding from the next hop node, then only it is treated as successful interaction or else it is declared as malicious behaviour. In some cases where the sender is not able to overhear the retransmission of its packet even though it happened or a destination node is at the unreachable position due to the wrong information regarding its routing, then the forwarding node is declared as a malicious node. Due to this reason, mobility is an important factor that needs to be considered during the trust computation. A node can evaluate the mobility mechanism or feature of its neighbor node by measuring the rate of link changes in the neighbourhood. The such link change rate is used to examine reasons for packet loss. The rate of link changes at the node in the IoT network na is mathematically determined as

$$\rho(q) = \alpha(q) + \beta(q)$$

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

$$\alpha(q)\max + \beta(q)\max = 2.\sigma\,(q)$$

Then the rate of link changes can be determined as

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

Based on Equation, the probability of successful packet forwarding to the rate of link changes is formulated as

$$p(q) = 1 - \rho$$

rate of link changes indicates a more dynamic nature and consequence to less probability of successful packet forwarding. Finally, the node na computes the node q_s trustworthiness according to the mobility rate of the link changed the overall trust is modified as

$$T_{p^q} = T_p^q * p(q)$$

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

III. RESULTS

In this section, the Results of proposed method are discussed. They are Malicious Detection Rate (MDR), False Positive Rate (FPR), False Negative Rate (FNR), Average Energy Consumption (AEC), Packet Delivery Ratio (PDR) and Average Trust (AT).

ISSN: 2456-5660 Volume 9, Issue 4 (April -2024)

DOI:https://doi.org/10.46243/jst.2024.v9.i4.pp74-83

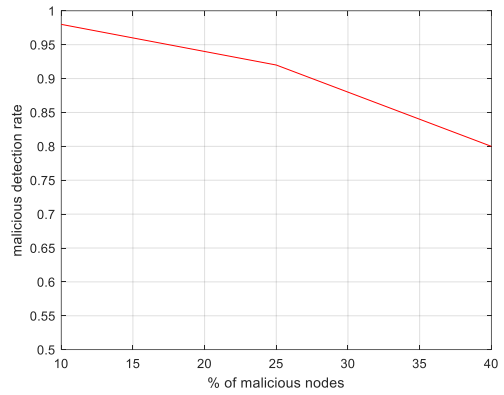

Figure4: Malicious Detection Rate

The MDR is more for the proposed LWCTS mechanism. When there are more malicious nodes in the network then there is a possibility to have various attacks in nodes. possibility to have various attacks in nodes. In the proposed system the sender node senses the trust to send the packets to receiver based on the Recommended Interaction Trust (RIT)

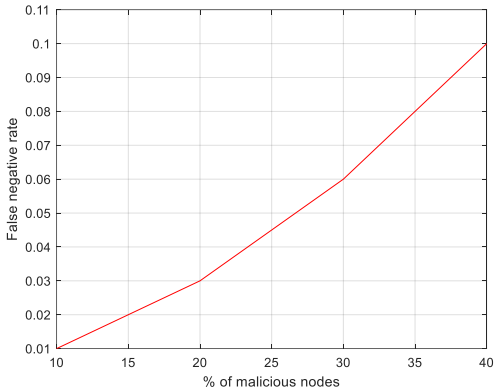

Figure5: False Negative Rate

FPR and FNR are the two execution parameters that explore the data approximately the negative execution or terrible execution in the location applications. These two parameters precisely take after inverse characteristics of MDR. This implies as the MDR increments, the FPR and FNR diminish and bad habit versa. The FNR is the one metric which measures the adversely identified hubs (for a given pernicious hub, the framework is identified as a non-malicious hub).

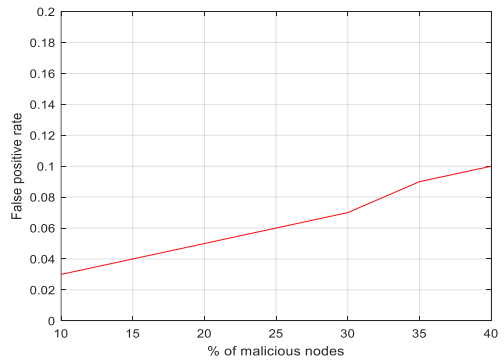

Figure6: False Positive Rate

Journal of Science and Technology

ISSN: 2456-5660 Volume 9, Issue 4 (April -2024)

DOI:https://doi.org/10.46243/jst.2024.v9.i4.pp74-83

Essentially, the FPR is the one metric that measures the contrarily recognized hubs (for a given non malicious hub, the framework is identified as a malicious node). In our approach, we have included the mobility factor to decrease the untrue positives tally, i.e. decrease of wrong location. In the IoT organize, due to the possibility of portability presence for IoT hubs, they may drop the packets if they move out of the communication extend of a sender hub. In such kind of circumstance, the sender node may misconstrue and may pronounce the individual node became noxious. This is a off-base statement because actually the bundle is dropped due to portability but not due to the assaults. If the sender hub pronounces the receiver node as malevolent, the negative behaviour of the receiver node increments and the remaining hubs in the network also take after the same supposition which results in a great loss. This kind of circumstance increments the FPR and to fathom this issue, we have connected the believe of a node with its versatility.

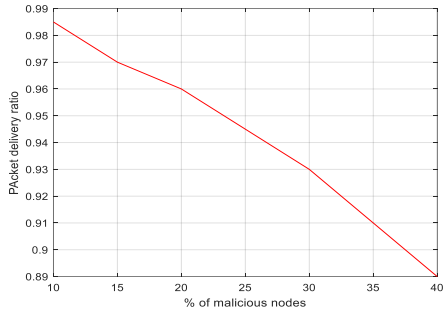

Figure7: Packet Delivery Ratio

Figure7 shows, the packet delivery ratio of proposed system. A more secure arrangement has a lower bundle misfortune and a taller bundle conveyance. In the secure arrange, the data transmitted are secure and effectively convey to the aiming goal. Accordingly, the packet conveyance proportion continuously takes after an inverse connection with nocuous nature. From Figure, we can see that the proposed LWCTS-IoT has picked up a good PDR.

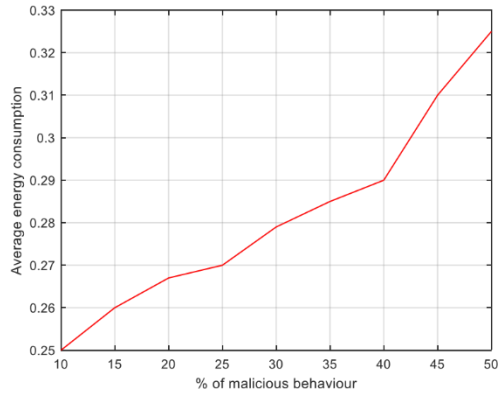

Figure8: Average Energy Consumption

The hubs in IoT are vitality obliged and if they are subjected to more preparing errands, at that point their energy will get exhausted rapidly and they will kick the bucket. Thus, energy subjected to the preparing errands.

Figure 9 appears the subtle elements of normal believe values of normal, trustworthy, and trust thresholds. This plot is drawn after the perception of 10 recreation tests. In every reenactment test, we have measured the average believe of ordinary hubs and noxious hubs. From this figure, we can see that the malevolent hubs is much veering off and they were perfectly differentiated due to the plan of an were perfectly differentiated due to the plan of an optimal trust edge.

.

ISSN: 2456-5660 Volume 9, Issue 4 (April -2024)

DOI:https://doi.org/10.46243/jst.2024.v9.i4.pp74-83

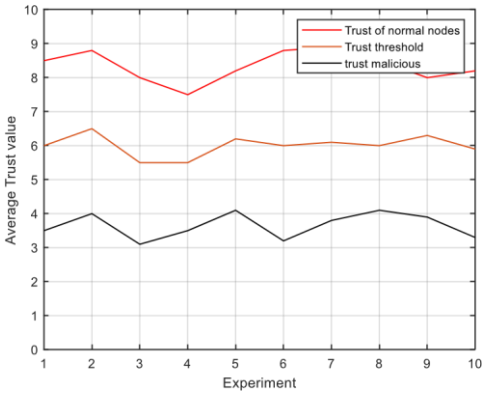

Figure9: Average Trust

IV.DISCUSSION

Trust-aware data transmission is a prime concern in IoT because the Internet is an open source that allows different devices to join and leave the network randomly. Due to this open nature, the devices connected to the network can suffer from serious threats. To ensure a secure data transmission in the IoT network, it is proposed a lightweight clustered trust sensing mode can provide better security along with a better Quality of Service to the network. The newly proposed clustering mechanism can provide the network with a greater network lifetime by reducing the energy consumption at normal nodes. Simultaneously, the proposed trust sensing model helps in the identification and isolation of malicious nodes from the network. For experimental validation, it is realized the proposed concept through an extensive simulation by varying the malicious nature of the network. The obtained results had proven that the proposed LWCTS-IoT is effective in the provision of QoS and security. In this work, the proposed model operated with the static node environment where the chance of hotspot node problem is high. This constraint degrades the overall performance of the IWSN. In future work, it can be extended to consider both static and mobile nodes in the sensing region. The mobile node can travel across the sensing area which mitigates the hotspot node problem in IWSN.

REFERENCE

1. R. H. Weber, Internet of things new security and privacy challenges, Computer Law & Security Review, vol. 26, pp. 23-30, 2010J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.6873

2. The EPC global Architecture Framework. EPC global Final Version 1.3, Approved 19 March, 2009. http://www.epcglobalinc.org

3. Zhuankun Wu. : Initial Study on IOT Security architecture. J. Strategy and decision-making research (2010)

4. T. Grandison and M. Sloman. Specifying and analysing trust for internet applications. In Proceedings of the Second IFIP Conference on e-Commerce, e-Business and e-Government, 2002

5. Buchegger S, Boudec J-YL. Performance analysis of the CONFIDANT protocol. In: Proc. 3rd ACM int. symp. mobile ad hoc netw. comput., Lausanne, Switzerland 2002. p. 226e36.

6. Michiardi P, Molva R. CORE: a Collaborative Reputation mechanism to enforce node cooperation in mobile ad hoc networks. In: Proc. 6th int. conf. commun. Multimedia security 2002. p. 107e21.

7. Ganeriwal S, Srivastava MB. Reputation based framework for high integrity sensor networks. In: Proc. ACM security for adhoc and sensor networks 2004. p. 66e7

ISSN: 2456-5660 Volume 9, Issue 4 (April -2024)

DOI:https://doi.org/10.46243/jst.2024.v9.i4.pp74-83

8. Chen D, Chang G, Sun D, Li J, Jia J, Wang X. TRM-IoT: a trust management model based on fuzzy reputation for Internet of Things. Comput Sci Inf Syst Oct. 2011;8(4):1207e28

9. Bao F, Chen IR. Dynamic trust management for Internet of Things Applications. In: 2012

International workshop on self-aware Internet of Things, San Jose, California, USA September 2012

10. Michele Nitti, Roberto Girau. A Subjective Model for Trustworthiness Evaluation in the Social Internet of Things. 23rd Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications

11. Chen D, Chang G, Sun D, Li J, Jia J, Wang X. TRM-IoT: a trust management model based on fuzzy reputation for Internet of Things. Comput Sci Inf Syst Oct. 2011;8(4):1207e28

12. Y.L. Sun, W. Yu, Z. Han, and K.J.R. Liu, Information Theoretic Framework of Trust Modelling and Evaluation for Ad Hoc Networks, IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 305-317, Feb. 2006

13. G. Theodorakopoulos and J.S. Baras, On Trust Models and Trust Evaluation Metrics for Ad Hoc Networks, IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 318-328, Feb. 2006

14. A.A. Pirzada and C. McDonald, Establishing Trust in Pure Ad-Hoc Networks, Proc. 27th Australasian Computer Science Conf. (ACSC 04), pp. 47-54, Jan. 2004.

15.Yin, X.; Li, S. Trust evaluation model with entropy-based weight assignment for malicious node's detection in wireless sensor networks. EURASIP Journal on Wireless Communications and Networking 2019, 198.

16. Wu, X.; Huang, J.; Ling, J.; Shu, L. BLTM: beta and LQI based trust model for wireless sensor networks. IEEE Access 2019,7, 4367943690.

17. Mohsenzadeh, A.; Bidgoly, A.J.; Farjami, Y. A novel reward and penalty trust evaluation model based on confidence interval using Petri Net. Journal of Network and Computer Applications 2020, 102533.

18. Malik , NA.; Rai, M. Enhanced Secure and Efficient Key Management Algorithm and Fuzzy With Trust Management for MANETs. Available at SSRN 3565898

Journal of Science and Technology

ISSN: 2456-5660 Volume 9, Issue 4 (April -2024)

DOI:https://doi.org/10.46243/jst.2024.v9.i4.pp74-83