Received: July 20, 2020. Revised: September 8, 2020.

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

LWTSM-IoT: Light Weight Trust Sensing Mechanism for Internet of Things

M. Rajendra Prasad[1]* **D. Krishna Reddy[2]**

[1]*Department of Electronics and Communication Engineering, Vidya Jyothi Institute of Technology, India*
[2]*Department of Electronics and Communication Engineering, Chaitanya Bharathi Institute of Technology, India*
* Corresponding author's Email: rajendraresearch@gmail.com

Abstract: In Internet of Things (IoT), secure communication is a prime concern since the open internet source and vast heterogeneity offers several challenges to the network. To achieve an enhanced security, an effective trust evaluation model is required through which the abnormal nodes can be detected and isolated. Towards this objective we have proposed a Light Weight Trust Sensing (LWTS) mechanism for IoT routing. Several factors like Packet Forwarding Factor, Packet Consistency Factor and Packet Repetition Factor are employed to analyze the behaviour of IoT nodes. Along with these factors, the proposed model also checks for energy efficiency to achieve an improved network lifetime. Trust Calculation process is accomplished in two phases; they are direct and indirect fashion. Finally based on obtained total trust, each neighbour node are categorized as No Trust, Average Trust, Fair Trust and Good Trust and the node with good trust is selected as next-hop forwarding node. For the proposed approach extensive simulations are carried out and the performance is measured through Packet Delivery Ratio, Malicious Detection Rate and Average Energy Consumption. The obtained results prove the effectiveness when compared to existing approaches.

Keywords: Security, Trust sensing, Internet of things, Energy cost, Consistency, Malicious detection rate.

1. Introduction

Recently, Internet of Things (IoT) has emerged as an important and most effective communication paradigm in the field of wireless communications [1]. IoT architecture uses widespread heterogeneous technologies, systems and evolved as an effective connectivity paradigm for several physical devices using TCP/IP protocols [2]. Due to the possibility of flexible connection through internet, IoT has found a widespread applicability in almost all areas, for example Smart Cities, Water Grid Management, Smart Grid Systems, Automation Management, building automation, smart agriculture, smart transportation systems, health care systems are some of them [3]. It was found in the survey conducted by Federal Trade Communication (FTC) that the total number of people working in the workstations is much less than the totals number of devices those which are working by connecting through Internet [4]. As a result, the IoT is trying to transform the real world into virtual world by connecting the wide variety of non-traditional computing devices.

One of the basic driving forces of IoT is routing, which makes the devices kept connected to each other and get communicated. In IoT routing, the major concerns which need to be considered are efficient resource (energy, bandwidth etc.) utilization, secure and autonomous communication and scalability [5]. Among these concerns, security is the major hurdle faced by the IoT architectures. According to the standard definition of IoT, it is defined as "the connectivity between the internet and everyday objects and the ability to exchange the data between them" [4]. The flexibility of opened connection to internet made the IoT to face several security problems, broadly ranging from internet to physical devices and there was a possibility to harm people. For instance, a compromised node may led to attack on the other IoT devices. Moreover, some attacks lead the devices to leak or misuse the personal information. Hence there is a need to design an efficient securing paradigm to protect the IoT from several threats and risks.

Trust Sensing is one of the security provision strategies that secures the user's personal information and ensures data confidentiality. In IoT, the devices are resource constrained and hence they seek the help of other devices in their vicinity to forward the data. In such environment, the helping devices may be compromised or selfish. Under trust sensing, the IoT devices measures the trustworthiness of helping devices before forwarding data to them. However, the main problem arises at the design of metrics based on which the trustworthiness is to be measured. Moreover, every attack has its individual characteristics and common metrics won't have much significance in the detection of compromised devices. For example, the Denial of Service attack is different from forging attack. Hence the trust sensing needs to consider multiple measures for the evaluation of trustworthiness.

Based on this inspiration we have developed a new trust sensing mechanism called as Light Weight Trust Sensing for IoT (LWTS_IoT). In LWTS_IoT, every node measures the trustworthiness of its neighbor nodes and selects one node as a next-hop node to forward the data to its destination. Under the trust evaluation, the trustworthiness is measured through three factors namely Packet Forwarding Factor, Packet Consistency Factor and Packet Repetition Factor. Along with these factors, the energy cost factor is also considered by which the Quality of Service is also achieved. Compared to the traditional cryptography techniques, this approach has very less computational complexity and hence is called as light weight mechanism.

Remaining paper is organized as follows, section 2 explores the details of literature survey. Section 3 shows the details of proposed LWTS_IoT. Simulation experiments and the obtained results are discussed in section 4 and finally the concluding remarks are inferred in section 5.

2. Literature survey

Various approaches were developed earlier to ensure a secured communication between nodes of IoT. In the starting of research over security in IoT, the authors focused on cryptography based algorithms such as key matching and hashing [6]. However, the main problem was a huge computational complexity due to a number of mathematic computations. To attain a less complex and more secured IoT, the node behaviour based analysis was required. Since the behaviour of a node varies with communication interactions, it would give more prominent results in the detection and identification of malicious nodes. Under this strategy, a new trust based node behaviour detection system was proposed by Liu, Gong and Feng in which the node's trustworthiness is measured based on direct, indirect and historical values of communication interactions [7]. Historical statistical trust and recommended trust were evaluated based on evidence combination by Liu and Xiong [8]. Further, Yu, Jia and Tao developed a novel quantitative mode for trust evaluation in IoT. This approach used several trust factors namely Integrity, Delay, Packet consistency, Repetition rate and forwarding capacity to measure the trustworthiness of a node. Each and every trust factor is determined through Shannon entropy and D-S theory adopted to synthesize and deduce the trust [9].

Hellaoui, Bouabdallah, and Koudil designed a trust adaptive security in IoT (TAS-IoT). In this approach, the trust evaluation is performed based on three factors, they are Own Experience, Observations and Recommendations. Under Own Experience, an evaluating node checks the authenticity of packet coming from evaluated node. If the packet is authenticated, then the respective node is trustworthy otherwise malicious. Next, under recommendation, the nodes' trustworthiness is recommended by another neighbor node [10]. D.Chen and G. Chang proposed a Trust and Reputation mode for IoT (TRM-IoT). This approach considered two metrics for trust evaluation; they are end-to-end packet forwarding ratio (EPFR), Average Energy Consumption (AEC) and Packet Delivery Ratio (PDR). Further this approach also evaluated local trust and global trust, modelled them through fuzzy reputation model [11].

Focusing on the data provenance, M. Elkhodr and B. Alsinglawi introduced a new trust management solution which provides a trust establishment mechanism amongst communicating devices in IoT. Under this data provenance, this approach checks the data freshness, originality, traceability, and accuracy [12]. V.Suryani, S. Sulistyo and W. Widyawan proposed ConTrust, a new trust assessment model based on inspiration of everyday life. ConTrust assesses the trust based in the form of two factors; they are history based reputation and current trust assessment. The history based reputation signifies the past object experiences. A trust rating is employed and the nodes are categorized as Very Trusted, Trusted, Very UnTrusted and Untrusted. However, ConTrust did not focus on the energy consumption at node level [13].

V. M. Carolina and H. K. João [14] strictly focused on the mitigation of on-off attacks to a multi-service IoT and proposed a new trust management model. This model utilizes the information obtained through directly connected links between nodes to analyze the behaviour of any node [14] [15]. Y. B. Saied and A. Olivereau a distributed model was designed in which the routing decision is autonomous was developed [16]. Recently, one more smart trust management method was proposed by J. Caminha and A. Perkusich for the detection of on-off attacks in IoT. This approach employed an elastic slide window along with machine learning to assess the resource trust of IoT nodes. Totally two types of machine learning algorithms were employed; they are one class and multi-class supported. Under one class, this approach employed One Class Support Vector Machine (SVM), Roust Covariance and isolation forest. Next, under multi-class support, K Nearest Neighbor (K-NN), Linear SVM, Naïve Bayes and Neural Network are employed [17]. Further, K. N. Ambili and J. Jose focused on the defection of three insider attacks; they are black hole, sink hole and wormhole. A distributed trust management mechanism is proposed for the detection. The current trust score are compared with earlier trust score and then decided to exclude or include a node [18].

P. K. Reddy and R.S. Babu introduced an Optimal Secure and Energy Aware Protocol (OSEAP) for IoT based on Improved Bacterial Foraging Optimization (IBFO) algorithm. In this approach, the Fuzzy C-means algorithm is employed for clustering and IBFO is employed for Cluster head Selection. Further the security is achieved through Group key Distribution. The optimal key selection is based on IBFO [19]. Recently, G. Sowmya and N. Venkatram proposed a Multi-Context Trust Aware Routing (MCTAR) for IoT. This is a secured and composite routing which considered multiple factors for trust evaluation. MCTAR considers the communication trust and energy trust to detect and identify the malicious nodes [20]. Further, this approach also employed a hop count factor to find an optimal path which has less hops as well less distances. Due to the consideration of both energy and trust factor, this approach has gained an optimal performance in both resource consumption as well as malicious node detection. However, this approach viewed the trust in the point of communication interactions only which is not sufficient for the detection of multiple attacks [21].

A light weight trust sensing mechanism called as SecTurst was proposed by D. Airehrour J. Gutierrez, S.K. Ray to identify and isolate common routing attacks in IoT. SecTrust totally considered with four metrics; they are Prospect of positive interactions between nodes, Node satisfaction (experience) with neighbour node, Checksum value, and Node energy level. However, this approach also considered the total number packets forwarded and communication interactions which are not sufficient for the detection of multiple attacks. For example, in IoT, there is a possibility of data forging and this can be detected by the consideration of data consistency which is not considered [22].

3. Proposed approach

3.1 Overview

In this section, we discuss about the newly proposed trust sensing framework for IoT routing. The proposed routing paradigm is named as LWTS_IoT. LWTS_IoTis a trust based framework for IoT network, ensures a secured communication by identifying and isolating the malicious nodes from the network. The proposed routing framework not only considers the trustworthiness but also the energy cost during the next hop neighbor node selection. At next-hop node selection, the capability of a node is defined with respect to both energy consumption and trustworthiness. Since the nodes which are more trustworthy may have less energy, thereby the entire packet received may get lost. Hence we have considered the energy consumption and the remaining left after previous transmission is considered and the node which satisfies both these constraints are only selected as efficient node. Further, under trust assessment, the node's behaviour is characterized based on three factors; (1) Packet Forwarding Factor, (2) Packet Consistency Factor and (3) Packet Repetition factor. Based on these three factors, a new trust metric is derived which analyze the node's behaviour in three aspects such as forwarding capability, consistency and repetition measure. Once if any source node is decided to transmit the data to destination node, then it follows multi-hop routing and evaluates the forwarding capabilities of all of its neighbors and selects one final node which has both sufficient energy and trustworthiness. Further the trustworthiness is *computed* in two phases; direct phase and indirect phase. The details are explored in the following sections;

3.2 Energy model

Generally, the nodes in IoT network are resource constrained. Hence, to achieve a sufficient network lifetime, we need to choose nodes in such a way that the nodes will have sufficient energy. For this purpose, we proposed an energy consumption model based on which the energy efficiency can be evaluated. An IoT node generally works under two modes; transmitting mode and receiving mode. Under transmission mode, it transmits the packets while under receiving mode it receives the packets from either single source or multiple source nodes. Hence, under both constrains, the IoT node have sufficient energy consumption. Hence we have considered both the energies for evaluating the total energy consumed at a node. The mathematical methodology of energy model is described as follows. Consider two nodes i and j separated from a distance d, the total energy consumed for receiving as well as for forwarding the data packet of size k bits is evaluated as;

$$C_E(k,d) = T_E(k,d) + R_E(k,d) \tag{1}$$

Where C_E is the complete energy consumed, T_E is the energy required for transmission of k bits and R_E is the energy required for receiving k bits. They are mathematically evaluated as

$$T_E(k,d) = E_e \times k + E_a \times k \times d^2 \tag{2}$$

and

$$R_E(k,d) = E_e \times k \tag{3}$$

Where E_e stands for energy consumed while transmitting or receiving one bit, E_a stands for the energy consumption when node amplifies 1 bit data thereby it can be transmitted for farther distances. d is the Euclidean distance between two nodes i and j. Next, let's consider that I_E be the initial energy; the remaining energy (R_E) left at node j after receiving and transmission of k bits is measured as

$$R_E = I_E - C_E \tag{4}$$

Based on the R_E, a node's forwarding capacity can be determined. The remaining energy R_E is compared with an energy threshold (E_T) and if it is found to be greater than the threshold, then that particular node is declared to have sufficient energy and it can used for further forwarding. Otherwise, it was simply removed from neighbor list. Based on this comparison, we have assigned a label which defines the trust degree of a node. The trust degree computation is evaluated as follows;

$$T_d^j = \begin{cases} 1, \ if\ R_E^j \ \geq T_d^j \\ 0, \ if\ R_E^j < T_d^j \end{cases} \tag{5}$$

Where T_d^j is trust degree of node j, and R_E^j is the remaining energy left at node j. Here the trust degree defines the node's trustworthiness based on its energy. Hence the trust degree is relative to energy consumption only. For a node with high remaining energy, it will be used for further communication otherwise it is removed from neighbor list.

3.3 Trust model

The proposed trust model is employed under two phases. The first phase is to calculate the node's trust value according to three factors such as packet forwarding factors, packet consistency factor and packet repetition factor. The second phase is trust rating process followed by next-hop node selection. The trust calculation is accomplished in two orientations, i.e., direct and indirect orientations. In LWTS_IoT, every node computes the trustworthiness of its neighbor nodes based on computed direct trust value and recommended trust value. The above specified three factors are viewed in both orientations and a composite trust factor is derived based on them. Based on the composite trust factor, the neighbor nodes are rated and the final node is selected as next hop node which has higher trust value. The detailed exploration is discussed in the following subsections;

3.3.1. Packet forwarding factor (P_F)

In the evaluation of packet forwarding factor, the evaluating node measures the packet forwarding capability based on the total number of packets forwarded by the evaluated node to its further nodes. For this purpose, we have introduced two thresholds; one is lower threshold (L_T) and another is higher threshold(H_T). To measure the P_F, the total number of packets sent from evaluating node i are compared with the expected number of packets . Depends on the result, (i.e., whether the total number of packets sent are less than or greater than the expected value of packets), the packet forwarding factor $(P_F(i,j))$ is measured as follows [23].

$$P_F(i,j) = \begin{cases} \frac{P_S(i,j)-L_T}{P_E(i,j)-L_T}, & if\ P_S(i,j) \leq P_E(i,j) \\ \frac{H_T-P_S(i,j)}{H_T-P_E(i,j)}, & if\ P_S(i,j) > P_E(i,j) \end{cases} \tag{6}$$

Where $P_F(i,j)$ is the obtained packet forwarding factor between evaluating node i and evaluated node j, $P_S(i,j)$ is the total number of packets sent from node i and node j, and $P_E(i,j)$ is the expected number of packets, L_T and H_T are lower threshold and higher threshold respectively.

From Eq. (6), we can understand that if the two values $P_S(i,j)$ and $P_E(i,j)$ are closer to each other, then the value of $P_F(i,j)$ is closer to 1, means the evaluated node j gets a higher trust value. Furthermore, we can understand that if$P_S(i,j) \gg P_E(i,j)$, and then we can declare that the respective node attacked with Denial of Service (DoS) attack. In the case of a node attacked with DoS attack, the attacker node tries to deplete the resources of other node quickly for example by transmitting the packet continuously. In that case, the total number of packets sent is far beyond the total number expected packets to be sent. On other side, if$P_S(i,j) \ll P_E(i,j)$, then we can declare that the evaluated node is compromised by selective forwarding attack. In this attack, the node sends only few packets from the packet which it received. Hence the range of packet sent must lie in the surroundings of expected number of packets.

3.3.2. Packet consistency factor (P_C)

In the evaluation of packet consistency factor, the evaluating node measures the trustworthiness of evaluated node based on the data consistency. Since some attacks are there in which the attacked or compromised node tries to forge that data, the evaluating node needs to check the consistency of data under spatial coherence. This evaluation is assessed based on a simple assumption that the nodes in the same local area of networks show a higher degree of spatial coherence. If the data packets of any node are found to be forged, then the data consistency of such data packets has much deviation with the data packets of other nodes. For an evaluating node, the data consistency factor based trust is measured by comparing the data collected by itself with data collected by its neighbor nodes. If it is found that the data consistency of any neighbor node has much deviation, then that node is declared as compromised or attacked. Under this evaluation, the data consistency is measured through the cross correlation of data collected by a set of neighbor nodes. The mathematical representation of data consistency factor evaluation is calculated as follows [23];

$$P_C(i,j) = \frac{C_P(i,j)}{C_P(i,j)+NC_P(i,j)} \tag{7}$$

Where $P_C(i,j)$ is the packet consistency factor between node i and node j, $C_P(i,j)$ is the total number of consistent packets and $NC_P(i,j)$ is the total number of non-consistent packets. And the sum of $C_P(i,j)$ and $NC_P(i,j)$ denotes that the total number of packet received at node i from its surroundings. The range of $P_C(i,j)$ lies in between 0 and 1, here the 0 denotes that there are no consistent packets which means the entire set of packets are forged and the value 1 denotes no packet is forged and the respective node is trustworthy.

3.3.3. Packet repetition factor (P_R)

Packet Repetition Factor is one of the most important factors in the determination of node's malicious behaviour. There are several reasons in which the forwarding node will ask the evaluating node or its previous-hop node to retransmit the packets. Low Link quality is the prime reason by which the packets transmitting over it are lost and hence the forwarding node may ask previous-hop node to retransmit. This is an unintentional behaviour of node and there is no matter of maliciousness or selfishness. The next reason for packet loss is attack, for example if any node is attacked or compromised by any attack, then it may drop the packets or it may forward only few number of packets. If the packets are dropped at the node, then we can say that the node is attacked by black hole attack. On the other hand, instead of dropping entire packets, if the node has forwarded only few packets, then we can say that the node is attacked by selective forwarding attack. In both cases, the evaluated node asks evaluating node to retransmitting the packets, called as replay attack. Hence, when determining the node's behaviour, normal or not, the evaluating node needs to check the growth rate of repeated transmission of data packets. If found a slight increase and it is not more than threshold, then such type of behaviour is considered as normal and the packet retransmission is due to the communication channel problems, otherwise it is considered as replay attack. As the packet repetition rate is approaching to threshold and also the value is much larger, the probability that the node is considered to be malicious is high and the node is more likely to be malicious node. The mathematical expression for packer repetition factor is expressed as;

$$P_R(i,j) = \frac{P_S(i,j)-P_{RS}(i,j)}{P_S(i,j)} \tag{8}$$

Where $P_S(i,j)$ is the total number of packets sent form node I to node j, $P_{RS}(i,j)$ is the total number of packets that are sent repeatedly from node *i* and node j.

The range of $P_R(i,j)$ lies in between 0 and 1, here the value 0 denotes that the total number of packets sent are equal to the total number of repeatedly sent packets, i.e., $P_S(i,j) = P_{RS}(i,j)$. On the other side, the value 1 denotes that the total number of packets sent are not equal to the total number of repeatedly sent packets, i.e., $P_S(i,j) \neq P_{RS}(i,j)$, means there is no single repeated packet. $P_R(i,j) = 1$is considered as an ideal condition which is impossible. Hence we consider the $P_R(i,j)$ value closer to 1.

3.3.4. Trust calculation process

In the trust calculation process, the evaluating node is called trustor node and the evaluated node is called trustee node. Here the trustor node evaluates the trustworthiness of trustee node and based on the obtained value, the trustor decides whether the trustee is malicious or not. Particularly, the trust computation process represents the competence, dependability, reliability and successful positive interactions between trustor and trustee. These features denote the performance of trustee node over the tasks given by trustor node, directly or indirectly [24]. In IoT network, the nodes maintain direct and indirect relations. Based on these two types of relations, two types of trusts are derived; they are namely direct trust and recommended trust. In the direct trust, the trustor node and trustee node are directly linked with each other while in recommended trust the trustor and trustee are connected indirectly through some common neighbor nodes.

Direct Trust: Direct trust is a belief of a trustor node on the trustee node which was connected directly to trustor and it is one of its neighbor nodes. Here the neighbor node is defined as a node which lies within the communication range such that it can offer a route to the destination node. When a node establishes a communication link with any of its neighbor then it is said to be directly linked. In this work, the trustor node measures the direct trust of a trustee node with respect to three factors as specified above. Mathematically the direct trust between node *i* and node *j* is expressed as;

$$D_T(i,j) = (w_1 \times P_F(i,j)) + (w_2 \times P_C(i,j)) + (w_3 \times P_R(i,j)) \quad (9)$$

Where w_1, w_2 and w_3 are arbitrary weights, w_1 signifies the weight of packet forwarding factor, w_2 signifies the weight of packet consistency factor, and w_3 signifies the weight of packet repetition factor. The selection of w_1, w_2 and w_3 must satisfy the condition, $w_1 + w_2 + w_3 = 1$. Generally, all weights are assigned with equal weights, as $w_1 = w_2 = w_3 = 0.333$. After the evaluation of direct trust for all neighbor nodes, one node is chosen as a next-hop forwarding node which has higher direct trust (D_T). The higher value of D_T specifies that the particular node j is resilient from DoS, forging and replay attacks.

Recommended Trust: This is an indirect trust evaluated by trustor node by considering the recommendations of its neighbor nodes which are commonly connected to trustor and trustee nodes. This is also a belief on the neighbor node to decide whether another node is consistent and dependable when recommending to other distant nodes. For a given trustor and trustee nodes, there exists a set of common neighbors. During the trust evaluation, the trustor node considers the opinions of its neighbors regarding the trustworthiness of trustee node. Particularly, the recommendation trust comes into picture when there is a need of data transmission to the distant nodes which are 2-hops and beyond. In this case a trustor node depends on the neighbors or neighbor nodes. Mathematically the recommendation trust is expressed as;

$$R_T(i,j) = D_T(i,m) \times D_T(m,j) \quad (10)$$

Where $D_T(i,m)$ is the direct trust between node *i* and node m, while $D_T(m,j)$ is the direct trust between node m and node j. Here node m is a common neighbor node for both node *i* and node *j*. The recommended trust is possible through common neighbor nodes only. Otherwise the nodes which are intended to recommend can't suggest to trustor node if they are not in the communication range of trustor node. There exist some nodes which are not common for trustor and trustee nodes. Such type of nodes can't recommend. One more point to notice is that there exists more than one common recommending node. In such condition, the recommending trust is measured as average recommended trust and it expressed as

$$R_T(i,j) = \frac{\sum_{m=1, m\neq j}^{N_n} D_T(i,m) \times D_T(m,j)}{N_n} \quad (11)$$

Where N_n is the total number of common neighbor nodes for trustor and trustee.

In the proposed model, for nodes beyond 1-hop, a node must depend on the trustworthy recommended nodes for accurate trust evaluation. Fig. 1 shows a simple demonstration about the direct and recommended trusts evaluation.

Total Trust: The total trust is obtained by the summation of direct and recommended trusts. The expression for total trust is expressed as;

$$T_T(i,j) = \big(\alpha \times D_T(i,j)\big) + \big(\beta \times R_T(i,j)\big) \quad (12)$$

Received: July 20, 2020. Revised: September 8, 2020.

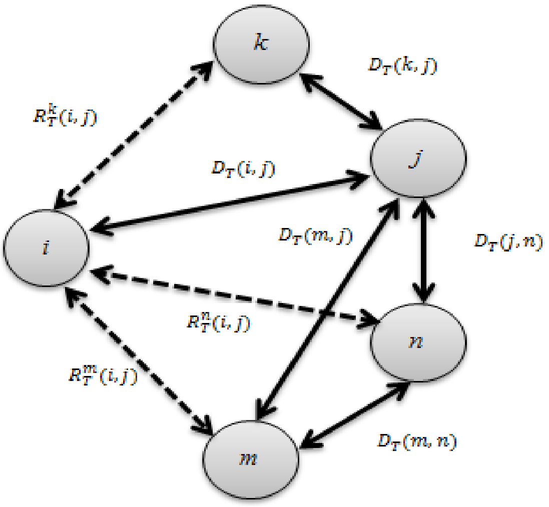

Figure.1 Trust evaluation example

Table. 1 Trust level categories

Level	**T_T Range**	**Trust Level**	**Consequence**
L1	0-0.25	No Trust	Attacked/Compromised
L2	0.26-0.50	Average Trust	Compromised or selfish
L3	0.51-0.75	Fair Trust	Selfish or Unintentional
L4	0.76-1.00	Good Trust	Unintentional

Where α and β are the two weight constants which signifies the importance of direct trust and recommended trust respectively. The selection of α and β must satisfy the condition, $\alpha + \beta = 1$. In this evaluation, a greater value of α denotes that the direct trust is more important and a greater value of β denotes that recommended trust is more important.

For direct or 1-hop communication, α value needs to set high while for distant communications, β value needs to set high. Based on the obtained total trust value, we have categorized the nodes into four categories, as shown in Table 1.

The maximum value of $T_T(i,j)$ is 1 and the minimum value is 0. By dividing the entire range from 0 to 1 into four categories, the trust level is defined into four levels such as No trust, Average Trust, Fair Trust and Good Trust. For $T_T(i,j)$ ranging from 0 to 0.25, the node is declared to be not trustworthy and it is strictly attacked or compromised. Next, for $T_T(i,j)$ ranging from 0.26 to 0.50, the node is declared to have average trust and the behavior is finalized as attacked or selfish. Next, for $T_T(i,j)$ ranging from 0.51 to 0.75, the node is declared to have Fair trust and the behavior is finalized as selfish or unintentional like lower quality of communication link or congestion etc. Finally for $T_T(i,j)$ ranging from 0.76 to 1.00, the node is declared to have good trust and the behavior is finalized as more trustworthy and not compromised by any attack.

Note: For a node having total trust value in between 0.76 and 0.85, the node is assumed to have less link quality or some other unintentional behaviors. Under this category, the node is declared to have good trust but the trust value is less than 1 because the trust value is linked with packet forwarding factor, and packet repetition factors. To get a total trust value as 1, the P_F andP_R must be 1, this is highly impossible due to lossy wireless channels. Hence the node which has maximum Total Trust is selected as final next-hop forwarding node for data forwarding.

4. Simulation results

In this section, we discuss the details of simulation experiments conducted over the proposed trust model and the observed results. To simulate the proposed model, we have created a random network with N number of nodes and the area is MXN, where M is the length and N is the width of the network. The simulation parameters are listed in Table 2. During the simulation, we have considered the IoT as a randomly deployed network and the routing protocol which are generally used for Wireless Sensor Networks are employed. Initially, we discuss about the simulation parameters those were used to set the network and then discuss about the performance metrics through which we have analyzed the performance. At the performance analysis, we have compared the proposed LWTS-IoT with conventional MCTAR-IoT [20], ETES [9].

4.1 Simulation setup

Table. 2 Simulation parameters

Parameter	Value
Network area	1000 x 1000 m^2
Number of node	30-100
Packet size	512 bytes
Communication Range (R)	¼ of network area
Traffic type	Constant Bit rate
% of malicious behaviour	0-50% of total nodes
α, β	$0 \leq \alpha, \beta \leq 1$
w_1, w_2 and w_3	0.3333
Trust Threshold	0.6
Energy Threshold (E_T)	20% of initial energy
Lower threshold (L_T)	300
Higher threshold (H_T)	700
Expected Packets (P_E)	500

4.2 Performance metrics

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

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

Malicious Detection Rate (MDR): MDR is defined as the total number of nodes detected as malicious when they are malicious. 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.

Average Energy Consumption (AEC): AEC is defined as the total energy consumed by several source and destination node pairs during the transmission of data from source to destination. In the simulation, we have simulated ten pairs of source and destinations and the energy consumed is averaged.

4.3 Results

In the simulation study, the performance is evaluated based on the above specified performance metrics. Varying simulation experiments are carried out by varying the % of malicious behaviour. Here the % of malicious behaviour is defined as total number of nodes declared as malicious out of present nodes in the network. To realize the concept of the proposed as well as existing models, in the simulation study, initially a x% of nodes are declared as malicious nodes and then the proposed and conventional approaches are employed to detect them. During this process, we measure the above specified performance metrics. The % of malicious behaviour is varied as 10, 20, 30, 40 and 50. For example, if 100 nodes are present in the network, only 10 nodes are considered as malicious at 10% maliciousness and 20 are the malicious nodes when we consider 20% maliciousness. In this way, the % of malicious behavior is varied and the performance results are measured. Simultaneously, we also employed a comparative analysis between proposed and conventional approaches MCTAR-IoT and ETES-IoT. In MCTAR-IoT, the trust evaluation is conducted based on two factors; they are energy trust and communication trust. Under the communication trust, the node's trustworthiness is measured through communication interactions only but does not analyse the packet forwarding capacity with respect to packet delivery ratio and packet repetition rate. Moreover, this approach is also not done for any trust rating process such that there is no option at the sudden drop of packets due to malicious nature or selfish nature. In the case of ETES-IoT, the trustworthiness is measured based on five factors but not considered the energy factor. Hence the nodes even if they are more trustworthy, then they do not have sufficient energy, the entire packet received may get lost. This has serious effect on the packet delivery ratio and packet loss ratio. Moreover, this approach is also not employed trust rating process and hence for a node which had lost its next hop node, don't have an alternative option and it has to start the route discover again.

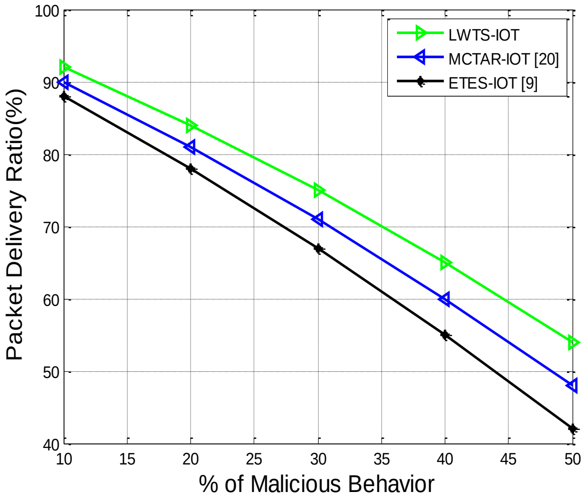

Figure. 2 PDR vs. % of malicious behaviour

Fig. 2 shows the PDR variations with varying number of malicious nodes in the network. From this figure, we can observe that as the % of malicious behaviour increases, the PDR decreases. As the number of malicious node increases in the network, for every pair of source and destination, there exists at least one malicious node in the path by which the packets received at that particular node may get lost. At this situation, there should be an option to select another node immediately which is trustworthy. This flexibility is present in the proposed LWTS because the neighbor nodes have individual priorities and the previous node can choose an alternative trustworthy node. Moreover, the proposed approach also considers the energy cost hence the node which has sufficient remaining energy and trustworthy is only selected. As the node with sufficient energy is selected as next hop node, it will be still alive until the entire packets get delivered at destination node.

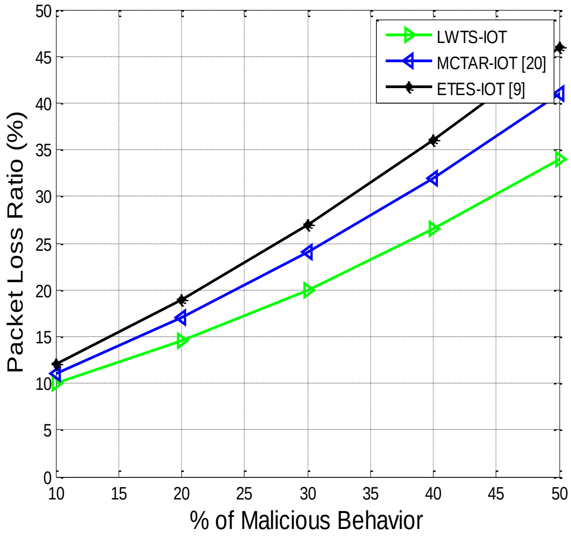

Figure. 3 PLR vs. % of malicious behavior

Fig. 3 shows the PLR variations with varying number of malicious nodes in the network. From this figure, we can observe that as the % of malicious behaviour increases, the PLR increases. As the number of malicious node increases in the network, the packet loss also increases because the nodes lies over the established will drop the packets. For a lower number of malicious nodes, the probability of trustworthy node selection is high and for all the source and destination pairs, the established paths will have almost trustworthy nodes. With an increase in the malicious node count, the probability decrease and the packet loss increase. Moreover, the proposed LWTS-IoT employed packet repetition factor through which the node with high packet repetitions will get detected. The higher number of repetitions is possible only when the node has become malicious and the node which was asking for packets repetitions will get detected easily. Since the conventional approaches don't have this flexibility, the PLR is high compared to proposed approach.

Fig. 4 shows the AEC variations with varying number of malicious nodes in the network. From this figure, we can observe that as the % of malicious behavior increases, the AEC increases. The higher AEC is observed for ETES-IoT, because at every phase of malicious node detection, the source nodes starts route discovery. And once the route discovery is started the node consumes maximum energy. Hence the AEC of ETES-IoT is high compared to the other methods. Next, even though MCTAR focused on energy, the required factors for proper and accurate detection of malicious nodes are less in number. In the proposed approach, at every round of packet transmission, the nodes will check the energy cost incurred at previous transmission and based on this the remaining energy left is calculated. Hence the

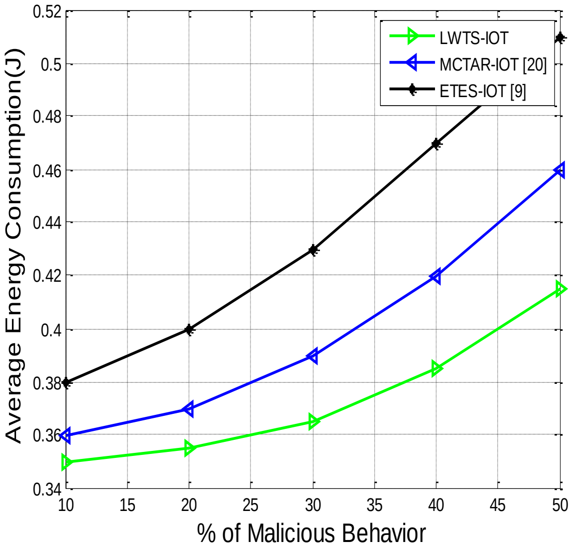

Figure. 4 AEC vs. % of malicious behavior

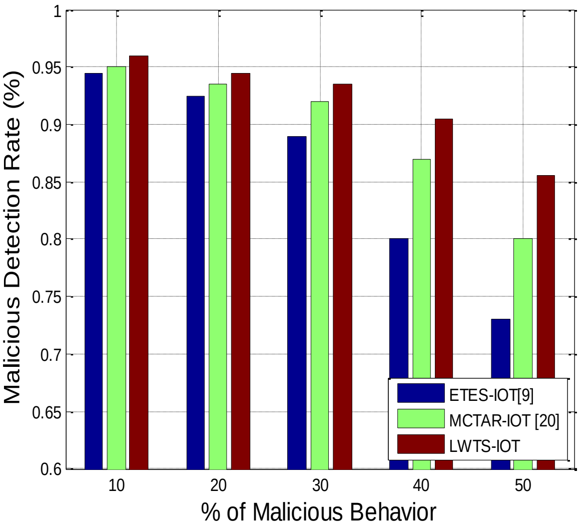

Figure. 5 MDR vs. % of malicious behavior

proposed LWTS-IoT has less energy consumption compared to the existing methods.

Fig. 5 shows the MDR variations with varying number of malicious nodes in the network. In this figure, we can observe that the MDR of MCTAR is high compared to ETES. Even though the ETES has employed multiple factors for trust evaluation, it was not focused on energy consumption.

As the number of factors to be analyzed increases, the system gains robustness to more number of attacks but won't get much significance in the generalized detection. For an approach which considers both energy and multiple trust factors, it can detect any type of attack and becomes resilient to more number of attacks. Further, some attacks are there like DoS which makes the node to get deplete quickly by spending its energy. Hence both the energy factor and multiple trust factors have considerable significance which is accomplished in

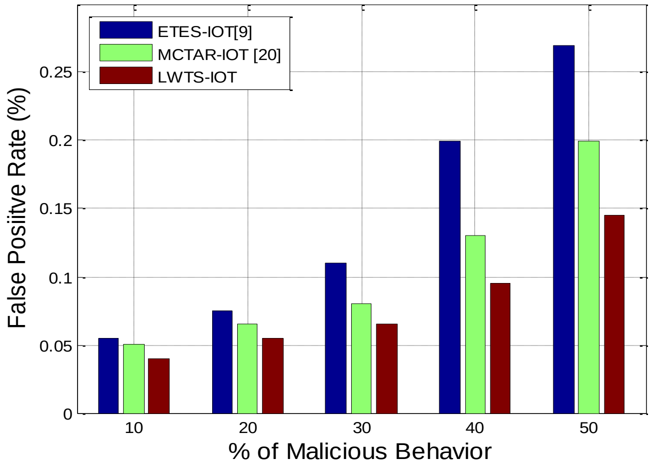

Figure. 6 FPR vs. % of malicious behavior

the proposed approach. The proposed approach is more flexible and can detect more types of attacks; hence the node compromised with any attack will get detected by which the MDR increases. From the above figure, we can notice that the proposed LWTS has high MDR compared to existing methods.

The FPR has simple inverse relation with MDR, as the MDR increases, the FPR decrease and vice versa. Further, the FPR has direct relation with % of malicious behavior, as shown in Fig. 6. As the malicious node count increases, the FRP also increases, because MDR decreases. From the above figure, we can observe that the proposed LWTS has less FPR compared with conventional approaches. Further, the efficiency of proposed approach is proved at an increase of FPR from 30% to 40% malicious nodes increment. At this phase, the conventional approaches got a higher increment while the proposed approach has nominal increment, because, the proposed approach has employed multiple trust factors like Packet Forwarding Factor (detects the node compromised with DoS attack), packet consistency factor (detects the node compromised with Forge attack) and packet repetition factor (detects the node compromised with Replay attack). Hence the proposed approach has less FPR compared to existing methods.

5. Conclusion

In this paper, we have proposed a new quantitative trust evaluation model based on energy and multiple trust factors. The direct trust of neighbor node is calculated from multiple aspects including, Packet Forwarding Factor, packet consistency factor and packet repetition factor. Further, aiming at the network lifetime, the remaining energy is also calculated based on energies consumed for transmitting and receiving the packets. A node will get selected only if it has sufficient energy as well as trustworthiness. The trustworthiness evaluation is employed in both direct and indirect fashions. The simulation results show that the proposed LWTS-IoT can effectively detect and isolate the malicious nodes. Compared with existing approaches, the proposed model can obtain more adaptability and robustness and also have advantages in the prospect of secure data forwarding. Comparison is conducted through five performance metrics such as PDR, PLR, AEC MDR and FRP. On An average, the proposed LWTS-IoT obtained an increased PDR of 4% and 8% from the MCTAR and ETES respectively. Next, the increment in the MDR through the proposed approach is noticed as 3.1012% and 7.2315% from the MCTAR and ETES respectively. Finally the average decrement in the AEC is observed as 3.8% and 6.4% from conventional approaches. Further this research work is extended to develop a robust trust framework through the collaboration of many factors in the detection of multiple attacks using novel trust vector assisted sensing mechanism.

Conflicts of Interest

The authors declare no conflict of interest in publishing this paper.

Acknowledgments

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

References

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

[2] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, “Evaluating Critical Security Issues of the IoT World: Present and Future Challenges”, *IEEE Internet of Things Journal*, Vol. 5, No. 4, 2018.

[3] 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.

[4] 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.

[5] T. K. L. Hui, R. S. Sherratt, and D. Sánchez, “Major requirements for building Smart Homes in Smart Cities based on Internet of Things

technologies", *Future Generation Computer System*, Vol. 76, pp. 358–369, 2017.

[6] S. Choudhary and N. Kesswani, "Detection and Prevention of Routing Attacks in Internet of Things", In: *Proc. of International Conf.* on Computer Systems and Applications, New York, NY, USA, pp. 1-8, 2018.

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

[8] 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. 12, No. 1, pp. 1842-1845, 2013.

[9] 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.

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

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

[12] M. Elkhodr and B. Alsinglawi, "Data provenance and trust establishment in the Internet of Things", *Security and Privacy*, pp. 1-11, 2020.

[13] V. Suryani, S. Sulistyo, and W. Widyawan, "ConTrust: A Trust Model to Enhance the Privacy in Internet of Things", *International Journal of Intelligent Engineering and Systems*, Vol. 10, No. 3, pp. 30-37, 2017.

[14] 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. No., pp. 1-8, 2015.

[15] Y. Chae, L. C. DiPippo, and Y. L. Sun, "Trust management for defending on-off attacks", *IEEE Transactions on Parallel and Distributed Systems*, Vol. 26, No. 4, pp. 1178–1191, 2015.

[16] Y. B. Saied, A. Olivereau, D. Zeghlache, and M. Laurent, "Trust management system design for the Internet of Things: a context- aware and multi-service approach", *Computers & Security*, Vol. 39, pp. 351–365, 2013.

[17] J. Caminha, A. Perkusich, and M. Perkusic, "A Smart Trust Management Method to Detect On-Off Attacks in the Internet of Things", *Hindawi Security and Communication Networks*, pp. 1-10, 2018.

[18] K. N. Ambili and J. Jose, Trust based Intrusion detection system to detect insider attacks in IoT systems, *Information Science and Applications*, Cryptology ePrint, 2019.

[19] 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.

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

[21] L. N. Devi and K. V. S. Reddy, "Secure and Composite Routing Strategy through Clustering in WSN", In: *Proc. of the 2ndInternational Conf. on Innovations in Electronics, Signal Processing and Communication (IESC),* Shillong, 2019.

[22] D. Airehrour, J. Gutierrez, S. K. Ray, "A lightweight trust design for IoT Routing", In: *Proc. of IEEE 14th Intl Conf. on Pervasive Intelligence and Computing*, pp. 552–557, 2016.

[23] Z. Chen, Min He, Wei Liang, and Kai Chen, "Trust-Aware and Low Energy Consumption Security Topology Protocol of Wireless Sensor Network", *Journal of Sensors,* Vol., No. pp. 1-10, 2015.

[24] J. Luo, X. Liu, and M. Fan, "A trust model based on fuzzy recommendation for mobile ad-hoc networks", *Computer Networks*, Vol. 53, No. 1, pp. 2396–407, 2009.