International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *05 July 2023* ***Revised:*** *25 August 2023* ***Accepted:*** *15 September 2023*

A Design of Improved Trust-based Clustering Approach to Enhance the Energy Computation in Secured Internet of Things (IoT)

Satish Kamble[1,2], Dr. Surendra Mahajan[3], Deepak D. Sapkal[4], Kimi Ramteke[5]
[1]Research Scholar, Department of Computer Engineering, SKNCOE, SPPU, Pune, India
[1]satkam53@gmail.com
[2,3]Department of Information Technology, PVG'S COET & GKPIOM, SPPU, Pune, India
[3]sa_mahajan@yahoo.com
[4]Department of Computer Engineering, PVG'S COET & GKPIOM, SPPU, Pune, India
[4]ddsapkal@gmail.com
[5]Department of Computer Engineering, I[2]IT, SPPU, Pune, India
[5]kimiramteke16@gmail.com

Abstract— The Internet of Things (IoT) is the trending area that occupies maximum of the applications of intelligent communication. The nodes in the IoT system are located in the monitoring environment to attain stable and reliable communication. In between the nodes and the sink, similar data is sensed and transmitted at maximum of the period and that leads to high energy consumption. On the other hand, it increases the security issues of the network. So the main objective is reducing power utilization and increasing the IoT network security. In this paper, we suggest an improved trust-based clustering approach to enhance energy computation and security (ITCES-IoT) in IoT networks which can able to reduce energy consumption and increase the security among the nodes in the network. We first introduced an effective system model that can able to reduce the transmitting and receiving power during communication. Secondly, the initial cluster setup phase, LEACH-based cluster head (CH) selection phase, and re-clustering principles are discussed. Then, the trust calculation is established for both the cluster members (CM) and the CH through direct and indirect trust calculation processes followed by the best solution of path selection is performed between the CM and the sink node. We constructed Bad mouthing attacks, Ballot stuffing attacks, and detection mechanisms with a Fast Entropy algorithm. Finally, intra-cluster and inter-cluster communication are elaborated in the communication phase. Through this process, the nodes and CHs can able to perform effective communication with minimum power utilization, and the nodes with the transmitted information are secured from the external environment. At the end stage, we validate our proposed ITCES-IoT approach in certain scenarios in network simulator NS2 and their performance analysis includes the parameters of packet delivery ratio, network throughput, and packet loss and energy consumption. Then the final outcomes are compared with the base methods such as ECET-IoT, DRTP-IoT, and RCDA-IoT. From the results it is understood that the proposed ITCES-IoT outperforms the baseline methods in terms of delivery ratio and throughput and as well it consumes less power at the time of data transmission.

Keywords- Internet of Things (IoT), Improved Trust Model, Clustering Approach, Bad Mouthing Attack and Ballot Stuffing Attack

I. INTRODUCTION

Internet of Things (IoT) has turned out to be the most popular technology, occupying most of the applications in modern times like healthcare, smart home, confidential communication, industrial sector, and environment condition analysis. Multi-hop IoT network is constructed to connect a huge number of devices. The devices can be sensors that work to transfer the information of the external environment from one place to another and control it with suitable strategies. The IoT protocols used to control its devices and help attain effective communication are ZigBee, Wi-Fi, Bluetooth, etc.

Through IoT composite services become possible and that benefit of human beings [1]. IoT follows object to object communication process so it is highly essential to measure the level of trustworthiness of the object which took part in communication [2]. Several earlier works have been developed in terms of trust calculation which consists of lots of definitions therefore fixing to suitable model for a particular network is complicated and it is still an open research area to obtain a suitable model to attain more accuracy [3]. A clustering-based model is used to minimize the power utilization in an IoT network [4]. The network is separated into several clusters and the cluster head (CH) will control the cluster and the other devices that are present inside the cluster. All other devices in the cluster are considered cluster members (CM). The clustering constructed IoT network model is illustrated in Figure 1. On the other hand, several vulnerable attacks are created in the IoT network and it becomes highly essential to construct the trust model according to the functionalities of the attacks [5] [6].

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *05 July 2023* ***Revised:*** *25 August 2023* ***Accepted:*** *15 September 2023*

Through attacks, the performance of the IoT network is degraded through high packet loss, depletion in battery power, and high delay than normal stage [7]. It becomes highly essential to develop a model that can able to reduce the power utility and attacking activities. For that purpose, in this research ITCES-IoT which highly concentrates on trust-based clustering and effective energy computation among the devices is proposed. The contribution of this article is described as follows.

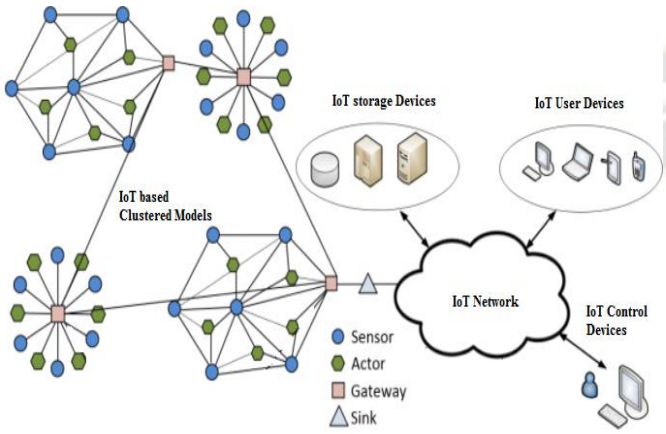

Figure 1. - Clustering Constructed IoT Network

An effective method to choose the CH selection process is performed which includes cluster setup, CH selection, and re-clustering process. The CH is selected through direct and indirect trust calculations. Trustworthy path selection is performed here to reduce the computational delay and overhead of the network. The simulation of the ITCES-IoT method is done in the NS2 simulator and the network is constructed with both the bad mouthing and ballot stuffing attacks. Attacks-based and parameters-based performance analysis is performed and the outcome proves that ITCES-IoT attains maximum results than baseline research in terms of energy consumption, delay, and routing overhead.

The rest part of the article is summarized as follows: section II discusses the details and drawbacks which is present in the earlier works on IoT. Section III elaborated on the process of the ITCES-IoT method. Sections IV and V, talk about the performance analysis and results discussion of the methods which are considered in the implementation. Section VI concludes the paper with summarized results of the contribution and its future research direction.

II. RELATED WORK

In [8], the author Sadrishojaei et al., (2021) presented the Mobile Internet of Thing (MIoT) using “Clustering and Location Prediction Routing Method based on Multiple Mobile Sinks” (CLRP-MMS). Before choosing CH nodes using the CH Choosing Function (CHCF), all of the nodes are first grouped into a number of clusters of varying sizes. According to the time sync, the CH nodes determine where the moving sinks are located. By using this technique, network performance and lifespan are increased. This approach has a large overload and a high cost, which is unfortunate.

In [9], the author Qiu et al., (2020) created a Shortcut Addition method for multi-sink networks based on the Particle Swarm algorithm (SAPS). On the basis of a small-world network, it builds network topologies with several sinks. Updated particles are created through crossover and mutation in order to get the best answer. In terms of load distribution, and quantity of additional shortcuts, this framework performs better. It is unsuitable for large-scale networks since it does not facilitate node mobility.

In [10], the author Panahi et al., (2023) provided an enhanced security method, taking into account the bit error rate and security level for wireless sensor networks. The user may select between unsecured or secure modes using this framework, which makes use of reserved bits in the frame control field of the Zigbee MAC header. When it comes to measures like end-to-end latency, battery life, throughput, and memory utilization, this framework performs better. It is unsuitable for large-scale networks since it does not facilitate node mobility.

In [11], the author Mishra et al., (2023) enhanced the Light Gradient Boosting Machine (LGBM) technique to detect the IoT network's invasive functions. The primary benefit of the anticipated development in ensemble learning is the ability to create advanced predictions using the results of many ML approaches. Its robustness is improved by this approach. But processing does consume more energy.

In [12], the author Roy et al., (2023) provided an authentication mechanism for the IoT in a fog environment. Cloud, fog, and edge devices were utilized in this framework. Additionally, it evaluated and employed a number of already-existing post-quantum cryptography-based cipher suites. The authentication methodology used for IoT gadgets in a fog computing environment is quick, hybrid, and secure. The strategy has a number of downsides, such as the requirement to deploy several sinks that are mobile and optimize the path of movement of the mobile sinks.

In [13], the author Mirdula et al., (2023) created a framework to dynamically monitor Manufacturer Usage Description (MUD) profile issues and difficulties and identify anomalous behavior. IoT devices are used in the implementation of the application for straightforward consumer and industrial contexts. Applications for Industry 4.0 are more secure, and protected, and have fewer problems thanks to the

MUD-DL. This approach has a high overload and, regrettably, a significant expense.

In [14], the author arac et al., (2021) provides an authentication solution for IoT gadget security. It offers the essential secrecy and versatility that digital infrastructure now lacks. The process increases the reliability of data sent to remote services by applying the proper algorithm for cryptography to the information before transmission. The fact that this approach does not support the nodes' mobility, which interferes with network connectivity, is a drawback.

In [15], the author Chauhan et al., (2022) sought to offer a method [15] for enhancing IoT security by integrating encryption structure with an elliptic curve with the fundamental structure-based blockchain technology. Data security for users is guaranteed by blockchain technology. If the chain of command is disrupted, the attacker will be unable to enter false information into the system or gain access to it. The drawbacks of this technique are high overload, a lack of clustering support, and excessive complexity.

In [16], the author Lal et al., (2023) offered a technique for cognitive cybersecurity which improves human cognitive ability in two ways. Disputed vulnerability reports should first be reconciled before sophisticated embedding indicators are pre-processed in order to provide reliable data sets. Both in terms of importance and execution for security review in software applications, the full potential of this suggested technique has not yet been realized.

In [17], the author Al Ahmed et al., (2022) presented a unique blockchain-based authentication architecture for the purpose of authenticating IoT gadgets. The design suggested a method for grouping IoT gadgets into "clusters" that had a multi-level structure, with a tiny blockchain to validate its constituents. This approach reduces the computing burden needed to complete transactions in the blockchain. The primary drawbacks of this technology are that it doesn't allow uneven clusters and nodes can move around.

In [18], the author Liu et al., (2023) developed an Adaptive Multi-channel Bayesian Graph Attention Network (AMBGAT) framework for identifying different kinds of Ethereum accounts. Amplifying node features, estimating graph topology structures that are consistent with the real world, and effectively extracting node features important to subsequent tasks are all achieved by AMBGAT by using attention. This approach has a high overload and, regrettably, a significant expense.

In [19], the author Elhaloui et al., (2023) devised and built an SDN-based network architecture for the Internet of Things. By using Snort to identify the undesired flow, this framework's primary goal is to increase data quality, guarantee its dependability, and prevent any kind of external assault. The mobile sink collects the data, however, is greatly impacted when the nodes are mobile and there is an obstruction in the nodes' dwelling.

In [20], the author Ravi et al. (2023) proposed a Cluster-based Reliable Data Aggregation (CRDA) approach for IoT networks that allows data gathering and aggregation efficiently. The “Monarch and Sine-Cosine” (MSC) method is applied to cluster the connected devices and guarantee effective transmission of information. The CRDA plan increases the quality of service while extending the lifetime of the network and using less energy. This approach has a high overload and, regrettably, a significant expense.

In [21], the author Priyanka et al., (2023) established a Region based energy efficient clustering model for IoT in Agricultural Environment (REAN). The "Shortest Routing and Less Cost algorithm (SRLC) and the Region Clustering and Cluster Head Selection algorithm (RCHS)" are used to construct the IoT apps and software, and both of these algorithms help to reduce energy consumption. This strategy led to a major energy optimization. The fact that this approach does not support the nodes' mobility, which interferes with network connectivity, is a drawback.

Sáez-de-Cámara et al. (2023), the authors of [22], designed and assessed a clustered federated learning-based IDS design for heterogeneous IoT sensors. Auto-encoders that were trained on non-hazardous examples of connected device data to replicate their normal behaviour are used to build the model for detection. The lifespan of the network was increased by this approach. The primary drawbacks of this technology are that it doesn't allow uneven clusters and nodes can move around.

In [23], the author Ajay et al., (2023) proposed a model to improve the performance in regards to both the optimization and power utilization reduction. For that purpose, an optimized clustering model is developed which includes a shortest-path strategy and CH selection process. This method greatly increased the data transmission count, threshold, and residual energy but however, the densities of nodes are moderate.

In [24], the author Feroz et al., (2023) introduced an approach to improve network security and efficiency called dynamic frequency hopping mechanism in the IoT environment. Through this process, the network computational cost and delay are reduced but however it consumes power more than the actual requirement and that leads to a reduction the performance.

In [25], the author Guguloth et al., (2023) presented a model to diminish the energy utilization of the network called cluster-based reliable communication. This design requirement

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 05 July 2023 **Revised:** 25 August 2023 **Accepted:** 15 September 2023*

includes a monarch and sine-cosine model and an improved sunflower optimization. Using these techniques CH selection is performed and it reduces the power utilization among the IoT sensors but however the obtained results are moderate which needs further improvisation.

After analyzing the former research, it is understood that the past methods still consist of certain drawbacks like improper CH selection, high energy utilization, lack of attack prevention, and so on. To overcome those drawbacks in this paper ITCES-IoT approach is proposed and it is elaborated in the upcoming section 3.

III. PROPOSED ITCES-IOT APPROACH

The proposed ITCES-IOT approach is mainly developed to increase the efficiency and network security of the IoT networks. The main sectional categories of this research are (i) network system model, (ii) clustering process which includes cluster set-up, CH selection, and re-clustering, (iii) trust established in nodes through direct and indirect trust calculation, (iv) trust establishment in CH, (v) trusty path selection and (vi) communication phase. The workflow of the proposed ITCES-IOT approach is illustrated in Figure 2.

Figure 2. - Workflow of the Proposed ITCES-IOT Approach

This section fixes the different issues with earlier techniques. This strategy is more effective in terms of the quantity of active nodes, overall energy use, and packets received by the sink. Listed below are the primary benefits of the proposed strategy and how it is distinct from the ones already in use:

- Supporting node mobility
- Implementing clustering and trust model simultaneously
- On-demand re-clustering
- Using several mobile sinks
- Effective cluster communication

Details on the proposed approach are provided in the subsequent sections.

A. System Model

The paths thus generated have a ring-like form if N and S are the numbers of nodes and sinks, respectively, and mobile sinks follow a circular, predictable course. According to these pathways in various segments, irregular clusters are generated. The battery life, storage, and processing power of mobile sinks are limitless. Via their CH nodes, IoT gadgets continually scan their surroundings and relay the information they acquire to mobile sinks. Planned in TDMA is the intra-cluster transition. Single-hop communications are used by CH nodes in order to receive information from CM nodes and send the reduced information to mobile sinks. The longevity of wireless networks may be greatly increased by transferring single-hop data to mobile sinks. The proposed strategy utilizes a one-hop link from CM nodes to CH nodes as well as from CH nodes to the sink, however, this data transfer design may result in an increased latency period because the nodes are mobile and, in numerous instances, it is not feasible to change their internal batteries and also because energy use has the highest priority.

The following logical presumptions must be taken into account while developing the framework design.

- Uniformly distributed homogeneous nodes.
- The nodes have the exact same beginning power.
- Both their position and speed are known to every node.
- The portable sinks feature a big storage capacity and an endless battery life.
- The two biggest energy-consuming operations are data sending and receiving.
- All connections are capable of transferring adequate information.

The distance to the node of the destination and the amount of data being transferred, as well as the power consumption E_{TX} per node, are factors that are taken into consideration in this technique.

$$E_{TX}(l,d) = \begin{cases} l \times E_{elec} + l \times \varepsilon_{fs} \times d^2, & if\ d < d_0 \\ l \times E_{elec} + l \times \varepsilon_{mp} \times d^4, & if\ d \geq d_0 \end{cases} \quad (1)$$

Where, the variables l and d stand for the volume of data transferred and the distance from the sending node, respectively. During data transmission, E_{elec} provides the energy used per bit. The open space transmission amplification coefficient is represented by the notation ε_{fs}. Sending multi-path indicates the amplification coefficient as ε_{mp}. The node's transfer threshold is often set to $\sqrt{\left(\varepsilon_{fs}/\varepsilon_{mp}\right)}$) and is set to d_0.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *05 July 2023* ***Revised:*** *25 August 2023* ***Accepted:*** *15 September 2023*

The receiver's energy consumption for its l bits is given by the numerical value of E_{RX} in (2).

$$E_{RX}(l) = l \times E_{elec} \quad (2)$$

Programs that track environmental conditions need to use network resources efficiently. In this study, the trust model is used to select the CH. Clusters are then constructed, and the CH node is chosen depending on the relevant function. The information is then gathered from the CH nodes by moving the sinks along the designated pathways.

B. Attacks Construction

The attacks that are considered in this network model are Bad Mouthing and Ballot stuffing which are elaborated on here. (i) Bad mouthing attack – It is one of the thread models that provide false ratings to the devices. Due to the process, the honesty of the nodes gets reduced. If this kind of attack increases in the network, it will create dishonest nodes due to its low trust values and that will lead to serious impacts on IoT applications. This type of attack is carried out by a group of nodes. (ii) Ballot stuffing attack – During the process of communication this kind of attacker will create duplicate ballots among the devices and affect the actual data transmission and it provides false results at the destination. Through these attacks, the trustworthiness of the network has been reduced and it becomes highly essential to create protective activities among these attacks. This type of attack is also carried out by a group of nodes.

C. Clustering Process

A round-based strategy with two key phases is used for this clustering process. The initial part of the process is known as setup and it entails network deployment, cluster construction, CH preference, and re-clustering. The communication stage, which comes after the first, establishes the relationships among nodes, CH, and sink within and outside of clusters. Based on network utilization and longevity, the number of cycles is determined. The process of clustering is described in Figure 3.

D. Cluster Setup

In this phase, new clusters are formed, CHs are chosen, and clusters are reconfigured. By using a new function, every node in the proposed technique is chosen to transform into CH nodes. Cluster formation, CH selection, and re-clustering are all three sub-phases that make up this stage. By using numerous mobile sinks in place of a permanent sink, every one of which is in charge of a particular number of clusters, the novel technique may avoid sending data that might otherwise clash with the mobile sink. The number of mobile sinks defines the total size of clusters, and during this sub-phase, the whole node is initially split into numerous pieces. The angles of the segments were established using the quantity of sinks. The suggested technique gathers information using two portable sinks. Because there is just one sink utilized, there may be instances when there is an excessively large distance between the CH node and the sink, and that may increase the power utilization.

Figure 3. – Clustering Process

E. CH selection

The majority of CH choices, according to recent research on the LEACH method, are based on the node's distance from the sink or residual power. However, a node leaving a cluster due to mobility can interrupt data transit and undermine the stability of a cluster. Because of this, it's crucial to consider slower nodes in addition to the aforementioned characteristics while choosing participants. Since each of the nodes in the cluster possesses the same energy, the node that is closest to it serves as CH for the initial cycle.

LEACH protocol assumes a sparse sensor network with corresponding nodes, and hence the main purpose is to transmit information to a sink node. As a result, the best CH for collecting and disseminating data to the sink node is determined. In certain circumstances, the sink is located far away, requiring extra energy for transmission. As a result, LEACH must choose a CH in a method that the chosen node has a greater energy level. To distribute the energy among the nodes LEACH follows a random number of CH rotations. The nodes in LEACH are totally distributed, so there is no need to get control information from the sink and they don't need the network's global information. The life of the network is focused and increased, and therefore no information about the node's location is required. Furthermore, implementing the LEACH helps the aggregation of the acquired data in the CH, which reduces network traffic. This approach is one kind of MAC model that implies a uniform network of nodes for information gathering and then reaches the sink. Due to the node's high power utilization, the LEACH equally distributes the energy in the nodes to reduce the energy load. The LEACH protocol is set up in a specific way here.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *05 July 2023* ***Revised:*** *25 August 2023* ***Accepted:*** *15 September 2023*

After identifying the optimal percentage of CH, the LEACH treatment is carried out in rounds. A bunch of CH is determined as $1/g$ for every round using size, hg, where h implies the total round count and g implies the CH. Each round includes a steady-state phase as well as a set-up phase. The setup step is divided into three sub-phases: advertisement, cluster setup, and broadcast scheduling. The following is the order in which the advertisement phase is carried out: By fixing the range of 0 and 1. Every node h produces an integer from that range and hence the crosschecks with the presumed threshold level.

$$Q(h) = \begin{cases} \frac{g}{1-g\times(c \bmod \frac{1}{g}} & if\ e \in \propto \\ 0 \ ; otherwiswe \end{cases} \quad (3)$$

Wherein, $\propto$ denotes a node that has never been a CH, g denotes a CH, and c indicates the present topology's iteration period. As a result, when a node decides to be a CH, it sends an announcement packet to its neighbor. All other nodes in the network respond to the CH advertisement to inform their actions throughout the CH setup phase. The responses of all nodes are collected during the broadcast phase in order to determine which cluster a node belongs to. The CH creates a TDMA program based on the cluster's total nodes. This scheduling hit a chord across nodes in terms of how often the message should be transmitted at a given moment. As a result, for transferring the data in an efficient way, the data must be stored in CH and then forwarded to the sink. The CH formed by the LEACH protocol is given by,

$$G = \{G_1, G_2, \ldots . G_t, \ldots . G_n\}; 1 \leq t \leq n \quad (4)$$

Wherein, n indicates the total number of cluster heads by applying the LEACH protocol. This depends on the total of the node boundaries, mobility velocity, and energy left in each node. The proposed method is influenced by a number of different variables, every one of which has a different weight and is thus given a coefficient in consideration. The CH node within the identical cluster chooses the node with the nearest position as the new CH node for the following round. The CM nodes get a broadcast announcing the newly established CH node's position. Nodes that are closest to one another in space and have the most residual energy are more likely to be CH nodes. Additionally, nodes with lower speeds have a decreased propensity to depart from the cluster range, making them a better choice for CH nodes. The CH node's re-selection is a distributed strategy that doesn't include the sink; therefore, it uses less energy for the control packet transmission than the centralized clustering technique since the sink doesn't intervene.

F. Re-clustering

Because CH nodes are subjected to loads that are far higher than those placed on conventional nodes, CH nodes experience a rapid loss of energy, making re-clustering an essential component of routing. The entire cluster's data will be lost if one of the CH nodes malfunctions. Therefore, the re-clustering procedure must be carried out on a regular basis in order to prevent CH nodes from failing. The re-clustering interval is quite difficult to choose the proper value for. There will be a significant amount of network overload if the setting is set too low (clustering is done for each gathering information cycle). The network is also unable to complete any other tasks while clustering. The packet loss is much higher when a very big number is chosen, though, because there is a considerable likelihood that a CH node may discharge its energy while collecting data. Re-clustering is only possible using a different technique when the CH node energy is below a certain threshold. Due to the failure of the CH node, it might stop packets from being lost. Based on the study, it is recommended the following given the above.

- When the present CH node's residual energy falls below a predefined energy threshold T, a new CH node is chosen from among the existing nodes. T is set at 30% of the starting energy for the sake of this study.
- When necessary, re-clustering is carried out rather than a cluster's complete network. By avoiding adding extra network cost, this kind of local re-clustering.

IV. TRUST ESTABLISHMENT IN NODES

Trust calculation is performed in three segments, they are; direct trust, indirect trust, and trust establishment process. The process of trust calculation is described in Figure 4.

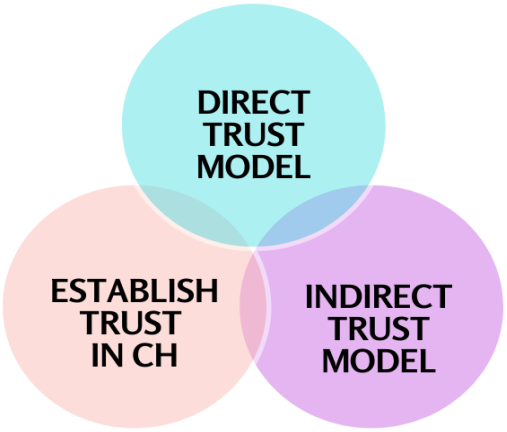

Figure 4. – Trust Establishment Process

A. Direct Trust

In this section initial step of direct trust calculation is performed between any two nodes which are influenced by the time taken for data transmission and the number of packets

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 05 July 2023 **Revised:** 25 August 2023 **Accepted:** 15 September 2023*

transmitted through that communication link. So the two parameters are considered for this initial direct trust calculation; they are factor time attenuation and transmitted packets count and the process of initial direct trust calculation is mathematically expressed in equation (5).

$$dt_{AB} = \frac{\sum_{i=1}^{t} \rho^{t-i} M_{AB}^{i}}{M} * t_d \quad (5)$$

In equation (5), the term $M = \sum_{i=1}^{t} \rho^{t-i}, \rho^{t-i} (0 < \rho < 1)$ implies the function for time attenuation, M^{i}_{AB} implies the number packets sent by the B node to node A during the considered time period of *Ti*. An increase in transmitted packets can able to increase its trust value. In case the communication among the node A and B is not taken in a direct way then the value of dt_{AB} get declared as 0.5.

Direct trust is established between nodes that interact with each other. It is also based on the previous interactions between the two devices. Our trust calculation algorithm in node uses both trust metrics: Quality of Service and Social trust. For the Quality of Service trust metric, our algorithm uses a ratio between the number of successful transactions to the total number of transactions between two interacting nodes. For the Social trust metric, our algorithm uses the community of interest and friendlist.
In our proposed approach we have used Algorithm1 for the trust calculation of node j by node i.

Algorithm1: Trust calculation

1. $Q_{ij}(t) = \frac{S_t}{T_t}$ // calculates Quality of service trust metric.
2. $B_{ij}(t) = \frac{|X_{ij}^{CoI}|}{|Y_i^{CoI}|}$ // calculates Community of Interest.
3. $F_{ij}(t) = \frac{|M_{ij}|}{|N_i|}$ // calculates friendlist.
4. $D_{ij}(t) = Q_{ij}(t) + B_{ij}(t) + F_{ij}(t)$ // add all to form direct trust.
5. $FT_{ij}(t) = (1 - \alpha)FT_{ij}(t - \Delta t) + \alpha D_{ij}(t)$ // Final trust value.

In Algorithm1. $Q_{ij}(t)$ represents the ratio among numbers of successful transactions S_t to the total transactions T_t between two interacting nodes in time t. It gives the quality of service trust metric. $B_{ij}(t)$ represents the ratio between the common communities between service consumer node i and service provider node j represented by X_{ij}^{Col} to the total number of communities of node i represented by Y_i^{CoI} . It gives one of the social trust. $F_{ij}(t)$ represents the ratio between the common friends between node i and node j represented by M_{ij} to the total number of friends of node i represented by N_i. It gives another social trust. $D_{ij}(t)$ gives direct trust value among node *i* and node *j* which is calculated by adding $Q_{ij}(t)$, $B_{ij}(t)$ and $F_{ij}(t)$. The final trust value $FT_{ij}(t)$ is calculated by using the equation in step 5 of the algorithm. Δt represents the elapsed time since the last trust update. A parameter α here determines the contribution of the previous trust value and the new trust value. If α has having higher value, it means more weightage is given to direct observations represented by $D_{ij}(t)$.

B. Indirect Trust

Indirect trust calculation is highly essential in terms of increasing network security. The indirect trust calculation among nodes A and B is calculated by considering certain parameters such as history of abnormal leaving, abnormal joining, and multi-distribution. To improve the authentication quality among the nodes this indirect trust factor is measured and it gets mathematically expressed in equation (6).

$$IDT_i^d(\tau) = \frac{1}{r}\sum_{i=1}^{r} DT_i^d(d) \quad (6)$$

In equation (6) the term *r* implies the node's overall neighbors *i.* Through this trust calculation process, the trustworthiness among the nodes is highly increased which results in the increased performance of network communication quality.

C. Trust Establishment in CH

The CH periodically transmits the requested information inside its cluster. In answering, all devices retransmit their trust values to CH. The CH maintains the matrix to store these values.

$$CH \rightarrow n_i(t)$$

$$= \begin{bmatrix} Dn_1n_1(t) & \dots & Dn_jn_1(t) & \dots & Dn_nn_1(t) \\ Dn_2n_2(t) & \dots & Dn_jn_2(t) & \dots & Dn_nn_2(t) \\ \dots & \dots & \dots & \dots & \dots \\ Dn_nn_n(t) & \dots & Dn_jn_n(t) & \dots & Dn_nn_n(t) \end{bmatrix} \quad (7)$$

The first row of the matrix gives trust values of all nodes in the cluster towards node n_1. The second row gives trust values of all nodes towards node n_2. The last row gives trust values of all nodes in the cluster towards node n_n. Bad mouthing attacks and Ballot stuffing attacks are detected at CH using the Fast Entropy theory.

Fast Entropy is described as follows:

- The major information that is considered in the fast entropy function is density.
- This process is mainly utilized to measure the received information.
- Through this process the data prediction is performed and the expected amount of information of the nodes can be measured.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 05 July 2023 **Revised:** 25 August 2023 **Accepted:** 15 September 2023*

- In this work we detect Bad mouthing and Ballot stuffing attacks with fast entropy.
- During the presence of attacks in the network the fast entropy decreases severely.

Fast Entropy formula:

$$F_{(i,t)} = -\log\frac{V_{(i,t)}}{N} + f_{(i,t)} \quad (8)$$

$$f_{(i,t)} = \begin{cases} \left|\log\frac{V_{(i,t+1)}}{V_{(i,t)}}\right|, & V_{(i,t)} \geq V_{(i,t+1)} \\ \left|\log\frac{V_{(i,t)}}{V_{(i,t+1)}}\right|, & V_{(i,t)} < V_{(i,t+1)} \end{cases} \quad (9)$$

- i: indicates the node number for which fast entropy is calculated.
- t: indicated the fixed time window where the fast entropy of a particular node i can get measured.
- $F_{(i,t)}$: indicates the nodes i fast entropy in a fixed time window.
- $V_{(i,t)}$: indicates the count of negative feedback if it is a bad mouthing attack and the count of positive feedback if it is a ballot stuffing attack.
- N: indicates node counts in a cluster.
- t+1: indicated the time window considered after the time window t.

- CH also calculates overall trust value using algorithm2

Algorithm2: Trust calculation of all nodes by Cluster Head node

1: Input: Matrix $CH \rightarrow n_i(\Delta t)$

2: Output: $\boldsymbol{CHFTn(\Delta t)}$

3: Start

4: $for(i = 1\ to\ n)\ do$

$for(j = 1\ to\ n)\ do$

$sum = sum + Dn_in_j(\Delta t);$

$end\ for$

$CHFTn_i(\Delta t)$= sum/n;

5. Apply Fast_Entropy_Algo(n_i) // If an attack is detected then n_i will not take part in the CH selection process

6: $end\ for$

7. End

V. COMMUNICATION PHASE

Communication between the CM nodes, the CH node, and the mobile sink is what this stage is about. During inter-cluster and intra-cluster interactions performed using single-hop architecture is utilized. This stage consists of two components: intra-cluster and inter-cluster communication. The node chosen as the CH broadcasts the membership message to the surrounding nodes. A node chooses the CH node with the greatest Received Signal Strength (RSS) and when it gets this message from a number of CHs. As a result, this procedure prevents cluster overlap, which further increases the lifespan of the network. The TDMA schedule, which controls each node's wake-up state, is provided by the CH node for cluster maintenance and to ensure that the CM nodes consume as little energy as possible. Every time slot allotted to a CM node determines how the transfer of data will proceed. Aside from CH nodes, idle nodes are perpetually turned off. The CH node aggregates the information from the CM nodes and transfers it to the sink node. Once all of the nodes' energy has been drained, this procedure is repeated.

A. Intra-cluster communication

Within the CH node is a list of every node for each of the clusters. Any node that doesn't send any information for 2 straight frames is removed from the list, and connected nodes are informed of the new TDMA schedule. Mobility is managed by cumulative ack, which the CH node distributes after each frame. Information from its nodes has been confirmed by the CH node. A node becomes orphaned if it doesn't get a confirmation message from its CH node due to its mobility. By submitting a Join Request (JReq), the orphan node solicits and collaborates with the newer CH node. When a newer node enters a cluster, its CH changes both its list and its TDMA schedule and then distributes it to all the cluster members. The CH node begins to process information when all of the CM nodes in the cluster have finished data transmission. To make the best possible use of bandwidth, the CH node collects the data to remove any duplication and reduces it as much as it can. The data is subsequently prepared for transmission to the sink via single-hop connections by CH nodes.

B. Inter-cluster communication

An adjustable sink may move in several distinct manners. The sink's propensity to move in advance was exploited in this investigation. The amount of energy consumed by the network will rise, and there will be a lot more collisions if the sink path keeps shifting and there's a need for regular updates of the sink position. In addition, the suggested approach enables a number

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *05 July 2023* ***Revised:*** *25 August 2023* ***Accepted:*** *15 September 2023*

of mobile sinks in the network, which will result in reduced network power utilization. Based on the periodic movements, CH transfers information to the sink at the suitable moment in accordance with the schedule and location of the sink which helps to reduce the power utilization and can increase the network performance.

C. Trusty Path Selection Process

Relay nodes are responsible for forwarding packets between the IoT node and to sink node. IoT nodes from one cluster can send data to sink present in another cluster. We used a trusted path algorithm for data transmission. The IoT node will send data packets to CH of the same cluster. Inter-cluster data transmission takes place through the CH of respective clusters. CH is selected as a relay node if its overall trust value is greater than 0.5. Finally, the CH of the sink node will forward data to the sink node.

VI. PERFORMANCE ANALYSES

In our research, we execute the simulation of the proposed ITCES-IoT using network simulation (NS2) software. It is a combination of Object Tool Command Language (OTCL) and C++. For experimentation, the nodes are localized in the coverage area of 1500*1500m. For the simulation evaluation, 200 nodes 200-node-based scenario is used where 5 percent of the nodes were attackers. The other considered parameters are listed in Table 1. The parameters used for the comparison are packet delivery ratio, network throughput, end-to-end delay, packet loss, and energy consumption in terms of vehicles. In terms of attack parameters like bad mouthing and ballot stuffing data delivery ratio, loss ratio, and delay are calculated. To perform comparative analysis, the results of the ITCES-IoT are compared with the baseline methods like ECET-IoT [23], DRTP-IoT [24], and RCDA-IoT [25].

Table 1. Simulation parameter of the Network

PARAMETER	VALUE
Coverage area	1500m*1500m
Nodes Count	200
Number of Cluster head	5
Node Deployment	Random
Malicious Nodes Count	10 to 20
Experimentation Time	100s
Channel type	Wireless Channel

A. Network Throughput Calculation

It is defined as the data flow rate of the communication channel among the nodes. The mathematical expression for the calculation of throughput is given in equation (11).

$$\text{Throughput (Kbps)} = \sum \frac{(\text{no of successful packets}) * (\text{average packet size})}{\text{Total Time taken in data transfer}} \quad (11)$$

The Figure 5. demonstrates the throughput results the proposed ITCES-IoT and comparison with the earlier work ECET-IoT, DRTP-IoT and RCDA-IoT. The x-axis shows values of a number of nodes and the y-axis shows throughput in Kbps respectively.

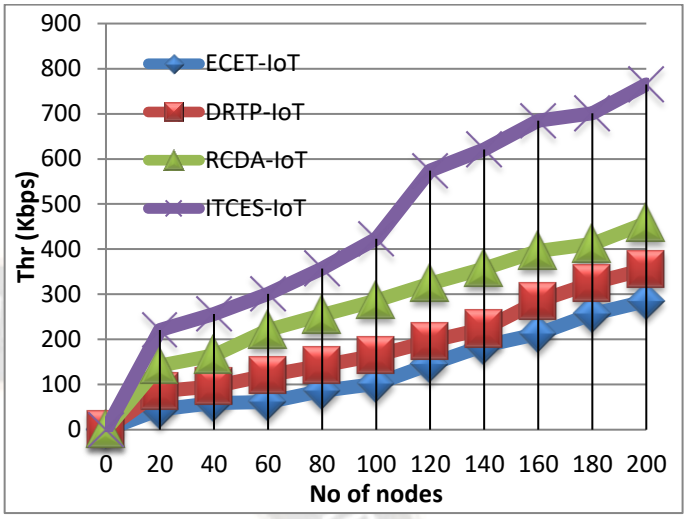

Figure 5. - Network Throughput Calculation

The throughput obtained by the baseline methods like ECET-IoT, DRTP-IoT and RCDA-IoT are 285 kbps, 356kbps and 458kbps respectively were the proposed ITCES-IoT attains about 765kbps which is around 480kbps better than ECET-IoT, 409 kbps better than DRTP-IoT and 307 kbps better than RCDA-IoT. The proposed ITCES-IoT attained maximum throughput hence it concentrates on both the reduction of power utilization and the increase of network security. Through this trust-based clustering process and node trust calculation, the malicious data transmission and data loss are neglected, leading to an increase in the generated ratio of data packets in the network, which increases throughput.

B. Packet Delivery Ratio (PDR) Calculation

It is the ratio between the amounts of data packets effectively transmitted from source to destination among the nodes. The mathematical analysis for the PDR is given in equation (12).

$$PDR = \frac{no\ of\ packet\ received}{Total\ number\ of\ packets\ sent} \times 100 \quad (12)$$

The Figure 6. depicts the PDR calculated of the proposed ITCES-IoT and earlier methods ECET-IoT, DRTP-IoT, and RCDA-IoT. The x-axis shows the node usage and the y-axis shows the values of PDR in percentage correspondingly.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *05 July 2023* ***Revised:*** *25 August 2023* ***Accepted:*** *15 September 2023*

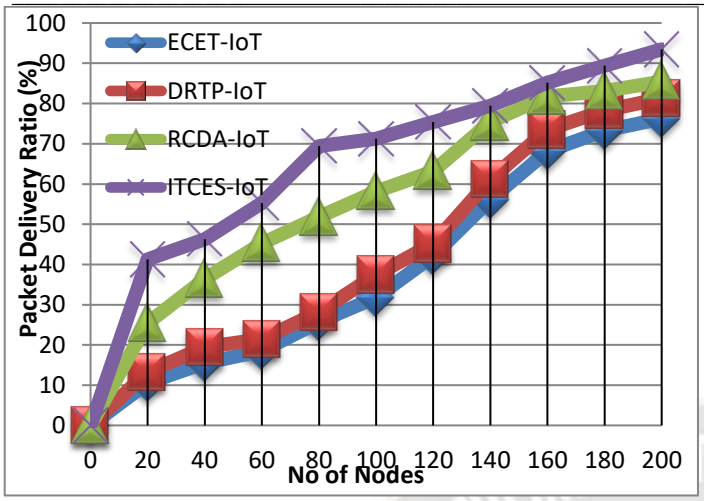

Figure 6. - Packet Delivery Ratio Calculation

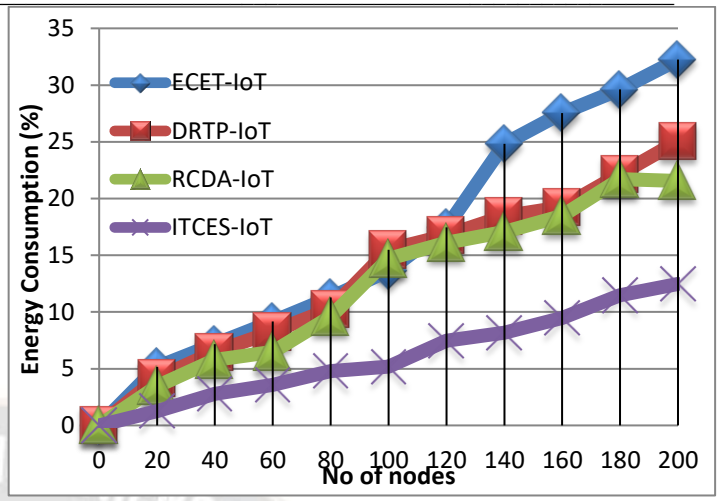

Figure 7 - Energy Consumption Calculation

The PDR obtained by the baseline methods like ECET-IoT, DRTP-IoT and RCDA-IoT are 76.25%, 81.27% and 85.47% respectively were the proposed ITCES-IoT attains about 93.46% which is around 15% better than ECET-IoT, 12% better than DRTP-IoT and 8% better than RCDA-IoT. The PDR is high in proposed ITCES-IoT comparatively and it is attained using the presence of both the trust analysis and clustering process. The rate of the packets which is successfully received by the destination is highly increased here because of the effective trust analysis that results in the increase of network stability.

C. Energy Consumption Calculation

It is defined as the total energy spent in the entire simulation. The mathematical manifestation of energy consumption is given in equation (13).

$$Energy_{Consumed} = \frac{1}{p}\sum_{n}^{p} E_n \qquad (13)$$

Where p represents the neighbors in multi-hop routing and E_n is the energy of the n^{th} hop node. The Figure 7. shows the energy consumption comparison of the methods such as ECET-IoT, DRTP-IoT, RCDA-IoT, and the proposed ITCES-IoT. The x-axis implies the node count and the y-axis implies the energy consumption in percentage.

The energy consumption obtained by the baseline methods like ECET-IoT, DRTP-IoT and RCDA-IoT are 32.25%, 25.05% and 21.56% respectively were the proposed ITCES-IoT attains about 12.47% which is around 20% lower than ECET-IoT, 13% lower than DRTP-IoT and 9% lower than RCDA-IoT. The energy consumption of ITCES-IoT is comparatively lower because it highly concentrates secured and energy-efficient communication among the nodes, CHs, and sink and that leads to an increase in the communication quality among the nodes.

D. Packet Loss Calculation

It is defined as the inconsistency of the time of packet arrival at the destination. Packet loss happens during the time of various network paths present to achieve a similar receiver place. Figure 8. shows the packet loss for protocols such as ECET-IoT, DRTP-IoT, RCDA-IoT, and the proposed ITCES-IoT approach. The x-axis represents the count utilized in the simulation and the y-axis represents the packet loss in packet count. The packet loss obtained by the baseline methods like ECET-IoT, DRTP-IoT, and RCDA-IoT are 546 packets, 412 packets, and 358 packets respectively where the proposed ITCES-IoT attains about 254 packets which are around 292 packets lower than ECET-IoT, 158 packets lower than DRTP-IoT and 104 packets lower than RCDA-IoT. With the presence of an effective trust-based clustering process and effective trusty path selection in the ITCES-IoT approach the transmitted packets are received by the destination nodes in an effectual way so that there is no change for this data loss in the network.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *05 July 2023* ***Revised:*** *25 August 2023* ***Accepted:*** *15 September 2023*

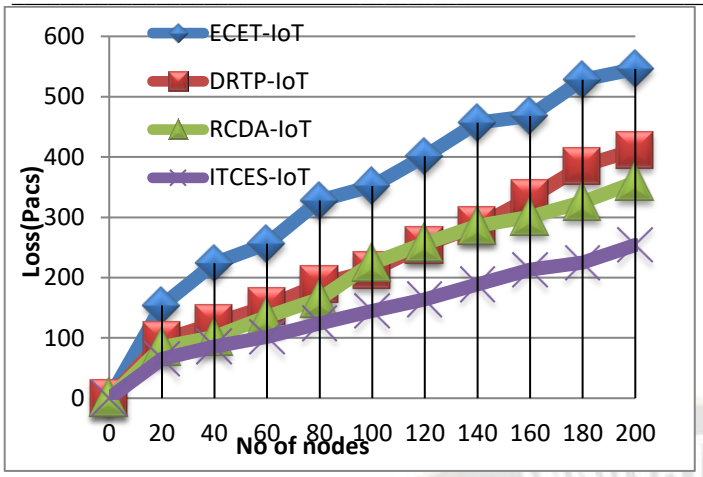

Figure 8 - Packet Loss Calculation

E. End-to-End Delay Calculation

It is the measure of time variation during the time of data transmission among the nodes. It is highly essential to reduce the delay to attain effective communication among the nodes. The Figure 9. shows the graphical representation of the delay calculation for the protocols such as ECET-IoT, DRTP-IoT, RCDA-IoT, and the proposed ITCES-IoT approach. The y-axis implies the node's utility and the y-axis implies the delay in terms of ms.

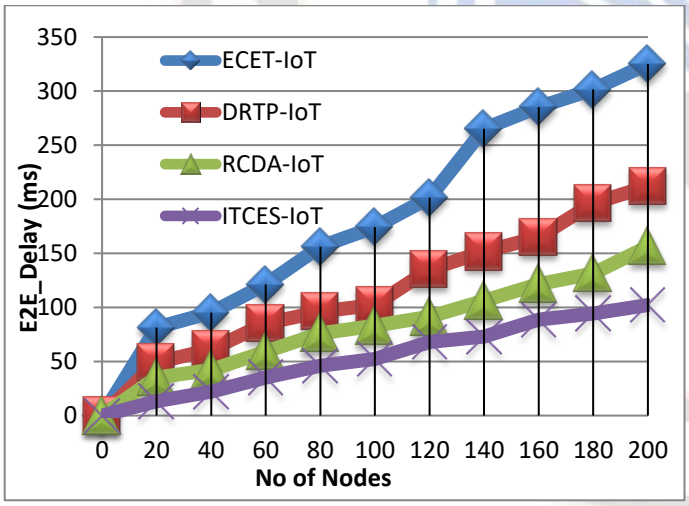

Figure 9. – End to End Delay Calculation

The delay obtained by the baseline methods like ECET-IoT, DRTP-IoT and RCDA-IoT are 325ms, 212ms and 156ms respectively were the proposed ITCES-IoT attains about 102ms which are around 223ms lower than ECET-IoT, 110ms lower than DRTP-IoT and 54ms lower than RCDA-IoT. The data which gets transmitted in the proposed ITCES-IoT approach selects the optimal path to reach the destination with minimum power utilization so that the overall end to end delay is lower for the nodes in the network and as the results the reliability of the network is increased.

F. Packet Delivery Ratio with Attacks

In Figure 10. the delivery ratio with the presence of bad mouthing and ballot stuffing attacks is calculated as without the presence of attacks are also noted. From this figure it is understood that with the presence of trust values calculation how much delivery ratio of the attacks are increased.

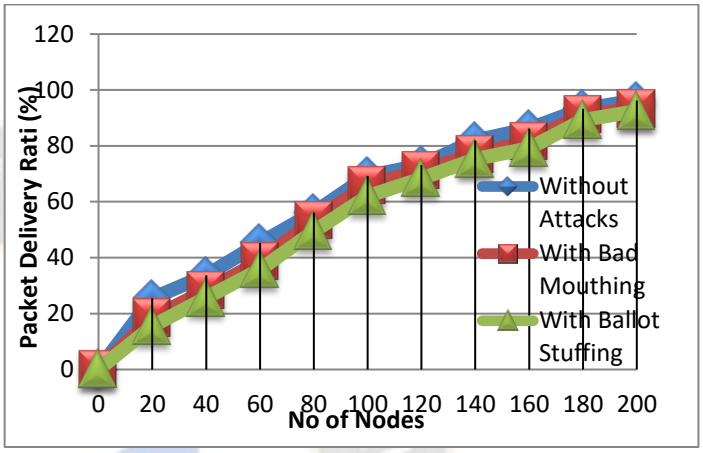

Figure 10. – Packet Delivery Ratio with Attacks

In this figure the performance is analyzed were the PDR without attacks reaches up to 96.25%, with bad mouthing and trust reaches up to 93.25% and with ballot stuffing attack with trust reaches up to 92.46%. With the presence of effective trust calculation and clustering process even with the intrusion of attacks the network performed communication in a stable manner

G. Packet Loss with Attacks

In Figure 11. the performance of the proposed ITCES-IoT approach is calculated with and without the presence of attacks. The curves in the figure represent without attacks, bad mouthing with trust, and ballot stuffing with trust calculations. In this figure the performance is analyzed were the packet loss without attacks reaches up to 754 packets, with bad mouthing and trust reaches up to 723 packets and with ballot stuffing attack with trust reaches up to 701 packets. The performance proves the betterment in the results with the presence of trust calculation and it is understood that the proposed ITCES-IoT attains effective performance even with the presence of attacks in the network.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *05 July 2023* ***Revised:*** *25 August 2023* ***Accepted:*** *15 September 2023*

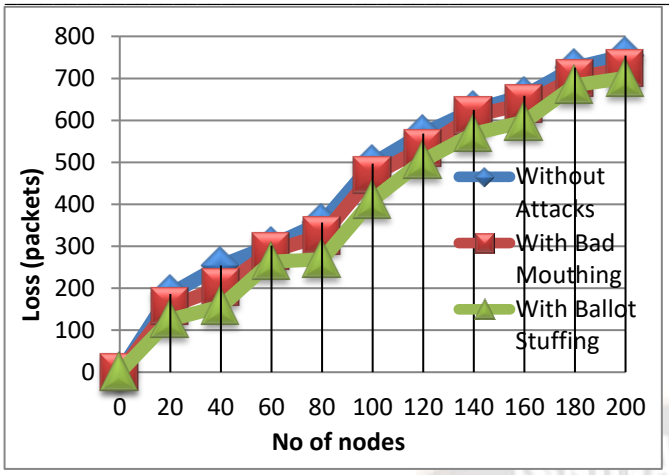

Figure 11. – Packet Loss Ratio with Attacks

H. Delay Calculation with Attacks

In Figure 12. the delay is measured with and without the presence of attacks like bad mouthing and ballot stuffing. In this figure, the performance is analyzed where the delay without attacks reaches up to 89ms, with bad mouthing and trust reach up to 102ms, and with ballot stuffing attack with trust reaches up to 115ms. From the final outcome, it is shown that the proposed ITCES-IoT performed better in terms of the trust-based clustering process.

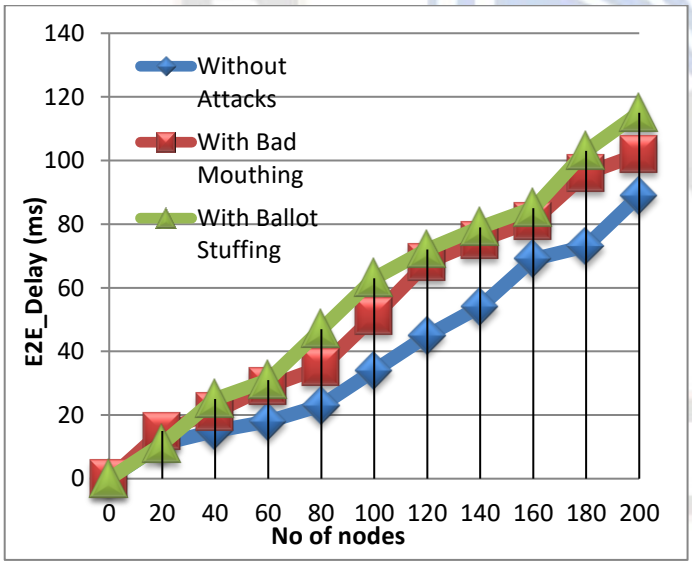

Figure 12. – Delay Calculation with Attacks

After analyzing the results, it is understood that the ITCES-IoT performance in terms of attacks is high comparatively. Through our trust-based CH selection process the attacks are neglected effectively in the IoT environment and that results in stable communication among the IoT devices.

VII. CONCLUSION

Finally, the research article titled “A Design of Improved Trust-based Clustering Approach to Enhance the Energy Computation in Secured Internet of Things (IoT)” demonstrates the major advantage of using the trusted clustering process in IoT. Due to improper CH selections and lack of security in the earlier research, certain drawbacks are created like high energy consumption, packet loss, and delay. In this proposed ITCES-IoT; network formation is customized, the clustering process is sequentially performed, trust-based node selection is established with selective pathways, and it includes an effective communication system, as the whole the proposed ITCES-IoT is effective enough to attain high-quality in data transmission. The simulation of this approach is experimentally demonstrated in NS2 network simulator and the parameters taken for value analysis are PDR, network throughput, and packet loss, and energy consumption. The results are compared to the earlier base methods such as ECET-IoT, DRTP-IoT, and RCDA-IoT. From the results it is proven that the proposed ITCES-IoT attains 307kbps to 480 kbps better throughput, 8% to 15% higher PDR, 9% to 20% lower energy consumption, 104 packets to 292 packets lower packet loss, 54ms to 223 ms lower delay when compared with baseline methods in terms of communication performance. In terms of attack performance, the differences are very low in the proposed ITCES-IoT so that it can able to attain effective communication among the nodes.

REFERENCES

[1] Z. Ma, L. Liu and W. Meng, Towards Multiple-Mix-Attack Detection via Consensus-based Trust Management in IoT Networks, Computers & Security (2020), doi:https://doi.org/10.1016/j.cose.2020.101898.

[2] C. Marche and M. Nitti, "Trust-Related Attacks and Their Detection: A Trust Management Model for the Social IoT," in IEEE Transactions on Network and Service Management, vol. 18, no. 3, pp. 3297-3308, Sept. 2021, doi: 10.1109/TNSM.2020.3046906.

[3] B. Qolomany, I. Mohammed, A. Al-Fuqaha, M. Guizani and J. Qadir, "Trust-Based Cloud Machine Learning Model Selection for Industrial IoT and Smart City Services," in IEEE Internet of Things Journal, vol. 8, no. 4, pp. 2943-2958, 15 Feb.15, 2021, doi: 10.1109/JIOT.2020.3022323.

[4] N. V. Abhishek, A. Tandon, T. J. Lim and B. Sikdar, "A GLRT-Based Mechanism for Detecting Relay Misbehavior in Clustered IoT Networks," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 435-446, 2020, doi: 10.1109/TIFS.2019.2922262.

[5] I. Hafeez, M. Antikainen, A. Y. Ding and S. Tarkoma, "IoT-KEEPER: Detecting Malicious IoT Network Activity Using Online Traffic Analysis at the Edge," in IEEE Transactions on Network and Service Management, vol. 17, no. 1, pp. 45-59, March 2020, doi: 10.1109/TNSM.2020.2966951.

[6] M. S. Abdalzaher and O. Muta, "A Game-Theoretic Approach for Enhancing Security and Data Trustworthiness

in IoT Applications," in IEEE Internet of Things Journal, vol. 7, no. 11, pp. 11250-11261, Nov. 2020, doi: 10.1109/JIOT.2020.2996671.

[7] X. Xu, N. Hu, M. Trovati, J. Ray, F. Palmieri and H. M. Pandey, "DLCD-CCE: A Local Community Detection Algorithm for Complex IoT Networks," in IEEE Internet of Things Journal, vol. 7, no. 5, pp. 4607-4615, May 2020, doi: 10.1109/JIOT.2019.2960743.

[8] M. Sadrishojaei, N. J. Navimipour, M. Reshadi and M. Hosseinzadeh, "A New Preventive Routing Method Based on Clustering and Location Prediction in the Mobile Internet of Things," in IEEE Internet of Things Journal, vol. 8, no. 13, pp. 10652-10664, 1 July1, 2021, doi: 10.1109/JIOT.2021.3049631.

[9] T. Qiu, B. Li, X. Zhou, H. Song, I. Lee and J. Lloret, "A Novel Shortcut Addition Algorithm With Particle Swarm for Multisink Internet of Things," in IEEE Transactions on Industrial Informatics, vol. 16, no. 5, pp. 3566-3577, May 2020, doi: 10.1109/TII.2019.2925023.

[10] U. Panahi, C. Bayılmıs, "Enabling secure data transmission for wireless sensor networks based IoT applications," Ain Shams Engineering Journal,vol.14, no. 101866, pp. 1-11, 2023.

[11] D. Mishra, B. Naik, J. Nayak, A. Souri, P. Byomakesha Dash, S. Vimal, " Light gradient boosting machine with optimized hyperparameters for identification of malicious access in IoT network," Digital Communications and Networks, vol. 3, pp. 125–137, 2023.

[12] K.S. Roy, S. Deb, H.K. Kalita, A novel hybrid authentication protocol utilizing lattice-based cryptography for IoT devices in fog networks, Digital Communications and Networks (2023), doi: https://doi.org/10.1016/j.dcan.2022.12.003.

[13] S. Mirdula, M. Roopa, "MUD enabled deep learning framework for anomaly detection in IoT integrated smart building," e-Prime - Advances in Electrical Engineering, Electronics and Energy, vol.5, no. 100186, pp.1-15, 2023.

[14] M. Šarac, N. Pavlović, N. Bacanin, F. Al-Turjman, S. Adamović, "Increasing privacy and security by integrating a Blockchain Secure Interface into an IoT Device Security Gateway Architecture," Energy Reports, vol.7, no. 8075-8082, pp. 1-8, 2021.

[15] C. Chauhan, M. K. Ramaiya, A. S. Rajawat, S B Goyal, C. Verma, M. S. Raboaca, "Improving IoT security using elliptic curve integrated encryption scheme with primary structure based block chain technology," International Conference on Innovative Data Communication Technology and application, Procedia Computer Science, vol. 215, pp. 1-11, 2022.

[16] B. Lal, S. Ravichandran, R. Kavin, N. Anil Kumar, Dibyahash Bordoloi, R. Ganesh Kumar, "IOT-based cyber security identification model through machine learning technique," Measurement: Sensors, vol. 27, no. 100791, pp. 1-8, 2023.

[17] M. T. Al Ahmed, F. Hashim, S. J. Hashim, A. Abdullah, "Hierarchical blockchain structure for node authentication in IoT Networks," Egyptian Informatics Journal, vol. 23, pp. 345-361, 2022.

[18] Z. Liu, D. Yang, S. Wang, H. Su, "Adaptive multi-channel Bayesian graph attention network for IoT transaction security," Digital Communications and Networks, 2023, doi: https:// doi.org/10.1016/j.dcan.2022.11.018.

[19] L. Elhaloui, M. Tabaa, S. ElfilalI, E. Benlahmer, "Dynamic security of IoT network traffic using SDN," Procedia Computer Science, vol. 220, pp.356–363, 2023.

[20] G. Ravi, M. Swamy Das, K. Karmakonda, "Reliable cluster based data aggregation scheme for IoT network using hybrid deep learning techniques," Measurement: Sensors, vol. 27, no.100744, pp. 1-12, 2023.

[21] B.H.D.D. Priyanka, P. Udayaraju, C. S. Koppireddy, A. Neethika, " Developing a region-based energy-efficient IoT agriculture network using region- based clustering and shortest path routing for making sustainable agriculture environment," Measurement: Sensors, vol. 27, no. 100734, pp. 1-14, 2023.

[22] X. Sáez-de-Cámara, J. L. Flores, C. Arellano , A. Urbieta, U. Zurutuza, "Clustered federate d learning architecture for network anomaly detection in large scale heterogeneous IoT networks," Computers & Security, vol. 131, no. 103299, 2023.

[23] P. Ajay, B. Nagaraj, R. Arunkumar and Ruihang Huang, "Enhancing computational energy transportation in IoT systems with an efficient wireless tree-based routing protocol", Results in Physics, vol. 51, no. 106747, 2023, doi: 10.1016/j.rinp.2023.106747.

[24] A.B. Feroz Khan, Mohammed Muzaffar Hussain, S. Kalpana Devi and M.A. Gunavathie, "DDoS attack modeling and resistance using trust based protocol for the security of Internet of Things", Journal of Engineering Research, vol. 11, 2023, doi:10.1016/j.jer.2023.100058.

[25] Guguloth Ravi, M. Swamy Das and Karthik Karmakonda, "Reliable cluster based data aggregation scheme for IoT network using hybrid deep learning techniques", Measurement: Sensors, vol. 27, no. 100744, 2023, doi: 10.1016/j.measen.2023.100744.