JOURNAL OF ENGINEERING AND COMPUTATIONAL INTELLIGENCE REVIEW (JECIR)

Volume 3, Issue 2, 2025
https://jecir.com/

A TRUST MANAGEMENT-BASED ENERGY EFFICIENT MESSAGE SCHEDULING ALGORITHM IN THE INTERNET OF THINGS SYSTEM

Shanza Ijaz[1], Muhammad Talah Zubair[2]

Affiliations

[1] Department of Computer Science and Information Technology Islamia University of Bahawalpur, Punjab
shanzamalik092@gmail.com
[2] Department of Computer Science National College of Business Administration & Economics (NCBAE), Multan
talhazubair009@gmail.com

Corresponding Author's Email

[1]talhazubair009@gmail.com

Abstract
Internet of Things (IoT) is an emerging concept in internet development that connects diverse objects by transmitting information from there to a central hub for interpretation. Though much work has been done individually either on message scheduling or provisioning of a secure environment to assure data accuracy in IoT systems, this paper focuses on a Trust Management-Based Scheme to defend against internal attacks while parallel handling Message Scheduling to improve overall IoT system efficiency. Choosing, secure cluster heads based on residual energy and node density to balance the network load through a trust-value scheme and operating the message scheduler on cluster heads to decide the transmission of messages is a salient feature of the proposed system. Managing traffic intensity for scheduling messages in a secure environment made the proposed algorithm more reliable against malicious attacks and energy consumption.
In this IoT environment, things/nodes are placed into subgroups with a trusted cluster head responsible for successful message delivery from the group to the receiver of the sensed data. The simulation results show the effectiveness and efficiency of the proposed algorithm.

Keywords
Internet of Things, Wireless Sensor Network, Scheduling, Energy Efficient, Message Scheduling, Trust Management

INTRODUCTION

Internet of things (IoT) and Wireless sensor networks (WSN) are today's rising technologies. The added technology in WSN is IoT which can connect the sensing objects to the cloud via the internet. The sensors (nodes) are tiny and low-priced computational objects that sense the valuable information from the surrounding, aggregate and then send it to the base station for necessary processing [1]. These networks are used in many fields, making them sophisticated like smart healthcare, smart home, smart city, smart transportation, smart agriculture system, and much more. Numerous sensor nodes deployed in a scattered manner in the wild and unattended surroundings, in addition to resource constraint issues, are the most challenging matter in WSN. Although there are, several research challenges still exist in the WSN domain, however, prolonging lifetime, routing strategy, and security issues are the most demanding ones to improve the efficiency and accuracy of the sensed data [2].

The lifetime of sensor nodes due to the limited power resources of sensor nodes is a supreme issue that can be sorted by proper message scheduling and routing. Routing protocols such as LEACH play a vital role in extending lifetime by minimizing the energy consumption in IoT systems. LEACH is a TDMA-based MAC hierarchal routing protocol [3]. It can distribute the energy load randomly using the probability algorithm. The first phase, which is the set-up state, sets up the cluster and selects the cluster heads. Then, it generates a random value for every node and compares it with the threshold function's value, thus improving the energy efficiency of the clustered-based network. The second phase is the steady state; it transmits the information

from the nodes to the cluster heads. The cluster heads will aggregate the received data, compress the gathered information and, following the routing rules, the cluster heads will send the data to the base station [4].

These two phases are applied for LEACH in every round. In the random selection of cluster heads, the probability of low-energy nodes becoming cluster heads also increases. Therefore, it can cease not only the entire network but also the security of the cluster. Moreover, LEACH does not guarantee the optimal number of cluster heads and their balanced load in the network. The security against internal attacks is also not supported in this protocol. Thus, a trust management-based approach can be incorporated to secure the network against malicious attacks [5].

Service provisioning for heterogeneous messages in energy-aware secured systems, sent by different nodes to their cluster head can affect the lifetime of nodes by reducing the response time. This is because different messages have different sizes and parameters like message expiry time, request time period, etc. So, poor data processing and poor data transmission mean a compromise in service quality and battery life of nodes. Thus, running a message scheduler on secured cluster heads at the application layer can enhance the lifetime of nodes and ultimately the entire network [6].

PROBLEM STATEMENT

IoT has become an emerging technology nowadays and is the root of the future of the internet. The basic idea that things can communicate takes the IoT devices to address the critical and unattended areas through the wireless sensor network otherwise, which are difficult to approach by humans. As the sensors(devices) are dispersed mostly primarily in an unattended environment, they are at the security risk of malicious attacks, more energy consumption, and network lifespan limitation due to non-rechargeable battery sources.

The primary purpose of the research is to make the entire IoT system energy efficient by combining trustworthy communication among nodes against internal attacks and controlling the traffic of heterogeneous messages by improving service response time. While most of the work in energy-aware schemes for WSNs has not considered this aspect. Therefore, implementing a trust management scheme along with application-level message scheduling will help retain the nodes' energy level for a longer lifetime. Moreover, it utilizes a LEACH-based clustered network along with targeting the load balancing of the cluster heads for data collection and network routing to improve the network's lifetime.

RESEARCH QUESTION

The questions behind the motivation were:

1. How effective will an algorithm be if I implemented it on a secure wireless sensor network based on trust management and message scheduling?
2. Is the scheme capable of providing a non-compromised trustworthy system that can manage the traffic intensity of incoming messages to provide a stable collision-free IoT environment?
3. Will, the proposed system, be efficient for saving the energy of sensors by implementing security and scheduling simultaneously as their batteries are non-rechargeable, so energy constraints are valued much.

BACKGROUND

A. Internet of Things

Nowadays, the internet of things is an emerging technology that uses wireless sensors to make a network that acts as a bridge between the virtual world and the physical world [7]. The wireless sensor network used in IoT is composed of sensors that sense any change in the surrounding environment and then send the sensed data to the base station (sink) for necessary action accordingly. WSNs have been rapidly used due to their low cost, simplicity, ease of deployment, and less area occupied by needed apparatus. In IoT, things are web-enabled, which can be any object having an assigned IP address to transfer information of sensed environment over the network. So, it is a network of networks that are groups of millions of interconnecting devices of daily requirements.

The idea of connecting things was originated by Kevin Ashton who invented the term internet of things (IoT) in 1999 for things talking to each other via the internet without human intrusion [8]. He was working at Procter and Gamble (now MIT's Auto-ID center) at that time. In the proposed methods, all things were supposed to be connected to global networks via communication methods. This brought attention to sensors and RFID (radio frequency identification). This technique enables the objects to gather and process the data using cloud computing for targeted results. Thus, the futuristic internet innovations will be the extension of IoT.

B. Elements of IoT:

The elements of IoT make this network perform well in the deployed area. It is composed of standard devices. Every device plays a vital role in the critical process of the IoT system. The detail is as:

C. Smart Devices and Sensors

One of the most important elements of IoT is sensors. A sensor is a small device that monitors the sensing field in which it is deployed. It gathers the required data and then sends it to the targeted device for further processing. Sensors are usually low-priced elements of an IoT network that uses considerably low battery power. A lot of work is going on towards low energy consumption to prolong the life of sensors. These devices can be linked to a wireless network via Zeebee, Zee-wave, WiFi or Bluetooth, etc. Devices and sensors belong to the device connectivity layer.

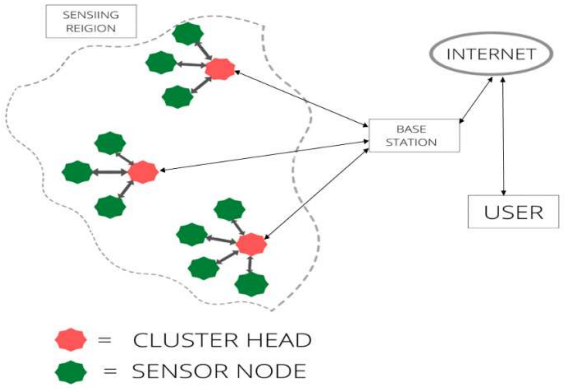
Common sensors are:

- Temperature sensors
- Pressure sensors
- Light intensity detector sensors
- Humidity sensors
- RFID tags
- Proximity Detection sensors

Table 1: Layers of IoT

Layer of IoT	Key Features	Technologies	Security Challenges
Perception Layer	Handles Sensing, Recognizing identification, actuation and communication	RFID, WSN, GPS, Bluetooth	Device tracking, spoofing secure localization, traceability, Unauthorized accessibility, Sybil attacks, Node subversion , false node, black hole attack, key hacking
Network layer	Establishes connectivity and transmits data	Ad hoc network, internet, routers, GPRS Wi_Fi	Malicious attacks, hacking of tranmiited information, routing information ID
Application Layer	Managing devices, terminal and user interfaces	Cloud based computing, Service support platforms	Physical meter tempring, customer privacy hacking, broad cast of forged information, session stealing attacks
Network management		Security management	Trust management

Fig 1. Typical wireless sensor network



A Wireless Sensor Network can be categorized as a **Structured** WSN, and an **un-structured** WSN. In structured WSN all nodes are deployed in a pre-planned manner whereas in un-structured WSN nodes are thick and deployed in an ad-hoc manner in a specific area.

In WSN, there are two ways of communication:

Single Hop: In this type direct communication of data takes place between the sensor node and base station. Nodes can communicate or transfer data with each other.

Multi-Hop: In this type of communication nodes send their information to the node which is nearest to the base station. That node that sends data to the base station is responsible for aggregating and sending the collected information of neighboring nodes to the base station for further processing of data. Many nodes can take part in this process.

In recent years, WSN has been widely used in different fields of life including environment monitoring, defense, medical sciences, etc. Along with its advantages, it has many disadvantages too.

Two major topologies or architectures of WSN:

The wireless sensor network is mostly based on two major topologies or architecture.

- **Distributed architecture (Flat architecture):** In this architecture, the **sensor node** directly sends its sensed data to the **sink node** or base station. The sink node will be liable for collecting the data from the sensor node and processing it.
- **Cluster-based architecture (Hierarchal architecture):** In this architecture**, the sensor node or cluster member** transmits its sensed data to the **cluster head.** Here, the cluster head is responsible for collecting the data from the sensor nodes of its region, aggregating it, and then forwarding it to the **base station/sink node** for further processing. The sink node will receive data from the cluster head and do the necessary action on it.

Cluster-based architecture is an ideal architecture for large networks. In the coming years, the things connected to the internet are going to be over 30 billion via wireless networks. As, the IoT network grows, connecting each device directly to the base station required an internet connection for each device. It will also increase the traffic load on the base station. Thus, it will affect the nodes' energy, especially in the case of long waiting queues. It can be overcome by dividing the sensor nodes of the IoT network into groups called clusters. Each cluster with a head node called a cluster head (CH) node. The cluster head will collect the data from the sensor nodes of its group, aggregates it, and then transfers it to the sink node. Thus, it saves energy by reducing the overhead of routing.

As the cluster head has a vital role in communication and transferring all data from sensor nodes of a cluster to the base station, for CH it is necessary to have more energy and trustworthiness. Therefore, the

election of a secure cluster head is necessary for the proper and trustful work of a group. Moreover, scheduling the traffic of messages on the cluster head side will help save energy for the entire cluster.

D. Trust Management Technique Literature Review

In this section, a literature review of the related work done on the trust management (TM) scheme and the protocol optimization relevant to this technique is going to be discussed. Here, we will also take a little glance at the enhancement in the evolution of the LEACH protocol. Up till now, many trust management techniques have been introduced for wireless sensor networks, social networks, and, peer-to-peer systems. In these techniques, trust calculation is mostly based on the direct observations of each sensor node regarding the others and the indirect recommendations received from other nodes about the service providers.

E. Trust management models and schemes

Trust management-based schemes are limited by hardware resources, so behavior-based trust schemes are adopted mostly. The said scheme was introduced by [9]. These schemes keep the WSN prone to internal attacks which otherwise can result in malicious behavior of nodes.

Trust management in IoT enables trustworthy data gathering and context awareness. It enhances privacy in terms of security. The said technique is grouped into four classes: recommended trust, prediction-based trust, policy-based trust, and, a reputation-based trust scheme. These groups are further compared in terms of some trust metrics like accuracy, adaptability, availability, heterogeneity, integrity, privacy, reliability, and scalability. Exploring more efficient and reliable methods for trust management in IoT in the future is also suggested [10].

A trust-based formal model for fault detection in WSN was suggested by [11] given the name of TFM. The authors previously described their work in the said field of fault detection with the name of 'A comprehensive trust model based on multifactor'. The current model is an enhancement for the redeployment of network parameter adjustment. TFM can tackle the fault discovery progression and check faults deprived of simulating and running a wireless sensor network. The proposed method is based on the 'Petri nets' by considering the time of data sensed, the weight of each factor, and the threshold for a decision. An efficient analysis algorithm of TFM is given for structured recognition models. The assessment of the node is obtained from the trust value, firing time, weights, and threshold parameters. Finally, the proposed model is implemented with the Generic Modelling Environment (GME) and the efficiency is illustrated with examples to describe the fault detection feature and identify faults in advance for the sensor network.

F. Protocol optimization and feature enhancement in LEACH

It is the set of rules that how trust management protocols will interact with TM- related decision information and how security can be implemented in this scenario.

An adaptive trust-based routing protocol (ATRP) is proposed by [12] that considers multiple factors like resources and security in a trustworthy manner in a pairwise comparison. The nodes in the wireless sensor network rely on neighboring nodes due to the absence of a centralized information hub. Thus, evaluation criteria for a reliable means of data have become a challenging task. In the proposed system, a hierarchical mechanism for nodes is adopted, and along with direct and indirect trust, a new form of trust, that is witness trust, also introduced that considers multiple factors about multiple hops decentralized and randomly distributed WSN nodes. The paper also considered a group of nodes for the best route to choose the best node, but having no inheritor can be eluded. The multi-criterion features considered in the trust metrics in ATRP fit well in randomly distributed networks. The proposed mechanism shows the good performance of the suggested protocol in terms of lifespan, transmission delay, packet loss, and energy consumption.

Though the cluster-based technique is the most suitable for WSN, unbalanced energy consumption and trusted data communication issues have to be faced in that hierarchal architecture. This work proposed an energy-effective secure routing protocol (EESRP) to enhance the security and energy conservation of the system. It merges three methods: trust management mechanism, optimization algorithm, and key management technique. First, the locations of the deployed sensor nodes are considered along with the trust values of neighboring nodes, which increases the search space and reduces the distance. The secure transfer of data is implemented using the method of Digital Signature Algorithm (DSA) and Elliptic Curve Cryptography (ECC).

After that, to find the secure shortest route trust, key encryption, node's location, and energy parameters are integrated into Particle Swarm Optimization (PSO) and meta-heuristic based Harmony Search (HS) method. The proposed protocol shows that its energy efficiency, scalability, reduced packet loss rate, average throughput, network lifetime, and the average PDR for the attacks are high compared to the rest of the approaches. The suggested framework is appropriate for intrusion detection and trust-based routing systems with the purpose of real-time information analysis [13].

G. The Low energy adaptive clustering hierarchy protocol (LEACH)

is considered one of the top hierarchical protocols. The protocol was proposed by [14] and the basic objective of the proposed LEACH protocol was to improve the energy efficiency in wireless sensor networks. Various modification has been proposed in the historical evolution of LEACH to make the said protocol work more efficient in utilizing less energy for prolonging the life of WSN. To remove the limitations faced in the LEACH (low energy adaptive clustering hierarchy) protocol, the protocol of cluster routing was proposed by [15]. It extends LEACH by finding an appropriate cluster head keeping the minimum degree of distance from the base station to lessen energy consumption in CH nodes and the entire network. The results reveal that the utilization of power is minimized, so the lifetime of a network will be prolonged. With an increase in the number of rounds, the power consumption will be reduced more.

The problems such as strong randomness in clustering and the local optimum number of the nodes in the path optimization in the LEACH protocol were addressed in the article proposed by [16]. The work proposes enhancement in LEACH based on a weighting strategy by optimally combined weighting (OCW) and the interactive ant colony optimization (IACO) algorithm. A dynamic replacement mechanism is adopted to update the cluster head nodes to minimize the network power consumption. It proposes the OCW mechanism to dynamically replace CH nodes in different areas concerning three factors: the node residual energy, density, and distance between the nodes. The transfer of information probability in IACO with a combined local and global update mechanism is used for network distribution and transmission routes in the clusters, which can prolong the life span of the network to a certain extent.

H. Message Scheduling Literature Review

The instruction given to grant the resources of the network to an application or process according to the pre-defined manner for safe resource allocation to save the time and energy of the system is known as the scheduling algorithm. It has an important role in wireless sensor networks and IoT systems and provides the dispersal of the queues including the purpose of which method to execute first.

Quality of Services (QoS) is one of the challenging issues in IoT networks for resource constraints to manage memory, bandwidth, processing power, and energy conservation for WSN nodes. [17], proposed a Virtual Node Schedule for Supporting QoS in Wireless Sensor Network(VNSQW).To increase the good-put, and decrease the latency of the data sent from critical nodes to the base station (sink node), VNSQW provides a service for critical nodes through the provision of additional time slots. VNSQW approach shows a fall in the latency for critical nodes even if the heavy traffic load in the network. The goodput is enhanced for such a network particularly when there is a large number of nodes in the network. But, to get these benefits a little trade-off in terms of additional power depletion by the critical node during excessive data transfer is seen here.

Energy must be preserved as; minimum depletion of energy is required to lengthen the life of WSN. A power-centered scheduling algorithm concerning sleep scheduling, fuzzy logic, and machine learning was proposed to achieve enhanced network efficiency. It distributes the energy consumption fairly among the sensor nodes and adapts a sleep/wake-up scheme to enhance energy preservation. The suggested algorithm manages the traffic of messages in intra-cluster data transmission. This approach makes the entire system energy efficient when no notable change is seen in the continually measured readings of the nodes. When analogous data is sensed for a longer time period, the nodes go to sleep. The algorithm integrates the ideology of fuzzy logic, sleep scheduling, and machine learning which extends the lifespan of the WSN. The proposed algorithm also proved the efficiency of several machine learning methods and minimizes clustering operating cost with dynamic successive cluster update cycles that matters well in clustering procedures. To determine the cluster update cycle; residual energy, average data rate, and distance from the sink have been taken. While,

for the sleep cycle; the residual energy, and cluster update cycle are considered. The algorithm is focused on wireless networks with stationary sensor nodes but, it can be used to manage mobile sensor nodes in the future [18].

Table 2.Comparative analysis

Protocol	QoS parameters	Security	Message Scheduling	Distributed/ Hierarchical	Hop Count	Energy Efficiency
LEACH	Yes	Not considered	No	Hierarchical	Single hop	Yes
TFM	Yes	Considered	No	Hierarchical	Multi hop	Not considered
LEACH-TM	Yes	Considered	No	Hierarchical	Multi hop	Yes
EOSR	No	Considered	No	Distributed	Multi hop	Yes
An Energy-efficient Message Scheduling Algorithm in Internet of Things Environment	Yes	Not considered	Yes	Hierarchical	Single hop	Yes
Fuzzy Based Sleep Scheduling Algorithm with Machine Learning Techniques	Yes	Not considered	Yes	Hierarchical	Multi hop	Yes
Proposed Model	Yes	Considered	Yes	Hierarchical	Multi hop	Yes

SYSTEM ARCHITECTURE

A. Proposed Trust Management-based Energy Efficient Message Scheduling Scheme

To deploy the proposed trust management-based message scheduling scheme; we are implementing a cluster-based hierarchical routing network. In these networks, the entire IoT group of sensor nodes is divided into subgroups. Each subgroup selects its head node which is known as a cluster head or broker and here every node can become a cluster head each time. The CH is responsible for collecting, aggregating, and transferring the data from its surrounding member nodes to the ultimate sink or base station.

The proposed trust management-based scheduling scheme will do the following tasks to reach its goal or purpose:

- The proposed system will use a beta distribution-based trust management scheme to choose the secure nodes along with trustworthy cluster heads and locate the malicious nodes.
- The proposed scheme will implement application layer message scheduling in terms of service provisioning by reducing response time.

- For scheduling, it will be based on SPT (shortest processing time) first concept and M/M/1 queuing model.
- The proposed scheme will implement the first-order radio energy consumption model to enhance the energy efficiency and lifespan of the wireless sensor network.

B. Energy Consumption Model

Here, the first-order radio energy consumption model is used as in [19, 20]. Consider a network having N randomly dispersed nodes. These nodes form clusters of different sizes in WSN and have a master node in each cluster called a cluster head. CH will receive messages from other nodes within its specific cluster or subgroup. It is assumed that initially, all sensing nodes have the same ability to sense, process, and transmit data with equal initial energy. Consider that the base station is fixed and exists far away from deployed sensors. To make the system scalable, data fusion is introduced into the routing protocol to reduce the load of data sent and minimize the energy consumption in the aggregation of packets being transferred to the base station.

In the transmission process, first, the cluster heads gather messages from its neighboring nodes and compress the gathered data, and then forward it to the base station. During this transmission of data, the signals are intensified to ensure a safe message communication to the destination. The energy used to send k bits of message r between the transmitter and the receiver circuitry is as follows:

$$E_{T_r}(k,d) = E_{elec} * k + \mathcal{E}_{amp} * k * d^n \quad (1)$$

Where E_{T_r} represents the total transmission energy consumed during the transmission of a 'k' bit message up to a distance d, E_{elec} the energy dissipated to run the transmitter or receiver circuit, $\mathcal{E}_{amp}$ is the amplification characteristic constant corresponding to the free space propagation model or the mulita-path attenuation propagation model (energy used to amplify the signal enough to reach the destination). d is the distance between two points that could be cluster heads, sensors, or base station/receiver, 'n' takes the value of 2 or 4 depending on the free space or multi-path fading.

At the receiving end the energy consumed to receive k bits of a message r:

$$E_{R_r}(k) = E_{elec} * k \quad (2)$$

C. Use of M/M/1 Queuing Model for Message Scheduling

To manage the arrival rate (request time) and service rate (transmission time), the M/M/1 queue model is used in the proposed system. As it is a clustered-based approach, one node works as a cluster head in each group. It is responsible for managing the working of all connected nodes of the network. A message scheduler runs at the CH level for a smooth communication process and works on the basis of the SPT first rule. The number of messages received by CH is denoted by r, *where* r= *{1, 2, 3, . . . , n}*. By using the M/M/1 queue model as in [21] with the same assumption, we calculate the traffic intensity and then modify the polling frequencies for messages to re-arrange the message requesting order based on the SPT rule first. The arrival and service rates of the r_{th} message are represented by λ_r and μ_r respectively. The traffic intensity ρ of the incoming messages r will be:

$$\rho_r = \frac{\lambda_r}{\mu_r} = \frac{T_{trans_r}}{T_{req_r}} \quad \text{for r=\{1,2,3,…….,n \}} \quad (3)$$

$$\text{so} \quad \rho = \sum_{r=1}^{n} \frac{T_{trans_r}}{T_{req_r}} < 1 \quad (4)$$

Here, T_{trans_r} is the successful transmission time of message *r*. T_{req_r} is the service request time of message *r,* at cluster head. Here, if the traffic intensity ρ is greater or equal to 1, the order of the arrival rate of messages should be adjusted and assigned again for keeping the system in a smooth state. It will be kept on re-calculating until ρ becomes less than 1. Infect, it seems that it is a trade-off between the stability and excellence of the service in an unstable network.

JOURNAL OF ENGINEERING AND COMPUTATIONAL INTELLIGENCE REVIEW (JECIR)

Volume 3, Issue 2, 2025
https://jecir.com/

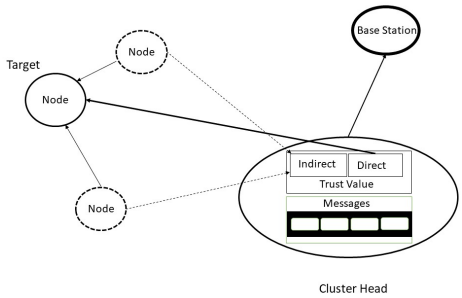


Fig 2. Trust and Message Scheduling of the proposed scheme

D. Beta distribution-based trust management model for the proposed system

The trust management scheme introduced in this paper is based on the work of [22]. The beta distribution system assumes that the interaction between any two nodes, like node 'i' and node 'j', is based on 'cooperative behavior' and 'non-cooperative behavior'. For cooperation, node 'i' will assign '1' to node 'j' otherwise it will rate '0', and similarly, node j will also do so. In this way, a rating will be maintained by a node for the behavior of neighboring nodes. Thus, the trust value range will be at [0,1].

Let α_j and β_j represent the cooperative and non-cooperative behavior of node j from the viewpoint of node 'i'. Then the trust value for the expected behavior of node 'i' to node 'j' will be: $T_{value_{ij}} = \frac{\alpha_j}{\alpha_j+\beta_j}$ (5)

The trust value can effectively increase the security of each node by avoiding the communication channel for compromised nodes.

Similarly, the cluster head will also calculate the trust value of each node. This will participate in a recommended trust value for the current node being evaluated for malicious behavior. This trust value acts as a trust value influencing factor for the election of a cluster head among the candidate cluster head nodes in the current round process. The trust value influencing factor is:

$$T_{value_{fac}} = \frac{node's\ current\ trust\ value}{Avg\ trust\ value\ of\ all\ nodes\ in\ the\ last\ round\ of\ cluster} \quad (6)$$

$$T_{value_{fac}} = \frac{TV_i}{TV_{avg}}$$

Here, TV_i represents the current trust value of node 'i' corresponding to its cluster head. TV_{avg} is the average trust value of all the nodes of that cluster belonging to node i. Therefore, if $T_{value_{fac}} < 1$ then the node is malicious, but if $T_{value_{fac}} \geq 1$ then the node is a trusted one for taking part in the desired process.

In LEACH protocol, the threshold for cluster head in the election round is:

$$Th_{LEACH} = \frac{p}{1-p*(r*mod(1/p))} \quad (7)$$

Where r is the current round number and p shows the anticipated percentage of cluster heads over all the nodes in the entire network. In LEACH, cluster head selection is random, which does not consider the

residual energy of every node. The trust value factor is also incorporated here to make the selection of CH non-compromising. Based on this, we will amend the thresh hold function for cluster head election as:

$$Th(i) = \begin{cases} Th_{LEACH} \times \frac{E_{resi}}{E_{max}} \times \frac{N(i)_{nbr}}{N_{alive}} \times T_{value_{fac}} & \text{if i} \in \text{G} \\ 0 & otherwise, \end{cases} \quad (8)$$

Where Th_{LEACH} is taken from equation(7), $T_{value_{fac}}$ is the trust value taken from equation(6), G is a group of nodes that have not yet become CH, E_{resi} is the remaining energy of the node, E_{max} is the initial energy of node, $N(i)_{nbr}$ is the number of alive neighbor nodes of node 'i', N_{alive} is the total number of alive nodes of the current cluster.

E. Operation Process of Trust Management-based Energy Efficient Message Scheduling Algorithm

[1]The set-up phase for cluster formation and CH selection, and the steady-state phase for the first round are based on the LEACH protocol.

[2]The existing information with the trust value of each node in aggregated form by the CH is sent to the base station via the control packets.

[3]Based on the received information, the base station calculates and broadcasts the number of cluster head nodes for the network.

[4]Each sensor node broadcasts a control packet to a node within a present radius of the cluster and simultaneously confirms the number of neighbor nodes by the number of the received control packet.

[5]Each candidate node for becoming a cluster head node compares with the threshold function value. If the node-generated trust value is greater than the threshold value then, this node can become the CH of the current round.

[6]Each CH has a message scheduler running on it to decide which message should be sent first.

[7]To check the traffic intensity and adjust the polling frequencies M/M/1 queuing architecture is applied at each CH level.

[8]If the traffic intensity of messages is greater or equal to 1, the message requesting order will be rearranged by the SPT rule until the traffic intensity becomes less than 1.

[9]The transmission process of information is based on the LEACH steady phase. Each member node in the cluster sends heterogeneous messages (information). The node transmits the sensed information and the current node information with different parameters (including trust value, message expiry time, request time period, etc) to the cluster head via the data packet and the control packet.

[10]The collected information is then aggregated by the cluster head and transmitted to the base station for further processing.

[11] Repeat the steps from step 3 to step 10 until the network has more dead nodes.

F. Algorithm for the Proposed Scheme

[1] Clustering {

[2] Initialization of the nodes' state;

[3] **For** (Every node) **do** // check node's security

[4] Get the current trust value of the expected behavior of node 'i' to node j:

[5] $T_{value_{ij}} = \frac{\alpha_j}{\alpha_j + \beta_j}$ //αj and βj represent cooperative and non-cooperative behavior

[6] $T_{value_{fac}} = \frac{TV_i}{TV_{avg}}$ // node's current trust value and average trust value of all nodes in the cluster

[7] ***If***$(T_{value_{fac}} \geq 1)$

[8] Secure sensor node; // trusted node

[9] ***else***
[10] Malicious node;
[11] **end if**
[12] **end for**
[13] **For** (Every node) **do** // Cluster head selection phase
[14] ***If*** $(E_{residual} > 0$ && $Flag_{candidate\ node} = TRUE)$ **do**
[15] Choose CH by threshold function;
[16] $$Th(i) = \begin{cases} Th_{LEACH} \times \frac{E_{resi}}{E_{max}} \times \frac{N(i)_{nbr}}{N_{alive}} \times T_{value_{fac}} & \text{if i} \in \text{G} \\ 0 & otherwise, \end{cases}$$
[17] Broadcast (CH-ID); // broadcast the cluster head ID
[18] **end if**
[19] **end for**
[20] **For** (Every Node) **do**
[21] ***If*** $(E_{residual} > 0$ && $Flag_{normal\ nod} = TRUE)$ **do**
[22] ***If*** (Distance in(CH-range) **do**
[23] Normal node sends join message to CH // clustering groups are creating.
[24] **end if**
[25] **end if**
[26] **end for**
[27] CH sends TDMA messages to its member nodes;
[28] **For** r_{th} message:$Message_r(T_{req_r}, T_{trans_r})$ **do**
[29] **For** r_{th} traffic intensity ρ_r **do**
[30] for all $T_{req_r} = T_{inreq_r}$ // T_{inreq_r} : the initial request time period
[31] $\rho_r = \frac{T_{trans_r}}{T_{req_r}}$ where r= {1,2,……,n}
[32] **While** ρ>1 **do**
[33] Sort $Message_r$ in a T_{req_r} descending order; for r={1,2,……,n}
[34] $T_{req_r} = T_{req_r} + \frac{T_{inreq_r}}{2^r}$
[35] $\rho = \sum_{r=1}^{n} \frac{T_{trans_r}}{T_{req_r}}$
[36] **end while**
[37] Request $Message_r$ in descending order of $\mu_r = \frac{1}{T_{trans_r}}$;
[38] **end for**
[39] **end for**
[40] }

G. Description of the Trust Management-based Message Scheduling Algorithm

A network system of sensor nodes is established; then initialization is carried on. Initially, the network nodes are supposed to have the same energy level and select their cluster heads randomly. At the creation of the wireless sensor network, all nodes are supposed to be trustworthy and well-performing. Once the system becomes operational, the chances for the compromised nodes arise. Therefore, to make the system more reliable and energy efficient, nodes' security is checked through the trust management scheme. Then, a

message scheduling scheme will be implemented on each broker which further enhances the energy efficiency. The step-by-step description is:

In the first round, initialization will be based on the LEACH protocol. In the next round, each node's trust value is calculated and sent to the respective cluster head. Each cluster head will also calculate the trust value of all the nodes belonging to its group, then also takes the average trust value of all the nodes in its cluster. On the base of these values, the trust value influencing factor $T_{value_{fac}}$ will be counted to decide whether the node is secured or compromised. If $T_{value_{fac}}$>=1, the node will be considered secured and trustworthy otherwise it is a malicious node.

After the confirmation of the trusty nodes, the cluster head selection procedure runs, then CH is selected on the base of the threshold function. The candidate nodes for the CH election should have a value greater than the threshold function. If it keeps a value lesser than the threshold value; it cannot be a cluster head for the existing round. But, if it qualifies for the cluster head; it will broadcast its CH-ID for the remaining nodes. If these nodes exist within the cluster head range; they will send a join message to their neighboring CH. In this way, the clustering groups will be created.

A secure environment for nodes is created which is safe from internal malicious attacks. Now, on each CH a message scheduler based on M/M/1 queuing model will run. Initially, all messages are supposed to have the same request rate. When the request period will increase gradually with the minimum request period T_{inreq_r}; the traffic intensity will be again calculated by the new value of T_{inreq_r}. If the value of ρ>1, the sequence of the messages will be altered and given a new value again to keep the system in a stable state. This process will carry on. The CH will aggregate and directs the scheduled messages toward the base station for further processing.

RESULT ANALYSIS

We will simulate the proposed system by comparing and analyzing LEACH-TM and LEACH with message scheduling. The energy efficiency, the number of alive nodes, and the lifetime of the network are considered performance metrics for analysis.

A. Simulation Setup and Parameters

MATLAB is used to simulate and confirm the assumed results of the said system. To analyze the network lifetime and its energy efficiency, the proposed model is compared with LEACH-TM and LEACH with features of message scheduling. It is supposed that all the nodes have the same energy level at the beginning, then for the coming rounds of simulation, their energy is deducted as per the role of nodes (cluster head or normal node). In addition, the impact of merging both the trust value and message scheduling in the proposed system is also considered by comparing the same model in the absence of either trust value or scheduling. The simulation parameters are considered from the work of [23, 24].

Parameters	Values
Sensed Area	100*100 m^2
Node number	100
Control Packet Length	150 bits
Data Packet Length	6400 bits
Base Coordinates	(50,200)
E_{elec}	0.01J/bit
E_{max}	0.3J
α, β	5,5

Table 3. Simulation Parameters

B. Network Lifetime and Nodes

The effect of an altered percentage of cluster heads against the number of alive nodes in the lifetime of the system is also analyzed. The graph in Fig. 4.1 shows a comparison of the proposed model with LEACH-TM and LEACH with message scheduling in terms of alive nodes against the percentage of cluster heads. For each proportion of cluster heads, we execute the simulation for up to five rounds. Blue bars depict the alive nodes for the proposed trust management-based message scheduling algorithm. Red bars are for the LEACH-TM (considering only the trust value), while black bars show the LEACH with scheduling (considering only the message scheduling). It confirms that the proposed model in terms of network lifetime is more efficient for saving energy and prolonging the life of the network.

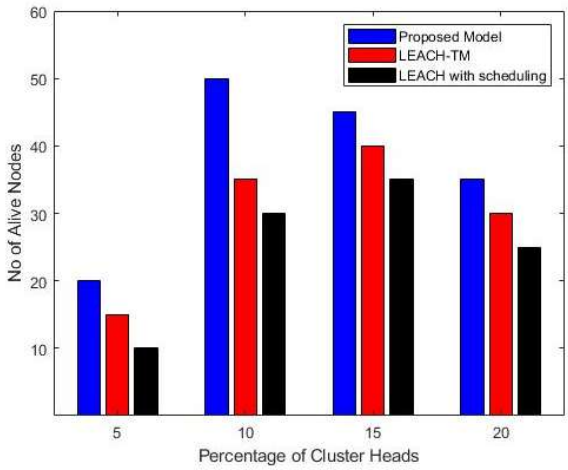


Fig 3 Alive nodes against different percentages of cluster heads

C. Residual Energy of Alive Node

The residual energy of the proposed scheme is analyzed against the LEACH-TM and LEACH with message scheduling. The proposed system with both of the features of trust management and message scheduling proved to be a good energy saver as compared to the protocols having the implementation of either trust value or message scheduling. Fig 4.2 shows that the energy curve for the proposed model is smoother compared to the remaining two methods. It ends at a residual energy level of about 0.05 after 600 hundred rounds. The protocol LEACH with scheduling, due to an imbalance in the selection of cluster heads and lack of security, experienced a rapid decline in the first 400 hundred rounds and ends at zero energy level before the 500 rounds. Therefore, the trust management-based message scheduling algorithm is more energy efficient and helpful for a long network lifetime.

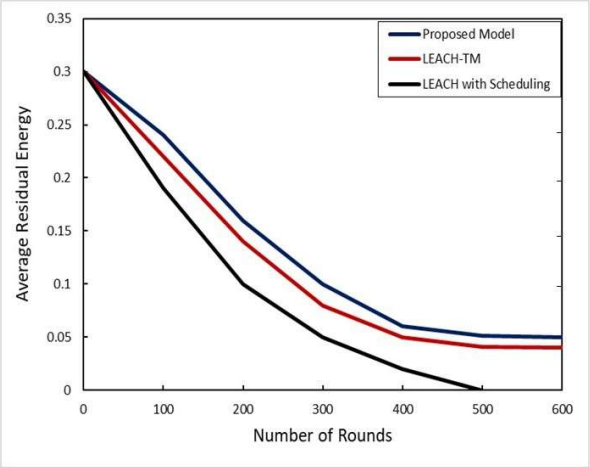


Fig 4. Average residual energy of nodes

D. Comparison of the proposed model in the same scenario without a trust value factor

The proposed system is tested to check whether the presence or absence of the trust value factor can influence the performance of the network under malicious attacks. We assumed that 7 percent of the nodes in the network are malicious. When the system is simulated, it is seen that in the first 25 rounds there is no difference in behavior, but after that, the malicious nodes start to influence the network, and packet loss gets started. Fig 4.3 shows that the packet loss is prominent from 50-200 rounds in the absence of trust value and after that, it inclines down as the malicious attack stops. As the proposed system has the feature of trust value so it can timely detect the compromised nodes. It also prohibits a malicious node to become a cluster head thus, prevent packet loss during the transmission of data, and increase the security of the system.

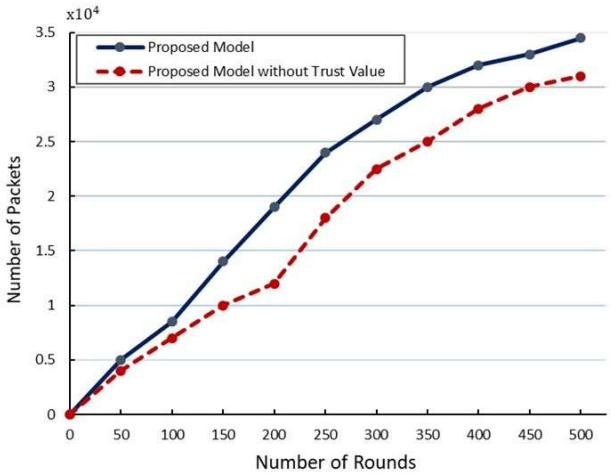


Fig 5 Effect of malicious nodes on the number of packets in the proposed system without trust value

E. Comparison of the proposed model in the same scenario without message scheduling

The model under consideration was also tested to confirm the impact on the system in the absence of the second feature, which is message scheduling. The comparison is done to analyze the impact on the data packets transmitted with and without running the message scheduler on the cluster-based network. The simulation results show that there is an almost smooth transmission of packets for the proposed system, represented by the blue line in fig 4. The transmission of packets is slow for the proposed model in the collision-based system. An unscheduled approach shows an increase in the response time at the cluster head level, resulting in a delay in the transmission time. The incoming messages have to wait for a long time, so it results in a significant slowdown in packet transmission. The simulation proved that the proposed model handles a proper data transmission as the response time has become shortened by the applied SPT rule for the arrangement of messages. Therefore, a timely response to the messages in a scheduled environment leads to a prolonged lifetime and an energy-efficient network.

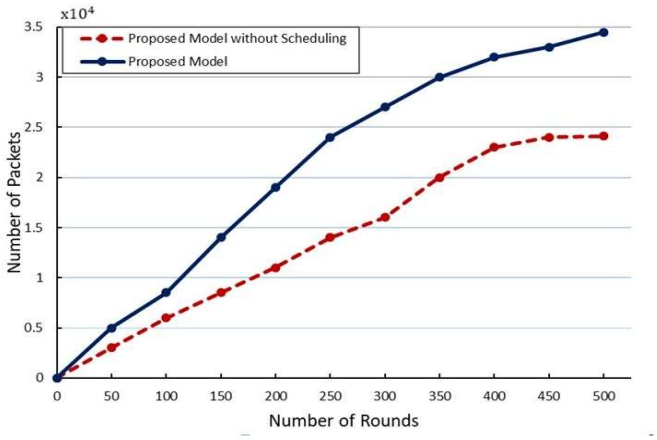


Fig 6 Effect of unscheduled approach on the proposed system

CONCLUSION AND FUTURE WORK

The most popular invention in the age of global networking is the Internet of Things. IoT emerged as the wireless sensor network as a technology through which things using sensors can be accessible to the internet through cloud computing. The limited energy of sensor nodes and their random distribution in the

scattered area is a serious issue to take care of. The most concerning area is how to make the network more energy efficient and reliable for the transfer of data.

This work proposed a trust management-based scheme with message scheduling for safe and collision-free data transmission in the clustered network. The trust management scheme introduced here made the system more secure and reliable against internal attacks. This scheme provides a trusty environment for the transfer of data by making the nodes more secure. Moreover, cluster heads responsible for managing all of the data of the group are selected on the basis of the trust value to make them non-compromised and energy efficient [25,26]. The factor of energy efficiency is further enhanced by introducing a message scheduler working on the cluster head level at the application layer of the network. The SPT approach applied here has shortened the message response time by the arrangement of the incoming stream of messages. Therefore, the unanimous implementation of both the trust management and message scheduling schemes made the proposed system more energy efficient, disciplined, and secure.

The simulation results depict the performance and advantage of the proposed scheme in terms of energy efficiency, network lifetime, effectiveness for mitigating malicious attacks, and managing the traffic intensity of messages.

The future work is to implement the approach of message scheduling while considering high priority and low priority incoming messages to make the proposed scheme more responsive and energy efficient. It can also be enhanced by securing the network not only from internal attacks but also by tackling external attacks.

REFERENCES

[1]. S. Abdullah, M. N. Asghar, M. Ashraf, and N. Abbas, "An energy-efficient message scheduling algorithm with joint routing mechanism at network layer in Internet of Things environment," *Wireless Personal Communications*, vol. 111, no. 3, pp. 1821–1835, 2020, doi: 10.1007/s11277-019-06959-x.

[2]. S. Abdullah and K. Yang, "An energy-efficient message scheduling algorithm in Internet of Things environment," in *Proc. 2013 9th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, 2013, pp. 311–316, doi: 10.1109/IWCMC.2013.6583578.

[3]. A. O. Abu Salem and N. Shudifat, "Enhanced LEACH protocol for increasing a lifetime of WSNs," *Personal and Ubiquitous Computing*, vol. 23, no. 5-6, pp. 901–907, 2019, doi: 10.1007/s00779-019-01205-4.

[4]. S. Ali et al., "An efficient cryptographic technique using modified Diffie–Hellman in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 16, no. 6, 2020, doi: 10.1177/1550147720925772.

[5]. W. Almobaideen, M. Qatawneh, and O. Abualghanam, "Virtual Node Schedule for Supporting QoS in Wireless Sensor Network," in *Proc. IEEE Jordan Int. Joint Conf. Elect. Eng. Inf. Technol. (JEEIT)*, 2019, pp. 281–285, doi: 10.1109/JEEIT.2019.8717465.

[6]. S. Amjad et al., "Blockchain Based Authentication and Cluster Head Selection Using DDR-LEACH in Internet of Sensor Things," *Sensors*, vol. 22, no. 5, 2022, doi: 10.3390/s22051972.

[7]. D. B. D. and F. Al-Turjman, "A hybrid secure routing and monitoring mechanism in IoT-based wireless sensor networks," *Ad Hoc Networks*, vol. 97, 2020, doi: 10.1016/j.adhoc.2019.102022.

[8]. X. Cheng, C. Xu, X. Liu, J. Li, and J. Zhang, "LEACH Protocol Optimization Based on Weighting Strategy and the Improved Ant Colony Algorithm," *Frontiers in Neurorobotics*, vol. 16, 2022, doi: 10.3389/fnbot.2022.840332.

[9]. W. Fang et al., "FETMS: Fast and Efficient Trust Management Scheme for Information-Centric Networking in Internet of Things," *IEEE Access*, vol. 7, pp. 13476–13485, 2019, doi: 10.1109/ACCESS.2019.2892712.

[10]. W. Fang, W. Zhang, W. Yang, Z. Li, W. Gao, and Y. Yang, "Trust management-based and energy efficient hierarchical routing protocol in wireless sensor networks," *Digital Communications*

and Networks, vol. 7, no. 4, pp. 470–478, 2021, doi: 10.1016/j.dcan.2021.03.005.

[11]. R. Fotohi, S. Firoozi Bari, and M. Yusefi, "Securing Wireless Sensor Networks Against Denial-of-Sleep Attacks Using RSA Cryptography Algorithm and Interlock Protocol," *International Journal of Communication Systems*, vol. 33, no. 4, pp. 1–25, 2020, doi: 10.1002/dac.4234.

[12]. S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," *ACM Transactions on Sensor Networks*, vol. 4, no. 3, pp. 1–37, 2008, doi: 10.1145/1362542.1362546.

[13]. A. Shaheen, "The Internet of Things (IoT): A Comprehensive Review of Technologies, Applications, Challenges, and Future Trends," *Journal of Engineering and Computational Intelligence Review*, vol. 2, no. 1, pp. 1-8, 2024.

[14]. U. Gulen and S. Baktir, "Elliptic curve cryptography for wireless sensor networks using the number theoretic transform," *Sensors*, vol. 20, no. 5, 2020, doi: 10.3390/s20051507.

[15]. B. B. Gupta and M. Quamara, "An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols," *Concurrency and Computation: Practice and Experience*, vol. 32, no. 21, 2020, doi: 10.1002/cpe.4946.

[16]. M. K. Khan and A. Ullah, "Implication of IoT and its impact on library services: An overview," *Inverge Journal of Social Sciences*, vol. 3, no. 2, pp. 63-72, 2024.

[17]. W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," *IEEE Trans. Wireless Commun.*, vol. 1, no. 4, pp. 660–670, 2002, doi: 10.1109/TWC.2002.804190.

[18]. W. Ji, L. Li, and W. Zhou, "Design and implementation of a RFID Reader/Router in RFID-WSN hybrid system," *Future Internet*, vol. 10, no. 11, 2018, doi: 10.3390/fi10110106.

[19]. S. Museera and H. Khan, "Internet of Things in Food Supply Chains: Enhancing Quality and Safety through Smart Technologies," *Journal of Engineering and Computational Intelligence Review*, vol. 1, no. 1, pp. 1-6, 2023.

[20]. V. Kanchana Devi and R. Ganesan, "Trust-based selfish node detection mechanism using beta distribution in wireless sensor network," *Journal of ICT Research and Applications*, vol. 13, no. 1, pp. 79–92, 2019, doi: 10.5614/itbj.ict.res.appl.2019.13.1.6.

[21]. N. A. Khalid, Q. Bai, and A. Al-Anbuky, "Adaptive Trust-Based Routing Protocol for Large Scale WSNs," *IEEE Access*, vol. 7, pp. 143539–143549, 2019, doi: 10.1109/ACCESS.2019.2944648.

[22]. M. K. Khan et al., "Hierarchical Routing Protocols for Wireless Sensor Networks: Functional and Performance Analysis," *Journal of Sensors*, vol. 2021, 2021, doi: 10.1155/2021/7459368.

[23]. M. N. Khan et al., "Improving energy efficiency with content-based adaptive and dynamic scheduling in wireless sensor networks," *IEEE Access*, vol. 8, pp. 176495–176520, 2020, doi: 10.1109/ACCESS.2020.3026939.

[24]. M. Natarajan and S. Subramanian, "A cross-layer design: energy efficient multilevel dynamic feedback scheduling in wireless sensor networks using deadline aware active time quantum for environmental monitoring," *International Journal of Electronics*, vol. 106, no. 1, pp. 87–108, 2019, doi: 10.1080/00207217.2018.1501615.

[25]. M. Asif, "The complexities of bioterrorism: Challenges and considerations," *International Journal of Contemporary Issues in Social Sciences*, vol. 3, no. 3, pp. 2175–2184, 2024. [Online]. Available: https://ijciss.org/index.php/ijciss/article/view/1391

[26]. Aurangzeb, D., & Asif, M. (2021). Role of leadership in digital transformation: A case of Pakistani SMEs. In *Fourth International Conference on Emerging Trends in Engineering, Management and Sciences (ICETEMS-2021)(4 (1), 219-229)*.