FOREX Publication
Open Access | Rapid and quality publishing

International Journal of
Electrical and Electronics Research (IJEER)
Research Article | Volume 11, Issue 2 | Pages 442-450 | e-ISSN: 2347-470X

Performance Analysis of Energy Efficiency and Security Solutions of Internet of Things Protocols

Manjunath Itagi[1], Dankan Gowda V[2*], KDV Prasad[3], Pullela SVVSR Kumar[4], Shekhar R[5] and B. Ashreetha[6]

[1]*Associate Professor, Department of Civil Engineering, Nagarjuna college of Engineering and Technology, Devanahalli, Bangalore, Karnataka, India, drmanjunath.itagi@ncetmail.com*
[2]*Department of Electronics and Communication Engineering, BMS Institute of Technology and Management, Bangalore, Karnataka, India, dankan.v@bmsit.in*
[3]*Assistant Professor (Research), Symbiosis Institute of Business Management, Hyderabad, Symbiosis International (Deemed University), Pune, India, Kdv.prasad@sibmhyd.edu.in*
[4]*Aditya College of Engineering, Surampalem, Andhra Pradesh, India, pullelark@yahoo.com*
[5]*Professor, Department of Computer science and Engineering, Alliance University, Bangalore, Karnataka, India, shekhar.r@alliance.edu.in*
[6]*Assistant Professor, Department of Electronics & Communication Engineering College, School of Engineering & Technology, Mohan Babu University (Erst while Sree Vidyanikethan Engineering College), Tirupati, Andhra Pradesh, India ashreetha.b@vidyanikethan.edu*

*__Correspondence:__ Dankan Gowda V; dankan.v@bmsit.in

ABSTRACT- The scientific and business communities are showing considerable interest in wireless sensor networks (WSN). The availability of low-cost, small-scale components like CPUs, radios, and sensors, which are often combined into a single chip, is crucial. Parallel to the evolution of WSNs, the concepts of the IoT have been evolving in recent years. Wireless communication technologies may play a significant role in the implementation of IoT, despite the fact that IoT does not need or require any particular technology for communication. WSN assisted IoT networks can drive several applications in many industries. The proposed research explores the possibility of enhancing energy efficiency in WSN-assisted IoTN by balancing various challenging sensor network performance metrics. The base station's current placement inside the sensing field is predetermined by the preexisting routing algorithms. Our study examines the impact of base station placement outside and within the prescribed sensing domains on energy consumption and network longevity. In addition, methods for transferring data from the distributed source sensor to the base station while minimizing energy consumption are investigated. In this preliminary study, we focus on developing an algorithm for WSN-Assisted IoTN that can balance network factors such as hop count, communication distance, and residual energy. To further optimize the routing route between local cluster heads and the base station, a novel network architecture is built based on the Ant-optimization model, which uses centroid routing to balance energy consumption among local clusters. An open-source Network Simulator (NS-3) is used to model the behaviour of the proposed routing protocols and compare them to comparable existing network protocols. All of the suggested protocols have the same fundamentals for creating networks, however they vary in terms of routing, optimization, and performance depending on the development effort under consideration.

Keywords: Internet of Things, Security, Protocols, Efficiency, Simulator and Optimization.

ARTICLE INFORMATION

Author(s): Manjunath Itagi, Dankan Gowda V, KDV Prasad, Pullela SVVSR Kumar, Shekhar R and B. Ashreetha;

Received: 25/02/2023; **Accepted**: 31/05/2023; **Published**: 26/06/2023;
e-ISSN: 2347-470X;
Paper Id: IJEER 2502-11;
Citation: 10.37391/IJEER.110226
Webpage-link:
https://ijeer.forexjournal.co.in/archive/volume-11/ijeer-110226.html

1. INTRODUCTION

Companies in a wide range of sectors are increasingly using IoT, a network of linked devices, for a variety of uses. In view of digital transformation of businesses, the IoT adoption has become essential for human and societal activities. To automate and collect data, many IoT devices are being deployed across the world. Many breakthrough innovations are achieved and supported by IoT in modern world. IoT technologies are being used to mitigate global warming, saving water and increasing yield in smart farming.

IoT is always a booming concept as its information processing capability became more reasonable due to its high computation power and cheap storage price [1]. As the available bandwidth of the network increased rapidly, sensors evolved to be smaller, affordable and more accurate. However, unlocking full potential of IoT generates key issues such as lowering the resolution complexity, solving security concerns and fighting the communication flaws in diverse environments.

Perception, the network, and applications are the three tiers that make up the Internet of Things. The perception layer consists of

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 11, Issue 2 | Pages 442-450 | e-ISSN: 2347-470X

a collection of devices that can see, sense, collect data, and share it with one another through the internet. This layer contains sensors [2]. The information obtained from the network layer is then processed by the application layer. To facilitate the creation of intelligent and context-aware software, the Internet of Things relies on WSNs, which function as "cells" to gather and disperse data. These sensor network devices are true enablers in IoT with regards to metrics like longevity, energy efficiency, reduced cost, and interface to resources since they use a variety of power sources and keep it running for a long time.

The "base station" in most Internet of Things designs is a collection of sensors that receives data from the many "things." The data will be sent to remote servers through the base station [3]. While there are Internet of Things (IoT) designs that use smartphones and other pervasive computing devices as "base stations" or "sensors," the emphasis of this study will be on using such devices as "sensors" in a simulated environment [4]. For enterprises and consumers alike to gain an edge via greater productivity and fewer overhead expenses, the data amassed by a sensor network must be made readily available to them in the form of actionable insight.

Setting up a 100-node network simulation in NS-3 (Network Simulator 3) involves creating a network topology with 100 nodes and configuring their communication and behavior. NS-3 is a discrete-event network simulator that provides a wide range of tools and modules to simulate network protocols, applications, and scenarios. Although NS-3 does not have specific tools dedicated to setting up a 100-node network, it provides a rich set of functionalities to facilitate the process.

In order to provide operational efficiency at lower costs, sensors conducting IoT operations are essential. The base station has superior processing capability, more memory, and an endless supply of electricity so that it can operate continuously [5]. The base station can collect, store, visualise, and evaluate the data sensed by the sensor nodes. The detected data may be sent to a distant server via the Internet, and the base station offers a Graphical User Interface (GUI) for communicating with user agents [6]. This information will be sent from the base station to the approved users through the internet. Access to sensing field data through web pages anywhere in the globe may improve data analysis beyond what is possible with a single base station [7]. *Figure 1* depicts a basic IoT setup that makes use of WSNs to some degree.

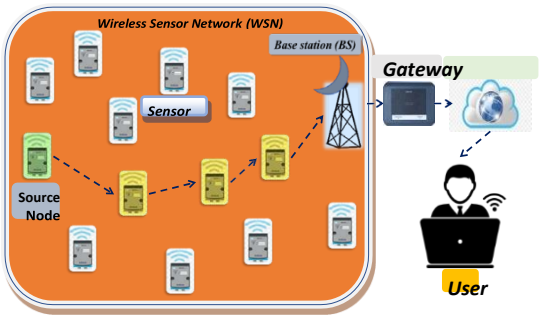

Figure 1: A basic WSN-assisted Internet-of-Things setting

The sensor network's "heartbeats" may be regularly sent from the base station to the cloud servers to update the latter on the network's operational state. The server responds to orders from the base station by acknowledging them and sending the base station any new config or software updates it has available. Water water features, parking lot surveillance systems, and vending machines may all benefit from having sensors included into their designs so that their status can be reported in real time [8]. Using the Internet of Things, cities may find problems like leaking pipes beneath. By putting RFID tags with the transported items and monitoring them using wireless sensors installed in nearby buildings and shipping containers, warehouse and logistic organisations like Amazon's delivery services may minimise misdirected shipments and prevent mistakenly lost merchandise [9]. Sensor data gathered in advance may alert Internet of Things gadgets to problems before they have an effect on the end user. Without the need for human labour and also data integration from diverse sources, previously stored IoT information may be utilised to make future planning choices via forecasting.

2. LITERATURE SURVEY

In a WSNs, energy efficiency is a very important performance metric. Several energy efficient routing schemes are introduced by researchers in the very recent years. To overcome multiple problems like energy consumption, load balancing and transmission cost many routing algorithms are published. The literature review in this paper is mostly based on Hierarchical routing in which multiple cluster-based routing techniques and route optimization algorithms are explored [10]. One of the biggest problems with WSNs is that the act of routing consumes a lot of power. Routing in this context means determining the most efficient and least energy-intensive route from a sensor's point of origin to the network's hub [11]. Therefore, when building a routing protocol for WSN, an intensive algorithm with reduced complexity is necessary. *Figure 2* depicts a classification of WSN routing methods.

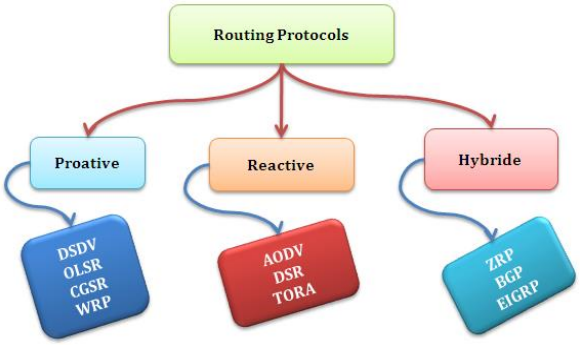

Figure 2: Schematic on a classification of WSN routing techniques

Figure 3 depicts a hierarchy of protocols, in which the lowest-energy sensor nodes are activated to collect data, while the highest-energy for processing and relaying the data to the final destination [12]. So, these protocols are utilised to accomplish routing while minimising energy use. Location-Based: These protocols don't assume any prior knowledge of the sensor nodes' coordinates.

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 11, Issue 2 | Pages 442-450 | e-ISSN: 2347-470X

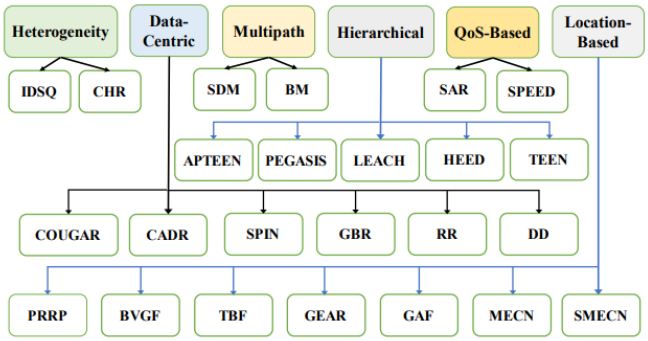

Figure 3: Existing energy efficient sensor network routing protocols

Using Global Positioning System (GPS) coordinates, sensor node locations may be determined; this data will then be utilised in conjunction with floods to determine the best possible route [13]. Data Centric Protocols: These protocols are dependent on the sequence number of the desired data and known to be query-based protocols. Base station will send a query to a region inside the sensor network to get certain information and waits for the acknowledgement from the sensor nodes in that region [14]. Procedures for Clustering: Here, the area covered by the sensor network is divided into smaller sections called "clusters," and leaders are chosen to oversee each section.

A reactive sensor network makes use of a protocol that reacts to rapid changes in variables like temperature. It has the ability to regulate a mission-critical data transmission and is designed to adapt quickly to changes in time-sensitive applications [15]. The lack of threshold-specific data at the base station may prevent it from accurately detecting the number of live and dead nodes [16]. A more realistic implementation may have prevented cluster collisions. It may be used to detect intrusions and explosions. Its inefficiency and uneven energy distribution are major drawbacks. Its usage of heterogeneous nodes and knowledge of residual energy for cluster head selection are both advantages when dealing with high energy levels [17]. The chosen cluster head has the disadvantage of sending data to the sink in a single hop [18]. The main drawback is that it has a large information processing overhead. Behera's I-SEP proposes a more reliable election process that evenly distributes power amongst cluster nodes and their members. Depending on their available starting energy, sensor nodes are divided into three categories: normal, intermediate, and advanced. In order to reduce power consumption, this protocol swaps energy states between CH and member nodes [19]. Using an opportunistic routing method, in which a group of candidate nodes is identified and employed to improve the dependability of long-distance node data transmission, the success rate in data transmission is raised. Power-saving and Safety-assured [20]. To solve the cluster formation issue with little costs and maximum coverage, a suggested protocol for an unequal-sized clustering technique is presented.

By calculating the ideal cluster size interval, ECUC is able to circumvent certain energy consumption constraints. A well-functioning design that meets the needs of the study requires optimisation. Sensor network lifespan may be increased by optimising the network to use as little energy as possible. Non-deterministic polynomial time hard (NPHard) issues are what optimisation is best at solving[21]. To solve a given issue, optimisation methods seek to maximise or minimise an objective function. These procedures might have one or several goals in mind. It may be classified as either a single- or multi-objective function, depending on the number of performance parameters chosen for optimisation. For most optimisation problems in science, the multi-objective function is the first choice [22].

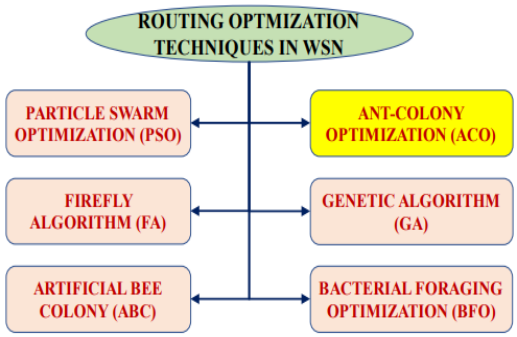

Figure 4: Efficient optimization techniques in WSNs

The majority of this study concerns a routing issue, whereas a subset concerns both routing and clustering. The primary goal of the optimisation approaches used to WSNs in *Figure 4* is to lessen the amount of power required to run the network and lengthen its useful lifespan [23]. Since the opted wireless sensor network is usually deployed in intricate areas or environment, only a few research approaches are found to be well suited. Various research sources provide better energy efficient schemes while simultaneously increasing network lifetime and to balance the network load among sensor nodes [24]. We reviewed an ample of load balancing and energy efficient protocols, where a quite few are found to be work excellent for energy consumption in sensor networks. Our research on several route optimisation methods has led us to the conclusion that Antcolony Optimisation (ACO) is the most trustworthy method for multi-hop data transmission in WSNs[25]. In view of real time computations, ACO shows superior performance when compared to other existing route optimization schemes. Although, ACO has a weak point of consuming more energy compared to PSO, it can be combined with centroid routing approach to build a hybrid protocol.

3. ENERGY SAVING SCHEME

The efficiency of data collection from the sensing field is improved by sink nodes in sensor networks. The sink node's job is to relay data from the sensor network's sensing field to the various user agents. The sink node collects all the information from the sensor nodes. The base station (BS), which acts as a central administrator by collecting and processing data, is the best possible sink. Therefore, a base station is seen as a unique node that constantly transmits data and has access to an infinite supply of power [26]. The ES3 method has two groups of nodes located inside the sensing area. First, the nodes in the network. Nodes outside of the network, number two. Packet transmission

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 11, Issue 2 | Pages 442-450 | e-ISSN: 2347-470X

occurs between network nodes and the base station, where the collected data is processed. In this paper, we present ES3, an Efficient Sink Selection Scheme for tree-like networks [27]. As was previously indicated, this design divides the connected devices in the network into three distinct categories. One: the primary hub or primary sink. There are also gateway nodes. Third, sensors that double as sinks. Each sensor node inside the sensing field is assigned an energy limit. If a sensor node's battery life drops below a certain percentage, it is removed from the network and its data isn't used in any further routing. This routing protocol may be used by mobile nodes in ad hoc networks [28]. The AODV is meant to reduce overhead and regulate traffic. The AODV routing system addresses both Route Discovery and Route Maintenance. Two separate functions are responsible for discovering new routes and fixing current ones, they are: Route Discovery and Maintenance. The reactive protocol maintains no permanent route table. AODV can analyze network topology changes fast. AODV routing protocols' information flow is seen in *figure 5*.

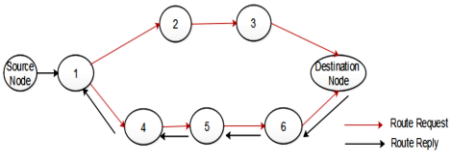

Figure 5: AODV Routing Protocols-Data Transfer

The ACO method for sensor network routing is inspired by the natural properties of ants and the related field of ACO. In ants, the ability to use Pheromone to find the quickest route between their colony and a food supply is the primary source of incentive (Impulsive Chemical Substance) [29]. Pheromones are left behind by ants when they go from one place to another. To find food, ants go out in high concentrations of pheromones. Faster completion of minimal pathways results in more significant amounts of pheromone. The colony can find the quickest route via the positive strengthening process. In generation u, the chance that an ant l at node k would move to node l is given by the equation 1.

$$Q_{J,L}{}^{K}(u) = \frac{tj,k(u){d_{j,k}}^{-\beta}}{\sum_{u\varepsilon}\Gamma^{kt}j,{v_{j,v}}^{d-\beta}}\ ,k\epsilon{\Gamma^{k}}_{j} \qquad (1)$$

The pheromone intensity at the edge is proportional to node I is proportional to the distance between these nodes. Pheromone-updating rules in equations 2, 3 and 4 are used to update the pheromone on all edges once all the ants have completed their tours.

$$t_{j,k}\ (t+1) = (1-\rho)_{j,k}(t) + \Delta t_{j,k}(t) \qquad (2)$$

$$\text{Where } \Delta t_{j,k}(t) = \sum_{K=1}^{NP}{\Delta t^{k}}_{j,k}(t) \qquad (3)$$

$$\Delta t_{j,k}(t) = \begin{cases} \dfrac{Q}{LK}\ ,if\ \ (j,k) \in tour\ done\ byantk \\ 0, \qquad\qquad otherwise \end{cases} \qquad (4)$$

Pheromone decay parameter, which measures the trial evaporation after the ant has decided where it will relocate is the pheromone decay parameter The ant k's tour duration is Lk, and the ant k's tour number is m. The administrative burden of centralized critical management systems may be reduced using this approach [30]. Additionally, the storage cost on each node is decreased since each node no longer has to store all public keys. After giving the cluster head the keys, it is essential to encrypt the information in the nodes not to be accessed by attackers. Encryption is explained in detail as follows.

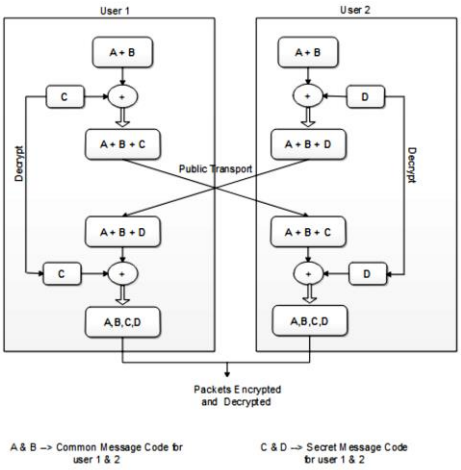

Figure 6: DHKE Method

Encryption: Data or information is encoded into a code to protect it from unwanted access. When it comes to data encryption, the DHKE technique is a good choice. The following is a detailed breakdown of how this algorithm works. Diffie-Hellman Key Exchange Algorithm: Using DHKE, cryptographic keys may be exchanged precisely. It's one of the first real-world applications of cryptography's key exchange mechanism. Any subsequent communications may be encrypted with the freshly generated private key using an asymmetric key cypher. *Figure 6* shows a block diagram for the DHKE Method.

The DHKE Cryptography is a widely used cryptography technology for ensuring network security. The DHKE's security perimeter should be raised. Duplicating P and Q subtracts the modulus n. In both the general population as well as amongst operators, the number is exploited. Using the secret key, a single user may transmit plain text to the encrypted public key.

4. PROPOSED METHOD

The ES3 network starts out with a single base station and a hop value of 0. The base station will then send out broadcast packets and look for its gateway node and its child nodes as the nodes are installed within the sensing field. Once they receive broadcast packets, that topology information is obtained by the neighboring non-network nodes. Then these non-networking nodes selfevaluate different metrics such as current energy level, hop count, communication distance to available sink and child node count of the available sink to match nearest sink weight and join the network and become one of the networking nodes. In a local tree, the sink for a given iteration of data is always the node with the highest weight. Usually, the selected sink in a local tree will have higher current energy level than the other sensor nodes which forms a local tree. The modeled

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 11, Issue 2 | Pages 442-450 | e-ISSN: 2347-470X

approach conserves power, builds a tree-based network quickly, and extends its lifespan by optimizing internal performance measures.

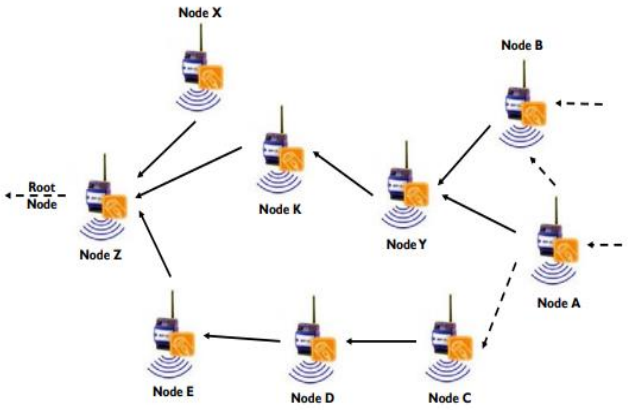

Figure 7: Local tree topology of sensor network in ES3

Figure 7 depicts the local tree topology in the hypothetical architecture. In this setup, Node A may share its data directly with Nodes B, Y, and C. In contrast. If Node A selects Node Y as the sink node, the packets will be routed to the node that is geographically closest to the sink. To account for this, each deployed sensor node's hop count and distance between sink nodes are recorded and considered. The number of a sensor node's offspring must be recorded as part of the decision-making process for which sink node to use. Node A's sink node in *figure 7*. Node B may serve as a sink node for Node A for a certain simulation period t sec, hence boosting Node A's lifespan. After a certain amount of time, Node A may reselect Node C as the sink node in order to equalise the power use of Nodes B and C. When Node A detects that Node B's energy has fallen below that of Node C, an event is triggered. While the simulated tree-based network organises itself. Therefore, in WSNs-assisted IoT contexts, a dependable network model and appropriate routing technique are needed to prolong the useful life of the networks.

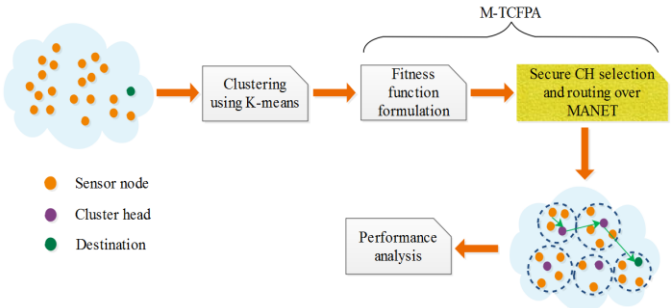

Figure 8: Block diagram of the M-TCFPA approach

5. ENERGY EFFICIENT OPTIMAL CLUSTERING

Selecting an ideal CH and routing path with this M-TCFPA algorithm ensures reliable data transfer across networks. For the clustering and CH selection phases of this M-TCFPA approach there are three stages.

Typically, network clustering is utilised to reduce energy consumption while aggregating data. Because it factors in trust and integrity into its fitness function, M-TCFPA can thwart attacks that are meant to do harm. *Figure 8* depicts a block schematic of the M-TCFPA method. First, nodes in the targeted network region are distributed randomly, and then clusters are formed using K-means. Since that time, K-means clustering has primarily utilised the calculation of euclidian distances. This section explains how to use the M-TCFPA to choose the best CHs in each cluster after the network has been grouped. Nodes' energy usage is reduced by selecting the most secure optimal CHs from the clusters in the second step of selection. The Flower Pollination Algorithm (FPA) was developed by Xin-She Yang, a population-based optimization method. This FPA mimics the pollination process of flowers. Pollination, in the broadest sense, refers to the process by which pollinators move pollen from one plant to another during the course of a mating cycle (e.g., insects). The flower/pollen of the M-TCFPA is used as a metaphor for the possible solution. An acceptable candidate node is selected from the population of sensor nodes. As the population grows, so does the demand for CHs in the network. One to N sensor nodes are assigned to each population and each population has a random node ID assigned between 1 and N. The equation for u-initialization TCFPA's can be found here (5).

$$x_i = \left(x_{i,1}, x_{i,2}, .., x_{i,NCH}\right) \quad (5)$$

Self-pollination and cross-pollination are the two methods used in the M-TCFPA for pollination. Self-pollination refers to the pollination of a single flower by the pollen of another flower. Cross-pollination occurs when a plant receives pollen grain from another plant and uses it to reproduce. Furthermore, there are a variety of techniques in which flowers attempt to disperse pollen. Pollen is dispersed by the wind in a biotic pollination, one of the several pollination techniques. The term "biotic pollination" refers to the process of pollination carried out by animals such as birds, bats, insects, and more. Insect pollinators, such as honeybees, are also checked for floral constancy. These pollinators prefer a specific type of bloom and shun the rest, which are employed to boost the reproduction of the same type of flower.

The mobile nodes in the MANET have built up enough mutual confidence to exchange data with one another. In this situation, the trust value is generated through direct discussions, whereas in the prior case, it was linked to packet forwarding behaviour.

$$\text{Trust} = \frac{\text{Amount of broadcasted packets}_{a,b}}{\text{Amount of received packets}_{a,b}} \quad (6)$$

The chosen CH must complete a challenging challenge in order to carry out be the best option for data transmission. Equation expresses the remaining energy (7).

$$RE = \sum_{i=1}^{NCH} E_{CH_i} \quad (7)$$

Where RE stands for residual energy and E_{CH_i} stands for the residual energy of the ith CH.

Keeping in mind the nodes' energy consumption, Euclidean distances between them, as well as between CH and their final destination, should be minimised. To make a single goal

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 11, Issue 2 | Pages 442-450 | e-ISSN: 2347-470X

function that can be represented mathematically, the weighted sum technique is employed (8).

$$\text{Fitness} = \beta_1 \times \text{Trust} + \beta_2 \times \text{IF} + \beta_3 \times \text{RE} + \beta_4 \times \text{Distance} \quad (8)$$

Where, $\beta_1, \beta_2, \beta_3$ and β_4 indicates the relative importance of the various fitness values (0.3, 0.3, 0.2, and 0.2). Using the previously described fitness function, the cluster's optimal CHs may be derived from the data. M-robustness TCFPA's against malicious attacks is boosted by the trust value it uses, while the integrity factor assesses whether or not data packets are correctly formatted and sent in a timely manner as specified by the protocol. As a result, the PDR benefits from the component of trust and integrity.

6. RESULTS AND DISCUSSION

Experimental set up: Install NS-3: Begin by installing NS-3 on your machine. You can download the latest version of NS-3 from the official NS-3 website. Create a network topology: NS-3 allows you to define network topologies using various classes and modules. You can create a network topology with 100 nodes by using the existing Node and Point-to-point Net Device classes provided by NS-3. Configure node behavior: Once the network topology is created, you can configure the behavior of each node in the simulation. This includes setting up network addresses, protocols, traffic patterns, and application-level behavior. Choose appropriate routing protocols: Depending on your simulation requirements, you may need to select and configure routing protocols for the network. NS-3 supports a wide range of routing protocols such as OSPF, RIP, and AODV. You can choose the appropriate routing protocol based on your simulation scenario. It's important to note that NS-3 is a highly flexible and customizable network simulator, and the specific tools required for a 100-node setup may vary depending on your simulation objectives. The above steps provide a general guideline for setting up a 100-node network simulation in NS-3, but you may need to further explore NS-3's documentation, examples, and modules to tailor the simulation to your specific requirements.

The focus of this section is on the NS-3 simulation findings, which includes data analysis. Using computer simulations, we can see how the network nodes respond to a Black Hole attack (see *figures 9-12*). Metrics including latency, throughput, and network load are used to approximate the potential behaviour of an intrusion-based black hole assault.

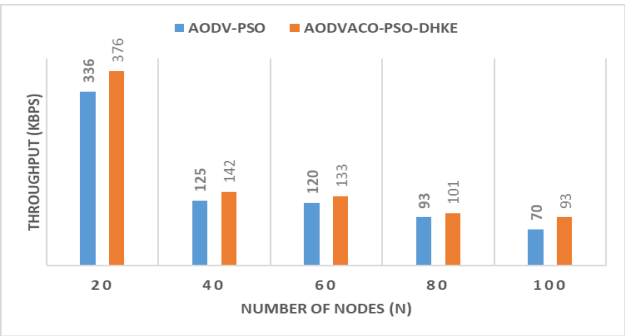

Figure 9: Node vs. Throughput

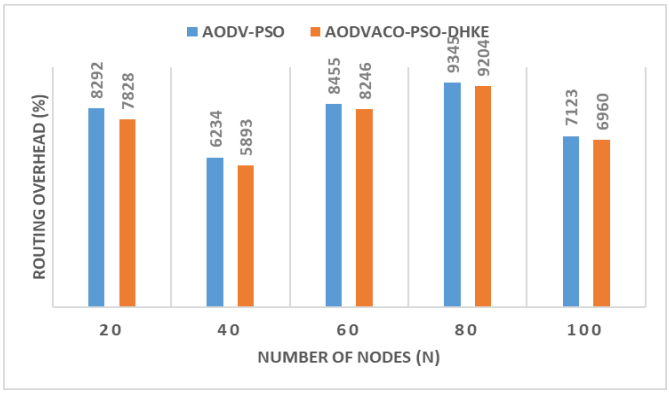

Figure 10: Node vs. routing overhead

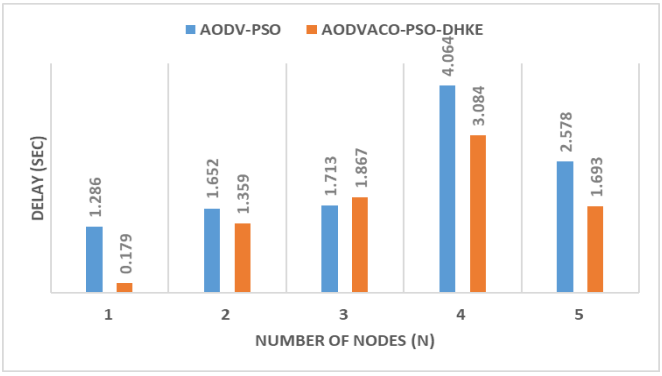

Figure 11: Node vs. delay

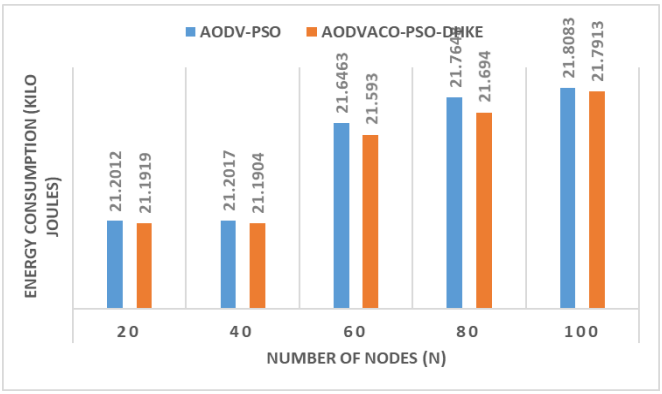

Figure 12: Node vs. Energy Consumption

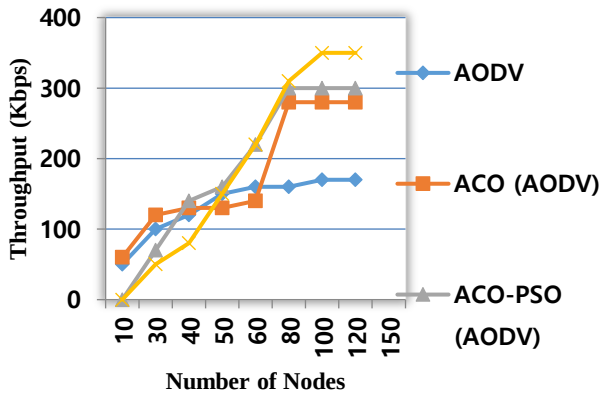

Figure 13: No. of Nodes versus Throughput

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 11, Issue 2 | Pages 442-450 | e-ISSN: 2347-470X

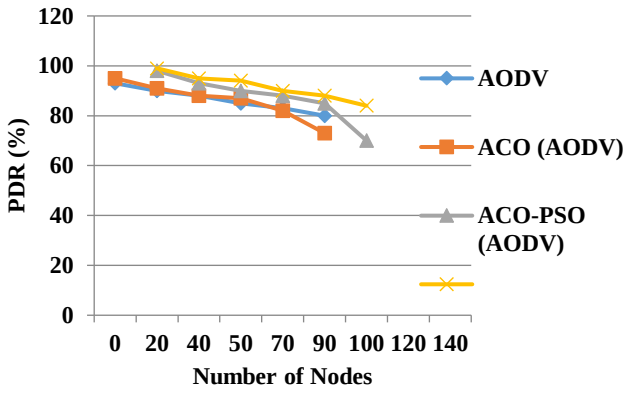

Figure 14: No. of Nodes versus PDR

A packet's end-to-end latency was tested using two simulations. As the number of nodes engaged grows, so does the likelihood of an assault being successful. When there are 20 nodes, as shown in *figure 9*, the AODV and OLSR delays are shown in red. To be able to observe the graph shown below shows how the black hole attack affects the network as a whole, relative to the normal operating protocol. The graph demonstrates a larger latency when there is no rogue node in the network. Similarly, a simulation would be performed with 40 nodes and the presence of a rogue node in the network. There is a notable lag when employing 40 nodes, as seen in *figure 13*. Both protocols' latency decreased dramatically when a rogue node was present. At 20 nodes, average latency rises by around 5%. This was shown to be the case for both protocols, which were tested to determine which was more affected by the attack.

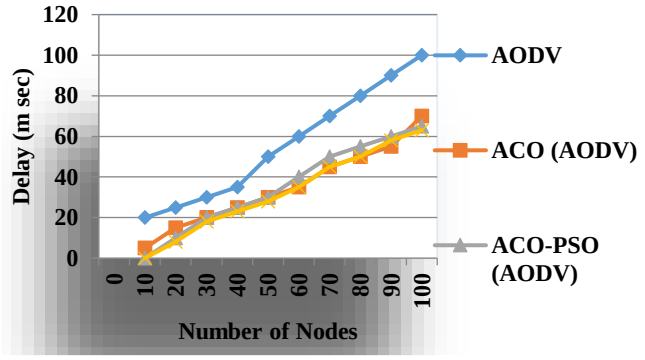

Figure 15: No. of Nodes versus Delay

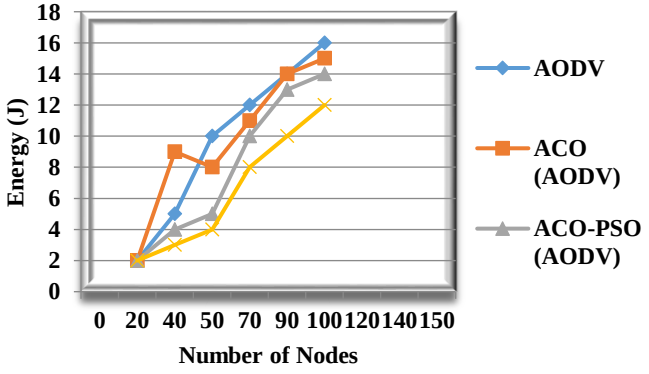

Figure 16: No. of Nodes versus Residual Energy

In comparison to the AODV, the OLSR has a little longer delay, as seen in *figure 14*. This is also true when there are fewer nodes. Latency increases as the number of nodes increases. A node network with 40 distinct integers may demonstrate this. *figure 15*. depicts that AODV has a substantial delay when compared to OLSR for a network of 40 nodes

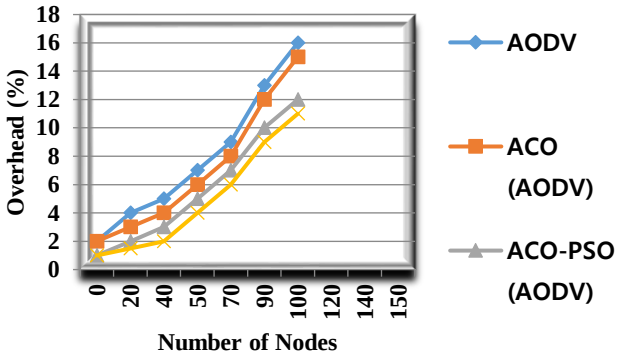

Figure 17: No. of Nodes versus overhead

There will be a higher throughput for OLSR if there is no attack (no malicious node present) (see *Figure 16* for 20 nodes). There is less routing forwarding and traffic going through the system as a consequence of this reduction in traffic. The rogue node just discards the data instead of delivering it, causing a reduction in total throughput. Also, when the malicious node is not destroying packets, AODV has superior throughput than while under assault. OLSR outperforms AODV in terms of throughput when compared side by side.

Figure 17 displays the same trends with 40 nodes, showing that although throughput rises with more nodes, the attack and non-attack throughput patterns are similar to those seen with 20 nodes. *Figures 14* and *15* show that there is a rogue node in the system. and ten more. OLSR and AODV's throughput is fairly high in a normal working protocol when no assaults are applied. These two protocols both drastically degrade throughput when attacked.

Table 1: Comparative analysis of M-TCFPA

Performances	Method	Number of Nodes				
		10	50	100	150	200
PDR (%)	TBSMR [20]	98	97	95	92	90
	M-TCFPA	99.77	99.37	98.50	99.04	98.85
PLR (%)	TBSMR [20]	2	3	5	8	10
	M-TCFPA	0.22	0.62	1.49	0.95	1.14
Throughput (kbps)	TBSMR [20]	510	500	470	440	410
	M-TCFPA	1090.36	1086.1	1077.85	1083.72	1083.27
AEED (sec)	TBSMR [20]	0.1	0.15	0.2	0.25	0.3
	M-TCFPA	0.024	0.027	0.038	0.060	0.070

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 11, Issue 2 | Pages 442-450 | e-ISSN: 2347-470X

In *table 1*, a comprehensive comparison is presented between the TBSMR [20] and M-TCFPA [21] methods in terms of accuracy. The comparison encompasses various configurations of sensor nodes, ranging from 10 to 200, providing insights into their performance across different scenarios. The results clearly demonstrate that the M-TCFPA method [21] outperforms the TBSMR method. The TBSMR approach [20] solely focuses on trust, traffic, and residual energy values during data transmission, disregarding the consideration of distance. As a consequence, there are delays in transmitting data packets. Conversely, the M-TCFPA method takes into account both trust and integrity, ensuring the reliability of nodes and accurate data exchange. Consequently, the M-TCFPA approach significantly improves data delivery while reducing transmission latency. When comparing the vulnerability of both protocols to a black hole attack, it was demonstrated that OLSR had a far higher throughput than AODV. Similarly, it is because OLSR is an active routing protocol that the protocol initially checks to verify whether there is a routing route before directing traffic to it. More sources have lesser influence on throughput than fewer sources, according to our research. AODV's low total throughput may be attributed to route reply. As soon as the malicious node delivers its route reply, the malicious node receives the data and may act quickly and discard it. Thus, network throughput suffers greatly as a result of this.

Twenty nodes were used to measure the load on the OLSR and AODV networks for the first time. During the experiment, 20 nodes and two scenarios were tested: one faulty node in a network and no bad nodes in a network (typically functional protocol). With and without a rogue node, the network load is shown in *figures 12 and 13*.

Figure 14 shows that OLSR and AODV have reduced network demands while the network is under attack. The rogue node doesn't send any data out into the network; instead, it just drops all of the packets it receives. For example, when there is no assault, it shows that OLSR is successfully routing its packets to their eventual destination, as seen in the accompanying picture. While the system is under attack, packet rejection minimises network traffic. AODV follows a similar path in the graph. When there are 40 nodes, there is a little difference between OLSR with and without assault. Routing traffic has grown as a result of the huge number of nodes. AODV doesn't alter even if there are 20 or 40 nodes.

There is a greater network cost on OLSR than AODV when malicious nodes are present, (as seen in *figures 15 and 16*) when the two protocols are pitted against one another. The OLSR network, whether it has 20 or 40 nodes, has high network load because the routing protocols can adjust to its variations between node restart and node halting. There is a delay in switching to new routes at higher speeds since the routing operations require more time for change. AODV is quicker to respond. The complexity of the OLSR increases as the number of nodes in the network increases, such that the pressure on the network is significantly reduced. As the node becomes more reliable, the strain on the network grows with each stop and restart.

7. CONCLUSION

This paper extensively discusses the weaknesses of routing protocols, the corresponding attacks exploiting these vulnerabilities, and various preventive measures. It becomes evident that no singular approach can ensure comprehensive security against all types of attacks. Therefore, it is necessary to address the vulnerabilities posed by external and internal attackers separately. Several secure variations of routing protocols have been proposed and developed in existing literature. However, none of these protocols have successfully provided protection against all forms of attacks. Additionally, the secure versions of routing protocols heavily rely on cryptographic techniques, which impose significant computational burdens on nodes with limited resources. After conducting a performance study, it has been determined that the M-TCFPA strategy surpasses the TBSMR approach. Addressing vulnerabilities from external and internal attackers necessitates separate approaches. Various secure versions of routing protocols have been proposed and developed in existing literature, but none have achieved comprehensive protection against all types of attacks. Furthermore, these secure routing protocols heavily rely on cryptographic techniques, resulting in excessive computational burdens for nodes with limited resources. Consequently, there is a need to develop a lightweight cryptographic technique that fulfills security objectives. Our investigation indicates that a Black Hole attack poses a greater threat to the AODV protocol compared to the OLSR protocol.

REFERENCES

[1] Hiremath, P. S., Anuradha, T. and Pattan, P., “Adaptive fuzzy inference system for detection and prevention of cooperative black hole attack in MANETs,” International Conference on Information Science (ICIS), pp. 245-251, 2019.

[2] S. Yang, K. Kang, Y. Cho and S.Y. Chae. “PAMP: Power-Aware Multi-Path Routing Protocol for a Wireless Ad Hoc Network”, Proc. IEEE International Conference on Wireless Communications and Networking, Las Vegas, USA, pp.2247-2252. 2018.

[3] A.K. N, S. A. Farooq, D. G. V, S. P. M, A. M. Reddy and R. Tanguturi, "Improved Secure Communication Mechanism for IoT Platform Devices," 2022 International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON), Bangalore, India, 2022, pp. 1-6, doi: 10.1109/SMARTGENCON56628.2022.10083714.

[4] Y. Kim, E. Lee and H. Park. “Ant Colony Optimization Based Energy Saving Routing for Energy-Efficient Networks”, IEEE Communications Letters, Vol. 15(7), pp. 779-781, 2019.

[5] S. R. Kawale, K. Prasad, N. Anil Kumar, N. S. Reddy and B. Ashreetha, "Technologies for Comprehensive Information Security in the IoT," 2023 International Conference for Advancement in Technology (ICONAT), Goa, India, 2023, pp. 1-5, doi: 10.1109/ICONAT57137.2023.10080332.

[6] R.R Rout and S.K. Ghosh. “Enhancement of Lifetime using Duty Cycle and Network Coding in Wireless Sensor Networks”, IEEE Transactions on Wireless Communications, Vol. 12(2), pp. 656-667, 2018.

[7] V. S. Chinamuttevi, K. Prasad, A. Y. Begum, R. C. Tanguturi and B. Ahmed, "Implementation of an Early Warning System using Internet of Things and Rainfall Threshold," 2022 6th International Conference on Electronics, Communication and Aerospace Technology, Coimbatore, India, 2022, pp. 491-496, doi: 10.1109/ICECA55336.2022.10009211.

[8] Merlin, R.T.: Ravi, R.: Novel Trust Based Energy Aware Routing Mechanism for Mitigation of Black Hole Attacks in MANET. Wireless Personal Communications, 104(4), 1599-1636. (2019).

International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 11, Issue 2 | Pages 442-450 | e-ISSN: 2347-470X

[9] G. Gondhalekar, B. Ashreeth, G. R. Thellaputta, D. Venkataramireddy, M. Sumithra and N. Karyemsetty, "A Safety Assessment Model for Automotive Embedded Systems Networks," 2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon), Mysuru, India, 2022, pp. 1-5, doi: 10.1109/MysuruCon55714.2022.9972628.

[10] Rajashanthi, M. and Valarmathi, K.: A Secure Trusted Multipath Routing and Optimal Fuzzy Logic for Enhancing QoS in MANETs. Wireless Personal Communications, 112, 75-90 (2020).

[11] K. N, S. Vijayalakshmi, D. Baswaraj, P. Selvarajan, S. Chandramohan and M. Tiwari, "Towards Internet of Things: Integration of Wireless Sensor Network to Cloud Services for Data Collection and Sharing," 2022 International Conference on Automation, Computing and Renewable Systems (ICACRS), Pudukkottai, India, 2022, pp. 363-369, doi: 10.1109/ICACRS55517.2022.10029163.

[12] Vanitha, K., Rahaman, A.Z.: Preventing malicious packet dropping nodes in MANET using IFHM based SAODV routing protocol. Cluster Computing, 22(6), pp.13453-13461 (2019).

[13] Avinash Sharma, K.D.V. Prasad, Sadashiva V. Chakrasali, Chanakya Kumar, Abhay Chaturvedi, A. Azhagu Jaisudhan Pazhani, Computer vision based healthcare system for identification of diabetes & its types using AI, Measurement: Sensors, Volume 27, 2023, 10075. https://doi.org/10.1016/j.measen.2023.100751.

[14] Ranjeet Suryawanshi, Revanna C R, B. Kameswara Rao and Parismita Sarma (2022), Enhanced Diagnostic Methods for Identifying Anomalies in Imaging of Skin Lesions. IJEER 10(4), 1077-1085. DOI: 10.37391/IJEER.100452.

[15] Parismita Sarma, Takrim UL Islam Laskar, and Ramesha M (2022), Human Emotion Recognition using Deep Learning with Special Emphasis on Infant's Face. IJEER 10(4), 1176-1183. DOI: 10.37391/IJEER.100466.

[16] Aarti Hemant Tirmare, Revanna C R, Ramesha M and N. K. Darwante (2022), A Morphological Change in Leaves-Based Image Processing Approach for Detecting Plant Diseases. IJEER 10(4), 1013-1020. DOI: 10.37391/IJEER.100443.

[17] El-Semary, A.M., Diab, H.: BP-AODV: Blackhole Protected AODV Routing Protocol for MANETs Based on Chaotic Map. IEEE Access, 7, 95185-95199 (2019).

[18] P, A. Sharma, S. Reddy P, P. S. Patwal, "Data Analytics and Cloud-Based Platform for Internet of Things Applications in Smart Cities," 2022 International Conference on Industry 4.0 Technology (I4Tech), 2022, pp. 1-6, doi: 10.1109/I4Tech55392.2022.9952780.

[19] S. B. M, P. Pavankumar, N. K. Darwante, "Performance Monitoring and Dynamic Scaling Algorithm for Queue Based Internet of Things," 2022 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES), 2022, pp. 1-7, doi: 10.1109/ICSES55317.2022.9914108.

[20] Desai, A.M. and Jhaveri, R.H., 2019. Secure routing in mobile Ad hoc networks: a predictive approach. International Journal of Information Technology, 11(2), pp.345-356.

[21] Puneeth Kumar, B.S., Ramesh Naidu, P., Sridhara, S.B. (2023). Internet of Things and Cognitive Radio Networks: Applications, Challenges and Future. In: Yadav, S., Chaudhary, K., Gahlot, A., Arya, Y., Dahiya, A., Garg, N. (Eds) Recent Advances in Metrology. Lecture Notes in Electrical Engineering, vol 906. Springer, Singapore. https://doi.org/10.1007/978-981-19-2468-2_3.

[22] B. Kameswara Rao, Ravi Shankar, Parismita Sarma, Abhay Chaturvedi, Naziya Hussain, Industrial quality healthcare services using Internet of Things and fog computing approach, Measurement: Sensors, Volume 24, 2022, 100517, ISSN 2665-9174, https://doi.org/10.1016/j.measen.2022.100517 .

[23] P, A. Sharma, A. Singla, N. Sharma, "IoT Group Key Management using Incremental Gaussian Mixture Model," 2022 3rd International Conference on Electronics and Sustainable Communication Systems (ICESC), 2022, pp. 469-474, doi: 10.1109/ICESC54411.2022.9885644.

[24] Sharma, K. S and M. R. Arun, "Priority Queueing Model-Based IoT Middleware for Load Balancing," 2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS), 2022, pp. 425-430, doi: 10.1109/ICICCS53718.2022.9788218.

[25] K. R. Swetha, Namitha A R, Manu Y M, Rashmi G R and Veera Sivakumar Chinamuttevi (2022), IOT Based Smart Health Care System to Monitor Covid-19 Patients. IJEER, 10(1), 36-40. DOI: 10.37391/IJEER.100105.

[26] Raja, R. and Ganeshkumar, P., 2018. QoSTRP: A trusted clustering based routing protocol for mobile ad-hoc networks. Programming and Computer Software, 44(6), pp.407-416.

[27] M. Swathi Pai, M. Shruthi and B. Naveen K, "Internet of Things: A Survey on Devices, Ecosystem, Components and Communication Protocols," 2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA), 2020, pp. 611-616, doi: 10.1109/ICECA49313.2020.9297458.

[28] K. B. Naveen, M. Ramesha, and G. N. Pai, "Internet of things: Internet revolution, impact, technology road map and features," Adv. Math. Sci. J., vol. 9, no. 7, pp. 4405–4414, 2020, doi: 10.37418/amsj.9.7.11.

[29] Usha, M.S. and Ravishankar, K.C., 2021. Implementation of Trust-Based Novel Approach for Security Enhancements in MANETs. SN Computer Science, 2(4), pp.1-7.

[30] Shivashankar, and S. Mehta, "MANET topology for disaster management using wireless sensor network," in International Conference on Communication and Signal Processing, ICCSP 2016, 2016, pp. 0736–0740, doi: 10.1109/ICCSP.2016.7754242.