

# Strengthening IoT-WSN Architecture for Environmental Monitoring



K.Akila, D.J.Evanjaline

**Abstract:** Saving the environment is the alarming red-hot topic of this trendy world. A proper arrangement is required to monitor different environmental pollutions. Many researchers and volunteers are developing and deploying Wireless Sensor Networks (WSN) for this purpose. Internet-of-Things (IoT) is one of the widely used cost-effective modern technologies to design wireless sensor nodes. Three fresh functional modules are introduced in this work to constitute the proposed work named as 'Strengthening IoT-WSN Architecture for Environmental Monitoring' (SIAEM) which is indented to overcome some impuissance of applying generalized wireless sensor network architecture in the field of environmental pollution monitoring. The functional modules introduced in this work are Customized Clustering of IoT-WSN Nodes (CCIN) and Energy Aware State Change Routing Protocol (EASCRP). The objective of this proposed IoT-WSN architecture is to reduce the Latency, Jitter, End-to-End delay and Power Consumption whereas, improving the performance parameters such as Throughput and Packet Delivery Ratio. The impact of proposed method in the performance of IoT-WSN network is measured and stated using benchmark network simulator.

**Keywords:** Clustering protocols, Routing Protocol, Environment Monitoring System, Internet-of-Things (IoT), Wireless Sensor Network (WSN)

## I. INTRODUCTION

Environmental pollution and improper natural resource conservations are causing many direct and indirect endangers to the living beings of the world. The nearest upcoming natural calamities are the Global warming [1] and Day Zero effect. The first one is triggered by the environmental pollutions and the second one is happening due to the improper handling of water resources. Many awareness programs were started during the last decade to prevent the disasters. Even though many conventional awareness programs are initiated [2], environmental pollutions are growing day-by-day.

Environmental pollutions are classified into five major categories such as Air pollution, Water Pollution, Soil Pollution, Sound Pollution and Light Pollution [3]. Poisonous gases are mixing in the atmosphere from various sources such as factories and vehicles [4]. There are a number of regulations declared for factory and vehicle smoke emissions. But there are a notable number of violations occurs due to human error or on purpose. Water pollution occurred due to the discharge of factory waste waters and chemical treated waters mixing with the pure water sources [5].

Manuscript published on 30 September 2019.

\*Correspondence Author(s)

Ms.K.Akila, Assistant Professor, Cauvery College for Women, Trichy.

Dr. D. J. Evanjaline, Assistant Professor, Rajah Serfoji Government Arts & Science (Autonomous) College, Tanjore.

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license <http://creativecommons.org/licenses/by-nc-nd/4.0/>

Factories are the prime accusations for the water pollutions. Soil pollution occurred because of huge chemical garbage, electronic wastes and many consumables' packages are dumping directly to the earth surface [6]. Factories, Nuclear Power Plants and people who are not bothering to separate bio-degradable materials from recyclable materials are sharing the responsibility for soil pollution. Sound and Light pollutions are also caused by various machineries and motor vehicles [7].

Inspecting the suspicious unlawful pollution creators periodically is time consuming and not enough to exert a strict ordinance. There are a number of pollution monitoring systems are in usage to avoid inadvertent pollution discharges. They are either decentralized individual units or costly resource consuming systems. A centralized pollution monitoring system is the immediate requirement to prevent the world from life decline. IoT is an emerging technology which makes any electronic device to communicate with other electronic devices through a local Wi-Fi or through internet. There are numerous possibilities possible when combining the forces of cost-effective IoT and cloud services [8][9][10]. Many WSN node manufacturers are already incorporating IoT technology to their nodes. Though some standard network architectures are available to connect the WSN nodes, dedicated network architecture and protocols for monitoring environmental pollutions can improve the performance of the network.

## II. EXISTING METHODS

There are some new methods introduced by researchers in recent days to construct IoT based wireless sensor networks. A set of existing communication protocols serve the purpose of connecting wireless sensor nodes and exchange the information among the network. More recent similar works are analyzed here to understand their key technologies, merits and limitations. The analysis is performed in terms of communication performance such as throughput, communication delays and power consumption. A Secure and Privacy Preserving Partial Deterministic RWP Model to Reduce Overlapping in IoT Sensing Environment [11], Efficient Fault-Tolerant Routing in IoT Wireless Sensor Networks Based on Bipartite-Flow Graph Modeling [12], Application-aware end-to-end delay and message loss estimation in Internet of Things (IoT)—MQTT-SN protocols [13] and Leveraging the power of the crowd and offloading urban IoT networks to extend their lifetime [14] are taken here for analysis and comparison.



### A. *Secure and Privacy Preserving Partial Deterministic RWP Model to Reduce Overlapping in IoT Sensing Environment (SPPPDRM)*

SPPPDRM [11] uses an ID-based authentication mechanism for joining nodes in a network. Intrusion detection and nodes survival strategies are clearly defined in this method. The main target of this method is to minimize the overlapping sensing coverage (OSC) in mobile wireless sensor networks. The general challenges of IoT-WSN such as Mobility, Data Transmission, Battery Life, Durability and accuracy are discussed in SPPPDRM. This work begins with the four initial assumptions - they are IoT sensors sends and receive data packets among neighbors, IoT sensors are aware of their locations, more than two IoT sensors are not colinear and the sensing target field is limited. Effective sensing coverage rate-based algorithms used in this work. SPPPDRM covers the subtasks such as pause time management, selection of member nodes; constituted nodes based prospective destinations selection, broadcast control messages, adjustment of prospective destinations by normal nodes, unauthorized nodes detection and malicious node detection. The evaluation of this method is performed in MATLAB R2017a. The simulation area size is limited to 200x200x200 cube meters in which 30 nodes with 30 meters transmission range are placed. The main disadvantage of this work is that the third and fourth initial assumptions limits wide the usage of this method. Limited number of nodes is another disadvantage of this method.

### B. *Efficient Fault-Tolerant Routing in IoT Wireless Sensor Networks Based on Bipartite-Flow Graph Modeling (EFRIWSN)*

EFRIWSN [12] overcomes some of the disadvantages of applying cluster-based routing in heterogeneous IoT-WSN. The concept of virtual cluster head for all cluster heads is introduced in this work. The virtual cluster heads are used to improve the fault tolerance of heterogeneous networks. Flow Bipartite Graph (FBG) is used to sense the failure of regular cluster heads and the assurance of data transmission acknowledgements by the virtual cluster heads. The transmission cost and energy cost are calculated for all edges in the network graph. NS2 network simulator is used to measure the performance of EFRIWSN. The simulation environment is set to 100 x 100 square meters with 1000 randomly deployed wireless sensor nodes in which 100 nodes are configured as powerful nodes. The size of the sensed data is limited to 500 Bytes. Experiments are conducted for a number of times and the readings presented as graphs. The main disadvantage of this model is that the immobility of the nodes. The initial deployment locations of the nodes cannot be changed in this method and the transmission-energy costs kept as constants during the entire network lifetime. It also not addressing the new node addition process or existing node failure situations.

### C. *Application-aware end-to-end delay and message loss estimation in Internet of Things (IoT)—MQTT-SN protocols (AEDMLE)*

AEDMLE [13] introduces a gateway load balancing solution for static defined wireless sensor cluster networks to use IoT devices as sensor nodes. The work depends on Message Queuing Telemetry Transport (MQTT) protocol based Wireless Sensor devices. A new gateway selection strategy and Sensor node to gateway connectivity are introduced in this work. Different network scenario such as unconstraint event/state, Occurrence of equality constraint event/state, inequality constraint event/state and fusion constraint event/state are handled separately in AEDMLE work. Crop field monitoring, flood controlling, industrial plant monitoring/controlling and smart home monitoring are some of the domains in which AEDMLE can be used. An emulated environment is used to evaluate the proposed method. Eclipse-Paho client library, Open source Mosquito Broker / Server, private cloud, Amazon web service and Android MQTT application are involved in the implementation. End-to-End delay and message loss are measured using this experimental setup for AEDMLE and some existing methods. AEDMLE maintains low End-to-End delays and Message Loss ratio. Power consumption not analyzed in this work. AEDMLE works only with statically defined networks.

### D. *Leveraging the power of the crowd and offloading urban IoT networks to extend their lifetime (LPCOUIN)*

LPCOUIN [14] crowded fixed IoT network of the urban area. It takes advantage of the IoT device density to optimize the power utilization of battery operated IoT-WSN nodes. The power saving is achieved by offloading some data transfer tasks to nearby mobile phones using crowd sensing technology. LPCOUIN introduces clear definitions for System model, Mobility model, Energy model, Network life time model, Load balancing, Routing optimizations and mobile sinks introduction to integrate the fixed IoT-WSN architecture with mobile network. The routing strategy algorithm is developed using Linear Program formulation (LP-formula) min-max method to improve the life time of the network. LPCOUIN provides theoretical proof of concept using the assumed network environment with 27 sensor nodes, 2500 mAh battery for each sensor, 2 $\mu$ A current rating for sleep mode, 50mA current rating for transmission and 100mA current for mobile nodes. Some of the disadvantages of LPCOUIN are Crowd sensing /offloading affects the security of the data, Requirement of mobile sinks, limited to fixed IoT-WSN environments and optimization is possible only in urban area. Some important metrics such as throughput, communication delays are not discussed in this work.

A summary of methodologies, advantages and limitations of existing methods is provided as Table 1 – given below

Author	Work	Methodology	Advantages	Limitations
A. S. M. S. Hosen et al.	A Secure and Privacy Preserving Partial Deterministic RWP Model to Reduce Overlapping in IoT Sensing Environment	Effective sensing coverage rate-based algorithm	Better Intrusion detection	small area and less number of nodes
J. Lin et al.	Efficient Fault-Tolerant Routing in IoT Wireless Sensor Networks Based on Bipartite-Flow Graph Modeling	Virtual Cluster head and Flow Bipartite Graph	Better Network Stability	Node mobility restriction
Deepsuhr a Guha Roy et al.	Application-aware end-to-end delay and message loss estimation in Internet of Things (IoT)—MQTT-SN protocols	Gateway Load balancing solution	Lesser communication delays and packet loss	Limited to static networks
Géraldine Texier et al.	Leveraging the power of the crowd and offloading urban IoT networks to extend their lifetime	Crowdsensing based offloading procedure	Optimized power usage and Improved Network life time	Limited to Urban area

**Table 1: Methodologies, Advantages and Limitations of existing methods**

**III. RELATED WORKS**

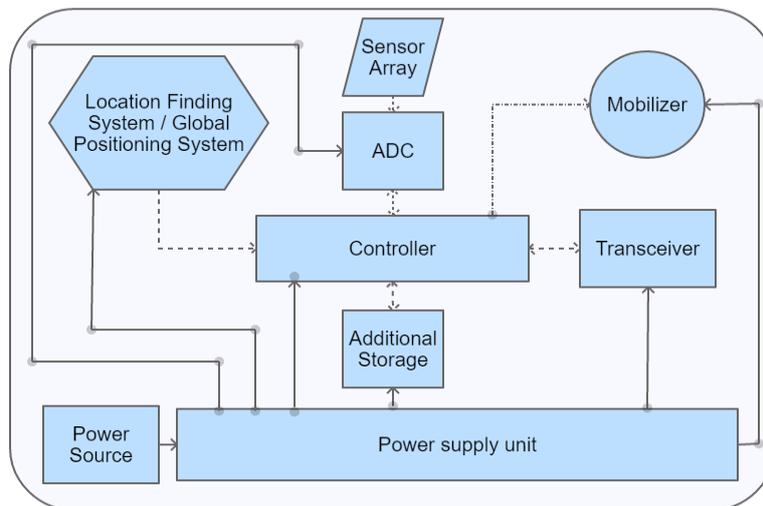
There are three essential components of IoT-WSN is discussed here in related works to simplify the explanation process of the proposed system. The related works are IoT-WSN clustering, IoT-WSN routing protocols.

**A. IoT-WSN Clustering**

Clustering is the process of grouping different member nodes based on their type, characteristics, data context, computational power, deployed locations and based on the process. Clustering is a fundamental process which determines the performance, availability, adoptability and security. The performance is measured by the standard metrics such as throughput, Packet Delivery Ratio and optimized power utilization. Communication delays such as

IP delay, latency, jitter and system delay are other parameters which have direct impact over throughput and packet delivery ratio. A good clustering method should keep communication delays in control while achieving higher security and power optimizations.

The WSN environment has many challenges while designing a clustering strategy. The main challenges in designing a network clustering procedure are to handle different network type, Node deployment and network management architecture. Homogeneous or Heterogeneous are different network types, Static deployment or dynamic deployments are the possible node deployment and Centralized or Distributed are the different management architectures followed in a WSN. The device architecture of a wireless sensor node is given in Figure 1.



**Figure 1: Wireless Sensor node Architecture**

Efficient cluster head selection and fault tolerance are the expected qualities of a clustering procedure. Cluster head selection should minimize the computational and communication costs. Both hardware-based and software-based faults such as energy depletion faults, insufficient storage faults, insufficient computation capacity faults and intruder attack-based faults are to be handled by the clustering procedures. Two algorithms are introduced in a related work named as strengthening clustering through

relay nodes in sensor networks [15]. This related work is referred for the clustering and cluster head selection. The cluster head selection algorithm and relay node selection algorithm are given below.

Algorithm 1: cluster head selection

*Input: Wireless sensor network with n number of nodes*

*Output: Cluster heads*

*Step 1. Each sensor node  $ID_i$  do advertisement of its residual energy  $E_{residual}$  within range of communication  $R_c$*

*Step 2. Each sensor node  $ID_i$  do  $Counter\_i = 0$ ;*

*Step 3. Each sensor node  $ID_i$  will maintain queue  $Q_i$  for received advertisements*

*Step 4. Each sensor node  $ID_i$  for all  $j$  in  $Q_i$*

*Step 5. For each  $j$  into  $Q_i$  do*

*If  $E_{residual\_i} \leq E_{residual\_j}$*

*Send OK message to  $ID_j$*

*Counter<sub>i</sub> = 1*

*Else make no-op for this advertisement from queue*

*Step 6. Each sensor node  $ID_i$  if  $Counter\_i = 0$  send cluster head declaration message in  $R_c$*

Algorithm 2: Relay node selection

*Input: Wireless sensor network with n number of nodes*

*Output: Selected Relay nodes*

*Step 1. For each sensor node  $ID_i$  if  $Counter = 0$*

*Search  $j$  in  $Q_i$  with maximum  $E_{residual\_j}$  in  $Q_i$*

*Assign Duty relay node to node  $j$*

*Node  $j$  will broadcast  $Relay\_Node\_Declaration$  message*

**B. IoT-WSN routing protocols**

Network protocols are a set of conventions followed in a network environment for initiating connections, manage communication resource stability, adoption of new nodes, discarding existing nodes and safely switching different connections based on the necessities. There are several types of protocols involved in a communication such as Basic network communication protocols, Network security protocols, Network routing protocols and Network management protocols. Here the routing protocols are used to establish connections by analyzing possible communication paths between source and destination nodes. The indent of a routing protocol can be communication speed, network stability, optimum power utilization or the combination of more than one objective. Commonly used protocols in IoT are Bluetooth protocol, WiFi IEEE 802.11 b/g/n, MQTT, CoAP, DDS, AMQP, LoRa and Zigbee.

One of the functional modules of the proposed method is developed based on MQTT protocol. MQTT plays a major role in IoT-WSN environments. The quality of this protocols is analyzed using mutation analysis of IoT Protocols [16]. The protocol model is developed in  $\pi$ -

calculus process algebra. The process definition  $P, Q \in p$  based on names  $x, y \in N$ : as

$$P, Q ::= \bar{x}(y) \cdot P \mid x(y) \cdot P \mid !P \mid (vx)P \mid (P|Q) \mid (P + Q) \mid 0 \mid A(x) \quad \text{Equation (1)}$$

where  $x(y) \cdot P$  is the input actions,  $\bar{x}(y) \cdot P$  is the output actions,  $!P$  is the process replication,  $(vx)P$  is the new name creation,  $(P|Q)$  is the parallel composition,  $(P + Q)$  is the non-deterministic choice,  $0$  is the NULL process and  $A(x)$  is the process definition name.

The MQTT protocol definition will be as follows

$$\begin{aligned} & Protocol() \\ & \stackrel{\text{def}}{=} (!((vPublish)Client(Publish))) \mid !Server() \\ & Client(z) \stackrel{\text{def}}{=} \bar{c}(z) \cdot 0 \quad \text{and} \\ & Server() \stackrel{\text{def}}{=} c(x) \cdot \overline{pub}(x) \cdot 0 \\ & Subscriber() \stackrel{\text{def}}{=} !(pub(\bar{x}) \cdot 0) \end{aligned}$$

**IV. PROJECTED WORKS**

**A. Strengthening IoT-WSN Architecture for Environmental Monitoring (SIAEM)**

SIAEM is the integration of three functional blocks to establish an IoT-WSN dedicated for Environmental Monitoring. The functional blocks are Customized Clustering of IoT-WSN Nodes (CCIN) and Energy Aware state change Routing Protocol (EASCRP). These blocks perform the tasks of clustering, routing with low power consumption.

*a. Customized Clustering of IoT-WSN Nodes (CCIN)*

The clustering process in a wireless sensor network generally follows some standard methods such as Euclidean distance-based clustering, Node type-based clustering, Data traffic-based clustering and Energy aware clustering. A new multi-factor clustering method is used in CCIN. The proposed method is a three-phase procedure in which Node initiations and authentications are performed in the first phase. Identifying different nodes types and locations are carried out in the second phase. Routing finalization and environment monitoring is performed in the third phase. The factors involved in CCIN clustering procedure are Euclidean distance ( $\epsilon$ ), Node Type ( $N_t$ ) and communication Data Type ( $\Gamma$ ). The Euclidean distance between two nodes are represented as  $\epsilon_{(N_x, N_y)}$  where  $x \neq y$ . The node types are categorized based on the computational and communication resources of the nodes which is defined as  $N_t = \{N_L, N_I, N_H\}$  where  $N_L$  refers the low powered devices,  $N_I$  refers the intermediate power devices and  $N_H$  refers the high-power devices. Small battery-operated single entity sensors are classified under  $N_L$  category, Multi-entity sensors, mobile nodes are classified under  $N_I$  category and Arbitrate data processing – logging devices are classified under  $N_H$  category.

The data contexts are also classified into three types as Control data ( $\Gamma_c$ ), Intermittent data ( $\Gamma_i$ ) and streaming data ( $\Gamma_s$ ). The weights ( $\omega_\epsilon, \omega_{N_t}$  &  $\omega_\Gamma$ ) of the clustering factors,  $N_t$  and  $\Gamma$  are assigned as  $\frac{3}{4}, \frac{1}{2}$  and  $\frac{1}{4}$  respectively [17]. In CCIN the suitable Nodes are selected as the cluster head, then each cluster head is allocated with a set of member nodes. Entire network nodes are defined in a node set as  $N = \{N1, N2 \dots Nn\}$  where  $n$  is the number of nodes in the network. The only initial requirement of CCIN is to manually define a data-logger and control center. This requirement is not peculiar in environmental pollution monitoring system because a dedicated data center has to be maintained for database maintenance. The computational capability  $\Delta$  of a network node is calculated using Equation (2) and the node type is assigned using Equation 3 – given below.

$$\Delta_x = \frac{\alpha_x \times \beta_x \times \gamma_x}{\alpha_{max} \times \beta_{max} \times \gamma_{max}} \quad \text{Equation (2)}$$

Where  $\Delta_x$  is the computational capability of Node  $N_x$ ,  $\alpha_x$  is the processing power which includes the processing frequency and number of cores,  $\beta_x$  is the available power source,  $\gamma_x$  is the available memory of the node and  $\alpha_{max}, \beta_{max} \neq \infty$  and  $\gamma_{max}$  are the maximum processor speed, maximum battery power and maximum memory available in the network. Here  $\beta_x := \infty$  for the nodes with continuous power supply and  $\beta_x := mAh$  for the battery-operated device.

$$N_T = \begin{cases} N_L \text{ if } \Delta < \frac{1}{3} \\ N_I \text{ if } \Delta \geq \frac{1}{3} \text{ and } < \frac{2}{3} \\ N_H \text{ if } \Delta \geq \frac{2}{3} \end{cases} \quad \text{Equation (3)}$$

Algorithm 3: Customized Clustering of IoT-WSN Nodes

Input:  $n$  number of IOT-WSN Nodes

Output: Clusters and Cluster heads

Step 1: Let First cluster flag  $f = 0$

Step 2:  $\forall i = 1 \rightarrow n$ : Report configurations  $\{\epsilon, N_t, \Gamma\}$  of  $N_i \in N$

Step 3: The base station sorts all nodes from high power device to low power device and creates a classified nodes set as  $N_c =$

$$\left\{ \{N_H 1, N_H 2 \dots N_H N_{Hmax}\}, \{N_I 1, N_I 2 \dots N_I N_{Imax}\}, \{N_L 1, N_L 2 \dots N_L N_{Lmax}\} \right\} \text{ where}$$

$N_{Hmax}$  is the number of high power nodes,  $N_{Imax}$  is the number of Intermediate power nodes and  $N_{Lmax}$  is the number of low power nodes by Equations 2 and 3

Step 4: Base station pings first  $m$  number of nodes in order where  $m$  is the required number of cluster heads

calculated based on  $\epsilon$ . The cluster set is defined as  $C = \{C_1, C_2 \dots C_m\}$ :  $C_x = \{H_x, \{n1, n2 \dots nm\}_x\}$  where  $H_x$  is the head of the cluster  $C_x$

Step 5:  $\forall i = 1 \rightarrow m$ :  $\forall j = 1 \rightarrow C_{x_m}$ : Aggregate all neighbor nodes, where  $C_{x_m}$  is the number of member nodes of a particular cluster  $C_x$ .

Step 6:  $\forall i = 1 \rightarrow m$ :  $C_i$  reports aggregated neighbor node details to the base station

Step 7: if  $f = 0$ , then assign  $f = 1$  and repeat from Step 2

Step 8: Proceed to the routing phase.

Algorithm 4: EASCRP – Intra-cluster

Input:  $C_x = \{H_x, \{n1, n2 \dots nm\}_x\}$

Output: Assorted shortest paths  $\delta_1, \delta_2$  and  $\delta_3$

Step 1: Initialize  $\delta_1 = \delta_2 = \delta_3 = \emptyset$

Step 2: Initialize  $v_c = 1$

Step 3:  $\forall i = 1 \rightarrow m$ :  $\delta_1 := \text{shortestPath}(H_x, ni_x, v_c)$

Step 4: if  $(\delta_1 = \emptyset)$ , then  $v_c = v_c + 1$ , Repeat from Step 3

Step 5: Initialize  $v_c = 1$

Step 6:  $\forall i = 1 \rightarrow m$ :  $\delta_2 := \text{shortestPath}(H_x, ni_x, v_c)$

Step 7: if  $(\delta_2 = \emptyset)$ , then  $v_c = v_c + 1$ , Repeat from Step 6

Step 8: Initialize  $v_c = 1$

Step 9:  $\forall i = 1 \rightarrow m$ :  $\delta_3 := \text{shortestPath}(H_x, ni_x, v_c)$

Step 10: if  $(\delta_3 = \emptyset)$ , then  $v_c = v_c + 1$ , Repeat from Step 9

While reaching step 8, all the farthest nodes which are not able to communicate with the base station in a single hop will be covered by the nearest cluster heads and included into the network.

The general IoT-WSN scenario for environmental monitoring in an economic way follows the nodes distribution as  $N_{Hmax} < N_{Imax} < N_{Lmax}$

B. Energy Aware State Change Routing Protocol (EASCRP)

EASCRP uses two routing phases, Intra-cluster routing phase and Inter-Cluster routing phase. Intra-cluster routing phase is performed by the cluster heads in parallel. Then the inter-cluster routing is performed by the base station.



The nodes  $\{n1_x, n2_x \dots nm_x\} \in C_x$  and cluster heads  $H_x \in C_x$  are treated as Vertices and the communication possibilities between the nodes are treated as Edges. Floyd-Warshall algorithm is used to find the shortest path between the nodes and the cluster head. Floyd-Warshall shortest path algorithm is selected here because of its efficiency in finding cost effective paths [18]. The Floyd-Warshall algorithm is used as  $shortestPath(n1, n2, v_c)$  where  $v_c$  is the maximum permitted number of edges for connect  $n_1$  and  $n_2$ . The EASCRP algorithm is given below

Algorithm 4: EASCRP – Intra-cluster

---

*Input:*  $C_x = \{H_x, \{n1, n2 \dots nm\}_x\}$   
*Output:* Assorted shortest paths  $\delta_1, \delta_2$  and  $\delta_3$   
*Step 1:* Initialize  $\delta_1 = \delta_2 = \delta_3 = \emptyset$   
*Step 2:* Initialize  $v_c = 1$   
*Step 3:*  $\forall i = 1 \rightarrow m: \delta_1 := shortestPath(H_x, ni_x, v_c)$   
*Step 4:* if  $(\delta_1 = \emptyset)$ , then  $v_c = v_c + 1$ , Repeat from Step 3  
*Step 5:* Initialize  $v_c = 1$   
*Step 6:*  $\forall i = 1 \rightarrow m: \delta_2 := shortestPath(H_x, ni_x, v_c)$   
*Step 7:* if  $(\delta_2 = \emptyset)$ , then  $v_c = v_c + 1$ , Repeat from Step 6  
*Step 8:* Initialize  $v_c = 1$   
*Step 9:*  $\forall i = 1 \rightarrow m: \delta_3 := shortestPath(H_x, ni_x, v_c)$   
*Step 10:* if  $(\delta_3 = \emptyset)$ , then  $v_c = v_c + 1$ , Repeat from Step 9

---

Inter-cluster routing follows the same algorithm with input  $N = \{H_1, H_2 \dots H_m\}$  where  $H_1, H_2 \dots H_m$  are the cluster heads of clusters  $C_1, C_2 \dots C_m$  in order. Every possible shortest path  $\delta_1$  has two alternative backup paths  $\delta_2$  and  $\delta_3$  in EASCRP. The alternate paths are used in two cases. First use is to include the Power aware state changing and the second use is to manage node failures. As the Base station knows the remaining power of the Cluster heads and cluster heads know the power of the member nodes, the paths are switched one-by-one sequentially where there is a power reduction of the node is about  $\frac{5 \times \beta_x}{100} mAh$ . This path switching process provides a balanced use of sensor nodes involved in communication. Finding a new alternative shortest path is not necessary in this first usage. The second usage of alternate shortest paths  $\delta_2$  and  $\delta_3$  occurs when there is an interrupt in communication with path  $\delta_1$ . This happens when there is a node in path  $\delta_1$  sends a SHUTDOWN message or its choppy failure. In this case  $\delta_2$  will be assigned as  $\delta_1$  and  $\delta_3$  will be assigned in place of  $\delta_2$ . Therefore, finding another possible shortest path is required in this situation. It is enough to execute from Step 8 to 10 of the EASCRP algorithm to get another alternate shortest path  $\delta_3$ . By this way EASCRP handles the network nodes optimally and covering the node failures rigidly.

## V. EXPERIMENTAL SETUP

OPNET is the latest network simulator from Riverbed Technology with state-of-the-art network simulation support. The graphical interface and scripting provision of OPNET makes it possible to design any kind of legacy network architectures and protocols [19]. It has the provision to inherit the real-world network environments by defining the latitude and longitude details. OPNET permits to define and override the default network node types, protocols and network communication strategies. OPNET has an advanced property of processing C++ codes to define the network strategies such as in Automatic Validation of Internet Security Protocols and Applications (AVISPA).

Experiments are carried out in OPNET repeatedly with different number of nodes for existing and proposed methods. In each iteration, 50% of nodes are declared to be in  $N_L$  category, 30% of nodes are declared as  $N_I$  category and remaining 20% are declared as  $N_H$  category. The Simulation world details are provided in the following Table.

S.No	Entity	Details
1	Simulation Area	10000 Square meters
2	Number of Nodes	100 to 1000 in step 100
3	IoT-Node types	ESP-32, ESP-8266, LoRa (Uniform Distribution)
4	Number of Routers	Automatic Selection
5	Node Placement	Random distribution
6	Network density	Default
7	RF Range of IoT-WSN Nodes	Based on the type from 100 meters to 1000 meters
8	Frequency bands	Auto-select
9	Simulation Time	168 real-world hours

Table 3: Simulation Parameters

## VI. RESULTS AND ANALYSIS

Throughput, Latency, End-to-End Delay, Packet Delivery Ratio and Energy consumption are the standard network performance measuring elements. These measurements are logged in OPNET for 10 different simulations with number of nodes from 100 to 1000 for every 100 nodes increment. The performance of existing SPPDRM, EFRIWSN, AEDMLE, LPCOUIN and proposed SIAEM are measured and analyzed in this section.



A. Throughput

Throughput refers the data flow rate of a communication channel. In IoT-WSN environments, throughput is an essential measurement while monitoring a set of continuous streaming data simultaneously. The higher throughput value denotes the higher quality of the network. The measured values of throughput are given in table 4 and the comparison graph is provided in Figure 3.

Throughput (Kbps)					
Nodes	SPPDRM	EFRIWSN	AEDMLE	LPCOUIN	SIAEM
100	30233	32644	33830	31114	34150
200	27810	29549	32483	29542	34115
300	24238	27215	28566	26715	32093
400	22425	24228	27014	24398	32341
500	20008	21783	24068	22299	30157
600	18231	17795	22882	19288	30053
700	14156	15583	20812	16414	28184
800	12929	11672	18606	15096	28077
900	9807	9678	16297	11458	26522
1000	8131	6607	13274	10162	26197

Table 4: Throughput

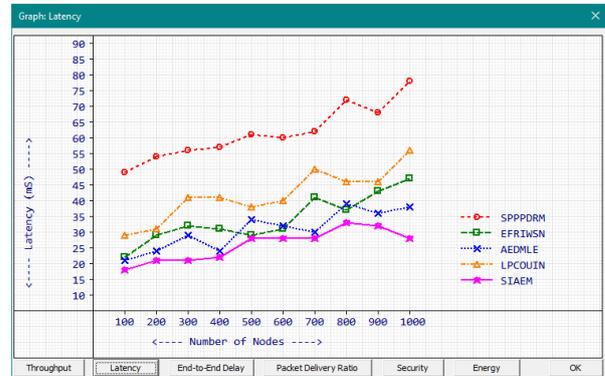


Based on the observations, existing methods AEDMLE and EFRIWSN and getting competitive values of throughput where there are 100 number of nodes in the network. The diminishing rate rapidly increases with the increase in number of nodes. The highest average throughput value 30189 kbps is achieved by the proposed SIAEM. AEDMLE, LPCOUIN, EFRIWSN and SPPDRM are scoring the throughput values average of 23873 kbps, 20649 kbps, 19675 kbps and 18797 kbps in order.

B. Latency

Latency is the time difference between data transmission triggering and the beginning of the data transmission. The lower value of latency will be achieved by higher quality networks that is, latency is inversely proportional to the performance of a network. Latency is measured in millisecond units. The measured latency values for existing and proposed methods are given in table 5 and the comparison graph is provided in Figure 4.

Latency (mS)					
Nodes	SPPDRM	EFRIWSN	AEDMLE	LPCOUIN	SIAEM
100	49	22	21	29	18
200	54	29	24	31	21
300	56	32	29	41	21
400	57	31	24	41	22
500	61	29	34	38	28
600	60	31	32	40	28
700	62	41	30	50	28
800	72	37	39	46	33
900	68	43	36	46	32
1000	78	47	38	56	28



SIAEM gets the lowest latency value of 18 for the network with 100 nodes. The highest latency value of SIAEM is 33mS measured during the simulation with 800 nodes. The latency average of SIAEM for all 10 simulations is 26mS. The nearest performer is AEDMLE with the latency average of 31mS. The proposed SIAEM secures the lowest latency value in all 10 simulations shows the better performance.

C. End-to-End Delay

End-to-End delay is the total value of all communications delay such as Jitter, IP-Delay and System delay. It refers the total travelling time of s data packet from source to destination. Since high delays affect the performance of a network, a good network architecture should keep this in control. End-to-End delays measured for the existing and proposed methods are given in Table 6. A comparison graph is provided for the same in Figure 5.

End-to-End Delay (mS)					
Nodes	SPPDRM	EFRIWSN	AEDMLE	LPCOUIN	SIAEM
100	167	125	119	169	99
200	190	138	144	191	104
300	216	154	174	206	111
400	246	158	199	235	110
500	276	177	227	257	116
600	301	187	255	273	113
700	331	200	286	293	121
800	351	211	314	311	123
900	386	223	349	335	127
1000	410	232	380	362	131

Table 6: End-to-End Delay

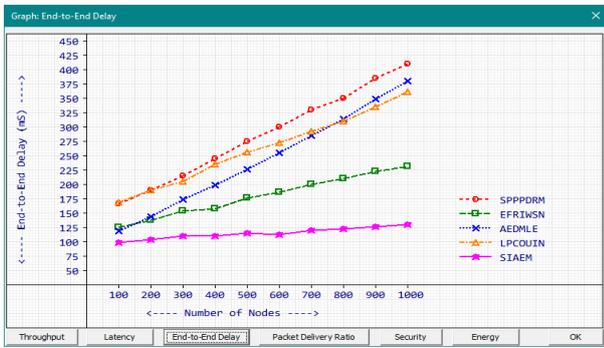


Figure 5: End-to-End Delay

SIAEM gets the minimum End-to-End delay of 99mS for 100 nodes and the maximum End-to-End delay is 131mS for 1000 nodes. The End-to-End delay average of SIAEM is 116mS in the overall simulation process. The second lowest End-to-End delay values achieved by EFRIWSN from 125mS to 232mS with the average value of 181mS. AEDMLE, LPCOUIN and SPPDRM are getting the End-to-End delay averages of 245mS, 263mS and 287mS respectively.

D. Packet Delivery Ratio (PDR)

PDR is the ratio between number of transmitted packets transmitted by the source and number of packets received by the destination. Packet drops occurs because of many reasons such as data collision, intermediate node failures, forced path changing, heavy data traffic and intruder attacks. The PDR values obtained from the simulations are tabulated as Table 7. A comparison graph of PDR is given in Figure 6.

Packet Delivery Ratio (%)					
Nodes	SPPDRM	EFRIWSN	AEDMLE	LPCOUIN	SIAEM
100	96	93	95	95	99
200	94	93	93	93	98
300	92	91	91	90	97
400	88	91	91	87	97
500	87	90	89	87	95
600	86	89	85	85	94
700	84	87	83	81	93
800	82	86	81	79	93
900	80	85	79	79	91
1000	78	84	78	75	90

Table 7: Packet Delivery Ratio

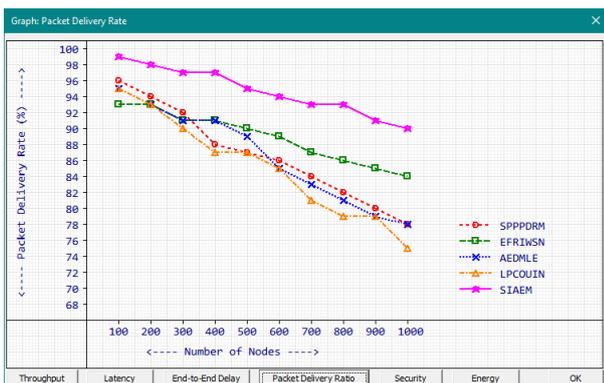


Figure 6: Packet Delivery Ratio

SIAEM maintains the PDR between 90 to 99%. The average PDR value of SIAEM is 95%. EFRIWSN secured the second-best PDR values of minimum 84%, maximum 93% and the average is 89%. The observation shows that the SIAEM has more fault tolerance and rigidity against security threats. SPPDRM, AEDMLE and LPCOUIN are scoring the PDR average of 86.7%, 86.5% and 85.1% in order.

E. Energy

Energy consumption is also one of the vital characteristics required in IoT-WSN based environmental monitoring. Many of the network nodes in environmental are come under the  $N_L$  type with a tiny battery as the power source. Therefore, conserving energy optimally without affecting the performance of the network in a vital and intriguing task in designing IoT-WSN environment. The average energy spent for a successful data packet transmission is observed by OPNET. Observed energy consumption of existing and proposed methods are given in Table 9. The comparison graph is given in Figure 8.

Nodes	Energy (uJ)				
	SPPDRM	EFRIWSN	AEDMLE	LPCOUIN	SIAEM
100	1272	907	705	706	386
200	1278	911	752	704	361
300	1316	947	758	746	389
400	1340	991	790	769	398
500	1369	1017	809	800	433
600	1385	1051	842	809	434
700	1425	1073	847	840	452
800	1419	1097	878	854	467
900	1446	1141	911	894	466
1000	1468	1162	924	920	478

Table 9: Energy

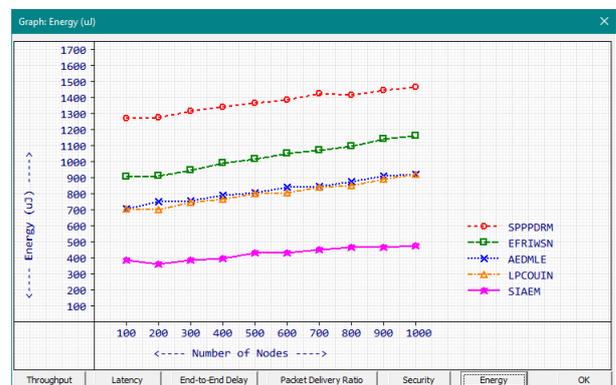


Figure 8: Energy consumption

SIAEM consumes lesser energy than other methods in all 10 simulations. When simulating with 100 nodes, SIAEM consumed 386uJ for a data transmission. The maximum energy used by SIAEM is 478uJ when operating with 1000 nodes.



The energy consumption average for SIAEM is 426.4uJ. LPCOUIN, AEDMLE, EFRIWSN and SPPDRM are getting the energy consumption average of 804.2uJ, 821.6uJ, 1029.7uJ and 1371.8uJ respectively.

## VII. CONCLUSION

Provides Routing along with energy optimization is one of the challenging tasks in networking. In this work a new model is developed using two functional blocks for clustering and routing management. When measuring the performance of the new method is analyzed in terms of throughput, latency, end-to-end delay, packet delivery ratio, and energy using the benchmark network simulation tool, the performance of the proposed method is better than other method in comparison. Thus, the proposed method will be an optimum solution recommendable for environmental monitoring in existing and upcoming smart cities.

## REFERENCES

1. Yongyun Hu, Han Huang and Chen Zhou, "Widening and weakening of the Hadley circulation under global warming" in Science Bulletin Volume 63 Issue 10, Elsevier 2018, Pages: 640-644
2. Sílvia Luís, Christin-Melanie Vauclair and Maria LuísaLima, "Raising awareness of climate change causes? Cross-national evidence for the normalization of societal risk perception of climate change" in Environmental Science & Policy Volume 80, Elsevier 2018, Pages: 74-81
3. Defeng Yang, Aric Xu Wang, Kevin Zheng Zhou and Wei Jiang, "Environmental Strategy, Institutional Force, and Innovation Capability: A Managerial Cognition Perspective" in Journal of Business Ethics, Springer 2018, Pages 1-15
4. Xi Ji, Yixin, Yao, and Xianling Long, "What causes PM2.5 pollution? Cross-economy empirical analysis from socioeconomic perspective" in Energy Policy Volume 119, Elsevier 2018, Pages: 458-472
5. Karin Mattsson, SimonneJocic, Isa Doverbratt and Lars-Anders Hansson, "Nanoplastics in the Aquatic Environment" in EnvironmentsAn Emerging Matter of Environmental Urgency, Elsevier 2018, Pages: 379-399
6. Jie Tang, JiyangQiao, QiangXue, Fei Liu, Honghan Chen and Guochen Zhang, "Leach of the weathering crust elution-deposited rare earth ore for low environmental pollution with a combination of (NH4)2SO4 and EDTA" in Chemosphere Volume 199, Elsevier 2018, Pages: 160-167
7. MichałCiach and Arkadiusz Fröhlich, "Ungulates in the city: light pollution and open habitats predict the probability of roe deer occurring in an urban environment" in Urban Ecosystems Volume 22 Issue 3, Springer 2019, Pages: 513-523
8. Hamdan Hejazi, Husam Rajab, Tibor Cinkler and László Lengyel, "Survey of platforms for massive IoT" in IEEE International Conference on Future IoT Technologies (Future IoT), IEEE 2018, Pages: 1-8
9. Christos Stergiou, Kostas E.Psannis, Byung-Gyu Kim and Brij Gupta, "Secure integration of IoT and Cloud Computing" in Future Generation Computer Systems Volume 78 Part 3, Elsevier 2018, Pages: 964-975
10. T. Wang, G. Zhang, A. Liu, M. Z. A. Bhuiyan and Q. Jin, "A Secure IoT Service Architecture With an Efficient Balance Dynamics Based on Cloud and Edge Computing," in IEEE Internet of Things Journal vol. 6 no. 3, IEEE 2019, Pages: 4831-4843
11. A. S. M. S. Hosen, S. Singh, V. Mariappan, M. Kaur and G. H. Cho, "A Secure and Privacy Preserving Partial Deterministic RWP Model to Reduce Overlapping in IoT Sensing Environment," in IEEE Access vol. 7, IEEE 2019, Pages: 39702-39716
12. J. Lin, P. R. Chelliah, M. Hsu and J. Hou, "Efficient Fault-Tolerant Routing in IoT Wireless Sensor Networks Based on Bipartite-Flow Graph Modeling," in IEEE Access vol. 7, IEEE 2019, Pages: 14022-14034
13. Deepsubhra Guha Roy, Bipasha Mahato, Debashis De and Rajkumar Buyya, "Application-aware end-to-end delay and message loss estimation in Internet of Things (IoT) — MQTT-SN protocols" in Future Generation Computer Systems Volume 89, Elsevier 2018, Pages: 300-316

14. GéraldineTexier and Valérie Issarny, "Leveraging the Power of the Crowd and Offloading Urban IoT Networks to Extend their Lifetime" in IEEE International Symposium on Local and Metropolitan Area Networks (LANMAN), IEEE 2018, Pages: 104-109
15. Amit Chugh and Supriya Panda, "Strengthening Clustering Through Relay Nodes in Sensor Networks" in Procedia Computer Science Volume 132, Elsevier 2018, Pages: 689-695
16. Benjamin Aziz, "Towards a mutation analysis of IoT protocols" in Information and Software Technology Volume 100, Elsevier 2018, Pages: 183-184
17. K. Xiao, Z. Chen and C. Yang, "Estimate Information Fusion Weight of WSNs Nodes Based on Truth Discovery Optimization Method Among Conflicting Sources of Data," in IEEE Access volume 7, IEEE 2019. Pages: 35606-35618
18. Zuhri Ramadhan, AndysahPutera Utama Siahaan and M Mesran, "Prim and Floyd-Warshall Comparative Algorithms in Shortest Path Problem" in ICASI - Joint Workshop 'KO2PI' and 'The 1st International Conference on Advance & Scientific Innovation', EU DL 2018, Pages: 1 - 12
19. Maryam Pahlevan and Roman Obermaisser, "Evaluation of Time-Triggered Traffic in Time-Sensitive Networks Using the OPNET Simulation Framework" in Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP), IEEE 2018, Pages: 283 - 287

## AUTHORS PROFILE



**Ms.K.Akila** M.Sc.M.E.M.Phil, Research Scholar, Working as a Assistant Professor in Cauvery College for Women, Trichy. She Published Survey paper on Wireless Sensor network based Internet of Things.



**1. Dr.D.J.Evanjaline** MCA. M.Phil.Ph.D , Working as a Assistant Professor in Rajah Serfoji Government Arts & Science (Autonomous) College, Tanjore.

**1. D. J. Evanjaline, N. Kalpana, P. Raja Kumar** published a paper "Security Enhancement of Wireless Protocol WPA (WI-FI Protected Access)" in the International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-4 Issue-3, July 2015.

**2. Dr. D. J. Evanjaline, P. Rajakumar, N. Kalpana** published a paper "Two Tier Security Enhancement for Wireless Protocol WEP (Wired Equivalent Privacy)" in the International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-5 Issue-1, March 2015.

**3. J. Emmanuel Robin N. Krishnamoorthy Dr. D. J. Evanjaline** published a paper "WEKA Tool based Knowledge Extraction Analysis of Independent Learning skills amongst engineering students" in the International Journal IJAMBU Volume 2 Issue 1Jan-Mar 2014 ISSN 2348-1382 (Online).

**4. D. J. Evanjaline, Dr. E.Kirubakaran , J.Saigeetha** published a paper "Security Enhancement for Wireless Protocol WEP by Random Shuffling Encryption" in International Journal of Network & Mobile Technologies(IJNMT) ISSN:2230-8903, Vol.2,No.1, June 2011

**5. D. J. Evanjaline, Dr. E.Kirubakaran** published a paper "Design of Multithreaded Security Algorithm using Session Keys to Secure Initialization Vector (IV) for Enhancing the Wireless Protocol WEP" in the International Journal of Computer Applications (0975 - 8887) Volume 3 - No.5, June 2010

**6. D. J. Evanjaline, Dr. E.Kirubakaran** Published a paper "Strengthening WEP Protocol for Wireless Networks by Enhancing the RC4 Algorithm using Random Addressing and Dual Encryption Mechanism" in the International Journal Of Emerging Technologies And Applications In Engineering, Technology And Sciences (IJ-ETA-ETS). ISSN: 0974-3588 | Jan '10 - June '10 | Volume 3 : Issue 1

**7. Published a book "Web Programming Essentials" Thakur Publishers, Chennai. ISBN:978-93-5163-049-4, 2014.**

