International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

An Energy Efficient Cloud-Based Routing Protocol for Wireless Sensor Network (WSN) for Improving Throughput and Packet Delivery Ratio

[1]Vishwas S., [2]Dr. Hareesh K.

Submitted: 29/11/2023 **Revised**: 09/01/2024 **Accepted**: 19/01/2024

Abstract: This study explores the integration of wireless sensor networks with cloud platforms to address inherent limitations, including processing, storage, and power constraints. Researchers leverage the specific requirements of Wireless Sensor Networks (WSN) to propose innovative solutions, particularly focusing on energy efficiency and minimizing delays in surveillance applications. The data collected from these applications undergo streamlined processing and analysis in a cloud database. To ensure efficient and reliable transmission from the WSN to the cloud server, a comprehensive Secured Energy Efficient Framework (SEEF) is introduced. SEEF incorporates cluster-based topology, Content Slot Allocation based Multi-Layer MAC (CSA-ML MAC) protocol, and a trust-based Sybil attack detection mechanism. CSA-ML MAC dynamically allocates variable-sized slots, achieving notable improvements in end-to-end delay, duty cycle, and packet delivery ratio. The Sybil attack detection mechanism enhances accuracy, leading to reduced false positives and improved true positives. The routing protocol optimizes intra-cluster and inter-cluster phases, utilizing a flower pollination algorithm to enhance inter-cluster routing. Collectively, these proposed mechanisms contribute to energy savings, reduced delay, and improved overall performance compared to existing protocols.

Key words: *Cloud Architecture, Energy Efficiency, Protocols, WSN, Location Awareness, Wireless Sensor Networks, Network Topology, Simulation, Throughput, Delays*

1. Introduction.

Wireless Sensor Network (WSN) is a type of ad-hoc network comprises of sensor nodes for collecting the environmental data depending upon the application requirements. It is widely adopted in various monitoring and tracking applications like healthcare, agriculture, environment monitoring, surveillance, etc., due to its potential benefits. There are various types of applications such as event detection, tracking, periodic measurements, function approximation and edge detection. The requirements of the sensor networks vary from one application to another, which laid certain constraints in designing WSN based applications. This gains attraction among recent researchers to propose various optimal solutions for addressing several issues related to WSN.

A. Wireless Sensor Networks

The sensor nodes in the network should be fault tolerant as the failure of a single node affects the entire network functionality. The node failure occurs due to factors such as battery depletion, node failure, link failure, environmental conditions and enemy attacks. The WSN architecture should be able to scale for inclusion of new nodes in case of node failure. Network scalability is the property with which the network can be expanded in terms of the number of sensors, topology, data quality and amount of data. The sensor nodes should be easily programmable and editable in case of the addition of new functions.[1]

Wireless sensor network is a collection of densely deployed sensor nodes that collects the environmental data and transfers it to the sink node. The data collected by the sensors are raw data that should be processed before sending them to the sink node. The sink node sends the data to the server through the Internet or other communication technologies. The communication between the source node and the sink node may be single hop communication or multi-hop communication. In single hop communication, the nodes directly communicate to the sink node and in multi-hop communication, the source node transmits the data through intermediate nodes. The architecture of the WSN is given in Figure 1

[1]*Research Scholar, Dept of CSE, VTU Belagavi, INDIA*
Vishwas1985october@gmail.com
Orchid id:0009-0007-6337-9299
[2]*Associate Professor, Dept of CSE, Govt Engineering College, K.R.PETE, INDIA*
Hareeshk.gec@gmail.com

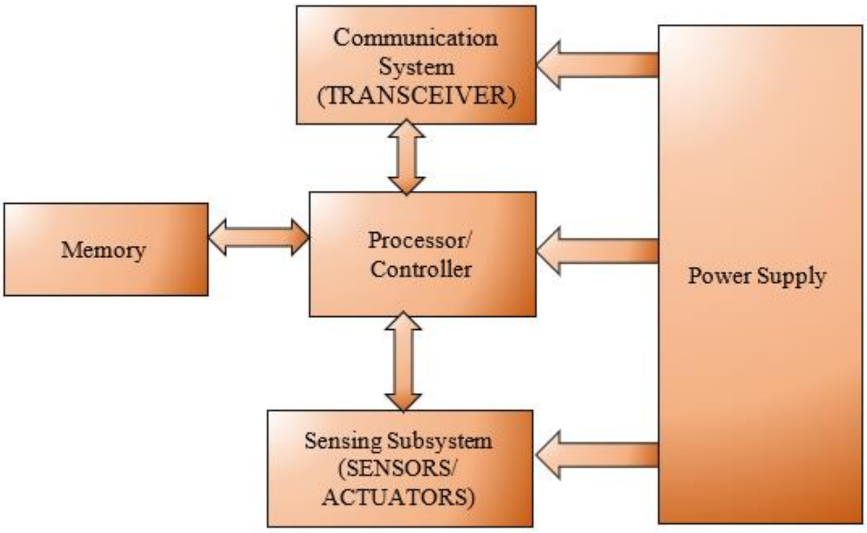

Communication System (TRANSCEIVER)
Memory
Processor/ Controller
Power Supply
Sensing Subsystem (SENSORS/ ACTUATORS)

Fig 2: Sensor node architecture

The nodes transmit the data to the base station via relay nodes through suitable communication technologies. The common methods are radio frequencies, optical communication, ultrasound and magnetic inductance. The underwater sensor networks use acoustic waves for communication among the sensor nodes. The transceiver is a combination of both transmitter and receiver which transmits and receives the data in half duplex operation mode.[2]

The controller is the processing unit of the sensor node which processes the data collected by the sensors. Some common processors available are Texas Instruments MSP430 and Atmel ATmega. The sensor nodes possess a limited memory due to which all the collected data cannot be stored. The schemes like aggregation are used for data reduction and sent to other nodes by User Datagram Protocol (UDP) type protocols.

There are several methods and standards developed for wireless communication to operate in the ISM (Industrial, Scientific and Medical) band [3]. These communication standards progressed over time to enable massive data transmission at high speed across the network. The common standards adopted by many applications are as follows:

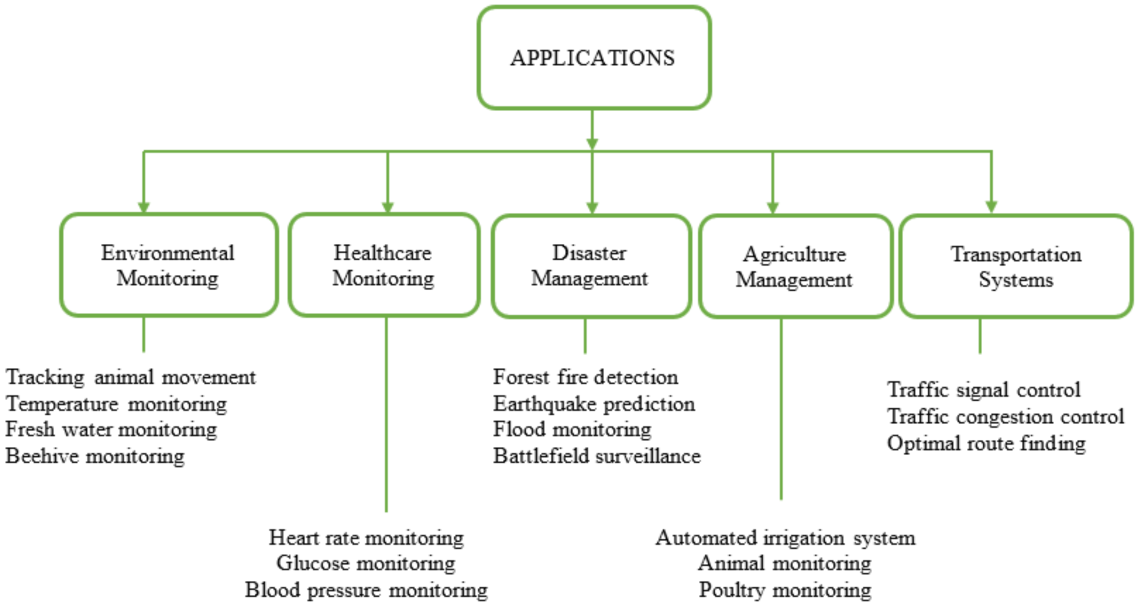


Fig 3: WSN applications

IEEE 802.15.4 is a standard developed for the wireless devices that are operating in Low Rate Wireless Personal Area Networks (LR-WPANs). It benefits with low power and low cost and suitable for applications having short range communication. The Full Functional Device (FFD) can act as a PAN (Personal Area Network) coordinator, a simple coordinator or a device and supports both star topology and mesh topology. The Reduced Functional

Device (RFD) is a simple device that cannot be a coordinator and can communicate only with FFD [4]. This standard defines the lower layers such as the physical and Medium Access Control (MAC) layer and the upper layers such as network and security layers are defined by Zigbee alliance.

The various monitoring and tracking applications using wireless sensor networks were presented. The taxonomy of applications and its design specific requirements are presented and application of WSN is depicted in Figure 3.

B. Challenges of Wireless Sensor Networks

The application of wireless sensor network in a wide variety of real time applications is increasing due to its potential benefits. However, a lot of challenges should be addressed by many researchers as follows:

- Fault Tolerance
- Energy Conservation
- Scalability
- Quality of Service
- Security
- Network Topology

C. Need for Integration Of Cloud Computing With WSN

Wireless Sensor Network (WSN) plays a vital role in diverse monitoring and tracking applications such as agriculture, military, healthcare, surveillance, environment monitoring, etc. Some monitoring applications like forest fire detection, battlefield surveillance and other security system involves dense deployment of sensor nodes. The nodes sense the environment continuously in such cases and collect a huge amount of data[5]. Due to the memory and power constrained nature of sensor nodes bulk data cannot be stored and transmitted. The data reduction schemes like data aggregation and compression are adopted with certain limitations which raises the need for efficient data management techniques.

The limitation of wireless sensor network in terms of energy, memory, computation, communication and data management can be well resolved by cloud computing. The integration of sensor networks into the cloud computing platform enables efficient mechanisms for data storage and data management [6]. The integration of WSN with cloud platform enables processing of the data gathered from several sensor networks, makes that information widely sharable, and collaborates with other cloud based applications. By the virtualization of physical sensor nodes, user‘s requirement can be satisfied on demand by serving Sensors as a Service (SE-aaS).

The routing protocol finds the shortest path to transmit the data from source to destination. It functions in three classes like on-demand routing, cluster based routing and cross layer-based mechanisms. The energy efficient routing is finding the optimal path for routing through cluster architecture, relay node placement, multipath routing, energy as a routing metric and sink mobility[7]. Cross layered approach enables the MAC protocol to provide support to the routing layer to reduce the latency and energy consumption. Further, the routing process is improved through optimization techniques by finding the optimal path between the source and destination based on certain constraints.

D. Introduction to cloud computing

Cloud computing is an emerging computing paradigm contributed from many technologies like grid computing, parallel computing, utility computing, ubiquitous computing and virtualization. It provides resources through three service models such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) as shown in figure 4. IaaS provides customizable infrastructure such as network devices, load balancers, database and web servers. PaaS provides platform for the development of various applications that are hosted in the cloud[8]. SaaS is a software delivery model that provides access to several applications as a web-based service. Cloud computing acts as a perfect solution for many resource constrained applications for its various benefits like flexibility, scalability, reliability and efficiency.

The cloud computing architecture is divided into different layers such as hardware layer, infrastructure layer, platform layer and application layer. The hardware layer is responsible for managing the physical resources of the cloud which is implemented in data centers. The infrastructure layer creates a pool of storage and computing resources through virtualization technologies. The platform layer consists of operating systems and application frameworks that minimize the burden of deploying applications directly into VM containers. The application layer, the highest layer comprises the actual cloud applications. The core middleware managed the physical infrastructure to accommodate runtime environment for various applications [9]. The cloud computing offers various services that should have the adaptability based on the resource availability and performance.

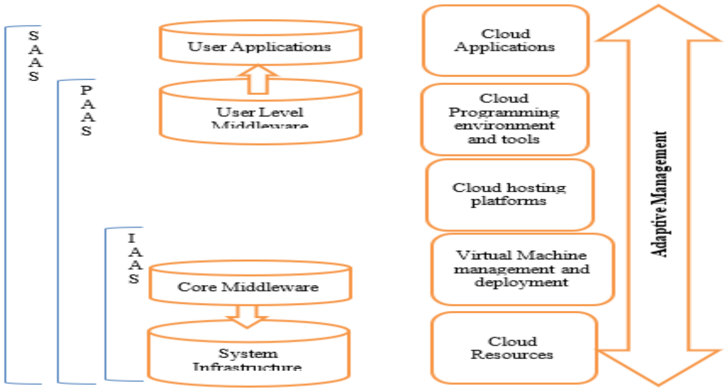


Fig 4 Cloud computing architecture

There are different types of cloud such as public cloud, private cloud and hybrid cloud. In public cloud, the service providers offer their resources as services to the general public whereas the private clouds are designed particularly for a single organization[10]. A hybrid cloud is a combination of public and private cloud models in which part of the service infrastructure runs in private clouds while the remaining part runs in public clouds. Cloud computing provides various features such as multi tenancy, shared resource pooling, ubiquitous network access, dynamic resource provisioning and utility based pricing.

2. Objectives of The Study

Delay is addressed through priority assignment using which the time between the packet generation and packet reception is reduced. Security is another important requirement to improve the performance of the network by sending only legal data [11]. The main objectives of the study are

- To propose a MAC protocol for scheduling the sensor nodes to minimize the delay and to improve the throughput and packet delivery ratio.
- To design a trust-based security system to detect Sybil attack and to improve the detection accuracy.
- To propose a routing protocol for improving the energy efficiency, throughput and packet delivery ratio.

3. Study of Existing System.

As traditional networks work towards minimizing response time, WSN is focused on minimizing energy consumption. The sensor nodes are battery powered and it is not easier to recharge the battery in all environments. The data collected from the environment should reach the base station in an energy efficient way [12]. Routing is the process of transmitting the data on the shortest path between multiple sender nodes and receiver nodes. The routing protocols should be designed based upon the application requirements by considering the WSN inherent features to provide power conservation and network longevity.

A. Classification of Routing Protocols

The routing protocols are categorized into hierarchical routing protocol, data centric routing protocol and location-based routing protocol as shown in Figure 5. The hierarchical routing protocol is suitable for large scale sensor networks and classified into cluster-based protocol and chain-based protocol [13]. In cluster-based protocol, the sensor nodes are arranged in the form of clusters and one leader node elected among the group acts as a head node. In chain-based protocol, the nodes are arranged in the form of a chain and one high energy node transmits the data from normal nodes to the base station.

The routing protocols are classified on the basis of routing decision making into proactive routing protocol, reactive routing protocol and hybrid routing protocol. In proactive routing, each node maintains the information about their neighbors in the routing table [14]. It reduces the overall delay but consumes more energy. Some popular proactive routing protocols are Destination-Sequenced Distance-Vector (DSDV), Wireless Routing Protocol (WRP) and Optimized Link State Routing Protocol (OLSR). In reactive routing strategy, the node that has data to transmit initiates the route discovery process to find the path to the destination. Some reactive routing protocols are Ad hoc On-demand Distance Vector Routing (AODV), Dynamic Source Routing (DSR) and Temporally Ordered Routing Algorithm (TORA).

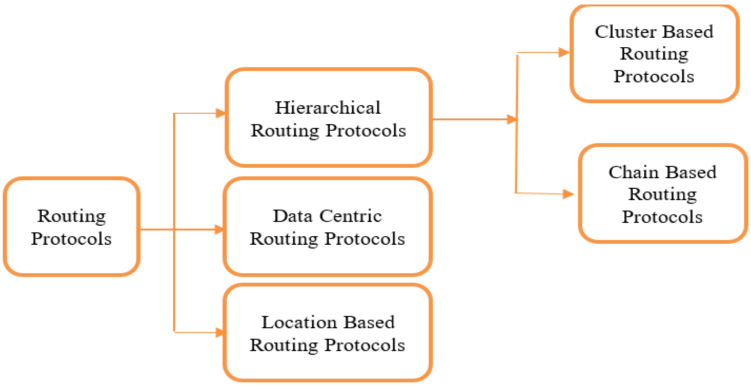

Routing Protocols
Hierarchical Routing Protocols
Data Centric Routing Protocols
Location Based Routing Protocols
Cluster Based Routing Protocols
Chain Based Routing Protocols

Fig 5. Routing protocol classification

B. Cluster Based Routing Protocols

In cluster-based routing protocols, the nodes are divided into clusters of equal or unequal size. The CH is the node responsible for various operations like data gathering from cluster members, data aggregation and data transmission to the base station [15]. Thus, the CH selection plays a major role for successful routing which leads to the discovery of many routing algorithms.

The LEACH protocol is the primary dynamic clustering protocol which is the basis for the emergence of many routing protocols. It operated under two phases namely setup phase and steady state phase. The CH was elected periodically for each round and all the nodes got a chance to become CH. The CH received the data from member nodes according to the TDMA schedule. This protocol achieved load balancing among the nodes, whereas the single hop communication between the CH and base station makes it unsuitable for large scale WSN.

In proposed a cluster-based routing protocol that distributed the nodes randomly. In Energy- Aware Clustering algorithm, the clusters were formed of even size with a random distribution of nodes. This algorithm elected the CHs based on the ratio of the average remaining energy of the neighbor members to the remaining energy of the current member competing for CH [16]. After the cluster formation phase, the data was transmitted through multi-hop communication to the base station. The selection of the next CH was based on the calculated relay value between the CH and its neighbors. The relay value was formulated from the ratio of the residual energy and the maximum initial energy and the total number of cluster members. This algorithm reduced the load of the CHs having more member nodes by selecting the next hop CH having lesser member nodes and improved the lifetime of the network.

C. Security in Wireless Sensor Networks

In the physical layer, jamming attacks and tampering attacks are the possible attacks. The jamming attack interferes with the radio frequencies and the tampering attack steals the node‘s information. The data link layer is affected by several types of attacks like exhaustion attack, collision attack and unfairness attack [17]. The network layer which is responsible for transmitting the data packets from source to destination is attacked by the attackers for unsuccessful data delivery. Several attacks in this layer are Sybil attack, selective forwarding attack, sinkhole attack, black hole attack, wormhole attack and acknowledgement spoofing attack. The transport layer is also affected by flooding attacks and desynchronization attacks.

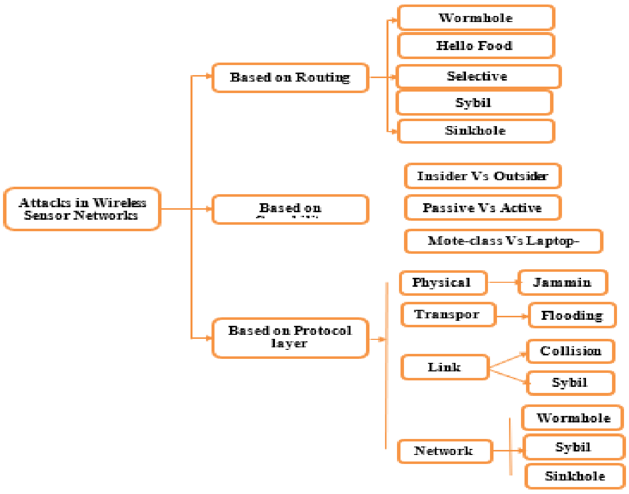


Fig 6 Security attacks classification

D. Classification of Security Attacks

The attackers misbehave in various ways like attacking radio transmission, altering the data by the addition of bits or dropping the data. The attacks are classified with respect to routing, capability and layer. The classification of security attacks is shown in Figure 6. The routing process is affected by misrouting the data, dropping the data, forwarding the only selected data and forwarding to the wrong destination[18]. Some of the possible attacks are Sybil attack, wormhole attack, selective forwarding attack, hello flood attack and sinkhole attack.

The insider attack and outsider attack are the attacks based on capability. In the insider attack, the trustworthy nodes behave maliciously, whereas the outsider attack is a form of attack by the nodes not belonging to the network. The passive attack involves monitoring the network traffic and the attackers access the data without any modification and without any interruption in communication. But the active attacks interrupt the data transmission, modify the data and include some faulty data in the network[19]. In the mote-class attack, the attackers attack with the nodes having similar capabilities as the network node. In the laptop class attack, the attackers attack with more powerful devices than the nodes in the network and can intrude the whole network.

Several types of attacks occur in various protocol layers like physical layer, data link layer, network layer and transport layer. The common attacks in physical layer are eavesdropping, tampering and jamming. The data link layer is subjected to various attacks like collision, interrogation and packet replay. The routing layer which is responsible for successful delivery between the source and destination is affected by wormhole attack, black hole attack, Sybil attack and selective forwarding attack. The flooding attack and de-synchronization attack are the common attacks in the transport layer.

E. Sybil Attack Detection Approaches

Sybil attack is a type of attack that affects routing in which a malicious node generates multiple fake identities to access a specific area of the network. This attack leads to many other attacks like wormhole attack, sinkhole attack, etc. There are various Sybil attack detection approaches such as Received Signal Strength Indicator (RSSI) based detection, Random Password Comparison (RPC) method, trust based detection, position verification and etc.

A trust based identity detection was developed to detect the Sybil attacks. The Sybil nodes were detected on the basis of identity modification and packet forwarding nature. The node‗s trust value was lowered during every modification of its id, which also resulted in the change of neighbors list. The CH collected the trust value of a node from all the member nodes. It compared the average trust value of the node with the threshold value. If the trust value was lesser than the threshold value, then the node was designated as a Sybil node. This achieved a better packet delivery ratio and reduced the delay and overhead.

F. Role of Optimization Algorithms In WSN.

The optimization algorithms are adopted in WSNs either to maximize or minimize a particular objective satisfying certain conditions. The objective may be a single objective or multi objective problem. The single objective problems are maximizing lifetime, minimizing energy consumption, minimizing delay and etc. The multi objective optimization problem deals with more number of objectives which may or may not conflict with each other.Many objectives such as energy conservation, coverage efficiency, packet error rate, average delay are considered together for multi objective problems to achieve better performance.[20]

In multi objective optimization problem, the objectives are integrated into a single problem by assigning different weights to the different problems. Several methods such as Eigen vector method, direct assignment, entropy methods were used for weight assignments. There exist multiple solutions for an optimization problem and one optimal solution is chosen based on the objective function.

The optimization algorithms are classified into Genetic Algorithm (GA), bio inspired algorithms like Particle Swarm Optimization algorithm (PSO), Flower Pollination Algorithm (FPA), Firefly Algorithm (FA), fuzzy logic-based algorithms and heuristic algorithm. The nature inspired optimization algorithms, finds the optimal solution based on local search and global search methods. These algorithms can be adopted in nonlinear and multi modal problems.

4. Sensor Cloud Architecture

The wide adoption of wireless sensor networks in various applications such as monitoring patient‗s health conditions, collecting data from the environment, etc, produces massive data. These large volumes of data should be stored in the sensor node for processing. As the sensor nodes are having limited storage and computation capabilities, huge data cannot be stored and processed. Cloud computing is a promising technology, which provides a solution for the issues in the sensor nodes by providing massive computing capabilities, a huge volume of storage, and software services for data analysis. [12]

A. System Architecture

The architecture comprises of three main modules such as clustering module, slot allocation module performed by MAC protocol, security module and routing module as shown in Figure 7.

Clustering Module

Sensor nodes are formed into clusters and a CH is selected among the cluster members having high residual energy. The distance between the CH and CMs and the load factor of the CHs are taken into consideration for cluster formation. The CHs are continuously monitored and when its residual energy drops to a threshold value, then another member in the cluster is elected as CH. Also, as the CHs nearer to the sink have to forward both their data and data from other CHs, their load is reduced by associating less number of member nodes compared with other CHs.

MAC Protocol

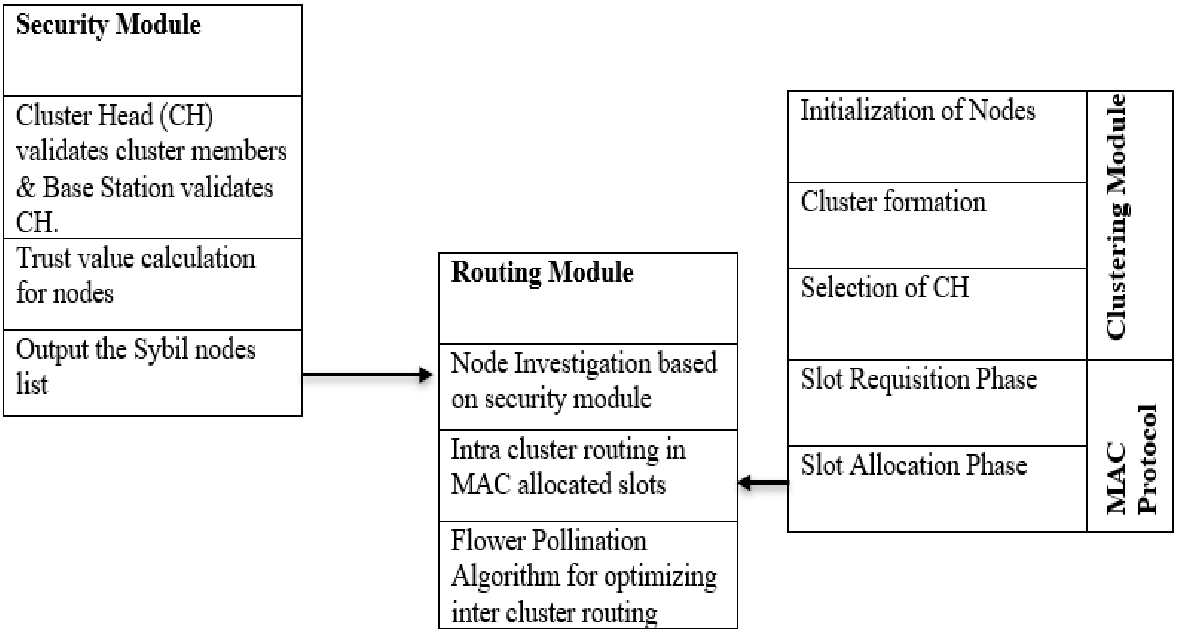
A CSA-ML MAC protocol is proposed for scheduling the sensor nodes based upon the priority and number of packets in the queue. The CSA-ML MAC protocol allocates the slots of variable size in multiple layers randomly to achieve energy efficiency. The CH allocates the slots to their CMs based upon their communication needs i.e. the time needed to transmit the number of packets in their queue. The nodes having a high priority is allocated first followed by low priority members and the number of packets in the queue is also considered to avoid packet loss. This reduces the delay in transmitting the data and improves the packet delivery ratio.[16]

Security Module

A trust based security system is proposed for detecting Sybil attack, an attack that affects routing. In Sybil attack, the malicious node creates multiple virtual identities to get control over the particular area of the network. The proposed detection mechanism detects the Sybil nodes in two level, first level by the CH and second level by the base station. The nodes are detected based upon their identity, location and node generation time. The trust value is calculated according to the residual energy and packet dropping rate of the sensor node at various time intervals. The nodes having the trust value, lesser than the threshold value are identified as Sybil nodes. This also identifies the Sybil nodes in the neighboring clusters and achieves better detection accuracy. These identified Sybil nodes are excluded in the routing process to improve the packet delivery ratio. [18]

Routing Protocol

A cross layer-based routing protocol is proposed and optimized through Flower Pollination Algorithm. The routing is performed in two phases such as intra cluster routing between the CMs and CH and inter-cluster routing between CHs and base station. In intra cluster routing, the CH receives the data packets from their CMs in the allocated slots by CSA-ML MAC protocol. In inter-cluster routing, the data aggregated in the CHs are transmitted to the base station through multiple hops. The routing path is optimized through Flower Pollination Algorithm based upon the total energy consumption of the path. During the routing process, the nodes are investigated based upon the trust-based Sybil attack detection mechanism. This proposed routing protocol minimizes the energy consumption and end-to- end delay and improves the throughput and packet delivery ratio.



Security Module
Cluster Head (CH) validates cluster members & Base Station validates CH.
Trust value calculation for nodes
Output the Sybil nodes list
Routing Module
Node Investigation based on security module
Intra cluster routing in MAC allocated slots
Flower Pollination Algorithm for optimizing inter cluster routing
Initialization of Nodes
Cluster formation
Selection of CH
Clustering Module
Slot Requisition Phase
Slot Allocation Phase
MAC Protocol

Fig 7. Proposed system architecture

5. Design of CSA-ML MAC Protocol

The main objective of the proposed MAC protocol is to reduce the delay and to improve the packet delivery ratio. The existing dynamic allocation schemes allocated the slots for the nodes such that they have to be in an active state in their allotted time period in the frame, resulting in wastage of energy. This problem is resolved through allocating variable size slots according to the communication requirements. Many MAC protocols allocated the slots for the nodes in a single layer, which is replaced in the proposed protocol through slot allocation in multiple layers. Moreover, by checking the queue size of the nodes, the slots are allocated to those nodes whose queue size is equal to the threshold value. The critical data is also transmitted prior to normal data through the priority indicator. Thus, the proposed protocol avoids the packet loss problem and also reduces the delay. The protocol functionalities are divided into two phases such as

- Cluster formation phase
- Optimal slot allocation phase

A. Cluster formation phase

The cluster based WSN is as shown in figure 8Clustering is one of the common techniques adopted in wireless sensor networks for improving the performance of the network. It is classified based upon the clustering methodology into centralized, distributed and hybrid. In the centralized clustering scheme, the formation of clustering and selection of the cluster head is performed by the controller node. This involves various communication messages between the nodes and the controller, which is not suitable for large scale sensor networks. In distributed clustering, the cluster head is elected and clusters are formed by the nodes themselves based on certain parameters and the role of CH is also rotated.

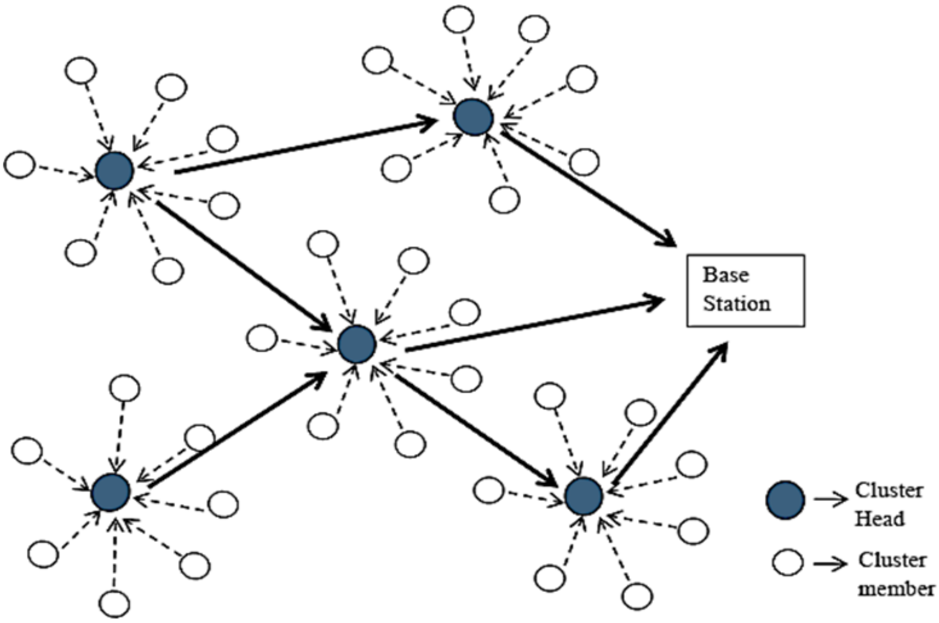


Fig 8. A cluster based wireless sensor network

A node is elected as a CH based upon three constraints such as residual energy, distance between the sensor node and CH and load factor of the CH. The primary constraint of a node to become CH is the node should have more residual energy than its neighboring nodes. The nodes transmit the data for long distance consumes more energy and therefore the distance between the CH and CMs is to be minimized. Thus, CMs are associated with the selected CH based upon the distance between them. Further, the number of nodes associated with the cluster head is also considered and the load is adjusted among the clusters.

B. Optimal slot allocation phase

The clustering phase is followed by the optimal slot allocation phase. In the clustering phase, the clusters are formed and the CHs are elected for each cluster. The data is transmitted from the CMs to the CH through intra cluster routing in the respective time slots. In the optimal slot allocation phase, the slots are allocated by the CH to collect data from their member nodes. The data transmission between the cluster members and the cluster head is performed through various transmission cycles. Each cycle comprises of Slot Requisition Phase (SRP), Slot Allocation Phase (SAP) and Data Transmission Phase (DTP) as shown in Figure 9.

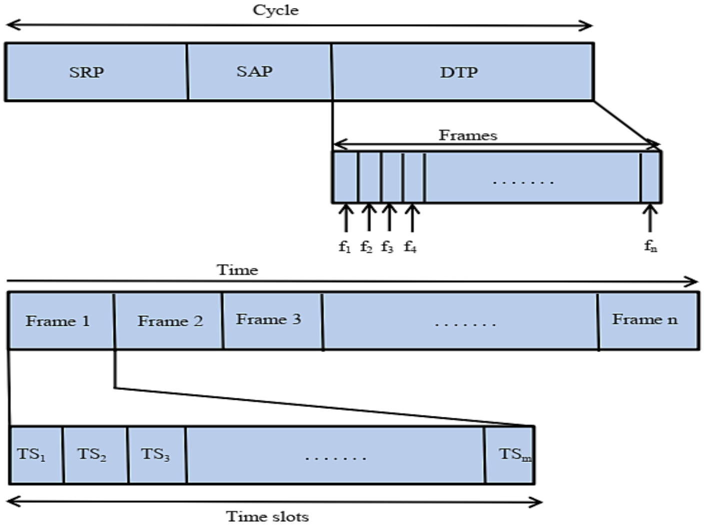


Fig 9. Transmission cycle Slot

The priority is assigned for the data packets generated by all the CMs of each cluster. It is assigned by the member nodes based upon the criticality of data and the same is communicated to the cluster head. The information about the priority is included in the packet header and sent to the CH node. It is set to 1 for emergency type data which should be reached to the base station without delay and set to 2 for normal periodic data as mentioned below in Algorithm 3. The priority assigned is utilized by the cluster head during slot allocation which is send by the cluster members. The slots are assigned for the data packets having priority 1 and the remaining slots are allocated for low priority packets.

Algorithm 3 Priority assignment

```
for all CMs in a cluster
        if category (data_CM [i]) = emergency_data then PRI_CM [i] = 1
                HPM .add (CM[i])
        else
                PRI_CM [i] = 0 LPM .add (CM[i])
        end if
end for
```

After the cluster members got segregated, they are sorted according to the number of data packets in their queue (Np). This sorting enables the CMs that have more packets in their queue to get the slots allocated prior to other CMs.

Experimental Results and Discussion

The proposed CSA-ML-MAC protocol is implemented in NS-2.35 simulator and the performance is assessed through the results obtained in the simulation. It is evaluated by examining the parameters such as Duty Cycle (DC), Packet Delivery Ratio (PDR) and delay and compared with WA-MAC. In this simulation, 100 regular sensor nodes are deployed in an area of 1500 X 1500 and other parameters are mentioned in Table 1.

Table 1: Simulation parameters.

Sl no	Parameters	Evaluation
01	**Simulation time**	**100 seconds**
02	**Relative delay ratio**	**0.25**
03	**Channel type**	**Connection less**
04	**Data Traffic type**	**Constant bit rate**
05	**Maximum number of nodes**	**250**
06	**Maximum Range of sensing**	**250m**

The entire transmission cycle is divided into equal size frames based upon the number of nodes. Each frame is divided into variable size slots according to the number of packets a node has to transmit. The slot length of each packet is calculated by the number of packets and the data transmission rate. A guard time is inserted between each slot of a frame to avoid the collision problem due to clock drift. The parameters of the time frame are mentioned in Table 2.

Table 2: Frame parameters

Sl no	Parameters	Evaluation
01	**Data rate**	**200 kbps**
02	**Maximum frame length**	**3s**
03	**Packet size**	**80 bytes**
04	**Packet Interval**	**10s to 50s**

C. Delivery delay

The Delivery Delay (DD) is measured as the time between the packet generation at source node and packet reception at destination node. The relative delay is the ratio between the DD and the average data arrival interval at each sensor node. The average DD is calculated under sunny and sunny rain weather conditions. It shows that an increase in the value of Packet Generation Interval (PGI) increases the DD. The simulation is carried out by increasing the PGI and the corresponding delivery delay is calculated. The PGI values are varied from 6s to 20s in the intervals like 6s, 8s, …, 20s in each round. When the packet generation interval is 6s, CSA-ML MAC achieves 4.2% whereas WA-MAC achieved 4.7%. The results show that, CSA-ML MAC protocol achieves 12.6% lesser delay on average compared with WA-MAC protocol as given in Figure 10 and Figure 11

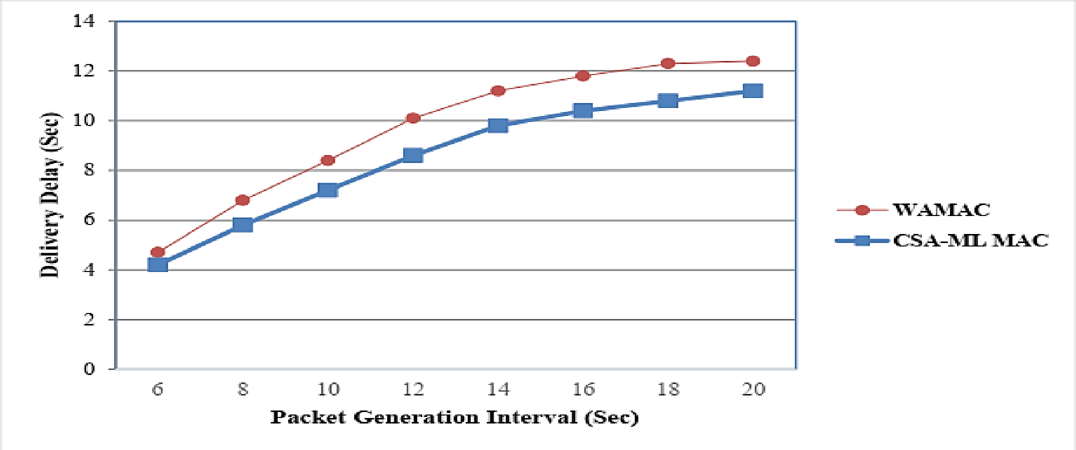


Fig 10. Effect of Packet Generation Interval on delivery delay (sunny weather)

D. Duty cycle

The duty cycle is measured as the portion of the active time utilized by a sensor node for transmission within the entire execution time. It is calculated under sunny and sunny-rain conditions and the results are shown in Figure 12 and Figure 13. From the results, it is observed that CSA-ML MAC protocol outperforms WA-MAC protocol. For example, when the packet generation interval is 6s, CSA-ML MAC attains 4% whereas WA-MAC attained 4.3%, which shows a reduction of 7% duty cycle. This reduction of duty cycle is due to the allocation of variable size time slots which leads the nodes to enter sleep state after their transmission.

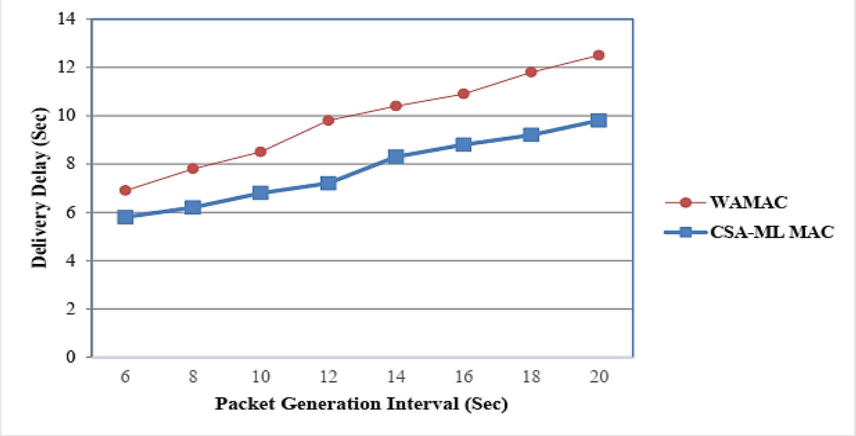
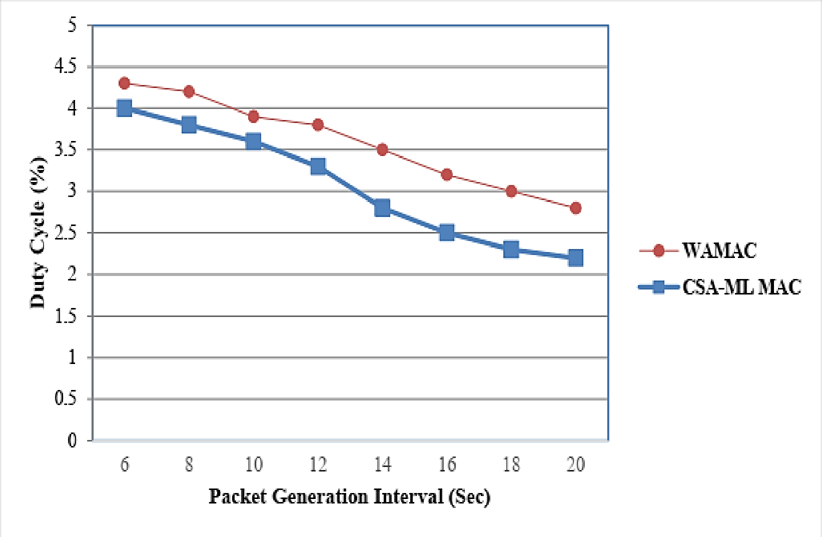


Fig 11. Effect of Packet Generation Interval on delivery delay (sunny-rain weather)



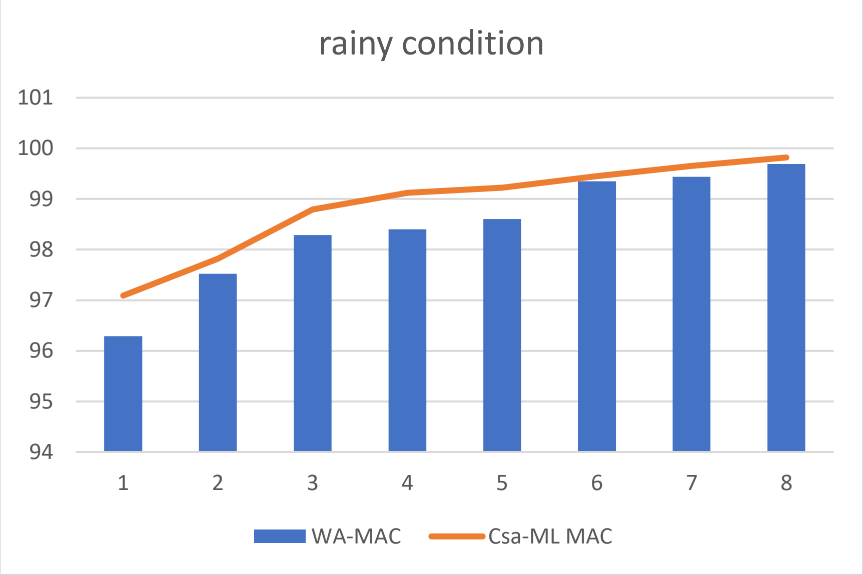


Fig 12 Effect of packet generation interval on duty cycle (sunny weather)

E. Packet delivery ratio

The PDR is the ratio of the total number of packets that reached the sink node to the total number of packets generated at the source node. It is the important performance metric considered in many applications. The PDR is calculated for varying packet generation intervals for CSA-ML MAC and WA-MAC under sunny and sunny rain conditions. From the results, it can be observed that CSA-ML MAC performs better than WA-MAC. For example, for the packet generation interval 5s, WA-MAC attained 97.52% and CSA- ML MAC attains 97.82% packet delivery ratio. This reduction is due to the consideration of the queue size for slot allocation which reduces the packet loss and improves PDR. The results are tabulated in the Table 3 and Table 4 as given below:

Table 3. Comparison of PDR of WA MAC and CSA-ML MAC under sunny weather conditions

Sl no		1	2	3	4	5	6	7	8
Packet generation interval (in sec)		5	7	9	11	13	15	17	19
PDR (%)	WA-MAC	96.29	97.52	98.29	98.4	98.6	99.35	99.44	99.69
	Csa-ML MAC	97.09	97.82	98.79	99.12	99.22	99.45	99.65	99.82

Table 4 Comparison of PDR of WA MAC with CSA-ML MAC under sunny and rainy weather conditions.

Sl no		1	2	3	4	5	6	7	8
Packet generation interval (in sec)		5	7	9	11	13	15	17	19
PDR (%)	WA-MAC	98.03	98.36	98.83	96.63	98.63	98.73	99.23	99.45
	Csa-ML MAC	98.99	98.73	99.01	99.25	99.35	99.45	99.52	99.75

F. Residual energy

The amount of energy consumed by the nodes is calculated based on the first order radio model. The nodes consume energy during data transmission and reception and also the energy gets lost due to various factors like collision and idle listening. The MDA-SMAC protocol reduced the collisions between the nodes using the back-off algorithm based on buffer utilization. The CSA-ML MAC protocol allocates the slots based on queue length, priority and node‘s communication requirements. This results in the reduction of energy consumption due to idle listening. By increasing the data transmission interval, CSA-ML MAC protocol achieved lesser energy consumption than MDA-SMAC protocol.

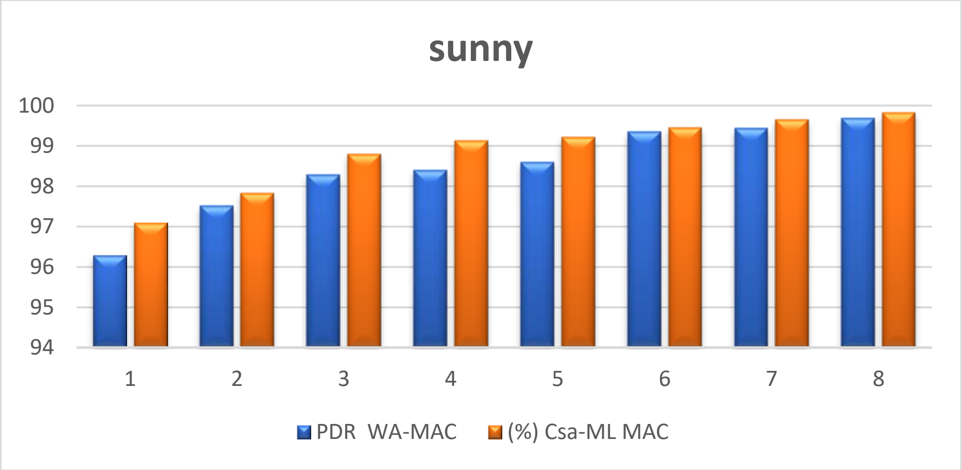


Fig 13. Effect of packet generation interval on duty cycle (sunny- rain weather)

6. Conclusion

The integration of a wireless sensor network with a cloud platform addresses the diverse limitations inherent in sensor networks, such as constrained processing capabilities, limited storage, and finite power sources. This necessitates the development of effective solutions to surmount these challenges. The application-specific requirements of Wireless Sensor Networks (WSN) provide a fertile ground for researchers to explore and propose innovative solutions. In surveillance-based applications, paramount considerations include achieving energy efficiency and minimizing delays.

The data collected by these applications find a home in a cloud database, facilitating streamlined processing and analysis. Therefore, it is imperative that the transmission of data from the Wireless Sensor Network (WSN) to the cloud server is not only efficient but also highly reliable. To address this, we introduce the Secured Energy Efficient Framework (SEEF), a comprehensive approach encompassing three essential modules: node scheduling, node investigation, and a robust routing mechanism. The SEEF framework aims to optimize the transmission process, ensuring the seamless and secure delivery of data from sensor nodes to the cloud server.

The integration of a wireless sensor network with a cloud platform addresses limitation like processing, storage, and power constraints in sensor nodes. Energy efficiency and low latency are crucial for surveillance applications. A Secured Energy Efficient Framework (SEEF) is proposed, incorporating cluster-based topology, Content Slot Allocation based Multi-Layer MAC (CSA-ML MAC) protocol, and a trust-based Sybil attack detection mechanism. CSA-ML MAC dynamically allocates variable-sized slots, reduces end-to-end delay by 12.6%, duty cycle by 7%, and improves packet delivery ratio. The Sybil attack detection mechanism enhances detection accuracy with a 22% reduction in false positives and a

10% improvement in true positives. The routing protocol employs intra-cluster and inter-cluster routing phases, optimizing inter-cluster routing using a flower pollination algorithm. The proposed mechanisms collectively achieve energy savings, reduced delay, improved packet delivery ratio, and throughput compared to existing protocols.

Scope for future work:

The proposed MAC protocol is designed for single-channel operation but can be extended to multi-channel environments. It accommodates static deployment of source and sink nodes, considering mobility for both types. Additionally, data collected in cloud storage can undergo analysis using various data mining methodologies. The system can incorporate energy harvesting approaches such as solar and wind for meeting energy requirements. Evaluation is conducted using a simulator adaptable to real-time applications like surveillance.

References

[1] V. A. Natarajan and M. S. Kumar, "Improving QoS in Wireless Sensor Network routing using Machine Learning Techniques," 2023 International Conference on Networking and Communications (ICNWC), Chennai, India, 2023, pp. 1-5, doi: 10.1109/ICNWC57852.2023.10127349.

[2] C. Karthick, C. Kathirvel, C. Jeevakarunya and P. Deepa, "Location based Energy Efficient Routing Protocol for Improving Network Lifetime in WSN," 2023 IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS), Raichur, India, 2023, pp. 1-6, doi: 10.1109/ICICACS57338.2023.10099892.

[3] L. Wang, V. Lehman, A. K. M. Mahmudul Hoque, B. Zhang, Y. Yu and L. Zhang, "A Secure Link State Routing Protocol for NDN," in IEEE Access, vol. 6, pp. 10470-10482, 2018, doi: 10.1109/ACCESS.2017.2789330.

[4] W. R. Heinzelman, A. Chandrakasan and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, Maui, HI, USA, 2000, pp. 10 pp. vol.2-, doi: 10.1109/HICSS.2000.926982.

[5] W. B. Heinzelman, A. P. Chandrakasan and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," in IEEE Transactions on Wireless Communications, vol. 1, no. 4, pp. 660-670, Oct. 2002, doi: 10.1109/TWC.2002.804190.

[6] S. Sasirekha and S. Swamynathan, "Cluster-chain mobile agent routing algorithm for efficient data aggregation in wireless sensor network," in Journal of Communications and Networks, vol. 19, no. 4, pp. 392-401, August 2017, doi: 10.1109/JCN.2017.000063.

[7] T. M. Behera, S. K. Mohapatra, U. C. Samal, M. S. Khan, M. Daneshmand and A. H. Gandomi, "Residual Energy-Based Cluster-Head Selection in WSNs for IoT Application," in IEEE Internet of Things Journal, vol. 6, no. 3, pp. 5132-5139, June 2019, doi: 10.1109/JIOT.2019.2897119.

[8] J. Xu, N. Jin, X. Lou, T. Peng, Q. Zhou and Y. Chen, "Improvement of LEACH protocol for WSN," 2012 9th International Conference on Fuzzy Systems and Knowledge Discovery, Chongqing, China, 2012, pp. 2174-2177, doi: 10.1109/FSKD.2012.6233907.

[9] N. Javaid, S. N. Mohammad, K. Latif, U. Qasim, Z. A. Khan and M. A. Khan, "HEER: Hybrid Energy Efficient Reactive protocol for Wireless Sensor Networks," 2013 Saudi International Electronics, Communications and Photonics Conference, Riyadh, Saudi Arabia, 2013, pp. 1-4, doi: 10.1109/SIECPC.2013.6550797.

[10] H. Yu and W. Xiaohui, "PSO-based Energy-balanced Double Cluster-heads Clustering Routing for wireless sensor networks", *Procedia Engineering*, vol. 15, pp. 3073-3077, 2011

[11] S. Tyagi and N Kumar, "A systematic review on clustering and routing techniques based upon LEACH protocol for wireless sensor networks", *Journal of Network and Computer Applications*, vol. 36, no. 2, pp. 623-645, 2013.

[12] M. Waqas, S. U. R. Malik, S. Akbar, A. Anjum and N Ahmad, "Convergence time analysis of OSPF routing protocol using social network metrics", *Future Generation Computer Systems*, vol. 94, pp. 62-71, 2019.

[13] W. B. Heinzelman, A. P. Chandrakasan and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks", *IEEE Transactions on Wireless Communications*, vol. 1, no. 4, pp. 660-670, October 2002.

[14] M. Faheem, R. A. Butt, B. Raza, M. W. Ashraf, A. Ngadi and V. C. Gungorb, "Energy efficient and reliable data athering using internet of software-defined mobile sinks for WSNs-based smart grid applications", *Computer Standards and Interfaces*, vol. 66, pp. 103341, 2019.

[15] Lavanya Vaishnavi DA and Anil Kumar C, “Various insights of Wireless Communication”, International Journal of advance researcher in science, communication and technology, Volume 3, Issue 2, August 2023, ISSN (Online) 2581-9429, DOI: 10.48175/IJARSCT-12729, Page 191-199

[16] L. Chen, D. Yang, D. Zhang, C. Wang and T.-M.-T Nguyen, "Deep mobile traffic forecast and

complementary base station clustering for C-RAN optimization", *Journal of Network and Computer Applications*, vol. 121, pp. 59-69, 2018.

[17] Anil Kumar C & et al “Cloud Computing based EHR”**,** International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8, Issue-1C, May 2019.

[18] Anil Kumar C, Chethan Venkatesh, Lavanya Vaishnavi D A, Harish S, “Computer vision based Hand gesture recognition system”, Neuro Quantology, Jul 2022, Volume 20, Issue 7, Page 2859-2866, DOI: 10.14704/nq.2022.20.7.NQ33365

[19] B. Bhushan and G. Sahoo, "Routing protocols in wireless sensor networks" in Computational Intelligence in Sensor Networks, Berlin:Springer, pp. 215-248, 2019.

[20] Rakhee and M. B. Srinivas, "Cluster Based Energy Efficient Routing Protocol Using ANT Colony Optimization and Breadth First Search", *Procedia Computer Science*, vol. 89, pp. 124-133, 2016.