International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 03 | Mar 2021 www.irjet.net p-ISSN: 2395-0072

Effective Implementation of Efficient Data Collection in WSN

C. Jisha Chandra[1], L.Suganya[2], J.Manjushree Kumari[3], R.Nagarajan[4], S.Kannadhasan[5]

[1]Research Scholar, Department of Electrical and Electronics Engineering, Gnanamani College of Technology, Tamilnadu, India.
[2]Assistant Professor, Department of Electrical and Electronics Engineering, PGP. College of Engineering &Technology Tamilnadu, India
[3]Research Scholar, Department of Electrical and Electronics Engineering, Gnanamani College of Technology, Tamilnadu, India.
[4]Professor, Department of Electrical and Electronics Engineering, Gnanamani College of Technology, Tamilnadu, India
[5]Assistant Professor, Department of Electronics and Communication Engineering, Cheran College of Engineering, India

---

Abstract - *Present wireless sensor network routing research has mainly centered on protocols that are energy conscious in order to increase the network's lifespan, are flexible to support a wide number of sensor nodes, and are immune to sensor damage and battery exhaustion. It is important to save resources in wireless sensor networks. Since energy considerations have overshadowed most sensor network science, the principles of delay have not been a primary concern in most of the published work. In WSANs, however, depending on the program, it may be appropriate to respond to sensor input quickly. Furthermore, in order to have effective behavior, sensor data must be current at the moment of operation. Routing focused on Forwarding Sets and the Random Wakeup Scheme is the two key components of AEPRA. The AEPRA routing approach is planned to take account of the dense implementation of sensor networks. The shortest route between two nodes is calculated proactively or reactively in standard routing protocols, and a node just forwards a packet to the next node on the computed shortest path. Because of the high node density, there are many routes between two nodes, many of which are very similar to the length of the shortest route.*

***Key Words*: Mobile Node, WSN, AEPRA, Shortest Path and Packet Ratio**

1. INTRODUCTION

Sensors probe their environments and transmit data to actor nodes in wireless sensor-actor networks. Actors collaborate together to accomplish a predetermined application task. Since actors must coordinate their behavior, a well-connected network topology must be maintained at all times. Furthermore, to satisfy latency criteria, the duration of inter-actor contact paths can be reduced. However, if one of the actors fails, the network can be partitioned into disjoint blocks, which would breach the communication target. To regain connectivity, one of the most successful recovery methodologies is to autonomously reposition a subset of the actor nodes. Modern recovery schemes either involve a lot of node relocation or expand any of the inter-actor data routes. The Adaptive energy Efficient Protocol for Fault Recovery Actors (AEPRA) algorithm presented in this paper addresses these flaws. AEPRA utilizes a node's local vision of the network to formulate a recovery strategy that relocates the fewest amount of nodes necessary while ensuring that no route between any two nodes is expanded. AEPRA is a distributed and localized algorithm that utilizes the network's current route exploration operations and introduces no extra pre-failure connectivity overhead [1]-[5].

AEPRA increases the network lifespan by changing the actors' energy use. AEPRA's output is mathematically evaluated and tested by detailed simulation studies. Replica node attacks are risky since they enable an intruder to take control over a significant portion of the network by leveraging the compromise of a few nodes. To protect against such attacks in static sensor networks, many replica node detection schemes have been suggested in the literature. These systems, on the other hand, are focused on fixed sensor positions and therefore do not operate in mobile sensor networks, where sensors are supposed to travel. Using the Sequential Likelihood Ratio Measure, we propose a quick and efficient mobile replica node detection scheme in this article. To our knowledge, this is the first paper to address the issue of replica node attacks in mobile sensor networks. The issues of node relation likelihood and ratio of mobile access nodes in a network are explored in this work, as well as the issue of energy-efficient data collection through mobile sensors with Three-Tier protection [6]-[10].

Mobile wireless sensor networks (MWSNs) are a type of WSN in which versatility is essential for the application's execution. Mobility has been a significant field of study for the WSN group in recent years. While WSN implementations were never meant to be entirely static, versatility was initially seen as presenting a range of challenges, including accessibility, coverage, and energy usage, to name a few. Latest research, on the other hand, has portrayed versatility in a more positive way. Rather than exacerbating these

challenges, it has been seen that introducing mobile institutions will help to overcome some of them. Furthermore, sensor nodes with versatility will target and track moving phenomena such as chemical clouds, cars, and parcels. The requirement for localization is one of the most important obstacles for MWSNs. Sensor location must be understood in order to understand sensor data in a spatial sense or for proper navigation in a sensing area. Since sensor nodes may be dynamically distributed (e.g., lowered from an aircraft) or shift location in real time (e.g., while connected to a shipping container), it's conceivable that no one knows where each node is at every given time [11]-[15].

This is less of an issue in static WSNs since node locations are unlikely to shift after they have been decided. Mobile sensors, on the other hand, must estimate their location periodically, which requires time and energy and absorbs other resources provided by the sensing program. Furthermore, mobile sensors cannot use localization schemes to include high-accuracy positioning information in WSNs because they usually need centralized processing, take too long to operate, or create assumptions about the world or network topology that do not extend to complex networks. The defense of unattended mobile nodes in inherently hostile conditions is important. The intruder can be able to catch and hack mobile nodes, which he or she will then use to inject false data, interrupt network activities, and listen in on network conversations. The key problem or downside of a wireless sensor network is its resource drawback. The word "strength" often refers to electricity. The lifetime of sensor networks is increased or decreased based on the strength. As a consequence, the wireless sensor network's strength or energy is a crucial parameter. The wake-up timing algorithm was used to save energy in certain wireless sensor networks. The wake-up receivers were included in that algorithm. Also in low-power wireless sensor network implementations, these receivers will prolong the existence of each and every sensor node [16]-[20].

2. PROPOSED METHOD

Often used is an effective attack-resilient computing algorithm. And if an attack were to arise, this algorithm would mean that the aggregate would be calculated successfully. Inter-actor connectivity is important considering the collective aspect of the WSAN operation. Coordination among actors is obviously impossible in a disconnected network topology. As a result, when actors travel, they try to maintain contact ties within themselves. However, if one or more actors fall, the network can be split into independent sub-networks. This may happen when reacting to a traumatic incident, such as a fire, which would necessitate a quick recovery to prevent the situation from spiraling out of control and causing catastrophic repercussions. Since WSAN is unattended and the deployment of spare actors can take some time, the recovery should be accomplished by network self-configuration utilizing established resources. In network aggregation algorithms to calculate aggregates such as predicate Count and Sum, there are protection problems. We spoke about how a compromised node might tamper with the base station's aggregate calculation, focusing on the ring-based hierarchical aggregation algorithm.

In the presence of an attack, a lightweight verification algorithm will enable the base station (BS) to check if the computed aggregate was correct, but it would not compute aggregate. As a consequence, we plan to create an attack-resistant computing algorithm. This algorithm would ensure that the sum would be calculated successfully even though there was an attack, as well as minimize contact overhead at a lower cost. Receiving a request from a source machine to store data, the request having an ownership and a data type, and directing the data to a computer memory whether the ownership and data type fit a matching entry in a store, and continuously forwarding the data from one computer memory to the next in a network of interconnected computer device nodes is referred to as selective data forwarding.

Data integration of wireless sensor networks cuts connectivity and energy usage significantly. A comprehensive aggregation architecture called synopsis diffusion is used in the current method, which incorporates multipath routing schemes with duplicate-insensitive algorithms to correctly calculate aggregates (e.g., predicate Count, Sum) despite message losses due to node and transmission failures. In the current method, a lightweight checking algorithm is used to decide if the calculated aggregate (predicate Count or Sum) contains any incorrect contributions. However, this aggregation system does not resolve the question of corrupted nodes contributing incorrect sub-aggregate values, resulting in significant errors in the aggregate computed at the base station, which is the aggregation hierarchy's root node. Selective forwarding systems, a modern novel strategy, would be focused on factors such as the node's usable battery, the packet delivery ratio expense of retransmitting a post, or the importance of packets. We want to build an attack-resistant computing algorithm here. And if an attack were to arise, this algorithm would mean that the aggregate would be calculated successfully.

More complicated schemes will do better in terms of importance, but they will also need data from other sensors. There are also suboptimal schemes that depend on local estimation algorithms and have a lower computational expense. WSN's main role is data processing. Its aim is to obtain sensor readings from sinks and analyze and process them using intermediate nodes. Owing to the high overhead of relaying signals, sensors close to a data sink deplete their battery power quicker than those farther apart, according to studies. Network efficiency suffers as a consequence of non-uniform energy usage, and network lifespan is shortened.

Sink mobility has recently been used to reduce and balance energy consumption among sensors.

The use of energy is a crucial factor in the design of WSANs, which usually rely on portable energy sources such as batteries for fuel. WSANs are large-scale networks of tiny embedded computers, each capable of sensing, computing, and connectivity. They've had a lot of attention in recent years. Sensor nodes in WSANs are limited in terms of computing capacity, contact bandwidth, and storage space, necessitating resource management. Clustering is used in WSANs because it enables network scalability, resource sharing, and optimal usage of constrained resources, as well as network topology reliability and energy saving attributes. Clustering systems have lower coordination overheads and more effective resource assignments, lowering total energy usage and reducing sensor node interference. With small clusters, a large number of clusters will clutter the region, and a small number of clusters will overwhelm the cluster head with large numbers of messages received from cluster participants.

AEPRA is a hierarchical routing protocol focused on clustering that determines the optimum number of clusters in WSANs to save energy and extend network lifetime. The importance of reducing connectivity energy usage at energy limited nodes and thereby increasing usable network lifespan was addressed in relation to a network architecture focused on the use of controllably mobile components. Increase the useful network lifespan by reducing energy usage at energy-constrained nodes. The infrastructure relies on network protocols and motion management techniques in particular. The important point to note is that the controllably mobile infrastructure experiments are conducted utilizing a real-world framework, rather than assuming idealistic radio spectrum models or service in unobstructed conditions.

To fix the problem of repeated position updates of actors contributing to both rapid energy usage of sensor nodes and increased collisions in wireless transmissions, a novel AEPRA routing for retrieving the defective actors has been suggested. The suggested scheme AEPRA takes advantage of the wireless sensor node's transmitted transmission design. During data transmission, as an agent travels, the latest position information is propagated through the reverse spatial routing direction to the source. Wireless sensor networks, on the other hand, are incredibly effective, yet they are unlike any other device or technology. Since it has a number of drawbacks and problems. The stronger, smaller sensor nodes characterize the wireless sensor network. A network is formed by a series of sensor nodes, each of which is very limited in size and continues to produce data.

The batteries were included with those sensors. As a consequence, the sensor nodes' lifetime has already been calculated, as seen in Figure 1. Furthermore, these batteries are not intended to be replaceable or rechargeable. As a result, in order to remain alive longer, certain sensor nodes must behave optimally. It could die due to power consumption if it required more energy to communicate, transmit, or perform other tasks. A sensor node would die as fast as it can if it proceeds to function and spend its energy resources. This entire function can replicate itself, resulting in the failure of the entire network. This is the most important concern for wireless sensor networks. However, in wireless sensor networks, there are a larger range of choices for conserving resources and monitoring additional parameters. To address the lack of the above parameters in a wireless sensor network, a greater number of protocols, algorithms, and concepts are usable. However, an independent parameter or two parameters in a situation may be resolved. In this scenario, the other parameter would fulfill their credibility criteria.

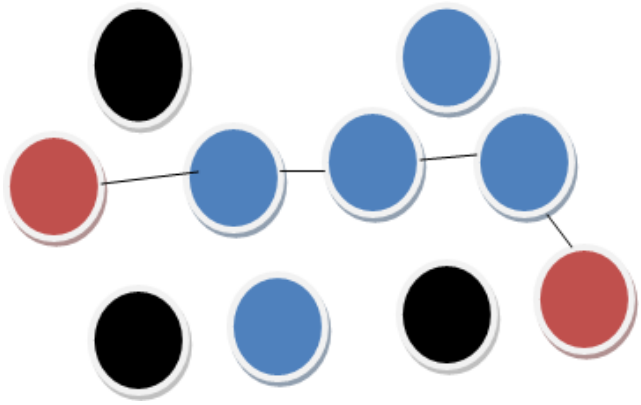

Figure. 1 Simple Proposed Method of WSN

However, not all sensor nodes function at the same time or do the same operation. While some sensor nodes are sensing, others are transmitting or receiving results. The sensor nodes' lifespan can be reduced depending on how they are actually used. If a sensor node sends or receives packets on a regular basis accompanied by sensing means, it will use more battery power or electricity. If we can reduce the active period of sensor nodes, we can expect them to last longer in a sensor network. In general, and though the sensor nodes are inactive, they can remain awake. As a result, idle sensor nodes do not engage in any operation such as sensing, sending, or receiving, but they do consume resources. If it's a big network, this is a major loss. When the sensor node is inactive, the wake-up scheduling is used to reduce energy usage. That is, when a sensor node is not engaged in any tasks for an extended period of time, it is switched to sleep mode. When the sensor node is inactive for a certain amount of time, the wake-up scheduling puts it into sleep mode.

In addition, the sensor nodes can go to sleep on a regular basis. The sleep node is awakened by the neighbor node's antenna whenever some sensor node sends packets to the sleeping nodes. Per sensor node in the sensor network has a wake-up antenna for potential operations. An external

power source is not needed for the antenna. In any case, it takes a lot of power to wake up neighbor nodes. The amount of power is approximately 6.6 micro amps. Here, electricity consumption is reduced, and the period is increased. However, as compared to other sensor nodes that do not have antennas, the wake-up antennas consume some electricity. In any case, the energy consumption is minimized to the greatest extent possible by using a sleep-wake timing algorithm. This is inadequate to boost the overall efficiency. In addition, we could increase the efficiency of wireless sensor networks by integrating further algorithms.

The sensor network has been the most important invention in the world since its inception. In the wireless sensor network, the problems are even greater. To solve these obstacles, certain methods, strategies, or principles must be used or implemented. However, through both of these strategies, there are more malicious actions that may impact the sensor network. As a consequence, the sensor network's total performance is given by a variety of algorithms, methods, or principles. This approach will assist in evaluating the utility of up to three parameters. In contrast to other networks, the network will therefore be an efficient sensor network. The mixture of algorithms will be used in wireless sensor networks in the future.

3. RESULTS AND DISCUSSION

WSNs are made up of a huge number of sensor nodes with insufficient battery capacity and the potential to connect wirelessly. These sensor nodes are used in WSN for sensing unexpected events (for example, a forest fire) and gathering sensed data from other nodes or the climate. When these sensor nodes identify suspicious activities, the data is transmitted via a hop-by-hop process to a specific node known as the sink node. As node d detects an anomalous occurrence, it sends an alert message to sink node. Notice that depending on the routing algorithm, the routing route may be static or interactive. WSNs have a broad variety of uses, including process control, health care tracking, environmental/ Earth sensors, forest fire prediction, and weather monitoring, among others. Sensors in a WSN are typically unaware of being recharged or substituted as the nodes' battery power runs out owing to Sensory Environments. As a consequence, these nodes can trigger a number of issues, including coverage gaps and connectivity issues.

Each node in a wireless sensor network conducts tasks such as sending, receiving, resting, detecting, interacting, and idle. According to their operations, each node in the sensor networks absorbs energy or battery power. Nodes, for example, use about 8 to 12 decibels of energy to communicate. Sensor nodes used between 7 to 10 decibels of energy while processing packets. When sensor nodes are idle, they consume very little power. When nodes are sensing, they produce about 10 decibels of noise. Per task absorbs a different amount of energy.

The increased delay in data collection caused by the pace at which data is obtained has been an issue in WSNs. As a consequence, a rendezvous point (RP) is used to effectively capture the data. The base station collects data here when visiting the rendezvous points. The data that has been buffered from multiple source nodes is aggregated at a certain point identified as RP by the rendezvous points. With agility and fixed monitoring, this paper proposes an effective rendezvous architecture algorithm with provable output bounds. The first approach is known as fixed tracking (FT), which includes gathering data following a fixed road. The second one is about versatility monitoring (MT), in which the track is formed using the shortest distance possible.

The rendezvous architecture issue for mobility activated WSNs, which aims to identify a series of RPs that can be visited by the BS within a specified pause whilst the network expense of transmitting data from sources to RPs is reduced, is one of its contributions. Consider the Steiner Minimal Tree principle, which effectively aggregates data at the RPs while reducing the BS data collection tour. The findings of simulations demonstrate that both algorithms will do well in a variety of situations. This architecture creates a network model with a multitude of nodes, positions, and energy levels. Data packets are relayed at a rate of several hundred meters per second in a WSN, which is considerably faster than the pace at which a handheld device travels. As a result, the deadline for data collection may be mapped to the full duration of the BS tour that visits all RPs. Figure.2 shows number of nodes alive

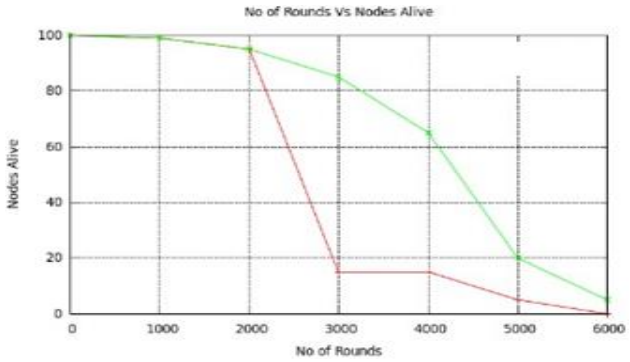

Figure.2. Number of Nodes Alive

It is presumed that data from multiple sources can be aggregated at a node before being relayed, and that each sensor node can be called by the consumer for recognition of which nodes submit data to the RP. To minimize network traffic, data storage applications have commonly embraced data consolidation. The nodes are densely spread in an area, and they all use the same transmitting capacity. The amount of energy required to transfer a data packet through a route is equal to the distance between the sender and the recipient. Figure.3. shows average latency of the proposed method and Figure.4 shows packet delivery ratio of the proposed method

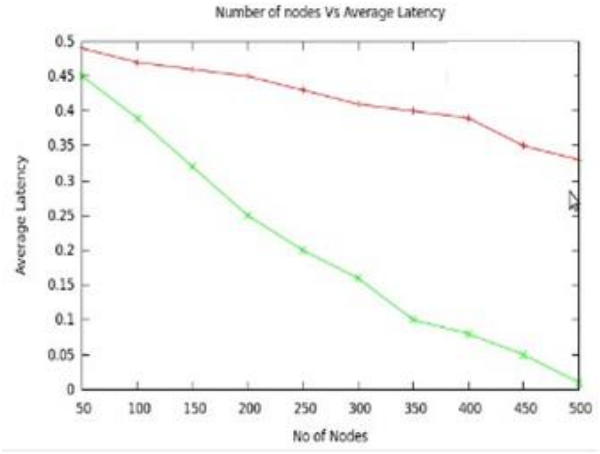

Figure.3. Average Latency of the Proposed Method

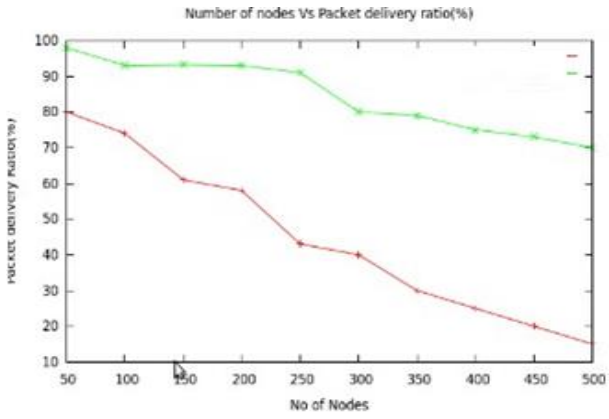

Figure.4. Packet Delivery Ratio of the Proposed Method

Since wireless sensor networks are unattended, an attacker can catch and hack sensor nodes, create replicas of them, and then use these replicas to launch a range of attacks. This replica node attacks are risky since they enable an intruder to gain control of a large portion of the network by exploiting the compromise of a few nodes. To protect against such attacks in static sensor networks, many replica node detection schemes have been suggested in the literature. These systems, on the other hand, are focused on fixed sensor positions and therefore do not operate in mobile sensor networks, where sensors are supposed to travel. Using the Sequential Likelihood Ratio Measure, we propose a quick and efficient mobile replica node detection scheme in this article. To our knowledge, this is the first paper to address the issue of replica node attacks in mobile sensor networks. We illustrate that our system identifies mobile replicas in an effective and accurate manner at a fair expense. A sensor node in a static sensor network is considered repeated if it is located in several locations. This strategy would not work while nodes switch about in the network, since a benign mobile node will be viewed as a duplicate due to the frequent shift in position. As a result, we'll have to depend on another method to detect replica nodes in mobile sensor networks.

4. CONCLUSION

We suggest a replica identification scheme for mobile sensor networks in this article. We've seen how intruder tactics to evade our tracking strategy have drawbacks. We first highlighted the drawbacks of a community assault technique in which the intruder is in charge of a group of replicas' gestures. We proposed a comparative study of the time period for avoiding identification and quarantine for a community of replicas. We have find a Nash equilibrium by modeling the relationship between the detector and the adversary as a repetitive game. Also the attacker's optimum benefits are severely constrained by the combination of identification and quarantine, as demonstrated by this Nash equilibrium. We tested the system using a random movement attack strategy, in which the attacker allows replicas to travel across the network at random, and a static positioning attack strategy, in which the attacker prevents his replicas from shifting to avoid detection. Our scheme easily identifies mobile replicas with a limited number of position statements against both strategies, according to the results of the set.

REFERENCES

[1] I. F. Akyildiz and I. H. Kasimoglu, "Wireless Sensor and actornetworks: Research Challenges," Elsevier Ad hoc Network Journal, Vol. 2, pp. 351-367, 2004.

[2]. M. Younis and K. Akkaya, "Strategies and techniques for node placement in wireless sensor networks: A survey," J. Ad Hoc Netw., vol. 6, no. 4,pp. 621–655, Jun. 2008.

[3] A. Abbasi, M. Younis, and K. Akkaya, "Movement-assisted connectivity restoration in wireless sensor and actor networks," IEEE Trans. Parallel Distrib. Syst., vol. 20, no. 9, pp. 1366–1379, Sep. 2009.

[4]. M. Younis, S. Lee, S. Gupta, and K. Fisher, "A localized self-healing algorithm for networks of moveable sensor nodes," in Proc. IEEE GLOBECOM, New Orleans, LA, Nov. 2008, pp. 1–5.

[5]. K. Akkaya, F. Senel, A. Thimmapuram, and S. Uludag, "Distributed recovery from network partitioning in movable sensor/actor networks via controlled mobility," IEEE Trans. Comput., vol. 59, no. 2, pp. 258–271, Feb. 2010.

[6]. K. Akkaya and M. Younis, "COLA: A coverage and latency aware actor placement for wireless sensor and actor networks," in Proc. IEEE VTC, Montreal, QC, Canada, Sep. 2006, pp. 1–5.

[7]. S.Kannadhasan and R.Nagarajan, Performance Analysis of Circular Shape Microstrip Antenna for Wireless Communication System, AICERA 2020, Amal Jyothi College of Engineering, Kerala, 14-16 December 2020, Published for IOP Conference Series: Materials Science

and Engineering, Vol: 1085, 012013, 2021, doi:10.1088/1757-899X/1085/1/012013

[8]. S. Yang, M. Li, and J.Wu, "Scan-based movement-assisted sensor deployment methods in wireless sensor networks," IEEE Trans. Parallel Distrib. Syst., vol. 18, no. 8, pp. 1108–1121, Aug. 2007.

[9] Wei Liu and Ming Yu, "AASR: Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments", IEEE Transactions on Vehicular Technology, Vol. X, No. Y, March 2014.

[10] Zhexiong Wei, Helen Tang, F. Richard Yu, Maoyu Wang, and Peter Mason, "Security Enhancements for Mobile Ad Hoc Networks with Trust Management Using Uncertain Reasoning", IEEE Transactions on Vehicular Technology, 2013.

[11] Yang Qin, Dijiang Huang, Senior Member, IEEE, and Bing Li, "STARS: A Statistical Traffic Pattern Discovery System for MANETs", IEEE Transactions on Dependable And Secure Computing, Vol. 11, No. 2, March/April 2014.

[12] Mustapha Reda Senouci, Abdelhamid Mellouk, and Khalid Assnoune, "Localized Movement-Assisted Sensor Deployment Algorithm for Hole Detection and Healing", IEEE Transactions on Parallel And Distributed Systems, Vol. 25, No. 5, May 2014.

[13] G.Ramya, R.Nagarajan and S.Kannadhasan, Energy Efficient Cluster Based Algorithm technique for Wireless Sensor Networks, AICERA 2020, Amal Jyothi College of Engineering, Kerala, 14-16 December 2020, Published for IOP Conference Series: Materials Science and Engineering, Vol: 1085, 012034, 2021, doi:10.1088/1757-899X/1085/1/012034

[14] Shan-Hung Wu, Jang-Ping Sheu, Fellow, IEEE, and Chung-Ta King, "Unilateral Wakeup for Mobile Ad Hoc Networks with Group Mobility", IEEE Transactions on Mobile Computing, Vol. 12, No. 12, December 2013.

[15] Qing Gao, and Orly Yadid-Pecht, "A Low-Power Block-Based CMOS Image Sensor With Dual VDD", IEEE SENSORS JOURNAL, VOL. 12, NO. 4, APRIL 2012.

[16] Yu Gu, Yusheng Ji, Jie Li, and Baohua Zhao, "Covering Targets in Sensor Networks: From Time Domain to Space Domain", IEEE Transactions On Parallel And Distributed Systems, Vol. 23, No. 9, September 2012.

[17] Issa M. Khalil, "ELMO: Energy Aware Local Monitoring in Sensor Networks", IEEE Transactions On Dependable And Secure Computing, Vol. 8, No. 4, July/August 2011.

[18] Raphael Njuguna, and Viktor Gruev, "Low Power Programmable Current Mode Computational Imaging Sensor", IEEE SENSORS JOURNAL, VOL. 12, NO. 4, APRIL 2012.

[19] A.Kansal, D.D. Jea, D. Estrin, and M.B. Srivastava, "Controllably Mobile Infrastructure for Low Energy Embedded Networks," IEEE Trans. Mobile Computing, vol. 5, no. 8, pp. 958-973, Aug.2006.

[20] D. Li, X. Jia, and H. Liu, "Energy Efficient Broadcast Routing in Ad Hoc Wireless Networks," IEEE Trans. Mobile Computing, vol. 3, no. 2, pp. 144-151, Apr.-June 2004.