DWMA: An Energy Hole Reduction Mechanism on RPL for 6LoWPAN

Viswanathan Saravanakumar

November 15, 2020

DWMA: An Energy Hole Reduction Mechanism on RPL for 6LoWPAN

Mr.V.Saravanakumar, M.E.,MISTE,IAEng,CSI,
Assistant Professor,
Department of Computer Science and Engineering,
School of Computers,
Madanapalle Institute of Technology and Science,
Chittoor, Andhra Pradesh, India.
saravanakumar@mits.ac.in

Abstract

Wireless (Adhoc) Sensor Networks (WSN) is an emerging researcher’s domain closely related to other current technologies and areas such Networking, Data Mining, Internet-of-Things (IoT), Artificial Intelligence, Machine Learning, Data Science etc. A Multi-hop WSN nodes are usually closer to Base Station (BS) necessary to relay traffic from other nodes of the network which makes their energy depleted agile and causes energy holes . This energy hole problem significantly decreases the lifetime of any deployed Low-Power Wireless Personal Area Networks (6LoWPAN) while used with IPv6 Routing Protocol (RPL) for Low-Power and Lossy Networks. Meanwhile, energy ingestion among nodes is imbalanced, since each nodes in WSN are non-uniform in distributing data or packets among neighbours. This always causes some sensing node to loss their energy faster. Moreover, in RPL, DODAG Information Solicitation (DIS) messages are passed by the node to link the network. A mischievous node can abuse this system to send illegitimate DIS messages to the neighbour nodes to perform a DIS flooding attack. To overcome these issues, the most standard techniques followed to reduce such glitches are mobile sinks instead of static sinks, extending the transmission range dynamically, and deploying redundant sensor nodes near the base station/sink. The shortcomings in multi-hop WSN nodes are nearer to BS need to relay traffic from other network nodes which creates their energy depleted faster and might leads residual energy very high. This made us to propose an effective mechanism to handle Energy hole problem and routing namely **D**istributed **W**edge **M**erging in Multi-Hop **A**ccess (**DWMA**). The main objective is to reduce energy holes as well as decreasing the probability of energy holes creation and this DWMA wedge merges with the neighbouring wedge to thwart the energy holes formation by utilising existing routing method. The proposed system implemented on NS2 simulation environment with the static and dynamic network scenario. The results obtained clearly shows that balancing of energy consumption among nodes are achieved and DWMA mechanism is much longer lifetime compared with standard RPL protocol like Power Efficient Gathering in Sensor Information Systems (PEGASIS), Concentric Clustering Scheme (CCS) and WEdge MERging (WEMER). In addition to that, the simulation results revealed that DWMA helps to decreases the average packet loss ratio, end to end delay, energy consumption, control overheads and boosts the packet delivery ratio, throughput and network lifespan.

Keywords: WSN, RPL, LLN, 6LoWPAN, Energy hole, flooding,IoT etc

1.1 Introduction

A Wireless Sensor Networks (WSN)[1] also well-known as Wireless Sensor & Actuator Networks (WSAN) is comprised of lots of tiny, inexpensive, less battery sensor nodes whereas each nodes have small internal memory, less computational ability (CA) with limited energy level. In general, sensor nodes are capable of monitoring, sensing, aggregation and transmission of data to nearest BSS or Sink node (central gathering point)[1-4]. WSNs are used in lot of real time applications including Precision Agriculture, Health care, Disaster Relief Monitoring, Intelligent building, Facility Management, Weather Monitoring, Traffic Monitoring, etc [2]. According to latest updates IDC, there will be more than 42 billion IoT's gadgets are available and which generates nearly 80 ZB of data in 2025[5]. Sensor nodes are useful to measure environmental parameters and passed the same either online or offline data to the BS for future use[6].

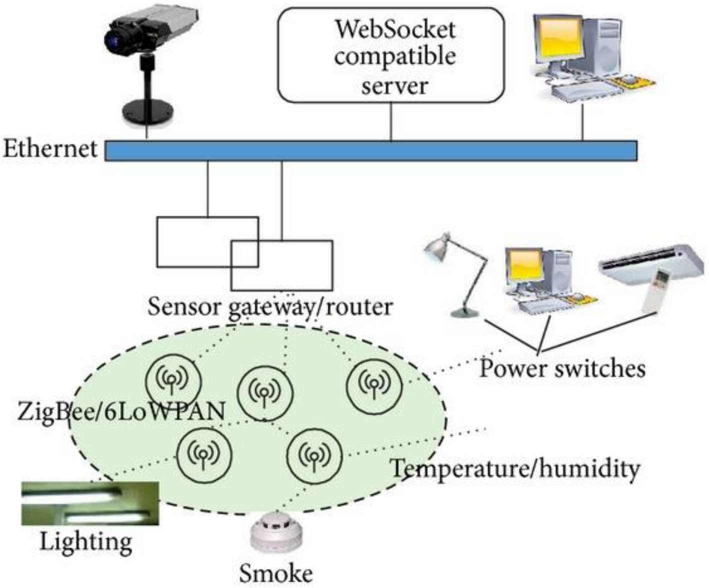

Figure 1.1 : Typical WSAN and its Major Components

Figure 1.1 shows a Typical WSN that comprise of hundreds or even more number of centres, which results strong surveillance of any applications and its components are described below for further understanding.

Components of WSNs

1. **Sensors**
   Sensors are used to detect the environmental variables for data acquisition. Sensed signals are transformed into electrical.
2. **Radio Nodes**
   It is used to receive the data produced by the devices and sends it to the WLAN access point (AP). Kits contained of microcontroller, transceiver, external memory, and power source[7].
3. **WLAN Access Point(AP)**
   It collects the data and directs the radio nodes over the internet.
4. **Evaluation Software**
   The data received by AP's are processed by a software called as Evaluation Software for presenting the report to user that helps for processing, analysis, storage, and mined data.

The sensed data (SD) are transmitted to the BS directly or by multi hop fashion. RPL is being utilized in a widely in IoT real-time products due to its ability to deliver energy-efficient routing in LLNs[7,8]. LLNs use resource-constrained devices, which operates on low power, limited energy with small onboard memory and low computational capabilities to work in highlight multipoint, multipoint-to-point and highlight point way. In addition, the cryptography-based guard components are strength ravenous and decrease the organization's exposition and period. In our proposal the size of the sector varies according to distance from BS and the sensor nodes of any sector are within each other's transmission range.

1.2 Objectives

Research objectives of proposed scheme for 6LoWPAN is discussed as follows:

1. To restructure the procedure 6LoWPAN by familiarising active wedge merging approach whenever an energy hole situation arises.
2. Through a set of performed simulations, we determined the energy consumption, lifetime of a base station and defined distinguished aspects of the multilevel analysis.
3. To restructure the procedure of clustering the sensing nodes and increase the PDR with maximum stability in designed network.

The remainder of this paper is organized as follows. Section 2 presents the overview of the related work and proposed work is described in section 3. Section 4 covers performance analysis and finally section 5 conclusion with future scope.

2. OVERVIEW OF THE RELATED WORK

Before formation of the sensor network and deployment of sensor nodes, network is needed to be more scalable and efficient.

2.1 WSAN Challenges and Opportunities

Some important challenges that the wireless sensor networks should overcome are Quality of Service (QoS), Security Issue, Energy Efficiency, Network Throughput, Ability to cope with node failure, Cross layer optimisation, Latency, and Scalability to large scale of deployment. Since WSN are scattered and easily attacked. Among the complications, the needed issues related to our work are described below[9,10].

- **Energy Efficiency:** Since the sensor nodes are battery powered and complex to change or recharge batteries frequently for sensor/actuator nodes; so energy utilization should be accomplished sensibly in order to encompass the network lifetime. Lot of scientists are fixing this issue to have an energy efficient network. Hence, if the batteries are drained, the sensors may fail and might not function within the budget.
- **Scalability:** with respect to the number and density of nodes is essential to prevent the degradation of network performance below the acceptable threshold.
- **Latency:** Depends on application usage, delay or relay occurred in the sensor network applications. The detected events must be reported to BS, that the applicable action could be taken immediately. The routing protocols and network topology must guarantee the delivery of data with minimum delay.
- **Throughput:** The required number of successful packet transmission of a given node per unit time is determined as throughput. Throughput requirement also varies with different applications.
- **Security:** One of the significant challenges in WSNs is to offer high security requests with reserved resources. The remote and unattended operation of sensor nodes builds their coverage to malicious infringements and spams. While this strong stress is taking over any IoT devices, attackers can try to slip into the back door unnoticed. As a consequence, sensor networks require new solutions for key establishment and distribution, node authentication, and secrecy.

2.2 Existing Modelling Approach

The modelling approach is mandatory to be considered for effective systems with a valuable, functional, and effective framework[16]. The different approaches used by researchers in the past decades are discussed shortly below.

1. Analytical Representation (AR): Mathematical representation model providing logical relationships, formulas and moreover specifies the ability of being executed and support of programmed tools being able to achieve the model.
2. Universality (U): General purpose approach particularly operated for building and analysing models for any type of network system.
3. Performance Evaluation (PE) gives the possibility of performance assessment of the analysed system.
4. Flexibility (F): An Agile modeling approach helps in investigating real environment.
5. Multilevel Analysis (MA) allows taking into account lots of different attributes, components, and aspects of the considered system during the modelling process.
6. Scalability (SCL) : Calibre to measure the strength and size of dynamic netork.
7. Energy Evaluation (EE): Used for knowing the efficiency of any WSNs.

2.3 Energy Hole Problem and Background Study

Nodes deployment is one of the essential area where many eminent peoples are involved to establish QoS network. Since sensor nodes are runs through battery pack energy and also non-sequentially mounted in destination. Apart from battery power limitations, the most challenging in WSN are processing power constraints, duplicate data gathering and limited memory. Figure 2.1 is shows scenario, in which nodes near sinks are deployed their energy with sensor devices[3,7]. This is the main reason for Energy holes creation and then made a partition in the network in such a way that it cannot make full connectivity in the network.

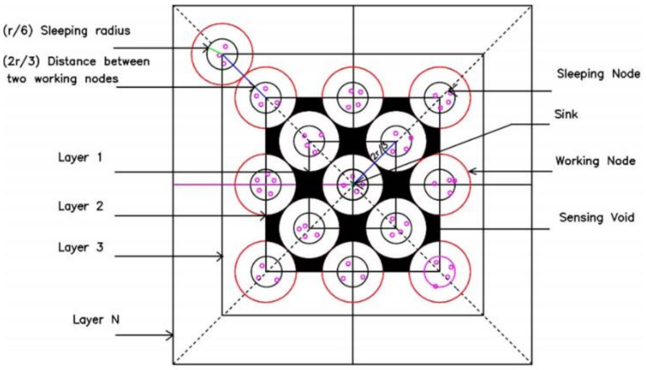

Figure 2.1 : Energy Hole Problems (EHP) in WSNs

Energy Coverage protocols are widely categorised as clustering and distributed protocols. Bases on probe and Computational geometry, this protocols are further classified as location aware and location unaware. Rest of the types and survey of existing methods & protocols of eminent researchers are summarized as shown in the Figure 2.2.

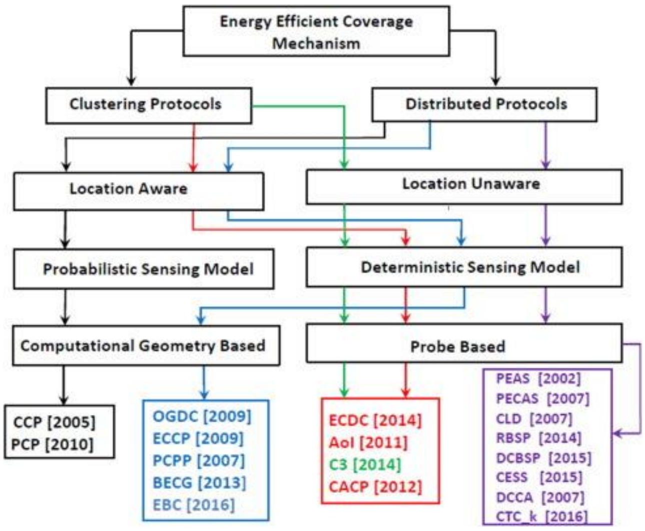

Figure 2.2 Category and Review Summary of Energy Efficient Coverage Mechanism

2.3.1 Techniques for Solving Energy Hole Problems (EHP)

Some techniques to alleviate the energy hole problem from real time environment are flexible transmission range, sink/node mobility and scattered non-uniform sensors mainly deploying redundant of the nodes near to the sink [10].

Optimizing the energy consumption is one of the major issues in WSNs to prolong the network lifetime[9,11]. Nodes near the sink region will be loss its energy earlier from external sub-zones due to these nodes send their own data as well as forward to other sub-regions data to the sink. This might help to interrupt by energy hole shortly. After that, data cannot be forwarded to sink even though energy is still remained in outer region nodes which drain the battery level. In this paper we investigate conjointly identified of effect of normal distribution of each nodes in the network and finally, relaying range parameter for data transmission to avoid the drain by increasing charging level of battery. Table 1 shows comparison of existing DDoS modeling approaches.

Table 1: Comparison of Prevailing DDOS modeling approaches

Approach	AR	S	PE	F	MA	SCL	EE
S. Yuan, D. Liang (2012)	Y	Y	N	Y	Y	Y	N
Eian and Mjolsness (2014)	Y	Y	Y	N	N	Y	N
S. Lin, D. Niyato (2014)	Y	Y	Y	Y	Y	N	N
S. M. AlTabbakh (2015)	Y	N	Y	N	Y	Y	Y
QoP ML's (2015)	Y	Y	Y	Y	Y	Y	Y

The energy-hole has the potential to drastically reduce the useful lifespan of sensor networks. So maximizing the effective network lifetime is equivalent to avoiding the energy-hole. Energy hole problem plays vital as data cannot be sent from other sensor nodes to the BS although the Residual Energy (RE) in the network remains high. Hence,network lifetime can be increased by increasing initial energy, decreasing individual energy consumption, transmission and reception energy[9].

2.4 DIS Flooding Attack

One of the most common types of attack that takes place while broadcasting any message in a public / private network is distributed denial of service (DDoS). DDoS attacks in

WSNs towards a set of legitimate nodes, with the intent of exhausting their limited resources. DDoS attacks can take on many forms[8], depending upon the target system and objectives of the attacker, but they all have the same goal: these attacks significantly affect the performance of the network and eventually lead to complete paralysis of network operation.

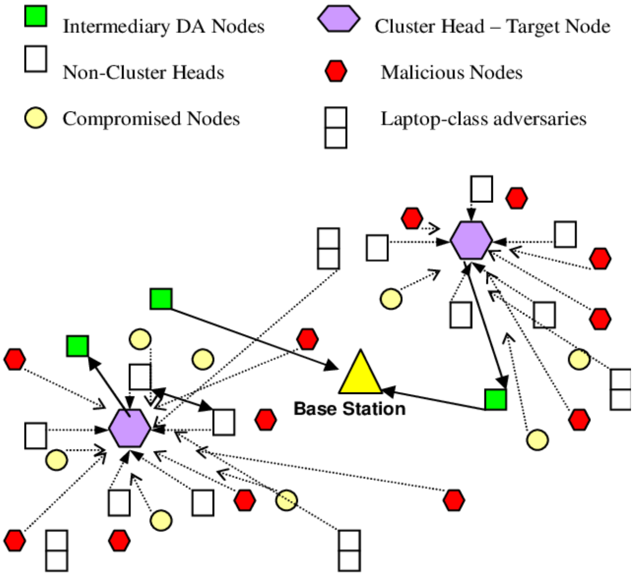

Figure 2.3 DIS Flooding Attack

As network devices proliferate, vulnerabilities could enable scammers to collect a huge information of nodes. If the vulnerability is forceful, then the sensors might fails to continue their assigned services as same like a normal sensor, even unpredictable and legitimate users cannot use them. While this intense strain is taking over devices, hacker can try to slip into the back door unnoticed. That is the reason why security needs to be backed into wireless sensor networks from the initial design phase; it needs to be built in as the foundation of WSN environments, with rigorous validity checks, authentication, and data verification, and all communication needs to be encrypted[8,9]. In light of the importance of what sensors have access to, it is essential to understand their security risks.

3. PROPOSED SYSTEM & METHODOLOGY

3.1 SYSTEM METHODELOGOGY

The main aims of this proposed system namely **D**istributed **W**edge **M**erging in Multi-Hop **A**ccess (**DWMA**) to reduce or eliminate as much as possible the formation of Energy hole problem in senor nodes in 6LoWPAN and also provide re-clustering methods to merger the routed sensor nodes to avoid the EHP occurrence. To achieve our goal, we studied and implemented various existing methods and protocols to control the EHP issue both in static and dynamic environment for that we compared our proposed scheme with standard RPL protocol like PEGASIS, CCS and WEMER. In addition to that, we try to expose the strength of DWMA, in which supports to minimise packet loss, hop to hop delay, energy depletion, increasing packet transmission rate, and network lifetime.

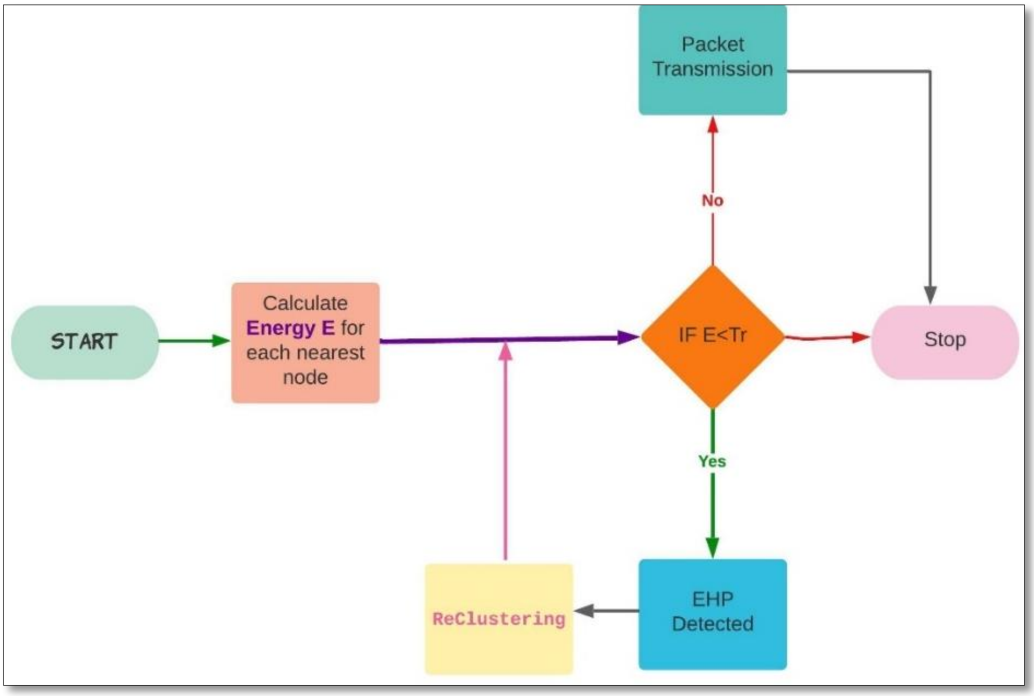

Figure 3.1 Flowchart for Energy Hole Problem and solution

Figure 3.1 is a simple flowchart to describe the flow of identification the EHP in network by periodically monitoring the status of neighbour nodes and its current status. Calculating E_i for each sensor nodes is a challenging task, since sensor sense the data changes in environment, transmission of data to appropriate destination either wired or wireless communication models and finally lookup the neighbour's status within fraction of millisecond. This is main reason that an energy of any node in BSS are drained and failed to achieve the tasks in specified time. To overcome these issues, a simple mechanism is prescribed in flowchart that to calculate energy of each node, if its level is than threshold value t_r, it might cause EHP in future, so Re-clustering is suggested to prevent from formation of EHP. Otherwise packets are transmitted as per delay time.

3.1.1 Proposed Algorithm

Procedure for Distributed **W**edge **M**erging in Multi-Hop **A**ccess (**DWMA**)

1. Circulate the Packet in WSN to know the periodic status of BS and AP to avoid congestion.
   a. If DDOS or DIS flooding problem came, apply the DIS Flooding mitigation algorithm and update the same in RPL routing table.
   b. Otherwise update the current status of each $Node_i$ in BSS, Step 2.
2. Calculate RE for each node E_i for all nearest i^{th} nodes in senor network and update in each Table RE_i.
3. Determine EHP arises or not by comparing with threshold value (tr_i).
   a. If Yes, Re-cluster the 6LoWPAN by applying WEMER, Goto Step 1.
   b. Otherwise, Continue Step 4.
4. Finally periodically determine and update the information.

3.2 SYSTEM MODEL AND ASSUMPTIONS

We form a three simple 6LoWPAN network topology model where each consists of N_{max} nodes with 100 ,300 and 500 sensor nodes. Each node is specifically recognized with a unique node ID. Each sensor/actuator nodes are responsible for collects data periodically that to be sends as DIS messages irrespective of interval. The sample simulated network topology taken for our research work is shown in Figure 1.

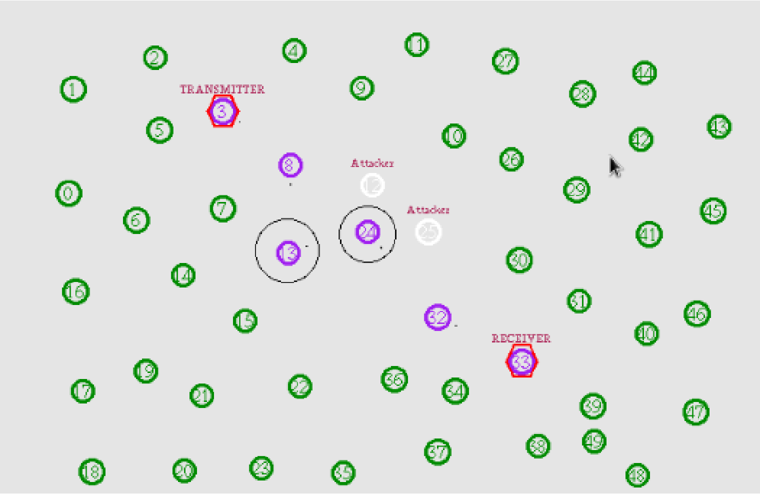

Figure 3.2 WSN Network Topology

The different colours used in simulation are to easily identify the status of sensor nodes during its functionality. It's possible to use TCL script to specify the colours for the nodes based on the work nature as a network administrator for easy identification and evaluation of the given network[15].

Section IV: PERFORMANCE EVALUATION

This section gives details evaluation of experimental setup used for conducting simulations to validate EHP in RPL is discussed. Mostly Secure-RPL is evaluated in terms of important performance indicators like control packet overhead and stability.

4.1 EXPERIMENTAL SETUP

Simulation is done with NS2 environment in order to evaluate the performance of the proposed approach DWMA with the other state-of-the-approach models like WEMER, CCS, and PEGASIS[14]. From the performance of simulation results with 100 and 500 nodes with DWMA is compared with the previous protocols.

Table 2. Simulation Network Parameters

Parameters	Value
Base Station Location	(100m, 100m)
Area	(180,180)
No. of Sensor Nodes	100, 500
Initial Energy	0.5 Joule
Total packet size	3500
(ETx, ERx)	(50nJ, 50nJ)

4.2 PERFORMANCE INDICATORS

The multilevel analysis performed here highlighted on lots of aspects especially network topology, data flows, utilized protocols, and communication mechanisms and to examines results in time, energy consumption with environmental influence. To examine network performance with different number of compromised, attacking nodes, we implemented with three scenarios for different approaches. During analyses and observations performed in this paper, we focused on the percentage of dropped packets in each flood wave and the time taken by the sink to handle incoming packets. Gathered results indicate that utilized security mechanisms significantly affect sink's performance. The results clears that the number of cooperated needs has a relationship impact on DDoS success probability. Sink's service time increases with the number of compromised devices as well.

Usually while estimating the network performance, the head node dead time define the *network stability period* and final node dead define the *overall network lifetime.*

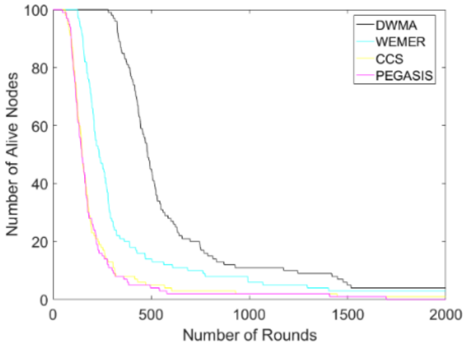

Figure 4.1 A Number of Rounds vs Alive nodes

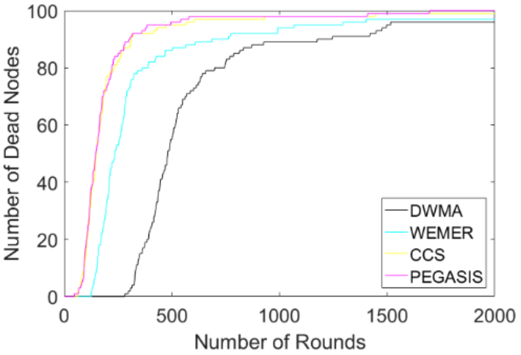

Figure 4.1 B Number of Rounds vs Dead nodes

Figure 4.1 A summarize that number of alive nodes are more in DWMA approach when the number of rounds are raised.

Figure 4.1 B shows that number of dead nodes are reduced in our approach compared with approaches like PEGASIS, CCS and WEMER for each number of rounds.

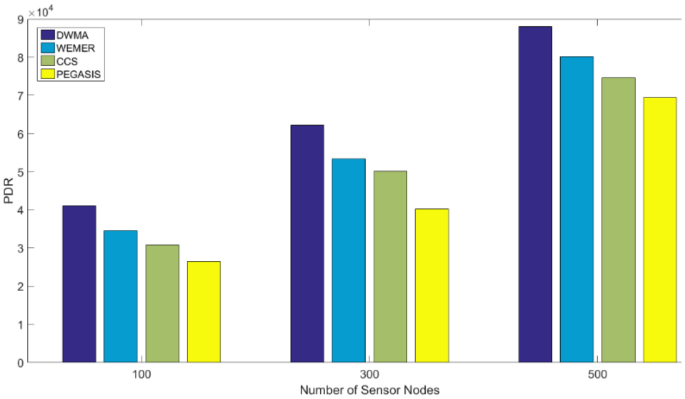

Figure 4.2 Number of Sensor nodes vs Packet Delivery Ratio (PDR)

Packet delivery ratio (PDR) is measured to know the ratio of sum of packets delivered to the aggregate packets sent from starting node to endpoint node in 6LoWPAN network. Figure 4.2 exhibit that number of sensing node in each methods has much packet loss than the proposed mechanism.

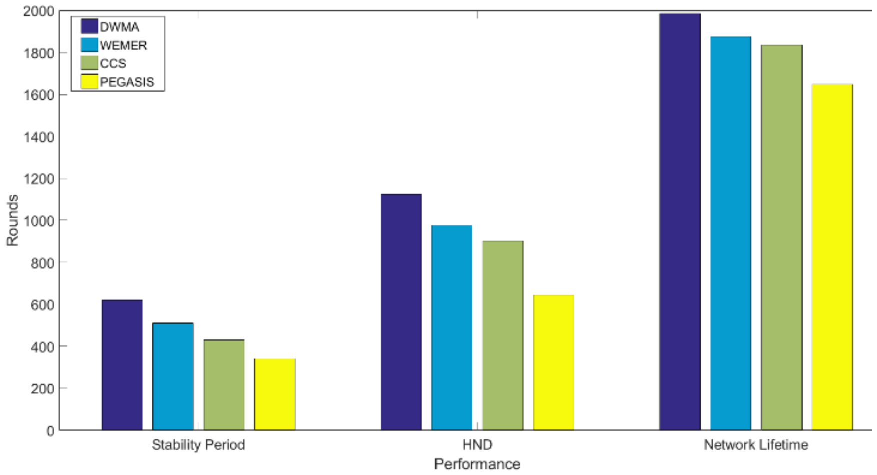

Figure 4.3 Number of Sensor nodes vs Overall Energy (E)

The paremeter's used for comparing efficiency of any sensor node depends on FND,HND and LND.The Figure 4.1 summarise the FND and LND in each rounds for sensing node. In this figure 4.3 comparing the major paremeters such as stability period, HND and network life time to calculate the actual energy of entire nodes for different approaches to easy cnclusion that *DWMA* is the best proposed approach for reclustering and reduction of EHP.

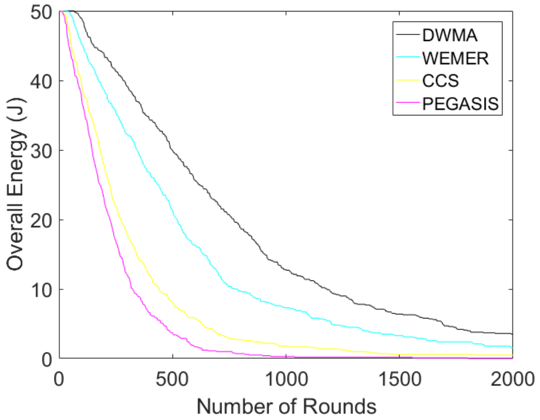

Figure 4.4 Number of Rounds vs Overall Energy (J)

Finally its easily to demonstrated that **D**istributed **W**edge **M**erging in Multi-Hop **A**ccess (**DWMA**) maintains the residual energy RE and reduced the energy hole issues such that overall energy of the nodes are greater than the existing approach. This illustrates in Figure 4.4 and achieve our main objective that less energy loss , so threshold value t_r for each node is obtained, this leads to very less packet dropped.

Section V : CONCLUSION AND FUTURE SCOPE

RPL based WSN are used in plenty of smart technologies to provide QoS in versatile environment with different variety of methodology, Cost, Quality, size etc based on the network topology and the organization constraints. However, WSN is communication through air medium and nodes used are sensor nodes, this always leads to lossy network. To prevent or reduce from this LLP only many existing work are enhanced. Our aim is resolve this problem as per available sources to produce high quality without affecting existing system. Finally we achieved through our proposed model DWMA and the simulation results holds true for it. In future , there are many other complex parameters for complex topologies to be examine and generate a network with less cost and more secure services.

REFERENCES

[1] Verma, A. and Ranga, V., 2020. Mitigation of DIS flooding attacks in RPL-based 6LoWPAN networks. *Transactions on Emerging Telecommunications Technologies*, *31*(2), p.e3802.

[2] Cˇ olakovic´ A, Hadžialic´ M. Internet of Things (IoT): a review of enabling technologies, challenges, and open research issues. Computer Networks. 2018;144:17-39.

[3] Musaddiq A, Zikria YB, Hahm O, Yu H, Bashir AK, Kim SW. A survey on resource management in IoT operating systems. IEEE Access. 2018;6:8459-8482.

[4] Chen, K.H.; Huang, J.M.; Hsiao, C.C. CHIRON: An energy-efficient chain-based hierarchical routing protocol in wireless sensor networks. In Proceedings of the Wireless Telecommunications Symposium,

[5] Prague, Czech Republic, 22–24 April 2009; pp. 1–5.

[6] Lindsey, S.; Raghavendra, C.S. PEGASIS: Power-efficient gathering in sensor information systems.

[7] In Proceedings of the Aerospace Conference Proceedings, Big Sky, MT, USA, 9–16 March 2002; Volume 3, p. 3.

[8] Zhang, Y.; Liu, M.; Liu, Q. An energy-balanced clustering protocol based on an improved CFSFDP algorithm for wireless sensor networks. Sensors 2018, 18, 881.

[9] Sharmin, N., Karmaker, A., Lambert, W.L., Alam, M.S. and Shawkat, M.S.T., 2020. Minimizing the Energy Hole Problem in Wireless Sensor Networks: A Wedge Merging Approach. *Sensors*, *20*(1), p.277.

[10] Sharmin, N., Alam, M.S. and Moni, S.S., 2016, December. WEMER: An energy hole mitigation scheme in Wireless Sensor Networks. In *2016 IEEE International WIE Conference on Electrical and Computer Engineering (WIECON-ECE)* (pp. 229-232). IEEE.

[11] N. Alvi, S. H. Bouk, S. H. Ahmed, M. A. Yaqub, N. Javaid, and D. Kim, Enhanced tdma based mac protocol for adaptive data control in wireless sensor networks," Journal of communications and networks, vol. 17, no. 3, pp. 247{255, 2015}.

[12] K.-H. Chen, J.-M. Huang, and C.-C. Hsiao, Chiron: an energy-efficient chain-based hierarchical routing protocol in wireless sensor networks," in Wireless Telecommunications Symposium, 2009. WTS 2009, pp. 1{5, IEEE, 2009}.

[13] P. K. Pal and P. Chatterjee, A survey on tdma-based mac protocols for wireless sensor network," International Journal of Emerging Technology and Advanced Engineering, vol. 4, no. 6, pp. 219{230, 2014}.

[14] T. Liu, J. Peng, J. Yang, G. Chen, and W. Xu, Avoidance of energy hole problem based on feedback mechanism for heterogeneous sensor networks," International Journal of Distributed Sensor Networks, vol. 13, no. 6, p. 1550147717713625, 2017.

[15] C. Li, M. Ye, G. Chen, and J. Wu, An energy-efficient unequal clustering mechanism for wireless sensor networks, mobile adhoc and sensor systems conference, 2005," in IEEE International Conference on, pp. 7{7, 2005}.

[16] Mohammadi P, Ghaffari A. Defending against flooding attacks in mobile ad-hoc networks based on statistical analysis. Wirel PersCommun. 2019;106(2):365-376.

[17] Mayzaud A, Badonnel R, Chrisment I. A distributed monitoring strategy for detecting version number attacks in RPL-based networks. IEEE Trans Netw Serv Manag. 2017;14(2):472-486.