International Journal of Mechanical Engineering

SECURITY IN TRANSMISSION OF DATA AND ENERGY AWARE PATH SELECTION IN WIRELESS SENSOR NETWORKS

P.Thirumoorthy*
Associate Professor, Department of CSE, Nandha Engineering College, Erode, Tamil Nadu, India.
thiru4u@gmail.com

P.Vanitha
Assistant Professor, Department of CSE, Nandha Engineering College, Erode, Tamil Nadu, India.

Gowsalya R
Assistant Professor, Department of CSE, Nandha Engineering College, Erode, Tamil Nadu, India.

Tamizharasi S
Professor, Department of Pharmaceutics, Nandha College of Pharmacy, Tamil Nadu, India.

Abstract:

Now in the Wireless Sensor Networks, the power consumption during the routing process still ruins a challenging task because the network mobile nodes consumes a inadequate battery-operating power. So, here we put forward a method to the increase network life span and minimize the disconnection by choosing routes on behalf of transmitting with one or more available energy. Now this article proposes two types of schemes based on the Adhoc on Demand Distance Vector (AODV), and a reactive routing protocol, together of which allows some limited network mobile nodes to be in the part of the routing process in order to decrease the control overhead of delivered packets. Thus, this overhead limitation is based on its energy per joule of a received signal. Then the obtainable energy-efficient route in relation to the remaining energy per joule is designated locally through the destination node or by the intermediate nodes. The results can be composed by using NS2 simulator. Hence, the results that are shown in this article are our proposed schemes leads to high energy-efficient routing when comparing to conventional AoDV.

Keywords: Path selection, Energy efficiency, Wireless sensor networks, Zones, Network life time, Packet overhead

I. INTRODUCTION

Wireless sensor networks (WSNs) may stand as a distributed gathering or collection of resources forced small node that are accomplished of operational by a minimum operator appearance. The speedy growth and development in the micro- electro-mechanical systems technique has provided with small size, low power, and an in-expensive sensor nodes with the aptitude towards intellect and sense varied styles of the physical and eco-friendly situations. WSNs increases the flexibility of individuals to observe in addition to management of physical location from distant spaces or places [1]. As the every device nodes that works severally with none vital management, the miscarriage of certain nodes does not have an effect on its alternative network services or network activities. WSNs is now additional trustworthy and safe & secure in comparison to alternative existing styles of networks. WSNs is that the pillar and backbone on behalf of forming smart surroundings. Every device or a sensor node is provided with one or more additional less powered sensors, processors, memory, an influence provide, radio and mechanisms, and supported infrastructure[2]. WSNs area unit of 2 categories: one is Structured WSNs and the other is Unstructured WSNs. The node’s area unit organized in planned manner in the Structured WSNs, while in Unstructured WSNs the node’s area unit treat random organized. Generally, the Structured WSNs takes densely organized sensor nodes, which cannot be simply managed in addition to the Unstructured WSNs can consume restricted variety of network device nodes which can easily be managed simply [3]. The battery of a sensor nodes are not same and not revocable, therefore conservation of energy had turn out to be a most important dare challenge for energy controlled WSNs. This leads elasticity to figure with none of human interference. The device sensor networks are unit have different applicable ranges, such as army, individual industry, farming and agriculture, goal pursuit, knowledge gathering, liberate operations, security of nation, observation areas of disaster, inventory management, taking care of health, security of home, also in environment educations [4].

The Wireless Sensor Networks (WSNs) that have limited energy resource are cleverly used to extend the lifetime of a sensor node. The sensor nodes are gathered and clustered together for recognizing high energy efficiency and to increase the lifetime of a network. The Wireless Sensor Networks containing cluster consists of sensor node with a range for every nodes. The clusters can often be shown a CH called as cluster- head, also the remaining sensor node becomes as CMs known by cluster members of that clusters. During cluster process, the sensor detects the cluster head (CH) or it can be pre assigned by the network designer [5]. The advantages of this clustering techniques are shown that the path setup can be localized, the bandwidth of a communication can be preserved, the redundant message exchanges are avoided, overhead of topology maintenance is reduced, the optimization management schemes are implemented for strengthening the operation of a network, activities are scheduled within the cluster, regulates the redundancy in coverage to prevent medium access collision, then also the quantity of relayed packets are reduced by combining the data assembled by the sensors within the network [6]. The cluster members i.e. the sensor nodes inside the cluster will transmit the data to the cluster head, which directly forward the combined data into a sink node. The above said transmission occurs directly or by via multi-hop routing over the other Cluster Heads. The network traffic during a clustered network consists of inter-cluster and intra-cluster traffic. The intra-cluster communications are single-hop or multi-hop, like wisely it is also an inter-cluster communications [7].

At the same time, the irregular energy consumption is caused in-between the inter-cluster communication (cluster heads) and intra-cluster communication (cluster members) by the hierarchic clustering model. So, the cluster head rotation method was brought forward to balance these energy overheads in our previous analysis [8-10]. The energy consumption of cluster heads and cluster members were balanced by cluster head rotation technique, but not in the inter-cluster multi-hop communications surrounded by Cluster Heads (CHs). The energy of the cluster heads on the edge of sink node drains faster because of relay traffic and have chance to die so earlier than the opposing cluster heads. This will cause network coverage deduction and partitioning the network. The cause can be referred to as emerging downside in Wireless Sensor Networks (WSNs). Towards resolving this downside, many uneven bunching methods have planned within the survey [11-14] that provides techniques to stable the consumption of energy between CHs. The clusters on the edge of sink node measures small in size by using unequal bunching method. Therefore, the CHs (Cluster heads) taking place at the point of sink node (base station/sink) will preserves certain energy for the inter-cluster communications.

II. RELATED WORK

Several algorithms have been brought into account for clustering method and cluster based routing protocols in Wireless Sensor Networks (WSNs). Previously, a lot of the certain algorithms have been planned and projected to provide an efficient data communications also the data handling prototypes (processing models) with optimum resource practice on wireless sensor networks (WSNs) [16]. From the two main techniques of cluster method and the design of network space, the zone based routing protocol for data communication in wireless sensor networks is intended. A key resolution in the zone based routing protocols is to stimulate the sensor network's lifetime by reducing the overall consumption of energy along with the limitation of control overhead on the communicating sensor nodes that present in the network. The bulk sized clusters are created using zone creation with minimal control overhead of packets along with their usage of location information at the sensor nodes [17-20]. This makes use of the random back off timer method to pick out the inter cluster communication (cluster heads) from every packet (data) forwarding inside its community fields. The next survey of communicating in wireless sensor network had put forward to (BNEPD) Bayes Node Energy and Polynomial Distribution technique along with power aware routing inside its Wi-Fi community. This BNEPD method will first of all allocates similar event node into a specific area with Bayes rules (i.e. the sensor node that locates an item of similar event like pressure, flow, temperature) [22]. In security of primarily based applications, the wireless networks are usually being involved. The recognition of the wireless sensor network may have great raise at present. The main principle to deal with Quality of Service (QoS) related issues are the routing protocols. Also the routing protocols deal with delayed tolerant, zone constructions, packet delivery, network lifetime, scalability of network, power consumption and the packet overhead [25].Sometimes an energy optimization is more complex in sensor networks because it involved not only in reduce of an energy depletion but also in prolonging the life of the network as much as possible. This can be done by having energy awareness in every facet of designs and operations. This warranties that the energy awareness is also integrated into the collections of communicating sensor nodes and the whole networks and not only in the individual nodes.

III. METHODOLOGY

A. ZONE CREATION

The network devices that are having similar trust levels could be a logical space and that is known as zone. When constructing a zone, the zone is allocated with associate degree edge at first. The traffic flow is restricted from a zone to other or different zone by default.

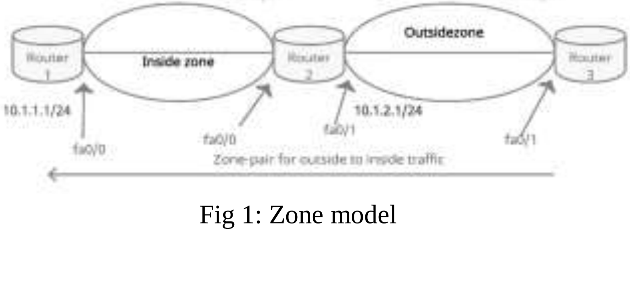

Fig 1: Zone model

For the known traffic (kind of traffic), the Zone-pair outlines the square policy measures, then the zone-pair decides on actions (such as to inspect, deny or permit) to be taken for the flow of traffic. Then we have to use this policies to a zone-pair. The zone-pairing is often un-official process. If we would like to create it duplex then we have to form another zone-pair. For an example, if we would like to permit the traffic from inside to outside network then we have to form a zone-pair. Finally, if we would like to permit the outside traffic to be ready to reach inside network then we have to create a separate zone-pair. This zone-pair can permit the traffic flow to succeed in the inside network if the traffic is generated from the outward network.

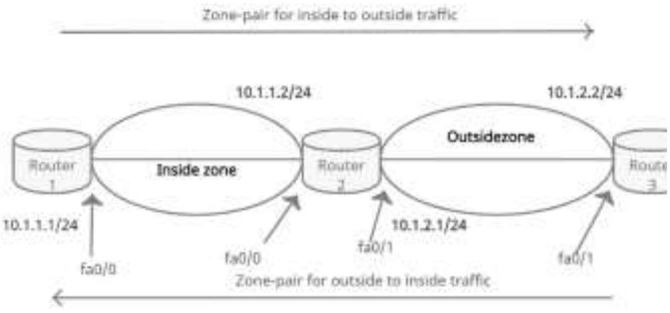

Fig 2: Outer Zone Model

Self-zone: The Traffic intended to the routing network itself, irrespective of that the network device has send, is known as self-zone. The traffic that are generated from router is believed as traffic returning from the self-zone. The traffic that are attending to router is taken into account as the traffic attending to self-zone. The traffic to the self-zone or from the self-zone is allowed by default nevertheless those are often modified in keeping with the policies applied. At first, the zones square measures are outlined and named. Even though, we will suggest any names however by the naming convention which produces sense, name the zones as the inside, outside and demilitarized zone.

•The Inside zone is the foremost trustworthy networks and also called as a private networks.

•The Outside zone is the foremost untrusted networks and is mentioned as public network.

• DMZ is the demilitarized zone and this contains the devices resembling the servers.

As the zones are named using naming conventions, the policies square measures created can hold what kind of traffic is allowed to be produced and what traffic permitted to travel throughout the network. Those actions are as follows: The Inspect action: This action associates degree entry are going to be created in state-full information for the routing protocols only for that the policies has been applied in order to the replies for within network will be returned. The Drop action: This is the default action if the traffic does not match the derived policies. The Pass action: In this action the traffic are going to be allowed from one zone to a different zone, however the sessions are not maintained so far. The traffics that cannot match the derived policies are going to be newly born because of the default policy. These policies are going to be drawn for one direction (such as within to outside) during a zone combine. If conditions needs to permit initial traffic to be generated in each directions (inside to outside network and out of doors to within network), then 2(two) separate zone-pairs are going to be created and separate policies square measures are applied.

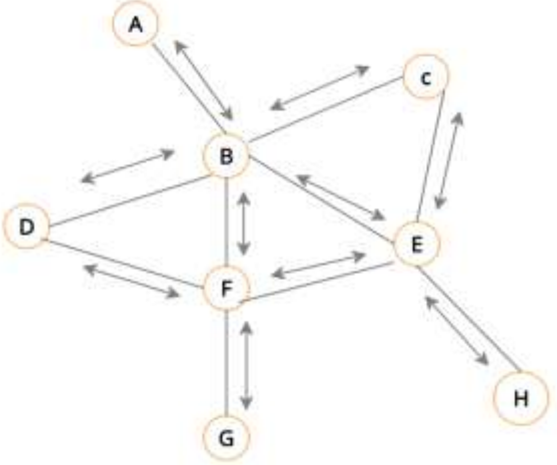

Fig 3: Path Selection

These works are centred on discovering the simplest route to induce the sink or base node. Now, path chosen is completely supported by the various metrics for estimating the node along with additional energy, the hop quantity, node distances, the visited node quantity, and goes on. The probabilistic guidelines and a self-organized strategy helps in accomplishing the network routing. The NS2 network simulator supports the results of energy aware path selection in wireless networks. The nodes that have bidirectional communications and the load of a link to transmit the information is directly proportional to the facility consumption of a node. As a result therefore, an enormous quantity of energy may be depleted. When one packet passes with a definite speed through a node, the node will take the primary steps to collect all the agents into a buffer so, it selects the best path from its routing table to transfer the packets. The cycles are avoided by adding a particular ID to the network path. This may be notified that this method will lead in heaps of memory, which is the one among the most limitations on device networks. The results of graphical interface regarding the performance of algorithm is excluded in this.

B. NEIGHBOUR MONITORING

Here, in this paper a neighbour monitoring based suspicious or malicious detection scheme has been proposed. During this neighbour monitoring process they consider an event and a periodic mode of operation, this is due to the temporary fault that misleads the network nodes that leads to the wastage of the energy and the improper decisions. Typically the normal failure nodes are removed from the wireless networks. The neighbour monitoring technique have 2 strategies to detect out the correct mischievous nodes as knowledge flattening, variant checks and confident level analysis. In knowledge flattening and variant check may vary, filter and variation check, the vary blocks and the variation checks have the same input, vary alliance checks whether the inputs vary or not and also it checks whether it is in traditional vary or not. The distinction in the input is determined using variation check in the presence of event/ node detection model. The flattering is performed using filtering mechanisms by reading with trustworthy edge nodes. The initial value one or zero is assigned to node in confidence level analysis that supports the neighbour node call. Now, this neighbour monitoring analysis represents the honourable node of a network, and every nodes will updates their node of confident level and their network neighbour node throughout the transmissions and its every intermittent detection. Neighbour monitoring technique accurately monitors and isolates the mischievous node that obeys usually. It corrects the malicious node from isolation. It results in low false rate.

IV. RESULTS AND PERFORMANCE

The performance meters that are used to estimate the performance of our proposed network routing protocols are ratio of packet delivery (PDR), Energy consumption of data packets, Network control overhead and Throughput. The foremost cause remains in the existing algorithms enhances decaying and zero sum noises to the invalid distributed average consensus process but then it does not consider the presence of the dishonest/ mischievous nodes.The figure 4 demonstrates throughput of the packet delivery. The throughput in this phase is the rate in packet per second (pps) at which the packets are successfully delivered over the communication nodes. The consumption of energy is the average energy consumed per joule of the nodes that attend the transmission process. The energy consumption of an existing algorithm and the proposed algorithm is fairly compared and shown in figure 5. The simulation result of figure 6 shows the control overhead of the transmitted data through nodes. The figure 7 shown below is the packet delivery ratio (PDR). The ratio of delivered packets is achieved on the basis of a received data (packets) by the destination node and generated packets recorded in the source file.

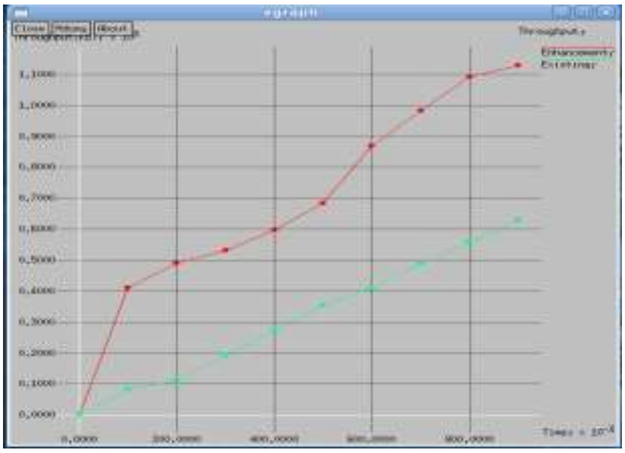

Fig 4: Throughput

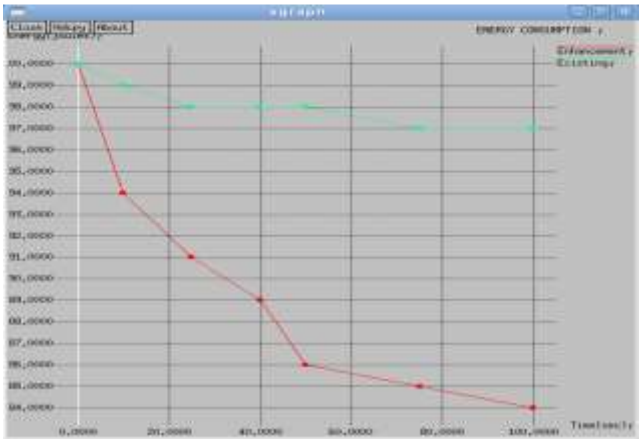

Fig 5: Energy Consumption

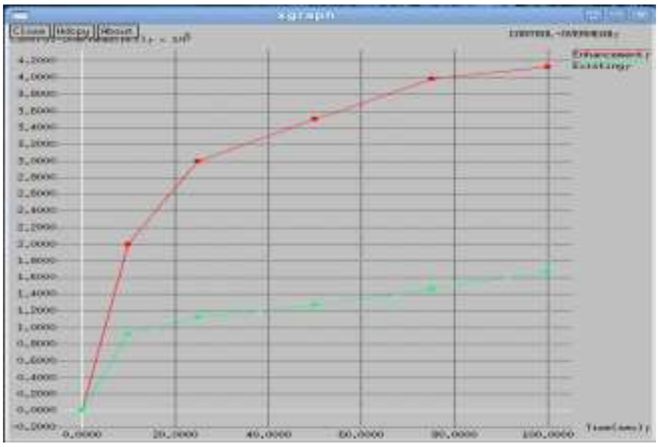

Fig 6: Control Overhead

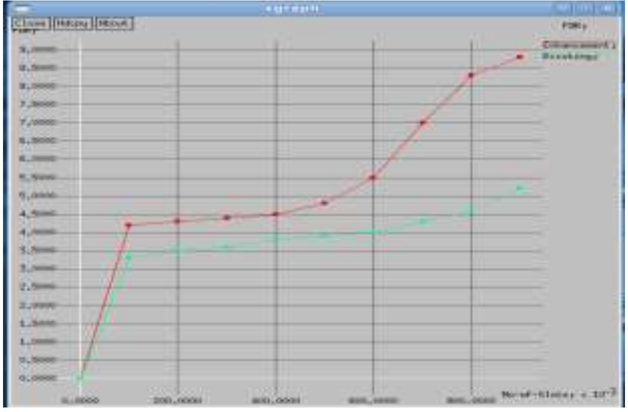

Fig 7: Packet Delivery Ratio

V. CONCLUSION

The most important concern in the wireless sensor network is that the security problem. In security of a wireless sensor networks, the secure routing is one main scheme to realize the security in WSNs. The various existing systems for routing and its inflexibilities in network routing had discussed in this paper. Many strategies have to pursue out the trustworthy node and secure routing. Through the works related previously, here we proposed reactive routing protocol that have achieved its confident level. This proposed model works well in homogeneous networks. We conclude that, most of the work does not give security in high level, and secure routing with energy efficiency and reduced overhead for a heterogeneous networks. Thus as planned work we have to take secure routing as a significant anxiety because we designed routing protocol as an agent based secure routing using honourable nodes. We simulated it by using NS2 simulator.

REFERENCES

[1] Jianping He, Lin Cai, Peng Cheng, Jianping Pan, Ling Shi,"DISTRIBUTED PRIVACY-PRESERVING DATA AGGREGATION AGAINST DISHONEST NODES IN NETWORK SYSTEMS", IEEE, VOLUME 6, ISSUE 2, APRIL 2019

[2] Dr.Debmalya Bhattacharya," SECURE DATA AGGREGATION IN WIRELESS SENSOR NETWORKS", IEEE TRANSACTION, ISSN: 2248-9622, Vol. 4,

[3] Mrs.B.Vidhya, Mrs. Mary Joseph , Mr. D. RajiniGirinath , Ms. A. Malathi ," ENVIRONMENT BASED SECURE TRANSFER OF DATA IN WIRELESS SENSOR NETWORKS", *International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 4, No 1, February 2015*

[4] S.Suresh, Giridhar. R" SECURED DATA TRANSMISSION IN WIRELESS SENSOR NETWORKS" International Journal of Computer Science and Information Security (IJCSIS), Vol. 14, No. 6, June 2016

[5] O.Deepa, Dr. G. Naga Rama Devi," PROVIDING END TO END DATA SECURITY IN WIRELESS SENSOR NETWORKS ", *International Research Journal of Engineering and Technology, Volume: 03 Issue: 07 | July-2016*

[6]RezaulKarim, Md. HasanFurhad, Md. Khaliluzzaman and Md. Ariful Islam Khandaker," IMPROVING THE PERFORMANCE OF DATA DELIVERY IN WIRELESS SENSOR NETWORKS", JOURNAL OF TELECOMMUNICATIONS, VOLUME 8, ISSUE 2, MAY 2015

[7] Ms.Sarita V. Halde, Prof.Sucheta T. Khot," BIG DATA IN WIRELESS SENSOR NETWORK: ISSUES &CHALLENGES ", International Journal of Advanced Engineering, Management and Science (IJAEMS), [Vol-2, Issue-9, Sept- 2016]

[8] SaeidPourroostaeiArdakani, AllamehTabataba'i , Tehran, Iran," DATA AGGREGATION ROUTING PROTOCOLS IN WIRELESS SENSOR NETWORKS: A TAXONOMY", *International Journal of Computer Networks & Communications (IJCNC) Vol.9, No.2, March 2017*

[9] M. Kowsigan, M.Rubasri, R.Sujithra, H.SumaiyaBanu," DATA SECURITY AND DATA DISSEMINATION OF DISTRIBUTED DATA IN WIRELESS SENSOR NETWORKS", Int. Journal of Engineering Research and Application, ISSN : 2248-9622, Vol. 7, Issue 3, (Part -4) March 2017, pp.26-31

[10] Dr.M.Sivaram, 2Dr. Amin Salih Mohammed, 3V.Porkodi, 4V.Manikandan," SECURING THE SENSOR NETWORKS ALONG WITH SECURED ROUTING PROTOCOLS FOR DATA TRANSFER IN WIRELESS SENSOR NETWORKS",*IEEE journal of selected topics on secure computing, October 2018, Volume 5, Issue 10*

[11] Jinwei Liu, HaiyingShen, Lei Yu, Husnu S. Narman, JiannanZhai, Jason O. Hallstrom" CHARACTERIZING DATA DELIVERABILITY OF GREEDY ROUTING IN WIRELESS SENSOR NETWORKS", *IEEE journal of selected topics on secure computing, Vol.5, No.3, April 2017*

[12]Lokesh B. Bhajantri, Shilpa H. Rathod," DATA AWARE ROUTING IN WIRELESS SENSOR NETWORKS", *International Journal on Future Revolution in Computer Science & Communication Engineering, March 2016, Volume: 4 Issue: 3*

[13] Andreas Willig, Holger Karl," DATA TRANSPORT RELIABILITY IN WIRELESS SENSOR NETWORKS —A SURVEY OF ISSUES AND SOLUTIONS" *EURASIP Journal on Wireless Communications and Networking, April 2016*

[14] NehaDhotreProf. Ramesh Jadhav," A MULTI OWNER – MULTI USER DATA TRANSMISSION FOR SECURED INFORMATION IN WIRELESS SENSOR NETWORKSA MULTI OWNER – MULTI USER DATA TRANSMISSION FOR SECURED INFORMATION IN WIRELESS SENSOR NETWORKS"*IJIRST –International Journal for Innovative Research in Science & Technology| Volume 3 | Issue 01 | June 2016*

[15] AnuChaudhary, Dr. Rajeev Kumar, "AN ASSESSMENT OF DATA TRANSMISSION IN WIRELESS SENSOR NETWORKS WITH ENHANCEMENT TO THE SECURITY AND RELIABILITY", *International Journal in IT and Engineering (Impact Factor- 6.341), Vol.05 Issue-01, (January, 2017)*

[16] Ashvinkumar K. SelokarArun G. Katara," IMPROVED SECURED DATA AGGREGATION IN WIRELESS SENSOR NETWORK BY ATTACK DETECTION AND RECOVERY MECHANISM", *International Journal for Scientific Research & Development| Vol. 3, Issue 08, 2016*

[17] GonuguntaTulasi, R.Suresh," SECURE DATA TRANSMISSION IN WIRELESS SENSOR NETWORKS: AGAINST PACKET DROPPING ATTACKS", *International Research Journal of Engineering and Technology, Volume: 03 Issue: 07 | July-2016*

[18] An Wang, Wentao Chang, Songqing Chen, Aziz Mohaisen" DELVING INTO INTERNET DDOS ATTACKS BY BOTNETS: CHARACTERIZATION AND ANALYSIS", *IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 7, NO. 3, JULY 2018*

[19] ArhamAlam Sachin Chaudhary," TRANSMISSION OF DATA IN WIRELESS SENSOR NETWORK USING ADAPTIVE CLUSTERING", International Journal for Scientific Research & Development| Vol. 5, Issue 09, 2017

[20] Guo Chen , Yuanwei Lu, Yuan Meng, Bojie Li, Kun Tan, Dan Pei , Peng Cheng, LayongLuo, YongqiangXiong, Xiaoliang Wang, and Youjian Zhao, "FUSO: FAST MULTI-PATH LOSS RECOVERY FOR DATA CENTER NETWORKS", *IEEE/ACM Transactions on Networking (Volume: 26, Issue: 3, June 2018)*

[21] SoheilFeizi, Muriel M´edard, Gerald Quon, ManolisKellis, and Ken Duffy," NETWORK INFUSION TO INFER INFORMATION SOURCES IN NETWORKS ",IEEE Transactions on Network Science and Engineering 2018

[22] ThirumoorthyPalanisamy, Karthikeyan N. Krishnasamy, "BAYES NODE ENERGY POLYNOMIAL DISTRIBUTION TO IMPROVE ROUTING IN WIRELESS

SENSOR NETWORK”, PLoS ONE 10(10):e0138932, October 1, 2015

[23] Sudha, S &Manimegalai, B & . P, Thirumoorthy& Scholars, P. (2014).“A STUDY ON ROUTING APPROACH FOR IN- NETWORK AGGREGATION IN WIRELESS SENSOR NETWORKS” 10.1109/ICCCI.2014.6921834, Jan 2014

[24] Thirumoorthy, P., Kalyanasundaram, P., Maheswar, R. *et al.* “TIME-CRITICAL ENERGY MINIMIZATION PROTOCOL USING PQM (TCEM-PQM) FOR WIRELESS BODY SENSOR NETWORK”, *J Supercomput* (2019). https://doi.org/10.1007/s11227-019-03042-x, October 2019

[25] Thirumoorthy, P., Kalyanasundaram, P., Karupusamy, S., &Prabhu.S, “ENERGY EFFICIENT ROUTING IN WSNS USING DELAY AWARE DYNAMIC ROUTING PROTOCOL” *Journal of Critical Reviews, 6*(6), 455-459. https://doi.org/10.31838/jcr.06.06.70

[26]K. Gunasekar, P. Vanitha, K. Kavitha and C. Navamani, “A STUDY ON SDN FOR AN OPTIMIZED NETWORK AND POWER IN TRAFFIC ENGINEERING” International Journal of Psychosocial Rehabilitation, Volume 23 - Issue 1, March 2019.

[27] Dr.S.Prabhadevi S. Anbumalar,”A Survey On Routing Issues And Routing Protocols In Wireless Sensor Networks”, International Journal Of Engineering And Computer Science ISSN: 2319-7242, Volume 4 Issue 6 June 2015, Page No. 12927-12931.

[28] Mr.P.Thirumoorthy,”Bayes node energy polynomial distribution to improvrrouting in wireless sensor networks”, PLOS One, Oct-2015.