Comparative Analysis of PDORP and Modified Trust Value based Technique to Secure Wireless Sensor Network

Pardeep Kaur
Department of Computer Science & Engineering
ACET, Amritsar, Punjab

Sandeep Kad
Department of Computer Science & Engineering
ACET, Amritsar, Punjab

ABSTRACT

Wireless Sensor Networks have a broad scope of uses however they are vanquished with numerous testing issues and difficulties that should be tended to. The power utilization of the hubs and the augmentation of the system lifetime are the center difficulties and the huge highlights of the routing technique keeping in mind the end goal to make it appropriate, viable and proficient for WSNs. As the sensor hubs are essentially battery controlled gadgets, so the best concern is dependable to how to diminish the power usage to broaden its lifetime. In a previous couple of years, WSNs has picked up a lot of consideration from both the exploration group and the genuine clients. The analysts additionally proposed a wide range of vitality proficient routing protocols to accomplish the coveted system tasks. In this paper, there is an endeavor to give a wide comparison of PDORP and Modified Trust based approach to Secure WSNs. Besides, removing the qualities and shortcomings of both the systems, giving an examination among them, including a few measurements like PFR, Throughput, Remaining energy, No. of packets sent, Average End to End delay to make it reasonable and easy to choose the most appropriate one according to the necessity of the system.

Keywords

PDORP, Trust value, DSR, Wireless Sensor Networks, Routing Protocols, Sensor nodes, Energy Efficiency, Power Management.

1. INTRODUCTION

A WSN is a gathering of hubs composed into a helpful system . Every hub comprises of handling ability (at least one microcontrollers, CPUs or DSP chips), may contain numerous sorts of memory (program, information and blaze recollections), have a RF handset (more often than not with a solitary omnidirectional reception apparatus), have a power source (e.g., batteries and sunlight based cells), and oblige different sensors and actuators. The hubs impart remotely and regularly self-sort out in the wake of being deployed in an ad-hoc fashion [1].

Presently a days Wireless system is the most well-known administrations used in modern and business applications, in light of its specialized progression in the processor, correspondence, and utilization of low power implanted registering gadgets. Sensor hubs are utilized to screen natural conditions like temperature, weight, moistness, sound, vibration, position etc.In numerous ongoing applications, the sensor hubs are performing distinctive undertakings like neighbor hub discovery, smart detecting, information storage and handling, information aggregation, target following, control and checking, hub localization, synchronization and effective directing amongst hubs and base station [2].

Wireless sensor nodes are outfitted with detecting unit, a preparing unit, correspondence unit, and power unit. Every single hub is able to perform information gathering, detecting, preparing and speaking with different hubs. The detecting unit detects nature, the preparing unit figures the restricted stages of the detected information, and the correspondence unit performs trade of handled data among neighboring sensor hubs[3,4]. The fundamental building block of a sensor node is shown in Figure 1.1.

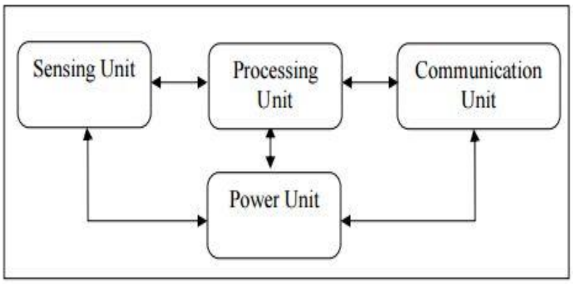

Figure 1: Basic Building Blocks of Sensor Node [3]

The sensing unit of sensor hubs coordinates diverse sorts of sensors like warm sensors, attractive sensors, vibration sensors, synthetic sensors, biosensors, and light sensors. The deliberate parameters from the outer condition by detecting unit of sensor hub are fed into the handling unit. The analog signal created by the sensors are digitized by utilizing Analog to Digital converter (ADC) and sent to the controller for additionally preparing [4,5,6]. The processing unit is the imperative center unit of the sensor hub. The processor executes distinctive assignments and controls the usefulness of different segments. The required administrations for the preparing unit are pre-modified and stacked into the processor of sensor hubs. The energy usage rate of the processor shifts relying on the usefulness of the hubs. The variety in the execution of the processor is recognized by the assessing factors like preparing speed, information rate, memory, and peripherals upheld by the processors. The calculations are performed in the processing unit and the gained result is transmitted to the base station through the correspondence unit. In correspondence unit, a typical handset goes about as a correspondence unit and it is basically used to transmit and get the data among the hubs and base station and the other way around. There are four states in the correspondence unit: transmit, receive, idle and sleep.The Wireless Sensor Network is a fast developing area with various applications. Intelligence and interoperability of system keep it sought after and henceforth comes the requirement for the effectiveness of the framework. The most imperative constraint on sensor hub is the low power utilization. Sensor nodes carry inadequate, generally irreplaceable power sources. Along these lines, while customary systems mean to accomplish high caliber of administration (QoS), Wireless Sensor Network protocols must emphasis prevalently on energy conservation [7, 8].

2. LITERATURE REVIEW

W. Liu and J. Yu [7] proposed a novel clustering plan instead of enabling the hubs to transmit straightforwardly to the base station. Clustering gives asset usage and limits power utilization in WSNs by decreasing the number of sensor hubs that include the long-distance communication. Chengfa Li, Mao Ye, Guihai Chen, Jie Wu [8] discovered that having lesser number of nodes in the clusters close to the base station as compared to the ones away from it is more advantages as compared to clustering with the equal number of nodes. This is due to larger overheads on the nodes closer to the base station. Joon-WooLee, Byoung-Suk Choi, Ju-JungLee[9] and Ali chamam, Samuel pierre [10] proved that TDMA slots along with scheduling algorithms to enhance the network lifespan. This caused all the nodes to be active during only their chosen time period. Johnson, Hu, et al. in [11] designed Dynamic Source Routing (DSR) protocol is a routing protocol chiefly for the multi-hop ad-hoc portable networks. This protocol allows nodes to find out and maintain routes to an arbitrary target for which it has two mechanisms i.e., route discovery and route maintenance. Ademola P. Abidoye, Nureni A. Azeez, Ademola O. Adesina, Kehinde K. Agbele [12] used LEACH(Low-energy adaptive clustering hierarchy) which is the earliest network protocol that uses hierarchal routing. In this, all the nodes are formed into groups called clusters and one node is arbitrarily selected as a cluster head. Ruperee A, Nema. S, Pawar S. [8] proposed a method of delta modulation to accomplish power efficiency. However, this faces a disadvantage that one cannot determine the real data.

3. PEGASIS- DSR OPTIMIZED ROUTING PROTOCOL (PDORP)

PEGASIS-DSR Optimized Routing Protocol (PDORP), ideally uses the qualities of both the proactive and reactive directing model [14].

In the event that a hub turns out to be more aggressive at the time of data exchange and beforehand it was not in the cache memory, the other hub will undoubtedly get a packet from it and in such a way it can make harm to existing courses. An answer to this issue could be checking of any hub at the time of getting an information packet yet this would cause unessential deferral. Thus, this method makes a trustiest without precedent for each round based on the parameters assigned to the hubs. After each round, the trust list is refreshed and after a specific number of rounds, the trust would not be checked to keep away from time delays. At the point when a source hub needs to transmit information to goal hub, it figures the separation from every one of the neighbors and forwards the information to the hub whose separation is not exactly or equivalents to the limit remove and just toward goal hubs and it likewise guarantees that the base separation neighbor hub ought to be toward the goal hub. After this procedure, every one of the hubs toward the goal is included into the trust list just in the first round of reproduction. At whatever point another information transmission is required, at that point, the trust list will be refreshed in the first round of reproduction and the information will be exchanged by means of just those hubs which are found in the trust vector.

4. MODIFIED TRUST VALUE BASED APPROACH TO SECURE WIRELESS SENSOR NETWORK

This method, considers the packet-forwarding behavior of the hubs thinking about their aggressive conduct as the criteria to identify the variation from the norm. Presently, if the hub has been distinguished effectively as the aggressive hub then the expulsion of such a hub from the current way would require second way promptly accessible for information transmission else re-constructing the way would create an unwelcome postponement in the system. In this manner, there must be in excess of one way put away in the storage memory for the quick accessibility of the second way [15].

At the point when the source node has a few information to transmit to the destination, it will utilize the GPS directing to define a way. It will first search for the neighbors in the correspondence going. Every one of the neighbors whose x and in addition y arranges are toward the path towards the goal hub is considered. From every one of these neighbors, the two hubs will be chosen that will be nearest to the goal hub in this manner bringing about two ways from source to goal. The source center point would transmit information to the goal utilizing the primary way. After the first round, the number of parcels sent by every hub would be checked keeping in mind the end goal to discover the wellness estimation of the trust of every hub. In the event that any hub has sent the more prominent number of bundles than the others, at that point its trust esteem would be lessened. After the finish of second round, if a similar hub is found to carry on forcefully then its trust esteem would be decreased to zero and source hub would get the second way from its reserve memory to forward the information [15].

5. RESULT AND ANALYSIS

For experimentation and execution, the proposed method is assessed utilizing NS 2.35 instrument. The assessment of proposed procedure is done on the starting point of following parameters, for example, PFR, Remaining Energy, Throughput, number of packets sent, E2E delay. Examination of PDORP and after effects of the proposed adjusted trust based outcomes i.e. sees Fig. 2-6. Additionally, quantitatively modified trust-based approach performs better as far as every one of the measures as demonstrated in Table 2.The simulation parameters used have been described in Table 1 below:

Table 1. Simulation parameters

Parameter	**Value**
Channel	Wireless
Number of nodes	60
Simulation Tool	NS2.35
Initial Energy	30 Joules
Mac	802.11
Propagation	Two Ray Ground
Sensing Region	1150m * 1100m
Antenna	Omni Directional
Routing Protocol	DSR

5.1 Packet Forwarding Ratio

This is the ratio of the number of packets forwarded by the hubs to the number of packets received by them. This is a critical factor in deciding the aggressive hub

Figure 2 shows the level of packets sent by the hubs in the system. Since this work was centered around aggressive information sending hub, the assessment of this parameter was fundamental, as this would enable us to quantify the effect of aggressor hub in the system. This speaks to the keep running of recreation for two rounds amid which the trust estimation of the hubs is being processed. This shows aggressive hubs are available on the way as the number of packets sent is substantially more. The third time, the trust estimation of the malignant hub lessens to zero and is expelled from the way finished which information is being sent. Thus, the estimation of PDR diminishes down showing not any more forceful information sending is occurring in the system. Fig. 2 plainly exhibits that Modified Trust Value Based approach is more viable than PDORP in finding the aggressive hub in the system.

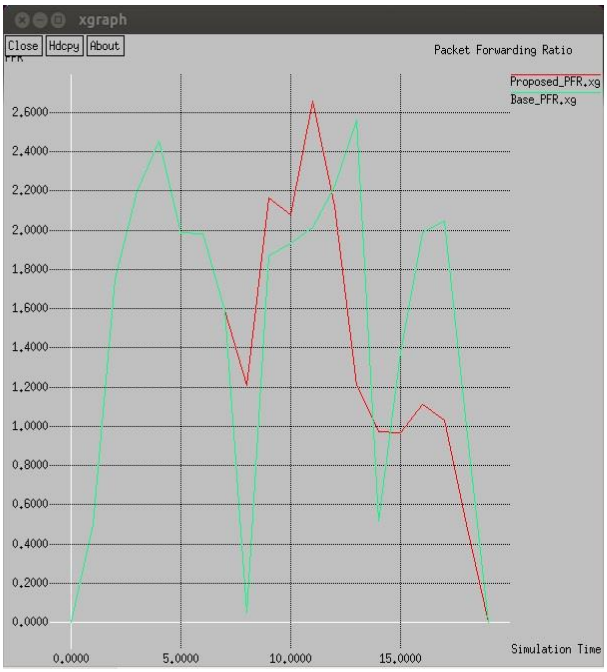

Figure 2. Correlation of packet forwarding ratio(PFR) of the modified trust-based approach - red to existing PDORP system - green.

5.2 Remaining energy

This factor shows the life expectancy of the framework. More is the remaining power, improved is the system's lifespan.

Figure 3 demonstrates the variation of residual energy in the system versus simulation time. At first, the system was provided with the underlying normal vitality of 30 Joules and remaining vitality in the system was approx. 21 Joules. Fig. 5 delineates that the energy utilization of existing PDORP strategy is somewhat higher than the Modified trust value based technique. Consequently Modified trust value based technique is performing superior to the PDORP strategy if there should arise an occurrence of energy preservation of the framework and enhancing the life expectancy of the framework.

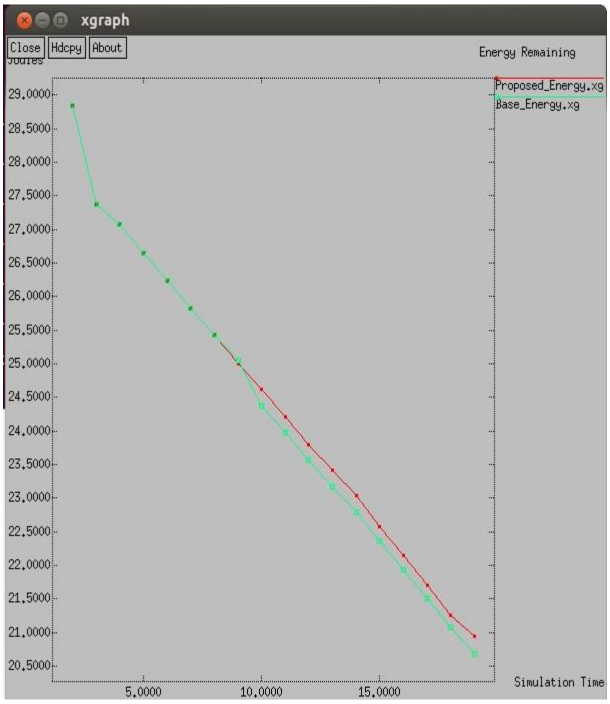

Figure 3. Correlation of remaining energy of Modified Trust Based approach- red to existing PDORP technique - green

5.3 Throughput

It is characterized as a measure of data received at the base station from the group heads. It is estimated in Kbps.

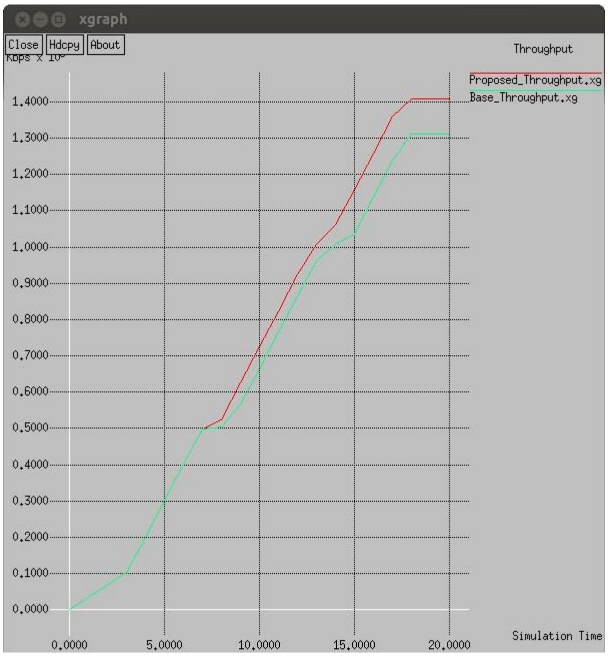

Figure 4. Correlation of throughput of the modified trust-based approach - red to PDORP technique - green.

Figure 4 outlines the estimation of throughput. The amount of information received at the goal is approx. 1400 Kbps. Amid the first round, the estimation of throughput expanded to 524 Kbps, amid the second round, its esteem was expanded by 536 Kbps. These two rounds demonstrate the aggressive sending of the information packets in the system, which builds the throughput. Amid the last round, when the assailant has been recognized, the throughput expanded by 350 Kbps.

Along these lines, the forceful sending gets diminished. Moreover, it is unmistakably shown by the outcomes that modified trust value based method outflanks than PDORP.

5.4 The number of packets forwarded:

The total number of packets forwarded in each round of transmission.

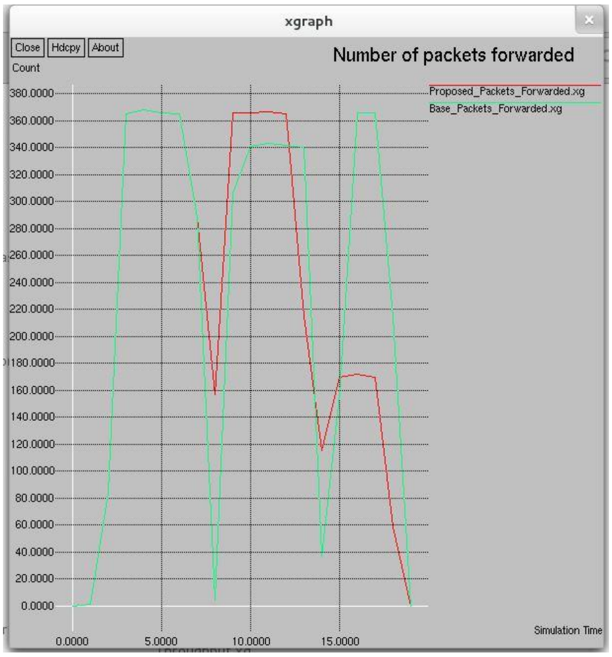

Figure 5. Correlation of the number of packets of modified trust based strategy - red to existing PDORP technique - green.

Figure 5 shows the no. of packets forwarded over the network. The no. of packets forwarded by modified trust value is average throughout the simulation period but in the third round the no. of packets forwarded by the PDORP is less. This indicates that the modified trust technique is losing nearly no packets but PDORP is losing packets when there is an aggressive node is removed from the path because its trust value is reduced and there is no other path readily available to transmit the data.

5.5 E2E delay:

End-to-end delay refers to the time taken for a packet to be transmitted across a network from source to destination.

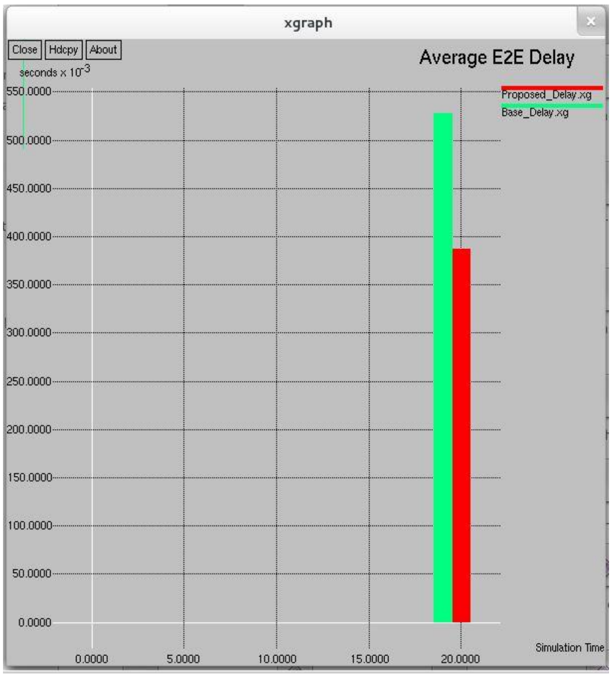

Figure 6. Correlation of E2Edelay of modified trust based strategy - red to existing PDORP technique – green.

Table 2. Quantitative comparison between modified trust based technique and PDORP method

Simulation Time								
Parameter	4.000 seconds		8.000 seconds		12.000 seconds		16.000 seconds	
	PDORP	**Modified Trust based Technique**	**PDORP**	**Modified Trust based Technique**	**PDORP**	**Modified Trust based Technique**	**PDORP**	**Modified Trust based Technique**
PFR	2.45333	2.454	0.4878	1.20769	2.22424	2.12209	1.98913	1.10968
Remaining energy	27.0847	27.0847	25.4251	25.4252	23.574	23.7938	21.9279	22.1479
Throughput	200.704	200.704	503.808	524.288	864.256	925.696	1138.69	1257.47
No. of packets forwarded	368	368	4	157	342	365	366	172
Average E2E Delay	–	_	–	–	–	–	0.527296	0.386903

6. CONCLUSION AND FUTURE SCOPE

The focal point of this investigation was to look at the PDORP and Modified Trust esteem based strategy to secure remote sensor systems. The estimation of PFR acquired went up to 2.4 out of the blue, 2.6 for the second time. Thusly, for the third time, the esteem was decreased. In like manner, the estimation of throughput expanded additionally amid the underlying two rounds and it diminished to bring down levels for the third round after fruitful location of the malicious hub. In this way, more rate of PFR in beginning two rounds of reenactment implies more power will be devoured for at least two adjusts just, (since energy is relative to the number of packets transmissions). Since, after the second round the estimation of PFR diminishes, this would imply that system's vitality utilization would happen regularly. This demonstrates fruitful recognition of the forceful hub of the system without much wastage of system assets.

A remarkable matter in routing is that most of the existing routing strategies perceive that the sensor hubs and the sink are immobile. In circumstances where the sink and possibly the sensors ought to be flexible. In such cases, new directing methods are fundamental remembering the end goal to manage the overhead of versatility and topology changes in such power obliged conditions. Incorporating WSN with wired networks(i.e. Web) is another conceivable future examination for steering conventions.

7. REFERENCES

[1] Kazem Sohraby, Daniel Minoli and Taieb Znati, “Wireless Sensor Networks”, ELSEVIER Inc., 2007.

[2] N. A. Pantazis, S. A. Nikolidakis, and D. D. Vergados, “Energy-efficient routing protocols in wireless sensor networks: A survey,” IEEE Commun. Surv. Tut., vol. 15, no. 2, pp. 551-591, 2013.

[3] Y. Li, M. T. Thai, W. Wu, “Wireless sensor networks and applications”, New York: Springer Science+Business Media, LLC pp. 7-11, 2008.

[4] Pallavi S. Katkar and Prof. (Dr.) Vijay R. Ghorpade, “A Survey on Energy Efficient Routing Protocol forWireless Sensor Networks”, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6, 2015.

[5] Jayashri Deb Sinha and Subhabrata Barman, "Energy Efficient Routing Mechanism in Wireless Sensor Network", IEEE conference on Recent Advances in Information Technology,2012.

[6] Akshay, N.; Kumar, M.P.; Harish, B.; Dhanorkar, “An efficient approach for sensor deployments in wireless sensor network” Emerging Trends in Robotics and Communication Technologies (INTERACT),2010 International Conference on , vol., no., pp.350,355, 3-5 Dec. 2010

[7] W. Liu and J. Yu, “Energy Efficient Clustering and Routing Scheme for Wireless Sensor Networks Proceeding” of the IEEE International Conference on Intelligent Computing and Intelligent Systems, Shanghai, 20-22 November 2009, pp. 612-616. doi:10.1109/ICICISYS.2009.5358113

[8] Chengfa Li, Mao Ye, Guihai Chen, Jie Wu, “Energy efficient unequal clustering mechanism for wireless sensor networks” IEEE conference MASS 2005., 0-7803-9466-6/05.

[9] Joon-WooLee, Byoung-Suk Choi, Ju-JungLee, “Energy Efficient coverage of wireless sensor networks using Ant colony optimization with three types of pheromones” IEEE transaction on industrial informatics, Vol7.No.3 August 2011.

[10] Ali chamam, Samuel pierre, “On The Planning Of Wireless Sensor Networks: Energy-Efficient Clustering Under The Joint Routing And Coverage Constraint”, IEEE transaction on Mobile computing, Vol8.No.6 August 2009.

[11] Johnson, Hu, et al., RFC 4728: “The dynamic source routing protocol (DSR) for mobile ad hoc networks for IPv4”, 2007, https://www.ietf.org.

[12] Ademola P. Abidoye, Nureni A. Azeez, Ademola O. Adesina, Kehinde K. Agbele, “ANCAEE: A Novel Clustering Algorithm for Energy Efficiency in Wireless Sensor Networks Wireless Sensor Network”, 2011, 3, 307-312 doi:10.4236/wsn.2011.39032 Published Online September 2011 (http://www.SciRP.org/journal/wsn)

[13] Ruperee A, Nema. S, Pawar S., “Acheiving energy efficiency and increasing network life in wireless sensor network”, Advance computing conference (IACC), 2014 IEEE international ,pp.: 171 175, 2014.

[14] Brar G. S. , Rani S. , Song H. and Ahmed S. H. , “Energy Efficient Direction-Based PDORP Routing Protocol for WSN”, IEEE Special Section on Green Communications and Networking for 5g Wireless, Vol. 4, pp: 3182-3194, 2016.

[15] Pardeep Kaur, Sandeep Kad , “Modified Trust Value based technique to secure Wireless Sensor Networks” , Springer conference Futuristic Trends in Network and Communication Technologies(FTNCT) 2018.

[16] H. Oh and K. Chae, "An Energy-Efficient Sensor Routing with Low Latency, Scalability in Wireless Sensor Networks," IEEE International Conference on Multimedia and Ubiquitous Engineering, Seoul, 26-28 April 2007, pp

[17] H. Oh, H. Bahn, and K. Chae, "An Energy-Efficient Sensor Routing Scheme for Home Automation Networks," IEEE Transactions on Consumer Electronics, Vol. 51, No. 3, 2005, pp. 836-839.

[18] M. H. Khodashahi, A. Norouzi, F. Amiri and M. Dabbag- hian, “A Novel Optimal Routing Algorithm by Creating Concentrically Sectors in Wireless Sensor Networks,” 8th IEEE Annual Communication Networks and Services R search Conference, Montreal, 11-14 May 2010, pp. 168- 173.

[19] J. N. Al-Karaki and A. E. Kamal. “Routing Techniques in Wireless Sensor Networks: A Survey,” IEEE Wireless Communications, Vol. 11, No. 6, 2004.