Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.199

IJCSMC, Vol. 8, Issue. 5, May 2019, pg.90 – 94

Analysis of Energy Efficient Techniques for Wireless Sensor Networks

Chirag Malik
Research Scholar, UIET, MDU, Rohtak
chirumalik@gmail.com

Vikas Sindhu
Assistant Professor, UIET, MDU, Rohtak
vikassindhu7@gmail.com

Abstract: The wireless sensor network is the decentralized type of network in which sensor can sense information and pass it to base station. The clustering is the efficient approach which reduces energy consumption of the network. The LEACH is the efficient approach to increase lifetime of WSN. The cluster heads are selected in LEACH protocol based on the distance and energy. The sensor node which has maximum energy and least distance to base station is selected as cluster head which transmit data to base station. In this paper, various energy efficient techniques of WSN are reviewed in terms of certain parameters
Keywords: WSN, LEACH, energy efficient

Introduction

A network which is generated by gathering numerous small-sized and light-weighted sensors is known as a wireless sensor network. The cost of these nodes is very less along with the less energy and number of processing capabilities. The wireless sensor networks are deployed within various applications in order to gather important information from the surroundings. The various measures such as temperature, pressure and humid of the surroundings are calculated by the sensors deployed in those regions [1]. There are numerous applications such as in military areas, intelligent communications, wildlife monitoring, observing critical infrastructures and so on in which these networks have been deployed in order to observe surroundings and take appropriate actions. Within the wireless sensor networks, there are two different types of sensor nodes. They are the sensor node as well as the sink node. The data is sensed and gathered by the numerous sensor nodes present within these networks and the gathered data is then forwarded to the sink node [2]. Multiple hops are single hops can be used in order to transmit this data to sink node. With the help of Internet, this data can be utilized locally or globally by the sink. There is a sensing unit, a processing unit, a communication unit as well as a power unit present within the wireless sensor node's architecture. The data can be sensed, collected, processed and then communicated to other nodes by each of the node present

within the network. The environment is sensed by the sensing unit present within these nodes. The permutations of the sensed data are confined by the processing unit [3]. Further, the processed information is exchanged amongst the neighboring sensor nodes through the communication unit. In order to provide an energy source, a battery is present within the sensor nodes. However, there is very limited amount of power present within the batteries and the replacement of the batteries that have no energy left is impractical. Thus, within the wireless sensor networks, the consumption of power in efficient manner is a major research area [4]. In order to increase the lifetime of the network, numerous energy efficient techniques are presented by various researchers. On the basis of number of queries generated per mean time, the traffic of WSN depends. A query is sent to the complete sensor field by sink node in order to transmit the information which has been sensed. The data that is gathered by the sensors is sent as a response to the query by sensor nodes. With the help of a routing protocol, the sensor node will reply to the sink node with the help of injected query. A single response is sent back to all the queries by sensor node which results in saving the number of packets that are being transmitted. There are large numbers of distributed nodes present within the network which include numerous sensors, embedded processor as well as low-power radio which includes battery in it. One of the major issues that arise during the planning of sensor network is the management of power consumption [5]. There is a need to provide operation of sensor nodes with highest energy efficiency and ensure that there is least amount of energy wastage by the battery present within the nodes. The most consuming tasks amongst the sensor node are the transmission and reception. In order to increase the performance of WSN, there is a need to provide proper configuration of these networks. The efficiency of overall network can be minimized by utilizing the transmission power that is higher than the requirement. The interferences amongst the nodes can be generated along with the increment in overall consumption of power with the higher retransmission probability involved [7]. The link quality that increases the error rate will be degraded when the transmission power is very less. Due to the requirement of higher number of retransmission the overall energy consumption in also increasing [6]. There are various routing protocols that have been introduced in order to ensure that there is less energy being consumed in the networks. In order to discover the path and disseminate the information between the wired and wireless ad hoc networks, a commonly utilized technique is flooding. This technique includes very simple routing strategy and the maintenance of network topology and designing of route discovery algorithms that are highly complex is not included within the overall cost. A reactive technique is utilized by flooding in which the data or control packets that are being received by each node are sent to the neighboring nodes further [7]. Gossiping technique has been introduced in order to solve the issues arising within the flooding method. Here, a simple forwarding rule is utilized by gossiping and there is no need of maintaining the topology or any complex route discovery methods within this approach. A data-centric negotiation-based family of information dissemination protocols that is used within the WSNs is known as Protocols for Information via Negotiation (SPIN). Low-Energy Adaptive Clustering Hierarchy (LEACH) is the gathering and delivering of data to the sink which is also known as a base station is done with the help of the routing algorithm [8]. There are two hierarchical-based routing protocols proposed by researchers which are TEEN (Threshold-sensitive Energy Efficient sensor Network protocol), and APTEEN (Adaptive Periodic Threshold-sensitive Energy Efficient sensor Network protocol) which are utilized within the various time-critical application areas [9]. Within the various routing and information-gathering protocols present in WSNS, the Power-efficient gathering in sensor information systems (PEGASIS) and hierarchical PEGASIS which is its extension are present.

Literature Review

Sneha Kamble, et.al [10] (2017) discussed that in WSN data sending directly to the sink node raise various problems. Information gathering technique is the center of the WSN. In this information aggregation technique is used to decrease the energy consumption as well as enhance the network lifetime. In this paper data aggregation is performed to avoid such problems related to energy. An energy effective system in which data collection nodes are utilized for gathering data from cluster head inside the cluster. The lifetime of the wireless network is improved by forwarding the data in aggregated format.

Alka Singh, et.al [11] (2016) discussed in this paper, Low Energy Adaptive Clustering Hierarchy (LEACH) a well known cluster based protocol. LEACH protocol is used for enhance the life time of the network. LEACH operation is divided into following rounds 1)Set up phase- In this phase nodes are selected as a cluster head(CH) on the basis of energy and distance.

2) Steady state phase- this stage is for data transmission. In this nodes sense data and send this data to their respective CH node. Then processed data will be sending to the base station. So LEACH is a balanced energy consumption protocol for wireless sensor network.

Ju young Kim et.al [12] (2014) presented the study of number of vulnerabilities, attacks and threats for Wireless Sensor Networks. In this, an analysis has done to find out the authorized treats to the attacks and discover various techniques for recovery of attacks. Wireless Sensor Networks provide a numerous opportunities for increasing productivity and minimizing costs. It provides significant advantages for many applications that would not have been possible for the past. The different vulnerabilities, threats and attacks that could possibly put WSNs in a vital or critical situation have been identified and discussed in their paper. The different categories for these threats are defined to identify a possible countermeasure scheme applicable for each threat classification.

Roshan Singh Sachan et.al [13] (2013) introduced in this paper, adhoc nature of deployment and threats of wireless media are some challenges for sensor network. There are number of attacks are triggered in WSN but misdirection attack is one of the type of DoS attack. It is extremely difficult to detect and defend. In this attack node misdirect the path to the other node and degrade performance of the network. In this paper discuss about detection and isolation of this attack with small amount of delay and throughput.

Yi Zhing Zang et.al [14] (2012) authors design a novel message in this paper, a novel message observation mechanism (MoM) to detect and defense the DoS attack. Based on the spatial-temporal correlation, MoM utilizes the similarity function to identify the content attack as well as the frequency attack. The MoM adopts rekey and reroute countermeasures to isolate the malicious node. The security analysis shows that their solution not only detects and defenses the DoS attack but also can reduce the energy consumption.

Kalpana Sharma and M K Ghose [15] (2010) introduced in this paper, the problem of safety is due to of the sensor network's nature. Moreover security architecture is not up to date to mitigate the attack. Furthermore, nodes are placed at an environment where nodes can be easily affected by the attack. They have presented the summery of the WSNs threats affecting different layers along with their defense mechanism. There are used in "layer-by-layer" basis as a security tool for security purposes. Through this paper they have tried to present the most common security threats in various layers and their most probable solution.

Guoxing Zhan, Weisong Shil, Julia Deng [16] (2010) proposed in this paper, TARF: A Trust-Aware Routing Framework for Wireless Sensor Networks, to secure multi-hop routing in WSNs against intruders exploiting the replay of routing information with the idea of trust management, TARF enables a node to keep track of the trustworthiness of its neighbors and thus to select a reliable route. Not only does TARF circumvent those malicious nodes misusing other nodes identities to misdirect network traffic, it also accomplishes efficient energy usage.

Hanlun Than et.al [17] (2009) introduced a new approach to achieving confidentiality in multi-hop code dissemination is presented. They integrate confidentiality and DoS-attack resistance in a multi-hop code dissemination protocol. The approach is based on Deluge, an open source, state-of-the-art code dissemination protocol for WSNs. In addition, they provide a performance evaluation in their scheme, compared with the original Deluge and the existing secure Deluge.

Table of Comparison

Authors Names	Year	Description	Outcomes
Sneha Kamble,	2017	In this paper data aggregation is performed to avoid such problems related to energy.	The lifetime of the wireless network is improved by forwarding the data in aggregated format.
Alka Singh,	2016	In this paper, Low Energy Adaptive Clustering Hierarchy (LEACH), a well known cluster based protocol is discussed.	Thus, LEACH is a balanced energy consumption protocol for wireless sensor network.
Ju young Kim	2014	The different vulnerabilities, threats and attacks that could possibly put WSNs in a vital or critical situation have been identified and discussed in their paper.	The different categories for these threats are defined to identify a possible countermeasure scheme applicable for each threat classification.
Roshan Singh Sachan	2013	It is studied that the adhoc nature of deployment and threats of wireless media are some challenges for sensor network.	The detection and isolation of this are discussed for the attack with small amount of delay and throughput.
Yi Zhing Zang	2012	A novel message observation mechanism (MoM) was proposed to detect and defense the DoS attack.	The security analysis shows that their solution not only detects and defenses the DoS attack but also can reduce the energy consumption.
Kalpana Sharma and M K Ghose	2010	This paper studied that the problem of safety is due to of the sensor network's nature.	Through this paper they have tried to present the most common security threats in various layers and their most probable solution.
Guoxing Zhan, Weisong Shil, Julia Deng	2010	TARF: A Trust-Aware Routing Framework was proposed for Wireless Sensor Networks, to secure multi-hop routing in WSNs against intruders.	Not only does TARF circumvent those malicious nodes misusing other nodes identities to misdirect network traffic, it also accomplishes efficient energy usage.
Hanlun Than	2009	A new approach is proposed to achieve confidentiality in multi-hop code dissemination is presented.	A performance evaluation was provided in their scheme compared with the original Deluge and the existing secure Deluge.

Conclusion

In this paper, it is concluded wireless sensor network is the self configuring type of network in which energy consumption is the major issue. The various energy efficient techniques are reviewed and analyzed in terms of certain parameters. In future, novel energy efficient approach will be designed for wireless sensor network which aggregate maximum data to base station by consuming least amount of energy from the network.

References

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci. "Wireless Sensor Networks: A survey" Broadband and Wireless Networking Laboratory, School of Electrical and Computer Engineering, Georgia institute of Technology, Atlanta, GA 30332, USA Received 12 December 2001; accepted 20 December 2001, pp . 392-422.

[2] G.H. Raghunandan, B.N. Lakshmi, "A Comparative Analysis of Routing Techniques for Wireless Sensor Networks", Proceedings of the National Conference on Innovations in Emerging Technology, IEEE 2011.

[3] Dr. G. Padmavathi, Mrs. D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009, pp. 1-9

[4] S. Chen, S. Tang, M. Huang, and Y. Wang, "Capacity of data collection in arbitrary wireless sensor networks", IEEE Trans. Parallel Diatribe. Syst., vol. 23, no. 1, pp.52-60, Jan. 2012.

[5] X. Liu, "A survey on clustering routing protocols in wireless sensor networks," Sensors, vol. 12, no. 8, pp. 11113- 11153, 2012.

[6] Q. Mamun, "A qualitative comparison of different logical topologies for wireless sensor networks," Sensors, vol. 12, no. 11, pp. 14887-14913,2012.

[7] K.-W. Fan, S. Liu, and P. Sinha, "Structure-free data aggregation in sensor networks," IEEE Trans. Mobile Comput., vol. 6, no. 8,pp. 929-942, Aug. 2007.

[8] Y. Yao and J. Gehrke, "The cougar approach to in-network query processing in sensor networks," ACM SIGMOD Rec., vol. 31, no. 3, pp. 9-18, 2002.

[9] M. Ye, C. Li, G. Chen, and J. Wu, "EECS: An energy efficient clustering schemein wireless sensor networks," in Proc. 24th IEEE Int. Perform., Comput., Commun.Conf. (IPCCC), Phoenix, AZ, USA, Apr. 2005, pp. 535-540.

[10] Sneha Kamble and Tanuja Dhope, "Reliable Routing Data Aggregation using Efficient Clustering in WSN ", International Conference on Communication Control and Computing Technologies,IEEE,2017,pp.246-250

[11] Alka Singh, Shubhangi Rathkanthiwar and Sandeep Kakde, "Energy Efficient Routing of WSN using Particle Swarm Optimization and V-Leach Protocol", International Conference on Communication and Signal Processing,IEEE,2016,India

[12] Ju young Kim, Ronnie D. Caytiles, Kyung Jung Kim, "A Review of the Vulnerabilities and Attacks for Wireless Sensor Networks" Journal of Security Engineering, 2014, pp.241-250

[13] Roshan Singh Sachan, Mohammad Wazid, Avita Katal, D P Singh, R H Goudar, "A Cluster Based Intrusion Detection and Prevention Technique for Misdirection Attack inside WSN", International conference on Communication and Signal Processing, April 3-5, 2013, India

[14] Yi-Ying ZHANG, Xiang-zhen LI, Yuan-an LIU, "The detection and defense of DoS attack for wireless sensor network", Elsevier Journal of China Universities of Posts and Telecommunications, Vol19, pp. 52-56, Oct-2012.

[15] Kalpana Sharma and M K Ghose, "Wireless Sensor Networks: An Overview on its Security Threats" IJCA Special Issue on "Mobile Ad-hoc Networks" MANETs, 2010, pp.42-45

[16] Guoxing Zhan, Weisong Shil, Julia Deng, "TARF: A Trust-Aware Routing Framework for Wireless Sensor Networks", EWSN 2010, LNCS 5970, pp. 65–80, 2010.

[17] Hailun Tan, Diethelm Ostry, JohnZic, SanjayJha, "A Confidential and DoS-Resistant Multi-hop Code Dissemination Protocol for Wireless Sensor Network", ACM WiSec09, Zurich, Switzerland, March 16-18, 2009.

