ISSN 1533-9211

DOI: 10.5281/zenodo.10360487

A DETAILED SURVEY ON SECURED AND LOAD BALANCED COOPERATIVE ROUTING PROTOCOLS IN WIRELESS SENSOR NETWORKS

R. J. KAVITHA [1] and P. ANANDAVALLI [2]

[1, 2] Department of Electronics and Communication Engineering, University College of Engineering Panruti.

Abstract

Wireless Sensor Networks are self-configurable and infrastructure-less networks. These networks consist of small sensors which are used for monitoring the physical environment. The applications of WSNs are ranged from small temperature monitoring of a patient to surveillance in military zones. The sensed data are collected in a sink node and then sent to the data center for analysis. Communicating network between the server and the sensor nodes is carried out through the intermediate sensor nodes by multi hop communication. Thus the cooperative routing protocols plays a predominant role in WSN. As the sensors are manufactured from diverse manufacturer, there is no standard routing protocols and security mechanism can be implemented. This study examines different secured and cooperative routing protocols.

Keywords: Wireless Sensor Networks, Sensors, Sink Nodes, Data Center, Multi-Hop Communication and Routing.

1. INTRODUCTION

WSN are the self-configurable and fault tolerant networks that consist of number of small sensors. These sensors are used in different applications. It includes temperature monitoring, area surveillance, attendance system, industrial sensors, fire detection in prescribed areas and so on. Karthikeyan et al. [2021]. The sensors reacts for a particular event and sends event packets to a sink to notify that a particular event has happened. Different sensors detect different events that may exist in a particular geographic area.

The sensors collect data through various sources and this data are sent to the server via sink nodes. The sensors may be static or mobile in position. The sink nodes are the nodes which are used to accumulate data through different sensor nodes and transfer these data to primary server node where the analysis of the aggregated data is performed. Clusters, also called a group of sensor nodes, where a cluster head is elected to aggregate this data, passing it to the sink nodes. Figure 1 portrays an architecture of a Wireless Sensor Networks and its working.

DOI: 10.5281/zenodo.10360487

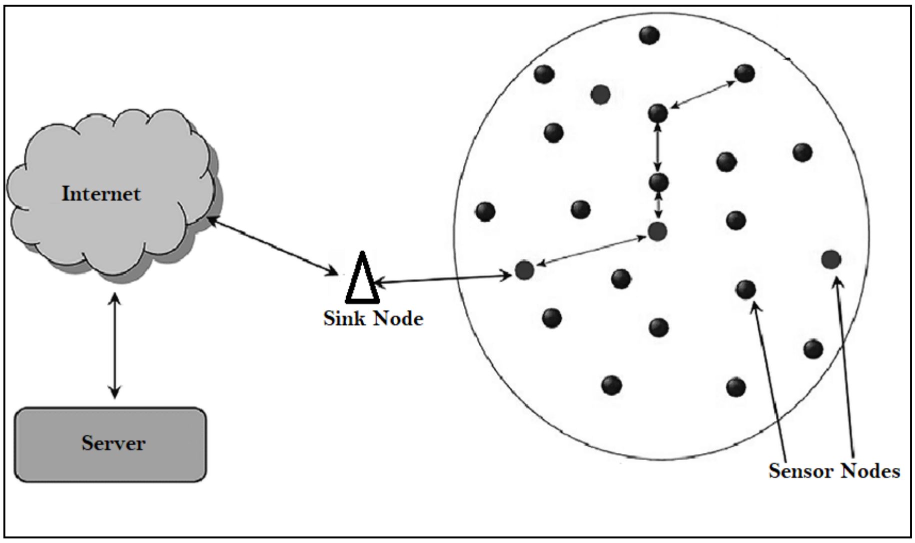

Figure 1: Structure of a WSN

The WSN follows multi-hop routing protocol like wireless networks. The data is gathered by sensor nodes needs to delivered to the server for analysis. The communication is carried out by passing the data to other sensor nodes in the path and so on to the sink nodes and then to the server nodes. The sensor nodes thus act as a node as well as the router.

First the sensor node that has the data, needs to establish a path to the server. Once the path has been established, the data will be transferred. If any node in the established path is failed or moved out from the vicinity of the other node, then the path has to be reestablished. This makes the network topology more dynamic.

As the wireless communication in the WSN uses broadcast communication and the channel is open, these networks are more vulnerable to attacks like eavesdropping, malicious packet injection, replay attacks etc. The above attacks are mainly categorized in to privacy and authentication. Privacy is defined as the data transmission is done in a secured manner so that no one else in the network sees the message. The authentication on the other hand ensures that the data are collected and forwarded from the authentic nodes. [Li] 2010.

As the WSN nodes have limited energy and computational capacity, the security implementations in the nodes are becoming a complex process. Even some of the sensors are deployed in the unprotected areas and the communication medium is open, making a network highly prone to attack. For securing the networks, the fundamental security mechanism used is cryptography. But this method requires more computation power and energy which are the main constraints of the WSN. A honey pot is another technique to attract the attacker as a trap to analyze their behaviors. [12]. Next "Intrusion Detection System" (IDS) is introduced for monitoring a network in a more effective manner.

The reminder of this study is structured as: Section 2 covers Literature survey. Various methods are compared in section 3. Section 4 concludes the study and future scope is also covered.

ISSN 1533-9211

DOI: 10.5281/zenodo.10360487

2. LITERATURE SURVEY

2.1 Energy Efficient Routing Protocols

Yahia and Gaafar [2019] proposed a MAN LEACH protocol which consists of three different categories of sensor nodes. They are master, advanced and normal nodes. They developed a clustering scheme for heterogeneous networks in which selecting a cluster head depends on the ratio between the current node energy to the network's average energy. The energy required to transmit the packet is considered in three levels. The lowest energy is used to transmit packets between the cluster nodes, the mid-level is used for transmission between cluster heads and the consumption of energy for transmitting cluster heads to the base stations is highest level.

An "Optimized and Energy Efficient Routing Scheme" (OEERS) was proposed by Harish and Reddy [2021]. For selecting a cluster head through this method, the probability values based on present energy available and the distance from base stations are considered. The probability value of a node is given higher, when nodes have high energy and is nearer to the base station.

Santhosh and Deshpande [2018] designed an "Energy Efficient Clustering Protocol for HWSN" (EECPEP-HWSN). They designed the protocol with three kinds of nodes. They are normal, super, and advanced nodes. Initial energy, remaining energy and hop-count were considered for selecting the cluster head.

For enhancing the lifetime of the network, Singh et al. [2017] presented a three-level heterogeneous network model. Selecting a cluster head, and selecting cluster members are done through threshold function and weighted election probability. The DEEC protocol is applied for level-1, level-2 and level-3 as DEEC-1, DEEC-2 and DEEC-3.

Abdelkader et al. [2022] designed a multi-hop routing protocol based on gateways. This method is used to increase the network lifetime and improves its throughput. According to this method, the network is divided into the following layers. The data fusion is done by sensor nodes in the center. The other nodes are grouped in to two equal clusters with one cluster head. The average energy of corresponding clusters and remaining node energy helps in deciding the cluster head.

To maintain load balancing among the sensors, clustering is a strategy that may effectively use the energy of the sensors, extending the life and scalability of the networks. A genetic algorithm-based cluster head selection was proposed by Aridaman et al [2021]. The distance, density and energy are factors used for selecting the cluster head node. The hot spot problem is eliminated by introducing the multiple movable sink nodes.

Existing clustering techniques only take heterogeneity in node density and network topology into account when choosing the heads of clusters. Xingchun et al. [2021] proposed a fuzzy logic scheme for enhancing the lifetime of the network, relative density, initial energy and distance from nodes to base stations used for selecting the cluster head.

Marigowda et al. [2018] proposed a Synchronized Incremental Counter (SIC) method to protect against the jamming and replay attacks. The AES algorithm is combined with OCB mode to implement the modified Constrained function.

A heterogeneous network is formed by the WSNs in the particular area to reduce the routing energy. Hung et al suggested “Energy-Efficient Cooperative Routing Scheme for Heterogeneous Wireless Sensor Networks” is the routing technique to conserve energy. In this method, the routing direction and remaining energy are considered to establish the dynamic routing. Additionally, to conserve delivery energy, the packets sent in a similar direction by same sensors are aggregated. Additionally, the EERH's network settings, such as event packet propagation delay and sensor transmission distance, are programmable to meet the demands of the real-world environment.

A reference architecture was proposed by Alvarez et al. [2019] for event driven applications in which data integration from the sensors and real time data processing were done. A spatial-temporal analytics is done from the data collected through sensors to detect geographical events.

Gousia and jayaprasad [2020] proposed a security based routing protocol with low latency. LLEECMP clustering method was proposed to select cluster head which exhibited a good tradeoff between network lifetime and latency. By this method, the real time packets take different path from the non-real time packets.

In WSNs, designing an efficient clustering is a major difficulty. To address this issue, Edla et al. [2019] proposed two methods. First method is a clustering algorithm based on “Shuffled Complex Evolution of Particle Swarm Optimization” (SCE-PSO) and the second one is a novel fitness function that takes into account gateway load, mean cluster distance, and the total heavily loaded gateways in a network.

2.2 Secured Routing Protocols

Lakshmi and Prasanth [2022] proposed a Modified Back propagation neural network based black hole detection and prevention method. This method eliminates the black hole nodes for improving the security of a routing protocol by using the Multiple Input Multiple Output (IMIMO) model concepts.

A trust management system was proposed by Liu and Wu [2015] which is based on neighbor monitoring. A distributed trust value can be estimated from indirect and direct trust values. The consistency check algorithm can defend attacks on trust concept. Additionally, an algorithm based on energy-balance is introduced to lengthen the MWSN lifespan due to the restricted energy of the sensor nodes.

Saeed et al. [2020] proposed a “Secure Energy Efficient and Cooperative Routing protocol” (SEECR) to secure the Under Water sensors. A light weight and load balancing mechanism was proposed by Zhou et al. [2021]. This algorithm is based on WSNs clustering. The authentication, confidentiality and integrity are maintained in this method. The network lifetime is increased. Based on hybrid trust model, a realistic trust based routing method was proposed by Khan et al. [2021]. The trust score of a node, remaining energy and path length are considered for finding out the secured route. The use of trusted nodes is to forward data and reduce the usage of energy using this multi-factor technique.

The Seybold REPORT

ISSN 1533-9211

DOI: 10.5281/zenodo.10360487

3. CONCLUSION

In the WSN, the security and energy efficiency are the major problems that are needed to be addressed, because the sensor nodes are very small in size and heterogeneous. The communication between the sensor nodes in WSN is through the intermediate sensors and in an open medium. In recent years, the research has been evolved in the WSN routing. So, in this paper, a detailed survey on cooperative and secured routing protocols were discussed. Further, the energy efficient routing protocols are also discussed.

References

1) Yahia I, Gaafar A. Energy Efficient Routing Protocol for Heterogeneous Wireless Sensor Networks. SUST Journal of Engineering and Computer Science (JECS). 2019;20(1).

2) Harish NJ, Reddy HSM (2021) Robustness Performance Analysis of OEERS Clustering Technique for Heterogeneous Network Models . Indian Journal of Science and Technology 14(42)

3) V. santosh, R.S. deshpande, "Energy Efficient Clustering Protocol to Enhance Performance of Heterogeneous Wireless Sensor Network: EECPEP-HWSN," Journal of Computer Networks and Communications, Vol 2018, pp.1-12

4) S. Singh, A. Malik, and R. Kumar, "Energy efficient heterogeneous DEEC protocol for enhancing lifetime in WSNs," Engineering Science and Technology an International Journal, vol. 20, no. 1, pp. 345–353, 2017.

5) Abdelkader Benelhouri, Hafida Idrissi-Saba, Jilali Antari, "An Improved Gateway-Based Energy-Aware Multi-Hop Routing Protocol for Enhancing Lifetime and Throughput in Heterogeneous WSNs", Simulation Modelling Practice and Theory, Volume 116, 2022, 102471,

6) Aridaman Singh Nandan, Samayveer Singh, Lalit K. Awasthi,"An efficient cluster head election based on optimized genetic algorithm for movable sinks in IoT enabled HWSNs", Applied Soft Computing, Volume 107, 2021, 107318

7) Xingchun Liu, Jingjing Yu, Wenqi Zhang, Hui Tian, "Low-energy dynamic clustering scheme for multi-layer wireless sensor networks", Computers & Electrical Engineering, Volume 91, 2021, 107093

8) Lakshmi, M., Prashanth, C.R. (2022). A Back Propagation Neural Network Model and Efficient Routing Security Mechanisms Against Blackhole Attack in HWSNs. In: Gunjan, V.K., Zurada, J.M. (eds) Proceedings of the 2nd International Conference on Recent Trends in Machine Learning, IoT, Smart Cities and Applications. Lecture Notes in Networks and Systems, vol 237. Springer, Singapore. https://doi.org/10.1007/978-981-16-6407-6_55

9) Patel MM, Aggarwal A (2013) Security attacks in wireless sensor networks: a survey. In: International conference on intelligent systems and signal processing (ISSP), pp 329–333

10) Marigowda CK, Thriveni J, Gowrishankar S, Venugopal KR (2018) An efficient secure algorithms to mitigate DoS, replay and jamming attacks in wireless sensor network. In: Proceedings of the world congress on engineering and computer science, vol 1, no 1, pp 1–7

11) L. . -L. Hung, F. . -Y. Leu, K. . -L. Tsai and C. . -Y. Ko, "Energy-Efficient Cooperative Routing Scheme for Heterogeneous Wireless Sensor Networks," in IEEE Access, vol. 8, pp. 56321-56332, 2020, doi: 10.1109/ACCESS.2020.2980877.

12) M. G. Alvarez, J. Morales and M.-J. Kraak, "Integration and exploitation of sensor data in smart cities through event-driven applications", Sensors, vol. 19, pp. 1372, 2019.

DOI: 10.5281/zenodo.10360487

13) Thahniyath, Gousia & Jayaprasad, M.. (2020). Secure and load balanced routing model for wireless sensor networks. Journal of King Saud University - Computer and Information Sciences. 10.1016/j.jksuci.2020.10.012.

14) Liu, B. and Wu, Y. (2015) A Secure and Energy-Balanced Routing Scheme for Mobile Wireless Sensor Network. Wireless Sensor Network, 7, 137-148.

15) K. Saeed, W. Khalil, S. Ahmed, I. Ahmad and M. N. K. Khattak, "SEECR: Secure Energy Efficient and Cooperative Routing Protocol for Underwater Wireless Sensor Networks," in IEEE Access, vol. 8, pp. 107419-107433, 2020, doi: 10.1109/ACCESS.2020.3000863.

16) B. Karthikeyan, K. Alhaf Malik, D. Bujji Babbu, K. Nithya, S. Jafar Ali Ibrahim, N. S. Kalyan Chakravarthy. (2021). Survey of Cooperative Routing Algorithms in Wireless Sensor Networks. Annals of the Romanian Society for Cell Biology, 5316–5320

17) Zhou J, Lin Z. Lightweight load-balanced and authentication scheme for a cluster-based wireless sensor network. International Journal of Distributed Sensor Networks. February 2021. doi:10.1177/1550147720980326

18) Edla, DR, Kongara, MC, Cheruku, R. SCE-PSO based clustering approach for load balancing of gateways in wireless sensor networks. Wirel Netw 2019; 25(3): 1067–1081.

19) Khan, Dr & Singh, Karan. (2021). TASRP: a trust aware secure routing protocol for wireless sensor networks. International Journal of Innovative Computing and Applications. 12. 108. 10.1504/IJICA.2021.113750.

20) C. Li, "Security of Wireless Sensor Networks: Current Status and Key Issues", in Smart Wireless Sensor Networks. London, United Kingdom: IntechOpen, 2010.