Improving Energy Conservation and Securing Wireless Sensor Networks – A Comprehensive Survey

[1]S.Sowndeswari, [2]E.Kavitha
[1]Research Scholar, [2]Prof. and Head,
[1]Sir M Visveswaraya Institute of Technology, Bangalore, India.

Abstract : In Technological world, Wireless sensor networks (WSNs) have achieved a lot of popularity and widely spread in various applications such as military, medical, Industrial, environmental monitoring. In most of the applications, the nodes of WSN are deployed in unreachable areas where the humans cannot intervene. Hence recharging or replacing the battery of nodes is one of constraints in WSN. Also, WSN security is one of the technical challenges. Therefore one must employ various techniques to conserve the energy and detect the malicious nodes in networks to improve the lifetime, reliability and throughput of the WSN. This paper discusses various techniques for improving energy conservation and securing WSNs by mitigating malicious nodes.

IndexTerms **- Energy conservation, Securing WSNs, Malicious nodes.**

I. INTRODUCTION

Wireless Sensor network (WSN) has become a challenging research area now-a-days. It has numerous applications which includes medical, military, environment monitoring, industrial monitoring etc., Wireless Sensor network consists of small wireless sensors. Sensors help each other to transmit the information to the base station. Sensor/Sensor nodes consist of sensing, processing and communicating components.

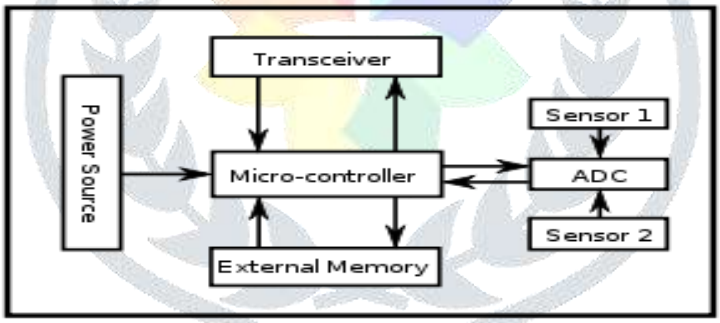

Fig.1. Architecture of Sensor Node in WSN

Each Sensor node in the network collects the data from its surroundings and sends the sensed data to a base station which results in considerable amount of energy consumption by the sensor nodes. These sensor nodes are randomly deployed in unattended areas. So it is quite difficult to replace the battery frequently and sometimes not even possible. Also, the external attacker attacks the network and internal node is invaded which becomes malicious node. A malicious node is a node which denies service to other nodes in the network and modifies the data before, during or after transmission. Hence, reliable and efficient protocols are employed to improve the network lifetime and throughput.

In this paper, we discuss various energy saving schemes and malicious node detection schemes to improve the energy conservation and efficient malicious node detection, thereby improving network lifetime and throughput.

II. DIFFERENT ENERGY CONSERVATION SCHEMES FOR WSN

1. A Dynamic Sleep Scheduling Protocol

Energy can be conserved in wsn by putting radio transceiver in sleep mode whenever communication is not needed. The radio transceiver can be switched on when data is available. The act of switching action between active and sleep mode depending upon data availability is called duty cycle. [1] The authors proposed a scheduling scheme and proved that number of live nodes and sensing capacity is increased even after more number of rounds, thus the lifetime of WSN is improved.

2. Routing Scheme

Routing is a significant phenomenon which is a great source of energy consumption. [1] The authors have discussed the energy aware routing protocols in WSN based on path, structure, protocol & next hop selection. Of all the routing protocols; hierarchical method in structure based routing protocols have special advantage of scalability and efficient communication. Hierarchical routing maintains energy consumption of sensor nodes and performs data aggregation which causes reduction in communication overhead in turn reduces the energy consumption and improves the lifetime of the network.

3. MAC Protocols

MAC protocols along with routing protocols further reduce the energy consumption and extend the lifetime of WSN. [1] Authors proposed different energy efficient MAC protocols in WSN. MAC protocols can be broadly divided into two types: centralized and distributed. Schedule based and contentions based are the two main types under centralized MAC protocols. Contention based MAC protocols consume more energy because they waste energy in idle listening and collisions. Scheduled based MAC protocol is more powerful which is collision free and avoids unwanted idle listening those are the two major sources of energy consumption. TDMA scheduling is mostly preferred because of its inherent energy conservation property.

4. Data Aggregation

Data aggregation is one of the techniques which reduce energy consumption in WSN. In WSN, thousands of nodes are deployed, thus data sensed by these nodes are highly correlated. Data aggregation reduces the redundant data before transmission. Thus transmission of redundant data is eliminated which reduces the energy consumption because only actual data utilizes the energy in the network.

Cluster based approach is used for data aggregation process. Nodes are divided into clusters where one node is selected as cluster head (CH). The nodes within same cluster send their data to CH node which in turn sends to base station. The residual energy of CH node is monitored periodically, if residual energy reaches below threshold level, then node with next highest energy within same cluster is chosen as new CH node.

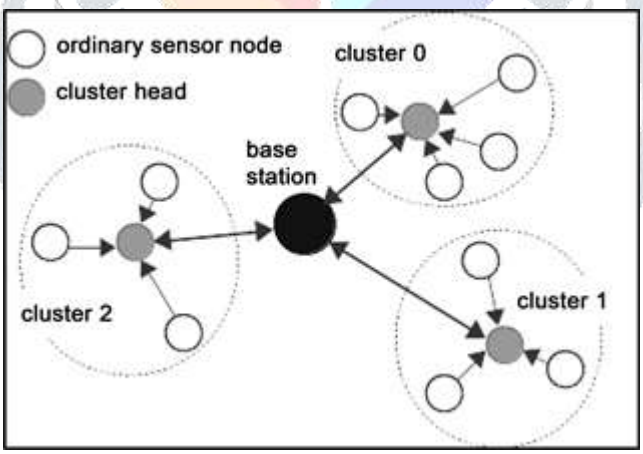

Fig.2. Depicts the Clustered WSN with CH in each cluster

III. DIFFERENT MALICIOUS NODE DETECTION TECHNIQUES

Malicious node attack occurs in the application layer of the network. There are basically two methods to detect the malicious nodes in the network. First method is based on trust model and second method is based on WSNs protocol. Trust model is the commonly used method for malicious node detection.

1.Neighbor weight Trust Determination Scheme

In any network, trust is the degree or level of confidence that a node can have on another node. Trust is a combined characteristics model enables security, reliability, privacy with respect to mobility. Neighbor weight trust determination (NWTD) algorithm [2] periodically updates the trust degree of the nodes and sets the minimum threshold for acceptance of the nodes.

2.Trust scheme based on D-S evidence theory and trust levels

D-S (Dempster-Shafer) evidence theory considers both indirect and direct trust of third part nodes[3]. Trust model is also based on calculation of Trust degree, direct and indirect trust levels with considerable internal attacks in WSN. This scheme effectively distinguishes the malicious nodes to provide security and reliability of the network by periodically updating the trust degree and also ensures reduced energy consumption. Reputation based model presents the indirect credibility of third party nodes and reputation distribution by integrating the trust values to isolate the malicious nodes in the network.

3. Protocol based detection scheme.

Enhanced leach protocol[4][5] can reduce the energy consumption and detect the malicious nodes in WSN. Detection scheme is based on sender to receiver ratio check. If the packet sends from neighboring nodes to CH is not equal to packets received rate at the base station, then node is marked as suspicious/malicious node.

Received signal strength indicator (RSSI) scheme[6] uses probabilistic method by considering shadowing and fading effects to detect the malicious nodes.

4. Based on Blockchain Technology

Blockchain[7] is a growing list of records called blocks which are linked using cryptography. Each block contains cryptographic hash of previous block, timestamp, and data. Blockchain is resistant to modification of data. It is a ledger that record transactions between two parties in a efficient way.

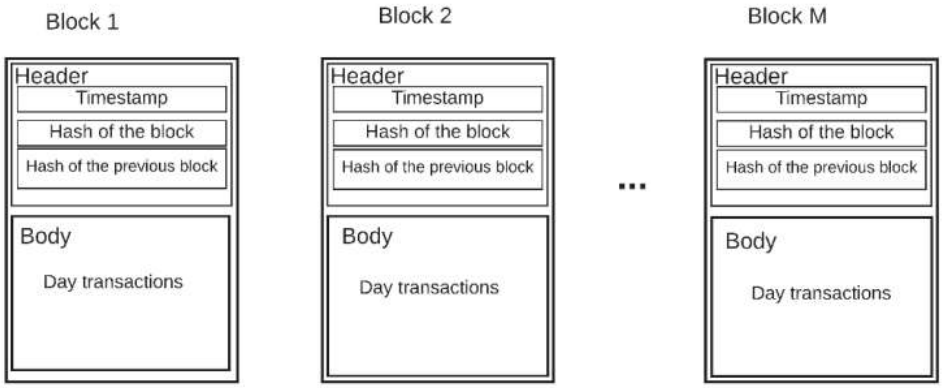

Fig.3. Block diagram of Block chain Technology

Block chain based trust model (BTM)[8] divides the wireless sensor network into base station, sensors and sink nodes. BTM uses eight parameters such as base station, sink node, sensor, malicious node detection block chain, smart contract of malicious node detection block chain, mapping from sensor and sink node to malicious node detection block chain.

Data structure[8] can be used for malicious node detection which has two parts – Block header and Block body. Header consists of Hash value of previous block which meets the integrity of malicious node detection block chain. Body contains information such as location, ID, state, delayed transmission, forwarding rate, response time, number of successful communication and number of failed communication. This information along with hash value of previous block is used to detect and isolate the malicious nodes in WSN.

IV. CONCLUSION

We have discussed different energy saving schemes and malicious node detection schemes to reduce energy consumption to improve lifetime of WSN and to secure WSN thereby throughput is improved. One can propose an algorithm using hybrid energy conservation schemes and malicious node detection schemes by combining more than one energy saving and malicious node detection scheme respectively.

REFERENCES

[1] S. M. Chowdhury and A. Hossain, “Different Energy Saving Schemes in Wireless Sensor Networks: A Survey,” *Wirel. Pers. Commun.*, no. 0123456789, 2020, doi: 10.1007/s11277-020-07461-5.

[2] F. Zawaideh, M. Salamah, and H. Al-Bahadili, “A fair trust-based malicious node detection and isolation scheme for WSNs,” *Proc. 2nd Int. Conf. Appl. Inf. Technol. Dev. Renew. Energy Process. Syst. IT-DREPS 2017*, vol. 2018-Janua, pp.

1–6, 2018, doi: 10.1109/IT-DREPS.2017.8277813.

[3] W. Zhang, S. Zhu, J. Tang, and N. Xiong, "A novel trust management scheme based on Dempster–Shafer evidence theory for malicious nodes detection in wireless sensor networks," *J. Supercomput.*, vol. 74, no. 4, pp. 1779–1801, 2018, doi: 10.1007/s11227-017-2150-3.

[4] S. Das and A. Das, "An algorithm to detect malicious nodes in wireless sensor network using enhanced LEACH protocol," *Conf. Proceeding - 2015 Int. Conf. Adv. Comput. Eng. Appl. ICACEA 2015*, pp. 875–881, 2015, doi: 10.1109/ICACEA.2015.7164828.

[5] M. Elshrkawey, S. M. Elsherif, and M. Elsayed Wahed, "An Enhancement Approach for Reducing the Energy Consumption in Wireless Sensor Networks," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 30, no. 2, pp. 259–267, 2018, doi: 10.1016/j.jksuci.2017.04.002.

[6] R. Goyat, G. Kumar, M. K. Rai, R. Saha, R. Thomas, and T. H. Kim, "Blockchain Powered Secure Range-Free Localization in Wireless Sensor Networks," *Arab. J. Sci. Eng.*, vol. 45, no. 8, pp. 6139–6155, 2020, doi: 10.1007/s13369-020-04493-8.

[7] A. E. Guerrero-Sanchez, E. A. Rivas-Araiza, J. L. Gonzalez-Cordoba, M. Toledano-Ayala, and A. Takacs, "Blockchain mechanism and symmetric encryption in a wireless sensor network," *Sensors (Switzerland)*, vol. 20, no. 10, 2020, doi: 10.3390/s20102798.

[8] W. She, Q. Liu, Z. Tian, J. Sen Chen, B. Wang, and W. Liu, "Blockchain trust model for malicious node detection in wireless sensor networks," *IEEE Access*, vol. 7, pp. 38947–38956, 2019, doi: 10.1109/ACCESS.2019.2902811.

[9] J. Chen, D. Zhang, J. Zhang, T. Zhang, H. Zhu, and J. Qiu, "New Approach of Energy-Efficient Hierarchical Clustering Based on Neighbor Rotation for RWSN," *IEEE Access*, vol. 8, pp. 123123–123134, 2020, doi: 10.1109/ACCESS.2020.3007478.

[10] R. Goyat, G. Kumar, M. K. Rai, R. Saha, R. Thomas, and T. H. Kim, "Blockchain Powered Secure Range-Free Localization in Wireless Sensor Networks," *Arab. J. Sci. Eng.*, vol. 45, no. 8, pp. 6139–6155, 2020, doi: 10.1007/s13369-020-04493-8.

[11] P. Taylor, S. O. Amara, R. Beghdad, and M. Oussalah, "Securing Wireless Sensor Networks : A Survey SECURING WIRELESS SENSOR NETWORKS : A SURVEY," no. April, pp. 37–41, 2013.

[12] P. Padmaja and G. V. Marutheswar, "Detection of milicious node in wireless sensor networks," *2017 Int. Conf. Comput. Commun. Informatics, ICCCI 2017*, pp. 1–6, 2017, doi: 10.1109/ICCCI.2017.8117758.

[13] R. E. Mohamed, A. I. Saleh, M. Abdelrazzak, and A. S. Samra, "Survey on Wireless Sensor Network Applications and Energy Efficient Routing Protocols," *Wirel. Pers. Commun.*, vol. 101, no. 2, pp. 1019–1055, 2018, doi: 10.1007/s11277-018-5747-9.