International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 04 | Apr 2019 www.irjet.net p-ISSN: 2395-0072

Energy Efficient Secure Communication In Wireless Sensor Networks: A Survey

Anu M R[1], SumiMol L[2]

[1]*Anu M R, M.Tech Student, Department of Computer Science and Engineering, LBS Institute Of technology For Women, Kerala, India*
[2]*SumiMol L, Assistant Professor, Department of Computer Science and Engineering, LBS Institute Of technology For Women, Kerala, India*

Abstract - *Sensors are most important components used in various electronic devices. Sensors are of tiny size so the power capacity is limited and the network life time is also very less. Wireless sensor networks consist of sensor nodes with sensing and communication capabilities. Sensor nodes are generally battery-powered devices. The critical aspect is to reduce the energy consumption of nodes, so that the network lifetime can be improved to reasonable times. In military applications, it is very difficult to replace or recharge the battery. Therefore, some energy consumption schemes are needed to extend the network lifetime. In this paper, it describes the various energy efficient techniques, security considerations and security methods in WSNs . To minimize the energy consumption in sensor networks various energy efficient routing protocols and data gathering methods were used.*

Key Words: **WSNs, Energy Efficient, Secure Communication, Network Lifetime, Sensor Nodes**

1.INTRODUCTION

In the technology era, there is a rapid growth in WSNs during the last two decades. The WSN consist of small sensor nodes which are composed of some integrated capabilities for data sensing, gathering, processing, but they have limited storage space. The sensor nodes have the platform for monitoring and sensing the network and the platform is battery dependent. The cost and size of a sensor nodes depends on the resources such as energy, memory, computational speed and bandwidth for communication.

The most crucial thing in sensor node is the battery drainage. Especially, in the applications like battle field, the node deployment and replacement is very difficult. So energy efficiency must maintained in such cases. The nodes that completely drains out the battery power are called dead nodes. Lots of research works are going based on how to improve the energy efficiency in WSNs. The researchers introduce different methods for the improvement of network lifetime. The performance and the network lifetime of WSN depends on the reliable transmission, energy consumption etc.

The inefficient transmission leads to data loss or packet drop and the network has to retransmit the same data until a successful transmission completes, thus it leads to bandwidth wastage in the network. Under such situation, WSN requires some fault tolerance and security mechanism against any data dissemination and eavesdropping. The well skilled use of wireless sensor network and computer adaptor may provide a way for eavesdropper in the network for attack. This is the reason that cause re-transmission of data packet and causes consumption of more energy. Thus, QoS delivery will be violated in such network. To overcome such issues, advanced security must be provided with the routing protocol. Several methods are introduce for secure data communication in WSNs. The survey paper describes the literature review on several secure routing protocols and energy efficient techniques which gives better throughput and increases the network lifetime in WSNs.

1.1 Limitations In WSNs

Wireless Sensor Networks are composed of small independent sensor nodes. The sensor nodes have limited processing power, energy, communication bandwidth and storage. The WSN challenges are follows:

1) Resource Utilization Issues: The main issue in WSN is the bandwidth consumption. Since, nodes are powered with battery, energy consumption must maintained in WSNs. To balanced consumption of energy in sensor nodes many solutions were introduced such as topology control, mobile relay nodes, deployment optimization and data aggregation.

2) Network Lifespan Issues: In WSNs, the sensor node is battery powered. Thus, the sensor nodes cannot survive for long period. Sensors nodes are scalable enough to adapt the topology and the density of node changes. Since the sensor nodes are heterogeneous in nature and thus, the devices heterogeneity is a major factor in network lifespan.

3) Critical Resource Use Issues: Accuracy and Timeliness are the main critical resource use issues in WSNs. Accuracy refers to providing security for the collected data while Timeliness refers to gathering data in the specified time period.

1.2 Security Requirements in WSNs

The important security needs in WSNs are briefly described below:

1) Data Integrity: In WSN, the data received at the receiver must be same as the data transmitted from the sender, for that data integrity must be maintained during transmission. Data integrity ensures that the data transmitted over the network were not manipulated by any venomous node. Data integrity prevents the unintentional changes to the information. During the case of data transmission between the neighbouring nodes, even in the absence of venomous nodes the probability of data modification cannot be avoided. In such cases, persuading data integrity become inexorable by extending the medium access control (MAC) of the protocol stack.

2) Data Confidentiality: In WSN, a node should not reveal any noteworthy data to neighbouring nodes. In such cases, the data confidentiality must be maintained. Data confidentiality is regarded as protecting against the unlawful, unintentional, or unauthorized access, theft or disclosure. In vital WSN routing protocol, symmetric encryption with a secret key requisite is preferred to attain data confidentiality.

3) Data Authentication: In WSN, between source and destination impeccable data exchange take place across the network. Here, the probability of data exchange with unaccredited nodes must be avoided. Data Authentication persuade receiver and transmitter that the data transmitted reaches to the authenticated receiver.

4) Accessibility: Accessibility indicates of providing WSN services in the case of Denial of Service (DoS) attacks. DoS attack force the network to experience the retransmission and hence leads to battery depletion. Thus network lifetime reduces significantly. Redundancy of sensor networks are taken into consideration to provide accessibility in sensor networks.

2. Energy Efficiency And Security Methods

In [1], the author proposed an Improved Distributed Energy Efficient Clustering (I-DEEC) scheme is introduced for extending the life of a sensor node. This is scheme is compared with DEEC and EESAA. DEEC (Distributed Energy Efficient Clustering) protocol is used to select cluster heads based on remaining power and estimates the network lifetime for enhancing. EESAA (Energy Efficient Sleep Awake Aware) protocol reduces the utilization of energy and provides the stability in network lifetime and works on pairing where neighbouring nodes makes the pair for data transmission and further communication. The proposed scheme I-DEEC implement to develop the energy function in existing protocol DEEC which finds the optimal path from sender to receiver.

In [2], the author developed an energy conservation solution for both routing layer and MAC layer protocols. First, they go for the designing of routing protocol which is based on the existing IECBR (Improved Energy Efficient Chain Based Routing) scheme. In this scheme, HBO (Honey Bee Optimization) technique is utilized for optimally selecting the nodes. To improve the energy efficiency, they modify the MAC protocol based on the dynamic back off algorithm called improved sensor MAC (IS-MAC). Here, contention window (CW) adjusted dynamically in the MAC protocol to achieve energy efficiency by handling the network load effectively .

In [3], the author proposed an energy efficient multihop transmission strategy in WSN. The paper present a system model for their network. The system model consist of multihop clusters of nodes and each cluster consist of N sensor nodes. The sensor node detection of the information in and around the monitoring area, after that transmit it to the cluster head which then deliver to the cluster head which in turn delivers to the centre of maintenance in order to take the appropriate intervention. The main objective is to define a new energy efficient transmission technique that allows to reduce the energy consumption for extending the lifetime of WSNs. Here, they assume that the transmitting signal is correctly received only if the signal to noise ratio (SNR) at the receiver is above the threshold. Each cluster consist of one source node, one destination node (CH) and N-2 relays. The relays that are selected are those that has least transmit power while maintaining SNR that is equal to the threshold. Thus it can be seen that the proposed scheme reduce the power consumption while comparing with the direct transmission and the transmission with a single relay.

In [4], the author refer some already existing routing protocol that work to achieve efficient routing along with some optimizing techniques such as ACO (Ant Colony Optimization), ABC (Ant Been Colony, HBO (Honey Bee Optimization). But these techniques failed to satisfy the WSN requirements like energy efficiency and monitoring the performance of network under different conditions. Here in this paper author proposed a novel routing protocol based on existing IECBR (Improved Energy Efficient Chain Based Routing). IECBR uses HBO method for optimum node selection. The HBO approach is modified with autonomous localization which is based on eligible energetic selection algorithm which ensure that no empty node in the network are out of the energy beyond their threshold, the strength of a node in the shortest path has reached its threshold. Thus the new routing protocol is known as Modified HIECBR (MH-IECBR). The result shows that the proposed scheme enhances the performance of network lifetime while compared with state of art methods.

In [5], the research is focused on network topology control which facilitate each node with an efficient power transmission to improve the network lifetime and enhance the network connectivity. The objective of WSN topology control is to plan the positioning of the nodes for the purpose of reducing the nodes transmission interference and increases the throughput for WSN communication.

In [6], the Virtual Grid Based Dynamic Routes Adjustment (VGDRA) scheme is introduced. VGDRA enhances the total performance of wireless sensor networks. The proposed scheme is dynamic approach instead of static, it can balance the load and the optimization creates much better result in minimum number of loops which are not possible in any other techniques. Thus, the proposed scheme is provides better energy efficiency when compared to LEACH approach.

In [7], according to the optimization technique called the Ant Colony Optimization (ACO) in which it shows the energy efficiency improvement in WSN, the author motivated for introducing the modified ACO based routing scheme. The goal of this modified ACO approach is to maximize the lifetime of the network in WSN and also improving the energy efficiency. The proposed scheme is based on two conditions, one is for finding the maximum disjoint connective covers, for satisfying the network connectivity and sensing coverage requirements. Through this way it can solve the searching and network connectivity problem. Thus it can improves the energy efficiency using ACO. Another condition is using the optimum path selection for data transmission considering the energy of sensor nodes as the constraint based on the set of rules that are predefined . Thus, it enhances the network lifetime of WSNs.

In [8], the paper demonstrate the security scheme and energy efficiency as the contradiction of power draining occurrence. The paper proposed a Two Tier Energy Efficient Secure Scheme (TE2S) in MAC protocol that is used for energy efficiency and security. The TE2S scheme consist of two tiers that is tier1and tier2 where tier1 is the sender initiated and tier2 is the receiver initiated scheme respectively. The scheme aims at protecting the WSN by preventing the sleep effect. In order to reducing the effect of power draining the proposed scheme decreases the authenticating procedure.

In [9], the paper presents various efficient routing protocols and data collection approaches to minimize the energy consumption in the networks. The paper also present the limitations of WSNs and various routing challenges. The paper provide a detailed study of four types of routing protocols that are hierarchical, info-centric, location-based and multi-path based routing.

In [10], the paper proposed a secure and energy efficient method of optimization using Dij-Huff Method (DHM). DHM is the combination of Dijkstra's algorithm and Huffman coding. The node with maximum energy take part in the data transfer process from source to destination. When the node have same energies Dijkstra's algorithm is used to select the proper node. The Binary Hop Count (BHC) security is used to provide security at each intermediate node. To prevent the malicious , black-hole and other type of attacks in the network , an end to end authentication is provided by developing a security code using Huffman coding. The proposed technique is used to avoid the network break down and to distribute the packet load according to the energies at the node. Thus the research shows that the proposed scheme minimize the delay, packet loss and improves the life span of the network.

In [11], to increase the network lifetime by consuming less energy, the paper introduced an intra and inter cluster head selection method. The author introduce an elliptic curve cryptography to achieve security at the cluster head level. The proposed scheme is developed based on the existing protocol like LEACH-C and LEACH. The proposed scheme performance is measured by considering the number of sensor node alive, the average energy dissipation and the packet delivery ratio.

In [12], the author implement an energy efficient clustering scheme along with collection of data to minimize the bandwidth requirement so that the network lifetime increases. The proposed scheme has two phases. In phase 1, the clustering is done by computing the potential score by the sensor nodes based on the density, mobility pattern and the available energy in the disseminated manner. Using the potential score, each sensor nodes decide who will become the next cluster head. In phase 2, the node having highest potential score is chosen as the next cluster head by every node. The data are collected at the cluster head from all the cluster member for encryption and aggregation, from there the collected data are transmitted to the base station. The paper shows that the proposed algorithm has lesser energy consumption, better packet delivery ratio with less packet drop, better throughput and also provide better security when compared with the LEACH.

In [13], the data aggregation technique is used in this paper for prevention technique and detecting attack. The system use an aggregator node (AN) for collecting data from cluster head. In case the cluster head itself being the attacker, the data from all the cluster members are recovered by the Aggregated Node (AN). Thus, energy wastage and packet drop ratio can be minimized. The paper uses an Iterative Filtering (IF) algorithm, which provides a trust evaluation to different sources. IF algorithm is used to detect the collusion attack and simple attack on nodes. When data is received from all the cluster members, system checks the truthfulness on the cluster head. For checking the integrating SHA1 algorithm is also used. Thus the proposed scheme provides better energy utilization, security and memory management along with attack detection on cluster head.

In [14], the author introduce symmetric key cryptography method for secure and energy efficient

communication between pairs of sensor nodes which provides integrity and authenticity of messages. An ECC-based public key cryptography is used to find each nodes uniquely so that to provide initial symmetric keys between the pair of nodes. In the proposed system a key generation technique is also introduced to minimize the frequency of key renewals. For minimizing the energy consumption symmetric key-based Deffie-Hellman key renewal scheme is used. In the case of key renewal the proposed scheme is compared with the basic secure communication that uses ECC-based public key cryptography.

In [15], a multi user broadcast scheme is introduced which is based on node ID along with ECC for decryption/encryption. Through signature verification mechanism using ECC the proposed scheme prevents the bogus information injection attack during broadcast of message. Using Zig Bee MAC standard 802.15.4 at mac layer, the energy efficiency is achieved. The standard ensures the low power communication in WSN. The proposed scheme provide better performance when compared with the existing system BASIS.

3. CONCLUSIONS

In this survey paper, we have studied various energy efficient security technique in WSNs. To protect the information that are transmitted by the sensor node is a challenging task due to scarce resources and the hostile environments. With several energy efficient methods and various security techniques, the network lifetime and throughput has been increased as well, but the problem of prolonging the network lifetime has not been solved completely. In future, we can find many security mechanisms and energy efficient techniques in WSNs.

REFERENCES

[1] Omkar Singh, Vinay Rishiwal, Mano Yadav.Energy Efficient Routing Scheme for Enhancing Lifetime in Wireless Sensor Networks, IEEE 2018.

[2] Deepshikha Sharma, Prof. Sukanya Kulkarni. Hybrid Technique for Improving the Network Lifetime of Wireless Sensor Networks, IEEE 2018.

[3] Maha Abderrahim, Hela Hakim, Hatem Boujemaa, Raed al Hamad. Multihop Transmission Strategy to improve Energy Efficiency in WSNs, IEEE 2018.

[4] Deepshikha Sharma, Prof. Sukanya Kulkarni.Network Lifetime Enhancement using Improved Honey Bee Optimization based Routing Protocol for WSN,IEEE 2018.

[5] Mohd Zaki Shahbuddin, Halabi Hasbullah,Izzatdin A Aziz. Preliminary Framework of Topology Control Algorithm in WSN to Achieve Nodes Energy Efficiency, IEEE 2016.

[6] Navdeep Singh Randhawa, Mandeep Dhami.Reduction of Energy Consumption in WSN using Hybrid VGDRA Approach, IEEE 2018.

[7] Prof. P. H. Kulkarni, Ms. Dhanashri Kadam, Dr. P. Malathi.To maximize Energy Efficiency in WSN using ACO, IEEE 2017.

[8] Veena M Kanthi.Tees-Two-Tier Energy Efficient Secure Scheme For Increased Network Performance In Wireless Sensor Networks, IEEE 2016.

[9] Bharat Bhushan, Dr. G. Sahoo.A comprehensive survey of secure and energy efficient routing protocols and data collection approaches in wireless sensor networks, IEEE 2017.

[10] TURKI A. ALGHAMDI.Secure and Energy Efficient Path Optimization Technique in Wireless Sensor Networks Using DH Method, IEEE 2018.

[11] C. Deepa, B. Latha.An Energy Efficient Secure Routing (EESR) using Elliptic Curve Cryptography for Wireless Sensor Networks, IEEE 2018.

[12] Mohan B A, K R Dayananda, Dr. Saroja Devi H.Energy Efficient Clustering Scheme with secure data aggregation for mobile wireless sensor networks (EECSSDA), IEEE 2016.

[13] Rutuja Ashtikar, Deepali Javale, Sujata Wakchaure. Energy Efficient Secured Data Routing Through Aggregation Node in WSN ,IEEE 2017.

[14] Ravi Babu Gudivada, R. C. Hansdah.Energy Efficient Secure Communication in Wireless Sensor Networks, IEEE 2018.

[15] Siri Maidhili R, Dr Karthik GM.Energy Efficient and Secure MultiUser Broadcast Authentication Scheme in Wireless Sensor Networks, IEEE 2018.