Parul Arora el at. International Journal of Recent Research Aspects ISSN: 2349-7688, Vol. 3, Issue 3, September 2016, pp. 100-103

Efficiency Maximization in Sensor Networks: A Survey

Parul Arora[1], Vikas Malik[2]

[1]M.Tech Scholar, CSE Deptt, B.P.S. Mahila Vishwavidyalaya, Khanpur Kalan, Haryana

[2]Astt. Prof, CSE Deptt, B.P.S. Mahila Vishwavidyalaya, Khanpur Kalan, Haryana

Abstract: **wireless sensor network is fastly growing network used in surveillance, military, and other emergency applications. It provides a very fast and low cost data transmission, but due to battery constraint in sensor nodes used to collect or transmit the information, their use are limited. A great number of researchers are working to minimize the energy consumption but along with this security of protocol shouldn't be breached. At present TinyOS is used in the WSNs to transmit and receive data. In our paper we have collected various research papers of good journals which worked on data security protocol along with consideration of energy minimization. On the basis of which we suggested the future modifications, which will be discussed in revised version.**

Keywords: WSN, Efficiency

I. INTRODUCTION

Wireless Sensor Networks have emerged as an important new area in wireless technology. In the near future, the wireless sensor networks are expected to consist of thousands of inexpensive nodes, each having sensing capability with limited computational and communication power which enable us to deploy a large-scale sensor network. A wireless network consisting of tiny devices which monitor physical or environmental conditions such as temperature, pressure, motion or pollutants etc. at different areas. Such sensor networks are expected to be widely deployed in a vast variety of environments for commercial, civil, and military applications such as surveillance, vehicle tracking, climate and habitat monitoring, intelligence, medical, and acoustic data gathering. The key limitations of wireless sensor networks are the storage, power and processing. These limitations and the specific architecture of sensor nodes call for energy efficient and secure communication protocols. The feasibility of these inexpensive sensor networks is accelerated by the advances in MEMS (Micro Electromechanical Systems) technology, combined with low power, low cost digital signal processors (DSPs) and radio frequency (RF) circuits. They consists of a radio transceiver, microcontroller, power supply, and the actual sensor. The sensing circuitry measures ambient condition related to the environment surrounding the sensor and transforms them into an electric signal. Processing such a signal reveals some properties about objects located and/or events happening in the vicinity of the sensor. The sensor sends such collected data, usually via radio transmitter, to a command center (sink) either directly or through a data concentration center (a gateway). Normally sensor nodes are spatially distributed throughout the region which has to be monitored; they self-organize in to a network through wireless communication, and collaborate with each other to accomplish the common task.Basic features of sensor networks are self-organizing capabilities, dynamic network topology, limited power, node failures and mobility of nodes, short-range broadcast communication and multi-hop routing, and large scale of deployment . The strength of wireless sensor network lies in their flexibility and scalability. The capability of self-organize and wireless communication made them to be deployed in an ad-hoc fashion in remote or hazardous location without the need of any existing infrastructure. Through multi-hop communication a sensor node can communicate a faraway node in the network. This allows the addition of sensor nodes in the network to expand the monitored area and hence proves its scalability and flexibility property. The key challenge in sensor networks is to maximize the lifetime of sensor nodes due to the fact that it is not feasible to replace the batteries of thousands of sensor nodes. Therefore, computational operations of nodes and communication protocols must be made as energy efficient as possible. Among these protocols data transmission protocols have much more importance in terms of energy, Since the energy required for data transmission takes 70 % of the total energy consumption of a wireless sensor network.

To study this energy consumption cause and methods adopted by various researchers to reduce consumption, various research papers have been analyzed. Some of them are quoted here which considered the security of protocol too. There is always tradeoff requirement of energy and security in sensor network as various attacks can occur in network which steal or alter the information which can be very destructive in emergency or highly confidential information. We have considered papers from 2012-2104 so that familiarity with latest issues can be done.

II. PREVIOUS WORK

Roslin, S.E. [1] developed a hierarchical network for WSN using genetic algorithm. This network controls the network topology without affecting the network properties. The impact of network performance is studied for various network densities. From the quantitative analysis of the proposed methodologies on the N-tier architecture with various node densities, it has been proved that two tier architecture provides reduced energy consumption

compared to others. Hence a two tier WSN developed using GA can be implemented in any hazardous applications. Though genetic algorithm gives an optimized list of cluster heads, there are possibilities of local minima. This could be further improvised by simulated annealing which results in global minima.

A.S. Uma Maheswari [2] used a new method which is based on AHYMN approaches and genetic algorithm is represented to choose a cluster head in WSNs in dynamically. Therefore, it is quicker and also more accurate to detect the node with higher energy and to select the cluster head. Moreover, this network has used nodes with heterogeneous characteristics. Some of the advantageous of heterogeneous nodes are: the long lifetime of networks, increase in network's reliability and decrease in data transference delay.

Kiranpreet Kaur [3] proposed EDCHBO a cluster head selection algorithm for effective cluster head selection which is improvement of HBO algorithm. This algorithm considers the energy and distance factor as parameter to improve cluster head selection. The main goal of EDC-HBO is to enhance the network lifetime as well as to improve the power consumption of network. Simulation results show that EDC-HBO is more energy efficient than LEACH and UCR protocol. As the WSN has data redundancy, how to design and realize routing protocol with optimal data aggregation will be our future research work.

R.Aiyshwariya [4] introduced the hierarchical fuzzy integral into the scheme in order to make the most criteria that can influence energy efficiency become a single one to determine the selection of the CHs, which is the main innovation and improvement of the classical algorithms. Moreover, the new scheme supports data fusion at CHs, which can eliminate the redundant data effectively so as to reduce the traffic and save the energy and this FMPDM is cost wise beneficial than existing algorithms, The simulation results demonstrate that the lifetime and energy efficiency of FAHP is better than other classical algorithms, time synchrony and fault tolerant problems are overcomed by using FAHP process it also improves the localization accuracy and efficiency, Classifying FAHP with FMPDM it improves Consistency of Decision making and also improves the parameters energy ,lifetime and throughput will be efficient..It also improves Robustness.

Ebin Deni Raj [5] suggested new protocol EDRLEACH is based on clustering with maximum lifetime for wireless sensor networks. It improves LEACH by using a very equally distributed cluster and decreasing the unequal topology of the clusters. The new network protocol can be built on the shortcomings of Leach to try and rectify them.The applications of the new algorithm are immense as the life period has increased considerably.

Nabil Ali Alrajeh [6] analyzed that WSNs have special vulnerabilities that do not exist in wire-line networks. Therefore, our protocols can't be simply transferred for wire-line networks to WSNs. Protocols must be designed with low computational power and low energy requirements in mind. In this paper it has been seen some of the protocols that are used, as well as some ways to determine where to check packets, including a new game theoretic approach in which it has been observed that by allowing the attack to have some utility, author is able to increase through energy saving for sufficiently large, resource constrained networks.

Ajith Abraham [7] presented a survey paper which states while designing a security mechanism, we must consider the limited resources of WSNs. Anomaly-based IDSs are lightweight in nature; however they create more false alarms. Signature-based IDSs are suitable for relatively large-sized WSNs; however they have some overheads such as updating and inserting new signatures. Cross layer IDSs are usually not recommended for networks having resources limitations, as more energy and computation are required for exchanging multilayer parameters.

Ioannis Krontiris [8] proposed the development of an Intrusion Detection Program (IDP) which could detect known attack patterns. An IDP does not eliminate the use of any preventive mechanism but it works as the last defensive mechanism in securing the system. Three variants of genetic programming techniques namely Linear Genetic Programming (LGP), Multi-Expression Programming (MEP) and Gene Expression Programming (GEP) were evaluated to design IDP. Several indices are used for comparisons and a detailed analysis of MEP technique is provided. Empirical results reveal that genetic programming technique could play a major role in developing IDP, which are light weight and accurate when compared to some of the conventional intrusion detection systems based on machine learning paradigms.

Djallel Eddine Boubiche [9] considered the problem of cooperative intrusion detection in wireless sensor networks where the nodes are equipped with local detector modules and have to identify the intruder in a distributed fashion. The detector modules issue suspicions about an intrusion in the sensor's neighborhood. We formally define the problem of intrusion detection and identify necessary and sufficient conditions for its solvability. Based on these conditions we develop a generic algorithm for intrusion detection and present simulations and experiments which show the effectiveness of our approach.

Shio Kumar Singh [10] introduced a new intrusion detection system based on cross layer interaction between the network, Mac and physical layers. Indeed it addressed the problem of intrusion detection in a different way in which the concept of cross layer is widely used leading to the birth of a new type of IDS. The proposed is experimentally evaluated using the NS simulator to demonstrate its effectiveness in detecting different types of attacks at multiple layers of the OSI model.

A.Anbumozhi [11] illustrated MAC address based intruder tracking system for cluster based wireless sensor networks. This proposed system implements base station based detection and thus is very energy-efficient for early detection and prevention of security threats and attacks. Early detection and prevention of the intruder by efficient security system can prevent many problems like slowing down of the network, sending of fake data, etc. By designing a security system in which the Base Station (BS) keeps track of the security of the Wireless network, high

security can be ensured without any significant energy overheads on individual nodes and cluster heads.

J. R. S. CEng [12] proposed the Extended Kalman Filter (EKF) mechanism to filter the false data in sensor network. The false data can be acted by some event namely malicious, emergency event. Malicious event are acted by intruders, and Emergency event are acted by some accident occurrence eg. Fire. Intruders make the sensors to get the false reading therefore EKF mechanism is proposed. EKF monitors the behaviour of neighbours and predict their future states, each node aims at setting up normal range of the neighbor's future transmitted aggregated values. Using different aggregation functions (average, sum, max, and min), theoretical threshold value is calculated. Combining Cumulative Summation (CUSUM) and Generalized Likelihood Ratio (GLR) detection sensitivity can be increased. Intrusion Detection Modules (IDM) and System Monitoring Modules (SMM) work together in order to provide intrusion detection capabilities for WSNs. EKF address various uncertainties in WSNs and create an effective local detection mechanism.

Nabil Ali Alrajeh [13] proposed an Advanced Intrusion Detection System. It improves the detection rate and efficiency so that almost all the Intrusions can be detected. Also the system is applicable to small, medium as well as large sized networks. That means it gives a wide range of flexibility in detection of Intrusions compared to the other existing systems. Also the energy efficiency and the system life time is greatly improved.

Quazi Mamun [14] presented in detail a secure routing protocol for WSN which is based on ant colonization technique. Hello packets are used for surrounding neighbor's discovery. This mechanism uses forward ants which collect and increment the reputation values along the path. Similarly, destination node uses backward ants which carry information and instruction from destination node about route security. The proposed mechanism uses two paths for data forwarding not only to overcome the problem of node failure but also to increase the efficiency of overall network. When compared to other routing protocols such as iACO and LEACH, our proposed routing scheme shows better performance in terms of end to end delay, routing overheads, and data forwarding efficiency. Furthermore, the proposed mechanisms show high data delivery rate in the presence of malicious nodes.

III. CONCLUSION

Wireless network is always backed by the battery constraint. Each WSN node has a limited battery source and once it is exhausted, it has to be replaced to keep the node in function. A lot of researcher are working towards developing algorithm which reduces energy consumption while WSN communication and security mechanism. Due to challenges in this field we have selected this field for our research work. Recent papers are studied relevant to this work. We have observed that many researcher have worked towards the clustering of nodes using optimization algorithms. Some has used two tier network to reduce the energy consumption.

IV. REFERENCES

[1]. Roslin, S.E., "Genetic algorithm based cluster head optimization using topology control for hazardous environment using WSN," in *Innovations in Information, Embedded and Communication Systems (ICIIECS), 2015 International Conference on* , vol., no., pp.1-7, 19-20 March 2015

[2]. A.S. Uma maheswari, Mrs. S. Pushpalatha," Cluster Head Selection Based On Genetic Algorithm Using AHYMN Approaches in WSN", International Journal of Innovative Research in Science, Engineering and Technology Volume 3, Special Issue 3, March 2014

[3]. Kiranpreet Kaur1, Harjit Singh," Cluster Head Selection using Honey Bee Optimization in Wireless Sensor Network" International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 5, May 2015

[4]. R.Aiyshwariya Devi,M.Buvana," Energy Efficient Cluster Head Selection Scheme Based On FMPDM for MANETs" International Journal of Innovative Research in Science, Engineering and Technology Volume 3, Special Issue 3, March 2014

[5]. Ebin Deni Raj," An Efficient Cluster Head Selection Algorithm for Wireless Sensor Networks –Edrleach", IOSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278-0661 Volume 2, Issue 2 (July-Aug. 2012)

[6]. Nabil Ali Alrajeh, S. Khan, and Bilal Shams," Intrusion Detection Systems in Wireless Sensor Networks: A Review" International Journal of Distributed Sensor Networks Volume 2013.

[7]. Ajith Abraham, Crina Grosan, and Carlos Martin-Vide," Evolutionary Design of Intrusion DetectionPrograms" International Journal of Network Security, Vol.4, No.3, 2007

[8]. Ioannis Krontiris, Zinaida Benenson, Thanassis Giannetsos, Felix C Freiling, Tassos Dimitriou," Cooperative Intrusion Detection in Wireless Sensor Networks", Wireless sensor networks, Springer Berlin Heidelberg,2009

[9]. Djallel Eddine Boubiche and Azeddine Bilami," Cross Layer Intrusion Detection System For Wireless Sensor Network" International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012.

[10]. Shio Kumar Singh, M P Singh, and D K Singh," Intrusion Detection Based Security Solution for Cluster-Based Wireless Sensor Networks" International Journal of Advanced Science and Technology Vol. 30, May, 2011

[11]. A.Anbumozhi, K.Muneeswaran," Detection of Intruders in Wireless Sensor Networks Using

Anomaly" IJIRSET Volume 3, Special Issue 3, March 2014

[12]. Joseph Rish Simenthy CEng , AMIE, K. Vijayan," Advanced Intrusion Detection System for Wireless Sensor Networks" IJAREEIE Vol. 3, Special Issue 3, April 2014

[13]. Nabil Ali Alrajeh,Mohamad Souheil Alabed, andMohamed Shaaban Elwahiby," Secure Ant-Based Routing Protocol for Wireless Sensor Network" International Journal of Distributed Sensor Networks Volume 2013

[14]. Quazi Mamun, Rafiqul Islam, and Mohammed Kaosar," Anomaly Detection in Wireless Sensor Network" Journal Of Networks, Vol. 9, No. 11, November 2014

