A Survey on Energy Efficient Routing Techniques and Security Measures in Wireless Sensor Network

Rajdip Paul
B.Tech 3rd Sem, CTIS
Assam down town University
rajdippaul005@gmail.com

Banani Das
Asst. Professor, CSE
Assam down town University
banani.das.bd@gmail.com

ABSTRACT

The development in technology has resulted in development of tiny, less expensive, low power consuming and multifunctional sensor nodes in wireless sensor networksThe concept of “3 any” is implemented here. By “3 any” we mean any person, anywhere and anytime.The factors affecting the design of these nodes are scalability, energy consumption, environment etc.The nodes perform activities like sensing, processing and communication. The maximum power consumption is done by communication process.Conserving energy is thus a dominant factor in WSN. The routing strategy is very important for proper delivery of packets. This paper presents a survey on different energy efficient routing protocols along with security measures to improve security of nodes in wireless sensor networks and aims to design protocols that needs less energy consumption during communication.

Keywords

Wireless Sensor Network(WSN),Mobile Wireless Sensor Network (MWSN), Energy Efficiency, Security.

1. INTRODUCTION

1.1. Wireless Sensor Networks

The availability of low cost, low power transmitters has resulted a lot of research interest towards WSN. Ultra small sensor nodes can be created/fabricated and deployed over a wide area in a feasible way.The nodes are nothing but radio enabled nodes with simple transducers connected to a microcontroller. Wireless sensor network consists of a large number of sensor nodes deployed densely over a large physical area or an area close to it. Radio frequency channels and wireless links are used by the channels to communicate. Once any event is detected by this nodes they need to communicate it to the gateways or users who tap into the network. To create this network multi-hop routes are used through other devices.

MWSN(Mobile Wireless Sensor Network)is a type of WSN where all the sensor nodes are mobile. The matter of concern with MWSNs is routing protocol. Mobility of nodes results in problems for routing protocols as they do not have any fixed path from source to destination. This results in concerns for the power unit. Algorithms and protocols that give maximum output with limited power resources should be designed. The rest of the paper is organized as follows:

A survey of energy efficient routing protocols is provided in Section 2. Then the Section 3 discussed about the secured routing protocols. And Section 4 will conclude the paper.

1.2. Sensor Architecture

Tiny devices called sensors monitor conditions like temperature, humidity, pressure and are later convert them to electrical signals. The communication is either directly between the sensor and base system or among the sensors. Program-able sensor nodes are used by WSN to monitor various parameters of the environment. Sink node, Sensor node, target node are the three essential parts of the sensor networks. Sensor nodes are the backbone of the whole network which are responsible for dataacquisition, processing and transmission.The sink node has great impact on lifetime and energy consumption of WSN as the collected data is forwarded to the sink node. The primary idea of sensor networks is to distributethe small sensing devices, which are capable of sensing some changes in incidents/parameters and communicate with other devices, over a fixed/defined geographic area for some specific purposes such as tracking a target, monitoring environment, surveillance. In order to increase the lifetime of the network it is very important to make efficient use of sensor’s energy since the sensors operate on battery power. Most of the sensor’s energy is consumed in data packet transmission of sensor or relaying packets of other sensors., so it is important to find paths from sensor to a destination

Communication Architecture

WSN communication structure consists of sensor nodes scattered in a specificgeographical area with each of these nodes being capable of collecting and routing data back to the sink or the end users as shown in Figure 1. Communication protocol has five standard layers, which areapplication layer,transport layer, network layer,data link layer,physical layer.

It has three management planes: i) power management plane, ii) mobility management plane and iii) task management plane. The hardware architecture shown in Figure 2 consists of four components: i) Sensing, ii) Processing, iii) Transmitter/Receiver iv) Power Unit. Depending on the applications they may also have a location finding system and a mobilizer. As an external power supplier a power generator may be present. The major concern of scientists and researchers is the power unit. Algorithms and protocols that make maximum output with limited power resources should be designedto optimize the life time of a node.

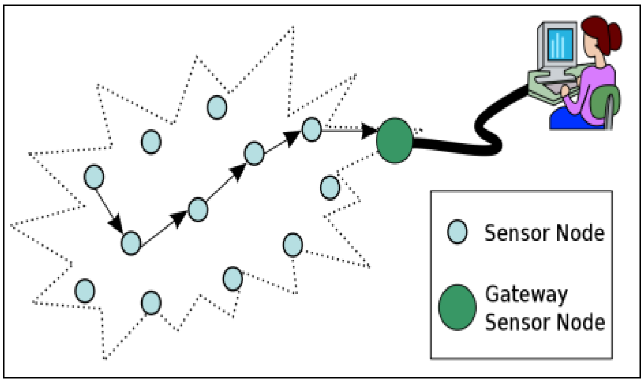

Figure 1:Communication Architecture

2. ENERGY EFFICIENT ROUTING TECHNIQUES IN WIRELESS SENSOR NETWORKS

Sensor nodes have limited energy and bandwidth. The main aim of network layeris to find different ways for energy efficient route setup as well as relaying of data reliably from sensor nodes to sink in order to maximize the lifetime. A prudent issue in WSNs is selection of a proper routing method. Providing survivability of network, availability and service are the main goals of all routing protocols also sensor network lifetime enhancement; complexity reduction; efficient controlling of energy consumption ; reducing delay of data transfer and improving WSN performance. To increase the lifetime of the network, it is very important to make efficient use of the energy of sensors. As a result it is very important to determine an optimal transmission path from its sensor to the destination.

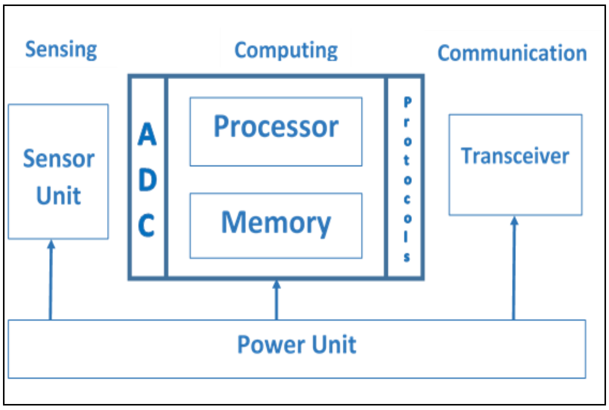

Figure 2: Hardware Architecture

Few of the most popular energy efficient routing techniques for WSNs are summarized in Table1 and the methods are briefly discussed as follows:

- The paper [1] has argued that optimal routing in sensor networks is infeasible. C.Schurgers and M.B. Srivastava have proposed a practical guideline that advocates a uniform resource utilization, which can be visualized by the energy histogram. The authors acknowledge however that this is only a first cut at tackling this complicated issue. It also proposes a number of practical algorithms that are inspired by this concept. The Data Combining Entity (DCE) combining scheme reduces the overall energy, while the spreading approaches aim at distributing the traffic in a more balanced way.
- Tom Hayes and Falah H.Ali, [2]proposedlocation aware sensor routing protocol (LASeR)in MWSNs, which uses locationinformation to maintain a gradient field even in highly mobile environments, while reducing the routing overhead.
- M. Kalantari and M. Shayman[3] gives a survey about wireless sensor networks, techniques of routing, the hierarchical architecture in wireless sensor networks and provides a brief introduction on harvesting ambient energy from the environment to power WSNs.
- M. M Warrier and Ajay Kumar in[4] provide a survey on wireless sensor networks, routing techniques, the hierarchical architecture in wireless sensor networks and ambient energy to power the nodes.
- In [5], G. Kaur presents a review on reliability of WSNs. Because of its special features WSN has attracted many concerns in different domains.

However improvement of the reliability of WSN is one of the essential challenges for WSN from theoretical research to actual application. An important facet of dependability and quality of service in wireless sensor network is reliable data transport. This paper discusses various techniques proposed for minimizing the energy consumption. This is done primarily to give an overview of the various techniques known today for reliable data transport problem and for minimizing the energy consumption in wireless sensor networks.

Table 1: Techniques for Energy Efficient Routing

Paper name	Objectives / Goals	Approaches / Findings
Energy efficient routing in wireless sensor networks [1]	This paper focuses on energy efficient routing as traditional routing protocols do not take into account the fact that a node contains only a limited energy supply.	This paper proposes two options for localized algorithms to increase the sensor network lifetime: 1. Aggregating packet streams in a robust way, resulting in minimizing the energy consumption of transmissions. 2. Exploiting the multi-hop aspect of network communications to obtain more uniform resource utilization.
Location aware sensor routing protocol for mobile wireless sensor networks [2]	This paper presents a geographic routing protocol, LASeR which uses location awareness to maintain an up-to-date gradient metric in highly mobile environments.	• LASeRs outstanding results and robustness in a variety of scenarios suggest that the protocol may be suitable for a large number of applications. • It is evaluated on packet delivery ratio, end-to-end delay, overhead, throughput and energy consumption.
Energy efficient routing in wireless networks [3]	This paper introduces an approach for the purpose of routing in the sensor networks that gives energy efficiency, and increases the network life. It proposes an approach for the case in which many sensors need to collect data and send it to a central node.	• In this paper, the main idea is to find routes that use places of higher residual energy. • In this paper a set of partial differential equations similar to the Maxwell's equations in the theory of electrostatic is being solved to find the routes that give a considerable improvement in the network performance in terms of energy efficiency and the life of the sensors.
Energy efficient routing in wireless sensor networks: A Survey [4]	In this paper a brief introduction on harvesting ambient energy from the environment to power WSNs has been given.	This paper suggests that the method of harvesting ambient energy will nullify the power efficiency problems of WSN in future.
Review paper on reliability of wireless sensor networks [5]	In this paper, the various techniques proposed for minimizing the energy consumption have been discussed. This is done primarily to give an overview of the various techniques known today for reliable data transport problem and for minimizing the energy consumption in wireless sensor networks.	Poles apart WSN applications necessitate unusual positions of reliability. Communication protocols for WSN should be reliable and energy-efficient to keep away from unproductive stabbing of energy resources through minimization of control and retransmission overhead. In this paper, WSN reliability research fields are discussed.

3. SECURITY MEASURES IN WSN

The features of wireless sensor networks attracted many researchers to work on various issues related to these types of networks. However, while the routing strategies and wireless sensor network modeling are getting much preference, the security issues are yet to receive extensive focus.Table2 summarizes some of the proposed security technologies to solve the security issues with WSNs and the same are discussed here briefly.

- Many routing protocols for sensor network have been proposed till now, but none of them have been designed to deal with securityissues. C. Karl of and D.Wagne, in [6] propose security goals for routing in sensor networks.
- A. S. Khan Pathan, H.W. Lee and C.S. Hong in [7] intend to investigate the security related issues and challenges in WSNs. This paper identifies the security threats and reviews the security mechanisms for WSNs. It also discusses the holistic view of security for ensuring layered and robust security in WSNs.
- M.U. Aftab, O. Ashraf, M.Irfan, M.Majid, A. Nisar and M.A. Habib in[8] describe the types of WSNs and the possible solutions tomany problems pertaining to them.
- P. Sherubha and M.M Priya in [9], focuses on developing original and efficient prevention, discovery and response mechanisms that looks after DoS flooding difficulty before, after and also during a definite attack. Detailed examination on all these constraints using different methodology was made in this work to reveal the efficiency of the internet resources.

  N.A.Alrajeh, S.Khan and B. Shamsin[10], suggests that while designing a security mechanism, one must consider the limited resources of WSNs. The factors that make WSNs highly vulnerable to security attacks at various level are its distributed nature, multihop data forwarding, and open wireless medium. Intrusion Detection Systems (IDSs) plays an important role in detecting & preventing security attacks. This paper also presentsopen research problems related WSNsecurity.

Table 2: Techniques to Secure the Wireless Sensor Nodes

Paper name	Objectives / Goals	Conclusion
Secure Routing in wireless sensor networks: attacks and countermeasures [6]	This paper presents the security goals for routing in sensor networks. This also presents the way to adapt the attacks against ad-hoc and peer-to-peer networks into powerful attacks against sensor networks.	This paper demonstrates that currently proposed routing protocols for sensor networks are insecure and highlights an open problem for the future to design a sensor network routing protocol to satisfy proposed security goals.
Security in Wireless Sensor Networks: Issues and Challenges [7]	This paper discusses the threats to ensure layered and robust security in WSN and suggests that most security threats are caused due to insertion of false reports.	This paper suggests that though the security mechanisms are well-established for each individual layer, combining all the mechanisms together for making them work in collaboration with each other will incur a hard research challenge.
A review study of wireless sensor networks and its security [8]	This paper presents a study of WSNs and its security related issues. It describes the types of WNSs and then the possible solutions to deal with problems of WSNs.	WSNs have a variety of features and types that have many problems arising in different scenarios. The only solution is the selection of the right approach for getting the maximum benefit from the WSN and its types.
A detailed survey on security attacks on wireless sensor network and its communication [9]	The primary purpose of this research is to inspire the research community to develop original, efficient discovery& response mechanisms to address the DoS flooding difficulty before, during and after a definite attack.	In this paper, a trust based mechanism is given to repel against misbehavior in the network. In their future work, they will improve their proposed method by introducing other constraints for detecting DoS attacks.
Intrusion detection systems in wireless sensor networks: A Review [10]	Intrusion Detection Systems (IDSs) can play an important role in detecting and preventing security attacks. This paper focuses on current IDS and some open research problems of WSN security.	This paper suggests the use of different types of IDSs like: • Anomaly-based IDSs are lightweight in nature, however they create more false alarms. • Signature-based IDSs are suitable for relatively large sized WSNs, however these required some overheads such as updating and inserting new signatures. • Cross layer IDSs are usually not recommended for networks where resources are limited as more energy and computation is required for exchanging multilayer parameters.

4. CONCLUSION

This paper discusses various aspects of efficient routing. Along with efficient routing techniques, means to implement better security features in WSNs are also discussed. The objectives of various routing protocols for WSN and MWSN are analyzed and future works that are required to be done to improve the network performance are also highlighted.

5. REFERENCES

[1] C. Schurgers and M.B. Srivastava, “Energy efficient routing in wireless sensor networks”, MILCOM Proceedings Communications for Network-Centric Operations: Creating the Information Force, ISBN: 0-7803-7225-5, pp. 1-5, August 2002.

[2] T. Hayes and F.H. Ali, “Location aware sensor routing protocol for mobile wireless sensor networks”, IET Wireless Sensor System, ISSN 2043-6386, pp. 49-57, January 2016.

[3] M. Kalantari and M.Shayman, “Energy efficient routing in wireless networks”, CISS, pp. 1- 15, March 2004.

[4] N. A. Pantazis, S. A. Nikolidakis and D. D. Vergados, “Energy-Efficient Routing Protocols in Wireless Sensor Networks: A Survey”, *IEEE Communications Surveys & Tutorials,* pp. 551-591.

[5] G. Kaur, “Reliability of wireless sensor networks”, published in *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET),* vol. 3, pp. 1926-1928, May 2014.

[6] C. Karlof and D. Wagner, “Secure Routing in wireless sensor networks: attacks and counter-measures”, Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications, ISBN: 0-7803-7879-2, pp. 293-315, June 2003.

[7] A.S. Pathan, H.W. Lee, C.S. Hong, “Security in WSNs: Issues & Challenges”, pp. 1043-1048, ICACT2006, MIC and ITRC Project ISBN 89-5519-129-4, 20-22, February 2006.

[8] M.U.Aftab,O. Ashraf, M. Irfan et al., “A review study of wireless sensor networks and its security”, Communications and Network, SciRes, pp. 172-179, Oct. 2015.

[9] P. Sherubha and M.M Priya, “A detailed survey on security attacks on wireless sensor network and its communication”, *Int. Journal of Soft Computing,* vol.11, no. 3, pp. 221-226, ISSN: 1816-9503, 2016.

[10] N.A. Alrajeh, S. Khan, B. Shames, “IDS in Wireless detector networks: A Review”, Int. Journal of Distributed detector Network, pp. 1-7, April 2013.