International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Performance Analysis of Hierarchical Routing Protocols of Wireless Sensor Network: A Survey

Sunny Chaudhary

Department of CCE, Galgotias University, Uttar Pradesh, India

Abstract: ***Wireless sensor network (WSN) consists of small sensor nodes with sensing, computation and wireless communication capabilities. In this paper we discuss the important hierarchical routing protocols for Wireless Sensor Networks. We will discuss the operations of the protocols and advantages and disadvantages of these hierarchical routing protocols. The main issue of the wireless sensor network is energy consumption because there is limited battery power. If the battery goes down, then the sensor nodes die quickly. So to solve this problem there is come so many routing protocols which are used for solving this problem. There are a lot hierarchical routing protocols like LEACH, TEEN and PEGASIS.***

Keywords: wireless sensor network, security threats of wireless sensor network, hierarchical routing protocols, Leach, Teen, Pegasis, comparison of hierarchical routing protocols.

1. Introduction

The node can sense the information of temperature, pressure or other things which are around it and send this information through the wireless communication devices. The node communicates with all the nodes that are in the range of its wireless communication device. A source node generates the information and a sink node is a node that collects the whole information which are sent by the sensor nodes in network. Hierarchical routing protocols also called cluster-based routing protocols. Hierarchical routing protocol is the efficient routing protocol to minimum energy consumption in the clustering of the nodes and by performing the data aggregation and fusion to decrease the number of transmitted data packets which are being transferred from the sensor nodes to the base station or we can say the sink.

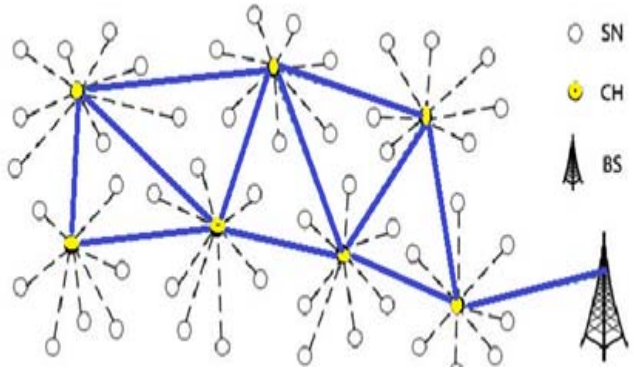


Figure 1: Structure of the wireless sensor network

2. Security Threats in Wireless Sensor Networks

Security in sensor networks is an important part such as the performance and low energy consumption in many applications. Since the wireless sensor network is unreliable in the nature because there are many security threats and issues which are faced in the communication of nodes during the transmission of the data packets. Security is not the separate department of the wireless sensor network or we can say that it is the inseparable part of any system. Security is such a state of the system that the system is being protected from the various attacks. So we attempt to highlight and discuss some threats and attacks in the following section and these threats are following below as:

2.1 Denial of Service

Denial of service attack is an attack that attempts to reduce the network's capability to perform its expected functions [4]. Dos attack just do the functions and services of the wireless sensor network unavailable to the users. It is very strong attack to deny the services of the system and very hard to stop this attack. It destroys the whole services of the nodes in wireless sensor network. It occurs in many layers of the wireless sensor network.

2.2 Attacks on Information in transit

This is also a threat that may occur into the wireless sensor network. This may occur when the information is transferred between the nodes and base station of the wsn. The information in transit may be altered, spoofed or we can say that it may be replayed again or vanished. Since the wireless communication is vulnerable to eavesdropping, so any attacker can control the traffic flow of the network and get into action to interrupt, intercept or modify the data packets thus and attacker can provide the wrong information to the base stations or sinks. Since sensor nodes have the short range of transmission, so the attacker could attack several sensors at the same time to modify the actual information during the data packets transmission [1].

2.3 Blackhole/Sinkhole Attack

In blackhole attack, a malicious node behaves as a blackhole to attract the traffic in wireless sensor network. In this attack, the attacker can listen the requests for routes and show to the target nodes that it has the high quality of service and shortest path to the base station. Once the malicious node has been able to insert itself between the sensor nodes then it can do anything with the data packets that are transmitting between nodes [1].

Licensed Under Creative Commons Attribution CC BY

2.4 Wormhole Attack

Wormhole attack is an attack in which the attacker records the data packets at one place in the network and tunnels those to the another place [1]. The retransmitting of packets may be done selectively. The wormhole attack is very difficult to detect in WSNs by using the routing protocols in which the routes are decided based on the advertised information such as minimum hop count to the sink. Wormhole attack can perform even at the starting state when sensors start to discover of their neighboring information. Wormhole attack may occur in two mode which are hidden mode and participation mode [3].

2.5 The Sybil attack

In Sybil attack, a single node presents multiple identities to other nodes in the network [2]. Sybil attack can perform for attacking the distributed storage, routing mechanism, data aggregation, voting, fair resource allocation. Basically, any peer-to-peer network is vulnerable to sybil attack However, detection of sybil nodes in a network is not so easy. Now there is used radio resource testing to detect the presence of sybil node in the wireless sensor network.

3. Hierarchical Routing Protocols

There are many existing hierarchical routing protocols but I am going to discuss some few hierarchical routing protocols which are following as below:

3.1 LEACH

LEACH stands for low energy adaptive clustering hierarchy routing protocol that is the first hierarchical routing protocol. In this protocol, the sensor nodes are organized themselves in the clustering form [5]. In LEACH routing protocol, the base station is stationary and located far from the sensor nodes. Nodes are homogeneous and energy constrained in this hierarchical routing protocol. In each cluster of the nodes, one node is known as cluster-head that acts like the local base station. LEACH is the clustering based routing protocol which minimizes the energy consumption in the wireless sensor networks. The main work of the LEACH protocol is to select the sensor nodes as cluster heads, so high energy consumption in communicating with the sink is spread to the all sensor nodes in the sensor network. The operation of LEACH is of two phases, the first phase is setup phase and second phase is steady phase. In setup phase, sensor node chooses a random number between 0 and 1. If this random number is less than the threshold T(n), then the sensor node becomes cluster head in the cluster. In the LEACH routing protocol, there is two phases which are following as below:

A. Setup phase:
1) for creating the network into the clusters of the sensor nodes.
2) Selection of the cluster heads.
3) Transmission schedule allocation to the sensor nodes [7].

B. Steady state phase:
4) The data aggregation in which data is collected on the clusters head.
5) Compression of the data packets that are transmitted from cluster head to the base station.
6) Transmission of the packets to the sink [9].

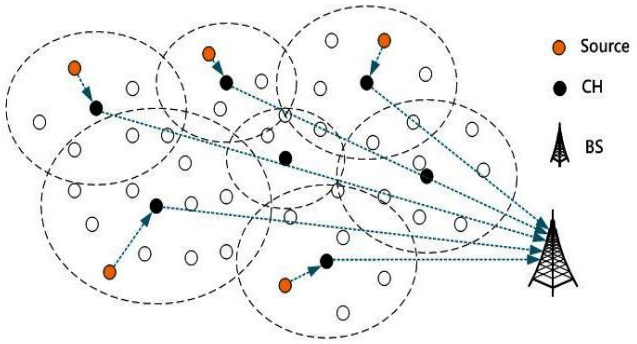


Figure 2: LEACH routing protocol architecture [7].

T (n) is calculated as:

$$T(n) = \frac{p}{1-p}[r \bmod(1/p)],\ n \in G = 0, \text{otherwise}$$

Figure 3: to calculate threshold [8].

Where P is the percentage to be a cluster head and r is the current round, and G is the set of nodes that did not being select as a cluster head in the last 1/P rounds. The cluster-heads make the schedules and send this information to all nodes in the clusters. All nodes send data to their respective cluster head nodes in the cluster, then the cluster-heads collects and send the data to the base station or sink

3.2 Power-Efficient Gathering in Sensor Information Systems (PEGASIS)

PEGASIS stands for Power-Efficient Gathering in Sensor Information Systems. PEGASIS is the extension form of the LEACH protocol [8]. In this protocol, there is formed the chains from one to another node in the network. That means each node send the data packets to its closest node and further this node will send the data packets to its neighbour and this process will continue. In this protocol, only one node will send the data to the base station finally which is near to the base station. PEGASIS routing protocol does not support to form the clusters. It assumes that all sensor nodes has the knowledge of the each node in the network by using the greedy algorithm. PEGASIS routing protocol increases the life time of wireless sensor network as compare to LEACH routing protocol. This routing protocol reduces the overhead and minimize the requirement of the bandwidth to transmit the data packets while in case of LEACH protocol, there is required the high bandwidth to transmit the data packets. Every Node uses the signal strength to know the distance to neighbour hood nodes in order to locate the closest nodes. After chain Formation, PEGASIS selects a leader from the chain in terms of residual energy in every round to be the one which will collect the data from the neighbours to be transmitted to the sink finally.

Licensed Under Creative Commons Attribution CC BY

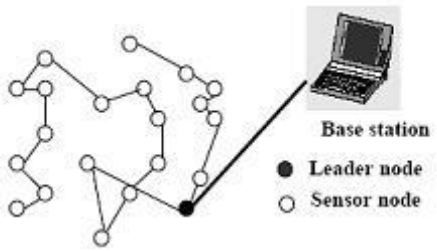


Figure 3: PEGASIS routing protocol architecture [6].

3.2.1 Drawback of PEGASIS routing protocol:

- In PEGASIS routing protocol, there is not considered the energy of the sensor node which is selected as leader to transmit the data packets to the sink. So this is the big drawback of the PEGASIS routing protocol.
- The second drawback of the PEGASIS routing protocol is that we don't consider the distance between the leader and the sink. So it can consume the total energy of the sensor node to transmit the data.
- Since there is only one leader which is transmitting the data, so it may be fail during the transmission of the packets and the data may be lost. So we can say that it is also the negative point of this protocol [10].

3.3 Threshold sensitive Energy Efficient sensor Network protocol (TEEN)

TEEN routing protocol is the hierarchical routing protocol which stands for Threshold Sensitive Energy Efficient Sensor Network protocol. TEEN protocol is used for the applications where the users can control the trade-off between the energy efficiency, data accuracy and response time. TEEN uses the data-centric method with hierarchical approach [8]. This protocol based on the strategy of LEACH routing protocol and it is used the LEACH strategy to form the clusters. TEEN protocol assumes that the base station and another sensor node in the network has the same level of the energy. This protocol assumes that sink can send the data packets directly to all the nodes.

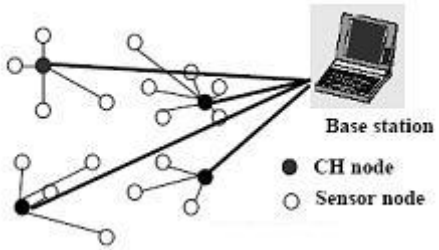


Figure 4: TEEN routing protocol [6]

There is two level which are formed between the sensor nodes and base station. In first level, the cluster head of sensor nodes are far away from the base station. But in second level, the cluster heads of sensor nodes are near to the base station. In this protocol, data is sent very less so the energy consumption is low as compare to another proactive routing protocols. In TEEN protocol, the cluster head sends two types of the threshold to its members of the cluster which are following as below:

- **Hard Threshold (Ht):** Hard threshold is for the value of the attributes which are being sensed by the sensor nodes. It is denoted by Ht.
- **Soft Threshold(St) :** Soft Threshold is denoted by St. it is sent by the cluster head of the nodes when there is occurred some kind of small change into the value of the attribute which signals to the node to activate the transmitter.

4. Comparison of hierarchical routing protocols

Table 1: Table for Existing Hierarchical Routing Protocols

Protocols	Energy efficiency	Data aggregation	Scalability	Power usage	Network life time	Multi -path
LEACH	yes	yes	Good	High	Less	No
TEEN	yes	yes	Good	High	High	No
PEGASIS	yes	no	Chains based	Max	High	No

5. Conclusion

Routing in the wireless sensor networks is the new area of research with a limited research area because there is the main problem related to the energy consumption but rapidly growing set of research results. In this paper, we presented a comprehensive survey of the hierarchical routing protocols in wireless sensor networks which have been presented in the literature. All these hierarchical routing protocols have the common objective of trying to extend the lifetime of the sensor network by reducing the energy consumption, so it is the challenging issue in wireless sensor network. Different hierarchical routing protocols have been proposed up till now to address this challenging issue. Clustering technique is one of them which is used to reduce the energy consumption by using the different routing protocols and this work is devoted to describe the efficiency of different clustering schemes. This comparison is based on the various parameters of these protocols. Each of this protocol is designed for the individual application. Some protocols work for a individual situation while other for different situations. So for the future perspective of this work may be well focused on modifying any of the above routing protocols such that the modified protocol may minimize the energy of the sensor networks. To reduce the energy consumption, we can use any hierarchical routing protocol but these routing protocols don't work in same condition. So to reduce the energy consumption in the wireless sensor network is the big challenge for us. Hierarchical routing protocols increase the scalability of the sensor network. The overall energy consumption of the nodes is reduced. The organization of the network into clusters tends itself to efficient data aggregation which gives the better utilization of the channel bandwidth to transfer the data packets.

References

[1] Security in Wireless Sensor Networks: Issues and Challenges Al-Sakib Khan Pathan Department of Computer Engg. Kyung Hee University, Korea spathan@networking.khu.ac.kr Hyung-Woo Lee Department of Software Hanshin University, Korea

Licensed Under Creative Commons Attribution CC BY

hwlee@hs.ac.kr Choong Seon Hong Department of Computer Engg. Kyung Hee University, Korea

[2] Security Threats in Wireless Sensor Networks Sushma1, Deepak Nandal2, Vikas Nandal3 1Asstt. Prof, HIT Asodha, (India) sushma21dalal@gmail.com 2Student, P.D.M. Bahadurgarh, (India) sinceredeepaknandal@yahoo.co.in 3Asstt. Prof, U.I.E.T. Rohtak, (India)nandalvikas@gmail.com

[3] The Wormhole Routing Attack in Wireless Sensor Networks (WSN) Lukman Sharif and Munir Ahmed.

[4] Security in Wireless Sensor Networks Jaydip Sen Department of Computer Science & Engineering, National Institute of Science & Technology, INDIA e-mail: Jaydip.Sen@acm.org

[5] Energy Aware and Clusterbased Routing Protocols for LargeScale Ambient Sensor Networks¤ Anahit Martirosyan, Azzedine Boukerche and Richard W. Nelem Pazzi PARADISE Research Laboratory SITE University of Ottawa, Canada famart013, boukerch, rwernerg@site.uottawa.ca

[6] http://alkautsarpens.wordpress.com/wsn/

[7] An Energy Efficient Quadrant based Clustering Approach for Wireless Sensor Networks K.Anbukkarasi#1, J.Gnanambigai#2 #1 Assistant Professor, Dr. Mahalingam College of Engineering & Technology Pollachi,Tamilnadu,9952446670,logicanbu@gmail.com #2 Associate Professor ,K.S.R College of Engineering, Tiruchengode, Tamilnadu, 9940703542, gnanadhamodharan@gmail.com.

[8] Statistical Analysis of Energy Efficient Hierarchical Routing Protocols in WSN Tintu Devasia1, Gopika S2 Department of Computer Science Rajagiri School of Engineering & Technology Rajagiri Valley, Kochi-39, Kerala, India1,2

[9] IMPROVED LEACH COMMUNICATION PROTOCOL FOR WSN Nitin Mittal#1, Davinder Pal Singh2, Amanjeet Panghal#3, R.S. Chauhan+4 # Electronics & Comm. Deptt., MIET, Mohri Central Scientific Instruments Org., Chandigarh + Electronics & Comm. Deptt., JMIT, Radaur. eced_miet@yahoo.com.

[10] Performance Analysis of a Concentric Cluster Based Hierarchical Routing Protocol for WSN Neha Rathi1, Partha Pratim Bhattacharya2 1Department of Electronics and Communication Engineering, Faculty of Engineering and Technology, Mody Institute of Technology & Science (Deemed University), Rajasthan - 332311, India 2Department of Electronics and Communication Engineering, Faculty of Engineering and Technology,

[11] Mody Institute of Technology & Science (Deemed University), Rajasthan - 332311, India.

Licensed Under Creative Commons Attribution CC BY