IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, March, 2013
ISSN: 2320 - 8791
www.ijreat.org

Routing Disruptions in Wireless Sensor Networks

M.Jeyaselvi[1] and Dr.C.Jayakumar[2]
[1]Department of Computer Science and Engineering, Agni College of Technology,
Chennai, Tamilnadu- 603 103, India.
[2]Department of Computer Science and Engineering, RMK Engineering College,
Chennai, Tamilnadu-601 206, India.

Abstract

Sensor networks are highly distributed networks which are deployed in large numbers to monitor the environment or system by the measurement of physical parameters such as temperature, pressure or relative humidity. Each node of the sensor network consists of three subsystems. They are the sensor subsystem which senses the environment, processing subsystem which performs local computations on the sensed data and the communication subsystem which is responsible for message exchange with the neighboring sensor nodes. Here the message exchange takes place by using the concept of cluster-based wireless sensor network (WSN).The cluster head is responsible for data collection and forwarding the sensed data to other nodes. The node which is having high energy is chosen as the cluster head. The purpose of a sensor network is to monitor and report the events or phenomena talking place in a particular areas or in a network. The main parameters for a quality of a sensor network are coverage and exposure. The overhearing and the malicious nodes are identified as misbehaving nodes and they are eliminated from the network. This enables us to know the status of the network by revealing the position of the nodes, number of packets delivered and received by each node.

Keywords **–Wireless Sensor Networks (WSN), Cluster Head, Cluster Based WSN, Malicious node.**

1. INTRODUCTION

1.1 Wireless Sensor Networks

Wireless Sensor Network has become one of the most interesting technologies. Wireless sensor networks are a collection of large number of nodes. They are of tiny disposable and low power sensor nodes which communicate together to achieve the given task. A sensor is a device that transforms a sensed attribute into a data form. Each sensor the capability to sense, communicate and has a memory and a small battery. Failure of one sensor node does not affect the performance of the network operation.

Various applications, such as detection of chemical activity in military field, health care monitoring and wild life sensing, etc exploit the strength of WSN [1]. They are deployed in remote or dangerous environment, allowing users to extract information in ways that would not have been possible otherwise. Hence it is inconvenient or even impossible to recharge node's battery once the deployment of the node is finished. Therefore the major challenge in the design of WSN is to lessen the battery consumption in order to enhance the network lifetime [2].Main issues in Wireless Sensor Networks are Bandwidth-constrained, Power-constrained, Limited security Unnecessary transmission, Security threats, Transmissions and computation loads, Attacks from malicious nodes.

2. Clustered Architecture

A clustered architecture organizes the sensor nodes into clusters. Each node is governed by a cluster head. The nodes in the cluster are involved in data exchange with their cluster head. Clustered architecture is especially useful for sensor networks because of its inherent suitability for data transmission. The information gathered by all members of the cluster can be fused at the cluster head and only the resulting information needs to be communicated. Sensor networks are self organizing. So the cluster formation and cluster head election must be autonomous and a distributed process. If the sensor nodes are grouped into clusters then the energy consumption can be reduced. Sensor networks are not overlapped. There is a always a leader in the cluster group. Leader is called as Cluster head. The leader is responsible for cluster formation, data gathering and transmission between inter and intra clusters. Sensor networks are in large scale.

Sensor networks have a scalable architectural and management strategy that are required to achieve goals such as extended lifetime, scalability, coverage, robustness and especially simplicity. To satisfy its requirements, it is necessary to design an efficient and scalable network layer protocol. The cluster head selection should be distributed uniformly to increase the lifetime of the network. This leads to less overhead and easy maintenance [17].

The remainder of the paper is organized as follows: In section II, Clustered architecture is discussed. The system model i.e. the design principles of cluster is described in section III. In section IV, The cluster head gateway switch routing protocol is described. Section V - the security goals in sensor networks is discussed. The proposed watchdog monitoring technique is summarized in Section VI. Section VII concludes the paper with directions for future work.

3. SYSTEM MODEL

3.1. Design Principles

Each round in the cluster is composed of setup phase and steady data communication phase. The first phase can be divided into two parts: CH election and cluster formation. The second phase can be divided into intra-cluster transmission, data aggregation and inter-cluster transmission. As shown in Fig.1.

1. CH Election: The energy consumption of CH is much more than regular nodes. In order to maintain the energyconsumption balance of nodes, CH is periodically elected by round. The broadcast message for the sensor node is received through the gateway for the election of cluster head. Then the cluster head broadcast the cluster head declaration message to its neighbor node.

2. Cluster Formation: Cluster head broadcast a message to its neighbor node to declare that it has become the new Cluster head for that cluster. The broadcasted message is recorded and stored in neighbor list. The regular nodes receive this broadcast message and decide to choose the nearest cluster head for further communication.

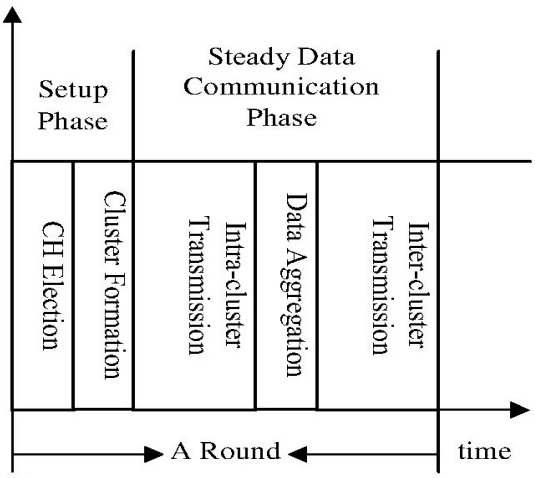

Fig. 1 Composition of a'Round' in Clustering.

3. Intra-cluster Transmission: This transmission involves communicating with other cluster heads. This intra cluster transmission increases the energy efficiency and network life time. Within the given time slots other node communicate with the cluster head.

4. Data Aggregation: CH gathers information from all the regular nodes, and then aggregates the data.

5. Inter-cluster Transmission: CH and gateway nodes are the virtual backbone for inter cluster transmission.ie communication is done with other nodes on behalf of their clusters. Cluster head send the gathered data to other sink node. Communication can take place either by single hop or multiple hops. If the particular node is within the radio range then single hop is used else multi hop is used for communication.

4. CLUSTER–HEAD GATEWAY SWITCH ROUTING PROTOCOL (CGSR)

It is a table driven routing protocol. It is an extension of DSDV .So it is called as hierarchical routing protocol. CGSR groups the nodes into clusters. With the coordination of the members of each cluster that is entrusted with a special node named as cluster head. This cluster head is elected based on the maximum energy of a node. Clustering provides a mechanism to allocate the bandwidth therefore it can be reused. Within the cluster, the cluster head coordinates the entire node. All member nodes of the cluster can reach the

cluster head in single hop. This enables the cluster head to provide an improved coordination among the nodes.

CGSR imagines that all communications take place through the cluster head. But the communications between two clusters take place through a common member node that are the members of both the clusters. The nodes which are the members of more than one cluster are called as gateways. Through this gateway the communication takes place between the clusters.

Each node maintains a routing table containing the destination cluster head for every node in the network. Each node also maintains the next hop nodes for reaching the destination cluster.[17]

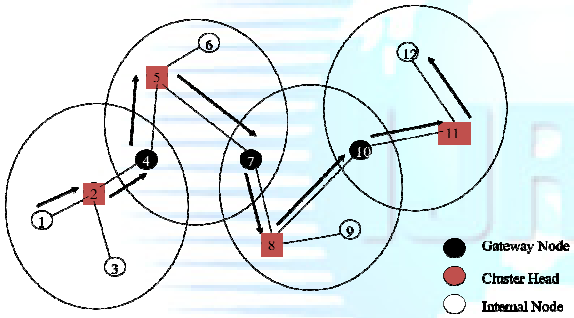

Fig.2 Routing in CGSR from node 1 to node 11

5. SECURITY GOALS IN SENSOR NETWORKS

Security is the main challenge in all types of wired and wireless networks. The unique characteristic of these networks and the application purpose makes them attractive targets for intruders and other attacks. Sensor networks are frequently used in remote areas to operate against the attackers. So the security protocols should adapt to the following criteria. Confidentiality, Integrity, Availability and Non-repudiation mechanism.

6. WATCHDOG TECHNIQUE

Normally the malicious node detection or overhearing node detection or selfish node detection or misbehavior node detection has to be removed from the entire network topology. These attacks are in the data link layer of protocol stack in WSN. Malicious node does not forward the packet to its neighbor nodes. Selfish node means if it wants consume other resources. Overhearing means if it overhears other the neighbor nodes during transmission. Misbehavior means if it does not behave to standard. To identify such nodes watchdog mechanism is used.

The mechanism of watchdog is to monitor the entire network topology in ad hoc and in sensor network. If it identifies any malicious or selfish or overhearing or misbehaving node then it detects an alarm and informs the corresponding source node that there attack in that path. Now the source node sends the data in an alternate way to forward the packet to the destination. This mechanism is capable of working in small scale and in large scale network.

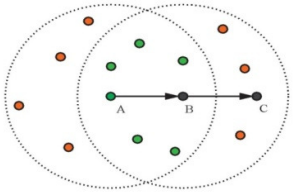

Fig. 3 Possible watchdogs

If node A wants to send a packet to node C and if it is outside of its radio range then it send its packet to the intermediate node B and node B forwards it to node C (Fig. 3). Let S_A be a set of all nodes that hear the message from A to B and S_B be the set of nodes that hear a message from B to C. Then a set of possible watchdogs with node B as an intersection of S_A and S_B is defined to monitor the network. With this it can be identified that node B forwards the packet that is received from node A.

Here in this paper, we track the information such as number of packets sent, received and dropped. From the collected information, we calculate the throughput for each link, the packet delivery and loss ratio. An alarm will be generated if the throughput is below the threshold or the desirable range. This is to inform the other nodes in the network that the corresponding node is malicious and to warn them not to use that node for route discovery or maintenance. The objective of this research is to provide reliable data transmission and to provide uninterrupted secure service to the network without any packet loss. If more number of packet loss then it degrades the performance of the network topology.

7. CONCLUSION AND FUTURE WORKS

In this paper, based on the energy of the node cluster head is elected in each round to maintain the load balance equally. Watchdog mechanism is used to detect the malicious node in this Cluster Head Gateway Switch routing protocol. This mechanism monitors the entire network and drops the node which is acting as a malicious one and forwards the packet to the destination with free of attacks. So this mechanism will provide a reliable packet transmission. By changing the cluster head in each round increases the network life time. The performance will be evaluated based on the number of packets sent, number of packets received, number of packets loss and by finding the average throughout and hop count.

Here communication between the nodes is assumed to be in the form of packets, which are prone to be attacked or modified by the attacker. In future we will work in transmitting the data in the form of objects rather than packets, such that even if the intruder gets a chance to hack the packet, he will not be able to access the data within the object.

REFERENCES

[1] Fei Xing, Wenye Wang, "On the Survivability of wireless Ad hoc Network with Node Misbehaviors and Failures, IEEE Transaction on dependable and secure computing, Vol. 7, No. 3, pp. 284 – 299, July - September 2010.

[2] MinJi Kim, Muriel Medard, Joao Barros, "Algebraic Watchdog: Mitigating Misbehavior in Wireless Network Coding", IEEE Journal on Selected Areas in Communications, Vol. 29, No. 10, pp. 1916-1925, December 2011.

[3] YaoyaoYin, Juwei Shi, Yinong Li, Ping Zhang, "Cluster Head Selection Using Analytical Hierarchy Process for Wireless Sensor Networks", in the 17th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'06).

[4] O. Younis, S. Fahmy, "HEED: A Hybrid, Energy Efficient Distributed Clustering Approach for Ad hoc Sensor Networks", IEEE Transactions Mobile Computing, Vol. 3, pp. 366-379, October 2004.

[5] Liang Ying, Yu Haibin, "Energy Adaptive Cluster Head Selection for Wireless Sensor Networks", Proceedings of the Sixth International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT'05)

[6] Amer Ahmed, Abbasi, Mohamed Younis, "A Survey on Clustering Algorithms for Wireless Sensor Networks", Elsevier Computer Communications, Vol. 30, pp. 2826-2841, 2007.

[7] S. Marti, T. J. Giuli, K. Lai, M. Baker, "Mitigating Routing Misbehavior in Mobile Ad hoc Networks", Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking, pp. 255-265, 2000.

[8] Rodrigo Roman, Jianying Zhou, Javier Lopez, "Applying Intrusion Dtection Systems to Wireless Sensor Networks",

[9] W. Heinzelman, A. Chandrakasan, H. Balakrishnan, "Energy-Efficient Communication Protocol for Wireless Micro sensor Networks", Proceedings of the 33rd Hawaii International Conference on System Sciences (HICSS '00).

[10] I. Akyildiz, E. Cayirci, W. Su, Y. Sankarasubramaniam, "A Survey on Sensor Networks", IEEE Communications Magazine, Vol. 40 (8) pp. 102-114, 2002.

[11] J. Kulik, W. R. Heinzelman, H. Balakrishnan, "Negotiation-Based Protocols for Disseminating Information in Wireless Sensor Networks".

[12] K. Akkaya, M. Younis, "A Survey on Routing Protocols for Wireless Sensor Networks", Ad Hoc Networks, Vol. 3, pp. 325-349,May 2005.

[13] A. Abbasi, M. Younis, "A Survey on Clustering Algorithms for Wireless Sensor Networks", Computer Communications, Vol. 30, pp. 2826-2841, October 2007.

[14] Y. Li, M. Thai, W. Wu, "Topology Control for Wireless Sensor Networks", Wireless Sensor Networks and Applications, Heidelberg: Springer, pp. 113-147, 2008.

[15] S. R. Das, B. M. Acharya, "Energy Efficient Routing Protocol using Clustering Technique", International Journal of Advances in Computer Networks and its Security, pp. 235-239.

[16] Guanfeng Liang, RanchitAgarwal, NitinVaidya, "When Watchdog Meets Coding II", Technical Report, July, 2009

[17] C.Siva Ram Murthy and B.S.Manoj,"Ad hoc Wireless Networks Architectures and Protocols "text book by Pearson Edu.