Volume 5, Issue 6, June 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Analyzing Parameters of Wireless Sensor Networks in Different Routing Schemes using MATLAB

Jyoti, Sunita Parashar
Department of Computer Science & Engineering,
HCTM Technical Campus, Kaithal, India

Abstract— Energy efficiency of Wireless Sensor Networks has become an essential requirement and is the main issue for researchers. Various energy efficient routing protocols have been designed for Wireless Sensor Networks where energy issue has been given more stress. Sensors in wireless sensor networks work on battery and have limited energy. Hence, network has limited lifetime. Routing protocol plays a major role in deciding for how much time a network will survive. All routing algorithms tend to increase the lifetime of WSN while maintaining factors like successful and real-time delivery of a message. This paper aims towards studying different categories of routing protocols and finally four cluster based routing protocols LEACH, PEGASIS, SCR and SECROUT have been simulated. The performance of each routing protocol has been measured on some performance metrics like network lifetime, packets transferred to BS, number of dead nodes etc and finally concluded that how a routing protocol can impact the different parameters of WSN.

Keywords— Hierarchical Routing Protocols, Wireless Sensor Networks, LEACH, PEGASIS, SCR, SECROUT Energy-efficient, Network Lifetime.

I. INTRODUCTION

The WSN is defined as highly distributed networks of small, lightweight wireless sensor nodes, deployed in large numbers to monitor the environment or system by the measurement of physical parameters such as temperature, pressure, or relative humidity [1]. Wireless sensor networks are increasingly used in several applications [2] such as Habitat Monitoring, Forest Fire Detection, Military Target Tracking & Surveillance. Biomedical Health Monitoring, Natural Disaster Relief. WSN have gained world-wide attention in recent years, particularly with the proliferation in Micro-Electro-Mechanical Systems (MEMS) technology which has facilitated the development of smart sensors. These sensors are small with limited processing and computing resources. These sensor nodes can sense, measure and gather information from the environment and based on some local decision process, they can transmit the sensed data to the user.

II. ROUTING IN WIRELESS SENSOR NETWORKS

Routing in WSNs[3] is very challenging due to the characteristics that differ these networks from other wireless networks. First, sensor nodes are resource poor in terms of energy, processing, and storage capacities. Thus, they require careful resource management. Second, in contrast to typical communication networks, almost all applications of sensor networks require the flow of sensed data from multiple sources to a particular BS. Third, due to the large number of sensor nodes, it is not possible to build a global addressing scheme for the deployment of sensor nodes as the overhead of ID maintenance is high. Thus, traditional IP-based protocols may not be applied to WSNs. Fourth, in most application scenarios; nodes in WSNs are generally stationary after deployment except for maybe a few mobile nodes. However, in some applications, some sensor nodes may be allowed to move and change their location (although with very low mobility). Fifth, sensor networks are application-specific i.e. design requirements of a sensor network change with application. Sixth, position awareness of sensor nodes is important since data collection is normally based on the location. Currently, it is not feasible to use Global Positioning System (GPS) hardware for this purpose. Finally, data collected by many sensors in WSNs is typically based on common phenomena, so there is a high probability that this data has some redundancy. Such redundancy needs to be exploited by the Routing in sensor networks differs from the one in the traditional IP Networks.

III. HIERARCHICAL ROUTING

Cluster-based routing protocols [4], [5] group sensor nodes to efficiently relay the sensed data to the sink. The cluster heads are sometimes chosen as specialized nodes that are less energy-constrained. A cluster-head[6] performs aggregation of data and sends it to the sink on behalf of the nodes within its cluster. The most interesting research issue regarding such protocols is how to form the clusters so that the energy consumption and contemporary communication metrics such as latency are optimized. Moreover, the process of data aggregation and fusion among clusters is also an interesting problem to explore.

A. LEACH (Low-Energy Adaptive Clustering Hierarchy):

LEACH [7] is a self-organizing, adaptive clustering protocol that uses randomization to distribute the energy load evenly among the sensors in the network. In LEACH, the nodes organize themselves into local clusters, with one node acting as the local base station or cluster-head. LEACH includes randomized rotation of the high-energy cluster-head position such that it rotates among the various sensors in order to not drain the battery of a single sensor. In addition, LEACH performs local data fusion to "compress" the amount of data being sent from the clusters to the base station, further reducing energy dissipation and enhancing system lifetime.

Sensors elect themselves to be local cluster-heads at any given time with a certain probability. These cluster-head nodes broadcast their status to the other sensors in the network. Each sensor node determines to which cluster it wants to belong by choosing the cluster-head that requires the minimum communication energy. Once all the nodes are organized into clusters, each cluster-head creates a schedule for the nodes in its cluster. This allows the radio components of each non-cluster-head node to be turned off at all times except during their transmit time, thus minimizing the energy dissipated in the individual sensors. Once the cluster-head has all the data from the nodes in its cluster, the cluster-head node aggregates the data and then transmits the compressed data to the base station.

LEACH Algorithm is executed in two phases. Advertisement Phase: Initially, when clusters are being created, each node decides whether or not to become a cluster-head for the current round. This decision is based on the suggested percentage of cluster heads for the network (determined a priori) and the number of times the node has been a cluster-head so far. This decision is made by the node n choosing a random number between 0 and 1. If the number is less than a threshold T(n), the node becomes a cluster-head for the current round. The threshold is set as:

$$T(s) = \begin{cases} \frac{Popt}{1 - popt \cdot (r \bmod \frac{1}{Popt})} & \text{if } s \in G \\ 0 & \text{otherwise} \end{cases}$$

Popt is an optimal percentage (determined a priori) of nodes that has to become cluster heads in each round assuming uniform distribution of nodes in space. If the nodes are homogeneous, which means that all the nodes in the field have the same initial energy, the LEACH protocol guarantees that everyone of them will become a cluster head exactly once every 1/popt rounds. The non-elected nodes belong to the set G and in order to maintain a steady number of cluster heads per round, the probability of nodes $\in$ G to become a cluster head increases after each round in the same epoch. The decision is made at the beginning of each round by each node s $\in$ G independently choosing a random number in [0, 1]. If the random number is less than a threshold T(s) then the node becomes a cluster head in the current round.

Cluster Set-up Phase: After each node has decided to which cluster it belongs, it must inform the cluster-head node that it will be a member of the cluster. Each node transmits this information back to the cluster-head again using a CSMA MAC protocol. During this phase, all cluster-head nodes must keep their receivers on.

B. PEGASIS (Power-efficient Gathering in Sensor Information Systems):

PEGASIS [8] is an improvement of the LEACH protocol. Rather than forming multiple clusters PEGASIS forms chains from sensor nodes so that each node transmits and receives from a neighbor and only one node is selected from that chain to transmit to the base station (sink). Gathered data moves from node to node, aggregated and eventually sent to the base station. The chain construction is performed in a greedy way. As shown in Figure 1, node c0 passes its data to node c1. Node c1 aggregates node c0's data with its own and then transmits to the leader. After node c2 passes the token to node c4, node c4 transmits its data to node c3. Node c3 aggregates node c4_s data with its own and then transmits to the leader. Node c2 waits to receive data from both neighbors and then aggregates its data with its neighbors_ data. Finally, node c2 transmits one message to the base station.

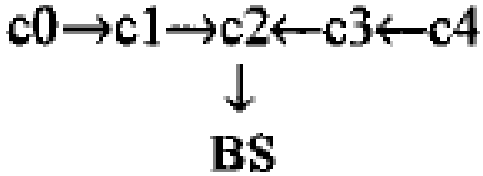

Figure 1: Chaining in PEGASIS

The difference from LEACH is to use multi-hop routing by forming chains and selecting only one node to transmit to the base station instead of using multiple nodes. PEGASIS has been shown to outperform LEACH by about 100–300% for different network sizes and topologies. Such performance gain is achieved through the elimination of the overhead caused by dynamic cluster formation in LEACH and through decreasing the number of transmissions and reception by using data aggregation. However, PEGASIS introduces excessive delay for distant node on the chain. In addition the single leader can become a bottleneck.

C. SCR (Secure cell relay):

SCR[9] routing protocol is designed to provide resistance against security attacks. SCR is a cluster-based algorithm where nodes form a cluster (cell) based on their locations. An active node becomes the relay node (cluster head) based on its remaining energy. In SCR, the entire network is divided into equal-sized square cells. Each sensor is statically aware of its own location and that of the base stations. It is assumed that the base stations can be trusted while sensors can be compromised. Before deployment, each sensor node and the base station share a common global key, KG, used for initial

neighbor discovery and handshake phase communication. It is assumed that, before deployment, all sensor nodes and the base station are synchronized. SCR uses symmetric encryption to secure packets. After deployment, the base station encrypts its location information with KG and floods it to all sensor nodes. In the neighbor discovery Phase, sensor nodes discover their neighbors via a three-way handshake protocol, which establishes the shared secret keys between neighbor nodes. After establishing a table of shared secret keys of all neighbors, each sensor node destroys KG and uses the shared secret key for future communication with its neighbors. Based on the location of the source and the sink, a routing path is formed through a series of cells in the direction from source to sink. SCR routing provides two or more backup paths determined by the source. When an adversary attacks a node, the backup paths will be used to forward packets. SCR provides defence against the following attacks: Sybil, wormhole and sinkhole, selective forwarding, and hello flood.

In Sybil attack, the adversary can pretend to be a node. Since shared keys are known only between the neighboring nodes, the attack will fail.

In wormhole and sinkhole attack, an adversary can broadcast a new route, tunnel, or fake link to the base station. Nodes that receive this new route will not use it because they route only through the routing cell path.

In selective forwarding, the adversary pretends to be a relay node in a cell and drops some packets while forwarding others. To prevent this attack, a node in a cell can only become a relay node for a user-defined number of times. After this number, the source will have to set up another path to route around this node. In addition, the sink will be notified that the current relay node will no longer be a relay node.

In hello flood attack, the adversary node tries to establish a unidirectional link with a sensor node. This will not work since a sensor node uses three-way handshake to establish its neighbors and the shared secret keys.

D. SecRout Protocol

SecRout[10] protocol guarantees secure packet delivery from the source to the sink. SecRout employs a two-level cluster-based approach to secure the network. The lower level contains sensors or cluster members while the upper level contains cluster heads. In the self-organization phase, sensor nodes are divided into clusters. Each cluster contains a cluster head. Sensor nodes communicate to the sink (or base station) via cluster heads. Data is first sent from the sensors to the cluster head. The cluster head aggregates the data from its members and sends it to the sink (or base station).

For secure packet delivery, SecRout uses symmetric cryptography to secure packets along the path. Each sensor node is given a unique identity (ID) and a preloaded key (KEY). The ID identifies the node and the KEY is used to secure messages sent to the sink. The sink is assumed to be a high power node with high memory and computation capability. The sink also knows about network topology and all sensor node information. A table containing each node's ID and KEY pair is maintained by the sink. It is assumed that the sink cannot be compromised and can be trusted.

Secure data transfer starts with a sensor node encrypting its data packet using a cluster key. The cluster key is generated by the cluster head during the self-organizing phase and is shared among sensor nodes within the cluster. Upon receiving the encrypted information, the cluster head verifies the data using its cluster key. If the verification succeeds, the cluster head will decrypt the data. The cluster head collects data from all its members and then aggregates the data to form a new data packet. The new data packet will be encrypted with the cluster head's preloaded key and sent to the sink via multi-hop routing. The sink receiving the packet again verifies the authenticity of the packet. If verification succeeds, it will decrypt the packet and store the information. SecRout guarantees that packets will reach the sink even if malicious nodes exist in the route. Routing packets and data packets contain only partial path information such as the next-hop neighbor. Each sensor node maintains a routing table containing partial routing path (previous and next node) to the sink. When a node is compromised, it will not be able to obtain information about the traversed intermediate nodes.

SecRout provides route maintenance to update the routing table and trigger new route discovery when it detects a malicious node.

IV. SIMULATION RESULTS

Performance of algorithms is analysed by simulations performed and implementing algorithms in MATLAB for a selected application environment against the set of qualitative performance metrics. Algorithms simulated are LEACH, PEGASIS, SCR, SecRout. Algorithms are compared on parameters like network lifetime, packet transmission rate, number of dead nodes.

A. Count of Dead Nodes and Energy Dissipation

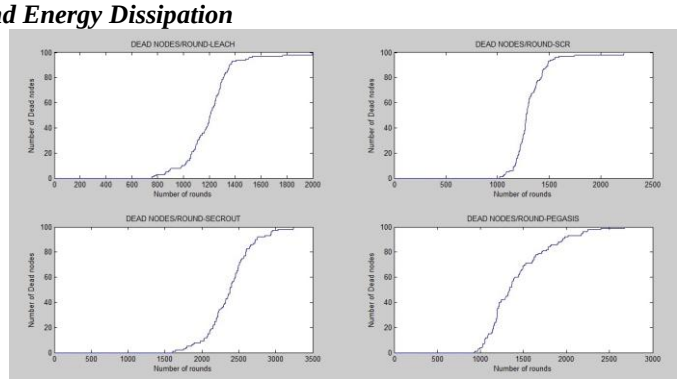

Figure.2 Count of Dead Nodes

First set of graphs shown above in Figure 2 shows a count of dead nodes and represents rate of nodes ending up consuming all their energy. X-axis represents number of simulation rounds and Y-axis represents number of dead nodes. Hence, this graph represents number of nodes that are dead till a particular simulation round. LEACH shows an early beginning of dead nodes in comparison to others. SecRout being optimal clustering shows best results. Otherwise, in PEGASIS count of dead nodes is lesser than LEAH and SCR.

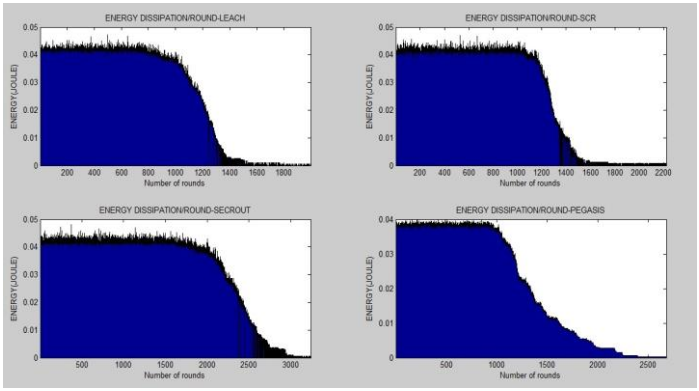

Figure.3 Energy Dissipation

Second set of graphs above in Figure 3 shows energy dissipation. X-axis represents number of simulation rounds and Y-axis represents amount of energy dissipated. Energy dissipation depends upon amount of overhead involved in routing.

B. Packet Transmission Rate and Network Lifetime

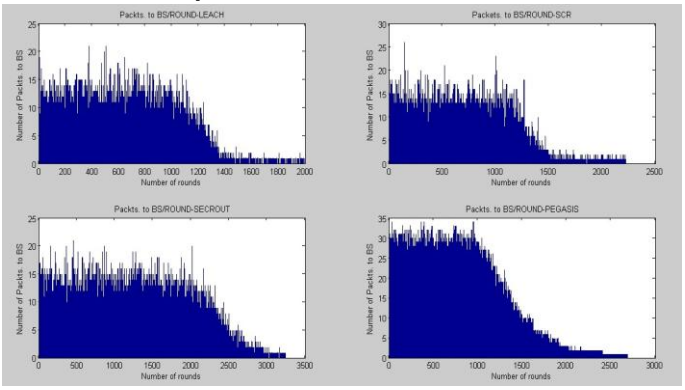

Figure.4 Example of an unacceptable low-resolution image

Third set of graphs shown above in Figure 4 shows a measure of packet transmission rate. X-axis represents number of simulation rounds and Y-axis represents number of packets transmitted to BS. PEGASIS shows highest rate of packet transmission as it has one of the maximum peak values than others.

Network lifetime means time period for which network stay alive. The definition of network lifetime used in this work as the time until all nodes have been drained of their energy. Figure5 shows measure of network lifetime for all the four algorithms.

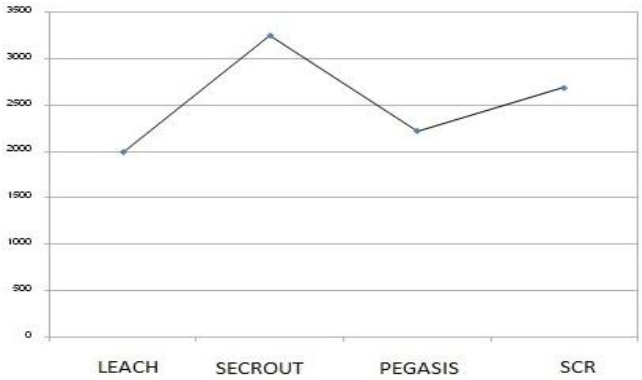

Figure.5 Network Lifetime

C. Comparison Matrix

Table below gives a snapshot of the comparison between the routing protocols in terms of their operation and performance.

TABLE I COMPARISON OF SELECTED PROTOCOLS

	Cluster Formation	Heterogeneity Consideration	Packet Transmission	Network Lifetime	Data Aggregation	Security
LEACH	Random, Poor	No	Average	Least	NO	NO
SCR	Good	Yes	Good	Average	NO	YES
P EGASIS	Best	Yes	Best	Good	NO	NO
SEC ROUT	Good	Yes	Average	Best	YES	YES

V. CONCLUSIONS

In this paper, objectives were studying hierarchical-based routing protocols where nodes are considered to be forming clusters and one of the nodes acts as a cluster-head in a cluster. Cluster formation and election of cluster-heads play a major role in determining network lifetime of a network. Optimal and efficient election of cluster-heads can enhance performance and lifetime of a network. Thus, our objective was to study various hierarchical routing protocols and analyse their performance. Four hierarchical routing protocols that are LEACH, PEGASIS, SecRout and SCR have been studied and implemented in MATLAB. Simulation Rounds of all these algorithms were analyzed and performance of each routing protocol is measured on some performance parameters like network lifetime, packets transferred to BS, number of dead nodes etc.

Due to energy limitations, main focus of most routing protocols in wireless sensor networks is to provide energy-efficient routing. Hierarchical routing protocols have shown noticeable energy improvements. Hierarchical algorithms have evolved to provide optimal clustering schemes thus minimizing energy requirements in cluster-head selection and enhancing the lifetime of whole network. The organization of the network into clusters lends itself to efficient data aggregation which in turn results in better utilization of the channel bandwidth. Due to energy limitations, main focus of most routing protocols in wireless sensor networks is to provide energy-efficient routing. Cluster based routing protocols have shown noticeable energy improvements. Cluster based algorithms have evolved to provide optimal clustering schemes thus minimizing energy requirements in cluster-head selection and enhancing the lifetime of whole network. The organization of the network into clusters lends itself to efficient data aggregation which in turn results in better utilization of the channel bandwidth. Based on the study and results analysis of various Cluster based routing algorithms, it can be seen that SECROUT algorithm provides maximum lifetime for a wireless sensor network since SECROUT allows for optimal distribution of extra energy over existing nodes. Whereas, PEGASIS shows a better performance in terms of number of data packets sent to the BS (Base Station).

REFERENCES

[1] C.Siva Ram Murthy, B.S. Manoj , "*Ad Hoc Wireless Sensor Networks Architectures and Protocols*", Prentice Hall PTR, Upper Saddle River, NJ, USA, ISBN:013147023X pp.647, 2004.

[2] H.Tian., P.Vicaire, T.Yan, L.Luo, L.Gu, G.Zhou,R.Stoleru,Q.Cao,J.Stankovic,T.Abdelzaher, "*Achieving Real-Ttime Target Tracking using Wireless Sensor Networks*", IEEE Real Time Tech. and Applications Symposium, IEEE Computer Society, pp. 37– 48,2006.

[3] Jamal N. Al-karaki, and Ahmed E. Kamal, "*Routing Techniques in Wireless Sensor Networks: A Survey* ", in IEEE Wireless Communications , Vol:11, Issue: 6 , Dec. 2004.

[4] Qing Bian, Yan Zhang, and Yanjuan Zhao, "*Research on Clustering Routing Algorithms in Wireless Sensor Networks*", In IEEE International Conference on Intelligent Computation Technology and Automation, pp: 1110 – 1113, 11-12 May 2010.

[5] Kemal Akkaya, and Mohamed Younis, "*A Survey on Routing Protocols for Wireless Sensor Networks*", in proceedings of Ad Hoc Networks,Vol. 3, pp.325–349,2005

[6] Xuxun Liu, "*A Survey on Clustering Routing Protocols in Wireless Sensor Networks*", in Sensors, Vol 12, Isssue 8, pp. 11113-11153, Aug 2012.

[7] Geetu, Sonia Juneja, "*Performance Analysis of SPIN and LEACH Routing Protocol in WSN* " , In International Journal of Computational Engineering Research, Vol. 2 , Issue5, pp.1179-1185, Sep. 2012.

[8] Lindsey, C. Raghavendra, "*PEGASIS: Power-Efficient Gathering in Sensor Information System*" in IEEE Aerospace Conference Proceedings , Vol. 3, pp.1125-1130, 2002.

[9] Xiaojiang Du,Yang Xiao, Hsiao-Hwa Chen, Qishi Wu, "*Secure Cell Relay Routing Protocol for Sensor Networks*" in Wireless Communications and Mobile Computing, Vol 6 , Issue 3, pp. 375-391,May 2006

[10] Jian Yin, Sanjay Madria," *SecRout: A Secure Routing Protocol for Sensor Networks*", in IEEE 20th International Conference on Advanced Information Networking and Applications,Vol. 1, 18-20 April 2006.

