Survey on Routing Protocols in Wireless Sensor Networks

Ankur Dongre[1] Prof. Sanjay Bansal[2]
[1,2]Department of Computer Science
[1,2]AITR, Indore

Abstract— Wireless sensor networks are formed by small sensor nodes communicating over wireless links without using a fixed network infrastructure. Sensor nodes have a limited transmission range, and their processing and storage capabilities as well as their energy resources are also limited. Routing protocols for wireless sensor networks have to ensure reliable multi-hop communication under these conditions. The nodes can be densely deployed in close proximity to the phenomenon to be observed. They can be deployed in hostile environments where the nodes may not be physically accessible and are subject to tampering. Nodes can be added to and deleted from the network at any time, resulting in unpredictable changes to the topology of the network. This presents new challenges in the design of routing protocols for sensor networks. In this paper, the constituent building blocks of sensor network routing protocols are identified and analyzed. The routing protocols are broadly classified into three categories: flat, hierarchical and Location aware Routing and further into subcategories based on the centrality of their theme. Several routing algorithms belonging to each category that have been proposed in the literature are explored.

Key words: Routing Protocols, WSN

I. INTRODUCTION

Due to the growth in wireless technology, the Wireless Sensor Networks (WSNs) have attracted many researchers for its scope, further development and enhancing the existing system. Sensors are also commonly known as "motes". One of the primary benefits of WSNs is their independence from the wiring costs and constraints. WSNs are composed of a set of highly planned deployed sensors, which are highly sensitive to the environment and capable of communication with each other through wireless channels [1]. It is a sensing technology where small, autonomous and compact devices are called sensor nodes. These nodes are deployed in a remote area to detect certain condition, gather and process data and transmit sensed information where required. The development of low-cost, low-power, dynamic sensor has catched attention from various industries. Sensor nodes in WSNs are tiny and are capable of sensing, gathering and operating that data while communicating with other connected sensor nodes in the network, with the help of radio frequency (RF) channel. WSN can be found in many devices ranging from laptops, PDA or mobile phones to very tiny and simple sensing devices.

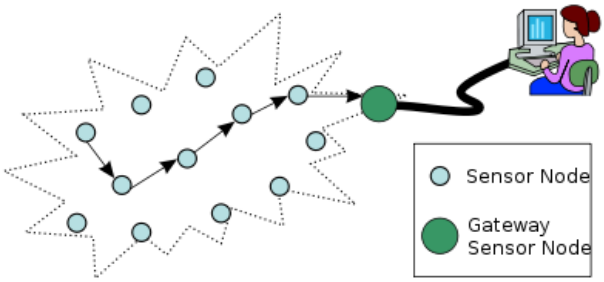

Fig. 1: A Typical Wireless Sensor Network

Figure-1 shows the architecture of a typical wireless sensor network with sensor nodes and gateway of sensor node [2]. Sensor networks may consist of many different types of sensors such as seismic, thermal, electrical, visual, acoustic, radar and so on. Sensor networks are finding a wide variety of applications in a number of domains. Some common applications of sensor networks are [3]:

- Military applications such as battlefield surveillance, nuclear, biological and chemical (NBC) attack detection, and reconnaissance over enemy territory.
- Environmental applications such as wild animal tracking, air and water pollution level monitoring, forest fire detection and precision agriculture.
- Health applications such as heart rate monitoring, telemedicine and drug administration.
- Commercial applications such as highway traffic analysis, building security, structural fault detection, and power consumption measurement.

Wireless sensor networks have some routing issues [4], which are as follows-

1) Infrastructure less: Since in wireless sensor networks the sensor nodes are randomly deployed, it is infrastructure less. So care should be taken while designing the routing protocols for wireless sensor networks.
2) Energy constraints: Sensor nodes mainly based on the battery for power. Since batteries cannot be replaced more care should be taken while using the available energy.
3) Network lifetime: Sensor node`s lifetime is mainly dependent on their batteries. When a node desires to send the data, it has to decide on the stumpy energy node. While selecting the stumpy energy node there may be a prospect of network partition. Hence a node with balanced energy must be selected to maximize the network lifetime.
4) Cost: Since the number of sensor nodes deployed in the sensing area may be in order of thousands, the cost of a single node has to be kept low.
5) Scalability: The sensor network should adapt to the changes in increasing size. Because some nodes may go to another location and some nodes may join newly to the network.
6) QoS: Sensor network should possess minimum delay, less control overhead, high throughput and efficient resource allocation.
7) Coverage: Coverage depends on the range, location and density of the sensing node. Hence the coverage area of the sensor network should be high enough.
8) Exposure: Sensors should be highly able to observe a target in the sensing area. Network should possess maximum exposure path (best case coverage).

9) Security: In military applications the sensing information is very confidential. Data loss or damage to the data can occur due to the malicious node in the network. Hence Security should be provided in terms of confidentiality and integrity.

II. LITERATURE SURVEY

A lot of work has been completed in the arena of routing algorithms in wireless sensor network and still a lot require to be done on it. Various researchers have suggested their work (means routing protocols) in this arena from which some of the most significant works are described below.

Routing protocols are classified into three categories. They are flat, Hierarchical and Location based routing protocols [5].

A. Flat Routing:

Usually WSN consists of sensor nodes and base station. In flat topology all sensor nodes are treated uniformly. When a node needs to send the data it calculates the shortest path from it to the base station. After that it sends their sensed data to the base station through intermediate (neighborhood) nodes [5]. Protocols under flat routing are: Directed Diffusion (DD), Rumor Routing (RR), Gradient Based Routing (GBR), Constrained Anisotropic Diffusion Routing (CADR), and Sensor Protocols for Information via Negotiation (SPIN) [6] [7] [8].

1) Directed Diffusion (DD):

Directed diffusion [9] is a data-centric routing algorithm for drawing information out of a sensor network. Base stations flood interests for named data, setting up gradients within the network designed to draw events (i.e., data matching the interest). Nodes able to satisfy the interest disseminate information along the reverse path of interest propagation. Nodes receiving the same interest from multiple neighboring nodes may propagate events along the corresponding multiple links. Interests initially specify a low rate of data flow, but once a base station starts receiving events it will reinforce one (or more) neighbor in order to request higher data rate events. This process proceeds recursively until it reaches the nodes generating the events, causing them to generate events at a higher data rate. Alternatively, paths may be negatively reinforced as well [6].

2) Rumor Routing (RR):

Rumor routing [11] is a variation of directed diffusion and is mainly intended for applications where geographic routing is not feasible. In general, directed diffusion uses flooding to inject the query to the entire network when there is no geographic criterion to diffuse tasks. However, in some cases there is only a little amount of data requested from the nodes and thus the use of flooding is unnecessary. An alternative approach is to flood the events if the number of events is small and the number of queries is large. The key idea is to route the queries to the nodes that have observed a particular event rather than flooding the entire network to retrieve information about the occurring events. In order to flood events through the network, the rumor routing algorithm employs long-lived packets, called agents. When a node detects an event, it adds such event to its local table, called events table, and generates an agent. Agents travel the network in order to propagate information about local events to distant nodes. When a node generates a query for an event, the nodes that know the route, may respond to the query by inspecting its event table. Hence, there is no need to flood the whole network, which reduces the communication cost. On the other hand, rumor routing maintains only one path between source and destination as opposed to directed diffusion where data can be routed through multiple paths at low rates. Simulation results showed that rumor routing can achieve significant energy savings when compared to event flooding and can also handle node's failure. However, rumor routing performs well only when the number of events is small. For a large number of events, the cost of maintaining agents and event-tables in each node becomes infeasible if there is not enough interest in these events from the BS. Moreover, the overhead associated with rumor routing is controlled by different parameters used in the algorithm such as time-to-live (TTL) pertaining to queries and agents. Since the nodes become aware of events through the event agents, the heuristic for defining the route of an event agent highly affects the performance of next hop selection in rumor routing [10].

3) Sensor Protocols for Information via Negotiation (SPIN):

It overcomes the deficiencies of flooding. SPIN has three types of messages: ADV, ACK and DATA [4].

Node uses this type of three way handshaking protocol only if it has adequate energy. If the energy level of the particular node is below the required threshold level, then it will not send or receive the data messages. In SPIN the source node sends the ADV (metadata) packets to its neighbour nodes. If the neighbour nodes need to receive data then it sends ACK message. Then only the source node sends the actual data packets to the neighbour nodes. The neighbour nodes send the ADV (metadata) for the received packets to their neighbours and this process will be continued to deliver the data throughout the network. When the application needs a reliable data delivery, this protocol does not support [12].

B. Hierarchical Routing:

In hierarchical or clustered topology various nodes are combined together to form clusters. And the data from that set of nodes are sent to the cluster head using multi-hops. Cluster head aggregates the data and sends it to sink using single hop. In this sensor node sends the data to cluster head and cluster head sends aggregated data directly to the base station [5]. Protocols under hierarchical routing are: Low Energy Adaptive Clustering Hierarchy (LEACH), Threshold sensitive Energy Efficient sensor Network (TEEN), Adaptive Threshold sensitive Energy Efficient sensor Network (APTEEN), The Power-Efficient GAthering in Sensor Information Systems (PEGASIS), and Hybrid, Energy-Efficient Distributed Clustering (HEED) [6] [7] [8].

1) Low Energy Adaptive Clustering Hierarchy (LEACH):

Heinzelman *et al.* [13] describe LEACH (Low Energy Adaptive Clustering Hierarchy), a cluster-based routing protocol. LEACH aims to uniformly distribute the energy consumed by sensor nodes across the network to extend system lifetime. This is accomplished by periodically rotating the cluster head nodes. The cluster heads collect the sensor readings from the other nodes in the cluster, perform local compression or aggregation on the data to reduce global communication and transmit a summary of the

readings back to a central base station. Thus the cluster heads are the most critical nodes in the network since the entire cluster would be disconnected if the corresponding cluster-head were to run out of energy. A fundamental assumption of the LEACH algorithm is that nodes can adjust their transmission power to transmit signals to varying distances.

2) Threshold Sensitive Energy Efficient Sensor Network (TEEN):

TEEN [14] is a hierarchical protocol designed to be responsive to sudden changes in the sensed attributes such as temperature. Responsiveness is important for time-critical applications, in which the network operated in a reactive mode. TEEN pursues a hierarchical approach along with the use of a data-centric mechanism. The sensor network architecture is based on a hierarchical grouping where closer nodes form clusters and this process goes on the second level until base station (sink) is reached. After the clusters are formed, the cluster head broadcasts two thresholds to the nodes. These are hard and soft thresholds for sensed attributes. Hard threshold is the minimum possible value of an attribute to trigger a sensor node to switch on its transmitter and transmit to the cluster head. Thus, the hard threshold allows the nodes to transmit only when the sensed attribute is in the range of interest, thus reducing the number of transmissions significantly. Once a node senses a value at or beyond the hard threshold, it transmits data only when the values of that attribute changes by an amount equal to or greater than the soft threshold. As a consequence, soft threshold will further reduce the number of transmissions if there is little or no change in the value of sensed attribute. One can adjust both hard and soft threshold values in order to control the number of packet transmissions. However, TEEN is not good for applications where periodic reports are needed since the user may not get any data at all if the thresholds are not reached [15].

3) The Power-Efficient GAthering in Sensor Information Systems (PEGASIS):

Unlike LEACH protocol the sensor nodes in the network form a chain based arrangement. In LEACH the nodes are arranged in clustered manner. And in PEGASIS there is no cluster head selection phase. Hence it avoids overhead fairly. The sensed data is sent to single hop neighbor node. Each node sends data to its neighbor and thus forms a chain arrangement. A token is passed to the nodes. After receiving the token the node delivers the data to neighbor [4] [16].

C. Location Aware Routing:

In this type of routing protocol, the nodes send the data to sink node by using geographical information [5]. Hence it reduces the control overhead. Protocols under location aware routing are: Geographic Adaptive Fidelity (GAF), Geographical and Energy Aware Routing (GEAR), Geographic Random Forwarding (GeRaF), Minimum Energy Communication Network (MECN), Small Minimum-Energy Communication Network (SMECN), Trajectory-Based Forwarding (TBF), and Bounded Voronoi Greedy Forwarding (BVGF): [6] [7] [8].

1) Geographic Adaptive Fidelity (GAF):

GAF [17] places nodes into virtual "grid squares" according to geographic location and expected radio range. Any pair of nodes in adjacent grid squares are able to communicate. Nodes are in one of three states: *sleeping*, *discovery*, and *active*. Active nodes participate in routing while discovery nodes probe the network to determine if their presence is needed. Sleeping nodes have their radio turned off. Nodes are ranked with respect to current state and expected lifetime. Discovery messages are used to exchange state and ranking information between nodes in the same grid. GAF attempts to reach a state in which each grid square has only one active node [6].

2) Geographical and Energy Aware Routing (GEAR):

GEAR [19] is an energy-efficient routing protocol proposed for routing queries to target regions in a sensor field, In GEAR, the sensors are supposed to have localization hardware equipped, for example, a GPS unit or a localization system [20] so that they know their current positions. Furthermore, the sensors are aware of their residual energy as well as the locations and residual energy of each of their neighbors. GEAR uses energy aware heuristics that are based on geographical information to select sensors to route a packet toward its destination region. Then, GEAR uses a recursive geographic forwarding algorithm to disseminate the packet inside the target region [7].

3) Small Minimum-Energy Communication Network (SMECN):

SMECN [18] is an extension of MECN protocol. MECN is location aware routing protocol where minimum energy is setup and maintained over the network. MECN has two steps.

- An enclosure graph is constructed, in which all sensor nodes as vertices that are interconnected. This construction is based on locality of the sensor nodes.
- Then find the optimal path to the sink in which the path with power consumption as cost metric is selected.

When using the nodes with mobility, the global positioning system is chosen for locating the nodes. In SMECN, the minimal sub network is constructed from MECN. The node uses broadcasting to find its immediate neighbor. It sends the neighbor discovery message with some initial potential power(p). The neighbor that possesses the power replies immediately. If no reply comes from neighbors, then the sensor node retransmits the broadcasts the discovery message with incremental updated power. Calculating a subset introduces more overhead [4].

Routing Catagory	Representative Protocols	Relevant Attacks
Flat Routing	DD, RR, GBR, CADR, SPIN	Bogus routing information, selective forwarding, sinkholes, Sybil, wormholes
Hierarchical Routing	LEACH, PEGASIS, HEED, TEEN, APTEEN MECN, SMECN, GAF.	Selective forwarding, HELLO floods Bogus routing information.
Location Based Routing	GEAR, Span, TBF, BVGF, GeRaF	Sybil, HELLO floods, selective forwarding

Table: 1 shows the wireless sensor network routing protocols with their category and relevant attacks.

III. CONCLUSION

Routing in sensor networks has involved a lot of devotion in the recent years and familiarized unique challenges associated to old-fashioned data routing in wired networks. In recent years because of the marvelous development of wireless sensor network (WSN), routing issues play an significant role. To develop a routing protocol in wireless sensor networks there are many open issues. To resolve this issues several routing protocols were established for wireless sensor networks. In this research paper, we have described some of the important routing issues involved with wireless sensor network and some most significant routing protocols.

REFERENCES

[1] F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," Communications Magazine, IEEE, vol. 40, pp. 102-114, 2002.
[2] https://en.wikipedia.org/wiki/Wireless_sensor_network.
[3] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey", Published by Elsevier Science, 2002.
[4] P.Krishnaveni, and Dr.J.Sutha, "Analysis of routing protocols for wireless sensor networks", International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 2, Issue 11, November 2012.
[5] Avni Kaushik, "A review on Routing Techniques in Wireless Sensor Networks", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 6, June 2014.
[6] Chris Karlof and David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", Funded in part by DARPA NEST contract F33615-01-C-1895.
[7] Shio Kumar Singh, M P Singh, and D K Singh, "Routing Protocols in Wireless Sensor Networks- A Survey", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.1, No.2, November 2010.
[8] Rajashree.V.Biradar, V.C .Patil, Dr. S. R. Sawant, and Dr. R. R. Mudholkar, "CLASSIFICATION AND COMPARISON OF ROUTING PROTOCOLS IN WIRELESS SENSOR NETWORKS", Special Issue on Ubiquitous Computing Security Systems, UbiCC Journal – Volume 4.
[9] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed diffusion: A scalable and robust communication paradigm for sensor networks," in proceedings of the Sixth Annual International Conference on Mobile Computing and Networks (MobiCOM '00), August 2000.
[10] Jamal N. Al-Karaki and Ahmed E. Kamal, "Routing Techniques in Wireless Sensor Networks: A Survey", supported in part by the ICUBE initiative of Iowa State University, Ames, IA 50011.
[11] D. Braginsky and D. Estrin, \Rumor Routing Algorithm for Sensor Networks," in the Proceedings of the First Workshop on Sensor Networks and Applications (WSNA), Atlanta, GA, October 2002.
[12] J. Kulik, W. R. Heinzelman, and H. Balakrishnan, "Negotiation-based protocols for disseminating information in wireless sensor networks," Wireless Networks, vol. 8, no. 2-3, pp. 169–185, 2002.
[13] Wendi Heinzelman, Anantha Chandrakasan, and Hari Balakrishnan, Energy-efficient communication protocol for wireless microsensor networks, Proc. 33rd Hawaii Int. Conf. on System Sciences, 2000.
[14] Kemal Akkaya, and Mohamed Younis, "A survey on routing protocols for wireless sensor networks", Published by Elsevier, 2003.
[15] A. Manjeshwar, D.P. Agrawal, TEEN: a protocol for enhanced efficiency in wireless sensor networks, in: Proceedings of the 1st International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing, San Francisco, CA, April 2001.
[16] S. Lindsey and C. Raghavendra, "PEGASIS: Power-efficient gathering in sensor information systems," in IEEE Aerospace Conference, March 2002.
[17] Y. Xu, J. Heidemann, and D. Estrin, "Geography-informed energy conservation for ad hoc routing," in Proceedings of the Seventh Annual ACM/IEEE International Conference on Mobile Computing and Networking, 2001.
[18] L. Li, J. Y Halpern, Minimum energy mobile wireless networks revisited, in: Proceedings of IEEE International Conference on Communications (ICC_01), Helsinki, Finland, June 2001.
[19] Y. Yu, R. Govindan, and D. Estrin, "Geographical and energy aware routing: A recursive data dissemination protocol for wireless sensor networks", Technical Report UCLA/CSD-TR-01-0023, UCLA Computer Science Department, May 2001.
[20] N. Bulusu, J. Heidemann, and D. Estrin, "GPS-less Low Cost Outdoor Localization for Very Small Devices", IEEE Personal Communication Magazine, vol. 7, no. 5, Oct. 2000, pp. 28-34.

