RESEARCH ARTICLE OPEN ACCESS

A Review Article on an Effective Routing Algorithm Based On Optimization in Wireless Sensor Networks

Vikram Pratap Singh Thakur, Dr. Prashant Kumar Jain
Department of Electronics and Telecommunication Jabalpur Engineering College
Department of Electronics and Telecommunication Jabalpur Engineering College

ABSTRACT
Recent advances in wireless communication lead to many improvements in application specific wireless sensor network (WSN) deployment. Sensing different data from different environments is essential to monitor and control the situations. For instance, it is very important to sense the forest fire as early as possible to control the upshot. So efficient and timely gathering of the data from a network of small sensor nodes is necessary. In WSN, the small sized sensor nodes are working with very small batteries with limited energy. Since those are randomly deployed over a wide area, replacement of battery or recharging is not feasible. So, for getting prolonged life time of WSN, energy efficient operation is the key factor. Among many protocols proposed for enhancing the life time of WSN, the clustering based hierarchical protocols are popular and gaining the attention of researchers because of their high energy efficiency. Low Energy Adaptive Clustering Hierarchy (LEACH) is energy efficient hierarchical, clustering based protocol. It is considered as the base of many hierarchical clustering protocols. In this paper, some of the recent tailored protocols proposed to strengthen LEACH are examined.

Keywords: LEACH protocol, Energy efficient protocol, Lifetime, Cluster, Wireless sensor networks.

Date of Submission: 15-08-2020 Date of Acceptance: 01-09-2020

I. INTRODUCTION

Advancement in wireless communication and electronics has enabled the development of low-cost, low-power multifunctional miniature devices for use in remote sensing applications. Such sensors can be widely deployed for commercial, civil and military applications such as surveillance, vehicle tracking, climate and habitat monitoring intelligence, medical and acoustic data gathering. A WSN is composed of large number of sensor nodes which consist of sensing, data processing and communication capabilities. Usually sensor nodes are scattered in the sensing field. They coordinate among themselves to get information about the physical environment. The information is routed to the Base Station either directly or through other sensor nodes. The BS is either a fixed or mobile node which is capable to connect the sensor network to the internet where user can access and process data.

II. WIRELESS SENSOR NETWORK

Wireless sensor networks are potentially one of the most important technologies of this century. Recent advancement in wireless communications and electronics has enabled the development of low-cost, low-power, multifunctional miniature devices for use in remote sensing applications. The combination of these factors have improved the viability of utilizing a sensor network consisting of a large number of intelligent sensors, enabling the collection, processing analysis and dissemination of valuable information gathered in a variety of environments. A sensor network is composed of a large number of sensor nodes which consist of sensing, data processing and communication capabilities.

Sensor networks are predominantly data-centric rather than address-centric. So sensed data are directed to an area containing a cluster of sensors rather than particular sensor addresses. Given the similarity in the data obtained by sensors in a dense cluster, aggregation of the data is performed locally. That is, a summary or analysis of the local data is prepared by an aggregator node within the cluster, thus reducing the communication bandwidth requirements.

III. SENSOR NETWORK CHALLENGES

Wireless sensor network uses a wide variety of application and to impact these applications in real world environments, we need more efficient protocols and algorithms. Designing a new protocol or algorithm address some challenges which are need to be clearly understood [1]. These challenges are summarized below:

Network scalability: When a WSN is deployed, some time new nodes need to be added to the network in order to cover more area or to prolong the life time of the current network. In both the cases the clustering scheme should be able to adapt to changes in the topology of the network. The key point in designing such management schemes should be if the algorithm is local and dynamic it will be easy for it to adapt to topology changes.

Network Dynamics: Most of the network architectures assume that sensor nodes are stationary. However, mobility of both BS's or sensor nodes is sometimes necessary in many applications [2]. Routing messages from or to moving nodes is more challenging since route stability becomes an important issue, in addition to energy, bandwidth etc. Moreover, the sensed phenomenon can be either dynamic or static depending on the application, e.g., it is dynamic in a target detection/tracking application, while it is static in forest monitoring for early fire prevention. Monitoring static events allows the network to work in a reactive mode, simply generating traffic when reporting. Dynamic events in most applications require periodic reporting and consequently generate significant traffic to be routed to the BS.

Multihop or single hop communication: The communication model that wireless sensor network uses is either single hop or multi hop. Since energy consumption in wireless systems is directly proportional to the square of the distance, single hop communication is expensive in terms of energy consumption. Most of the routing algorithms use multi hop communication model since it is more energy efficient in terms of energy consumption however, with multi hop communication the nodes which are closer to the cluster head are under heavy traffic and can create gaps near the cluster head when their energy terminates.

Cluster Dynamics: Cluster dynamics means how the different parameters of the cluster are determined for example, the number of clusters in a particular network. In some cases the number might be preassinged and in some cases it is dynamic. The cluster head performs the function of compression as well as transmission of data. The distance between the cluster heads is a major issue. It can be dynamic or can be set in accordance with some minimum value. In case of dynamic, there is a possibility of forming unbalanced clusters. While limiting it by some pre-assigned, minimum distance can be effective in some cases but this is an open research issue. Also cluster head selection can either be centralized or decentralized which both have advantages and disadvantages. The number of clusters might be fixed or dynamic. Fixed number of clusters cause less overhead in that the network will not have to repeatedly go through the set up phase in which clusters are formed. In terms of scalability it is poor.

Quality of Service: In some applications, data should be delivered within a certain period of time from the moment it is sensed, otherwise the data will be useless. Therefore bounded latency for data delivery is another condition for time-constrained applications. However, in many applications, conservation of energy, which is directly related to network lifetime, is considered relatively more important than the quality of data sent. As the energy gets depleted, the network may be required to reduce the quality of the results in order to reduce the energy dissipation in the nodes and hence lengthen the total network lifetime. Hence, energy-aware routing protocols are required to capture this requirement.

Unattended operation: In many application sensor networks is deployed once, and after deployment have no human intervention. Hence the nodes themselves are responsible for reconfiguration in case of any changes.

Security: Security is very critical parameter in sensor networks, given some of the proposed applications. An effective compromise must be obtained, between the low bandwidth requirements of sensor network applications and security demands for secure data communication in the sensor networks (which traditionally place considerable strain on resources)Thus, unlike traditional networks, where the focus is on maximizing channel throughput with secure transmission.

IV. SYSTEM ARCHITECTURE AND DESIGN ISSUES

Depending on the application, different architectures and design goals/constraints have been considered for sensor networks. Since the performance of a routing protocol is closely related to the architectural model, in this section we discuss the architectural issues and highlight their implications.

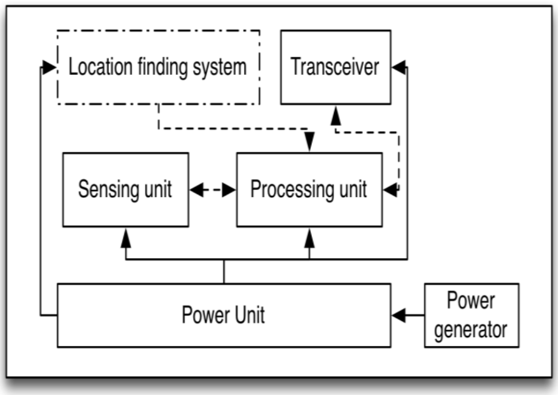

Fig4.1. The components of a sensor node.

Energy Considerations: Energy is very important parameter during the creation of an infrastructure, and the process of selecting the routes for transmission. Since the transmission power of a wireless radio is proportional to distance squared or even higher order in the presence of obstacles, multihop routing will consume less energy than direct communication. However, multihop routing introduces significant overhead for topology management and medium access control. Direct routing would perform well enough if all the nodes were very close to the sink[2,3]. However most of the time sensors are scattered randomly over an area of interest and multi-hop routing becomes unavoidable.

Security Implementation: Security is data communication is main concerning parameter for providing secure communication in sensor networks, while designing wireless networks, as wireless sensor networks may be deployed in hostile areas such as battlefields .therefore, design of protocol should work with the data communication security protocols, as any conflict between these protocols might create challenge in network security.

Network Dynamics: There are three basic components, sensor nodes, sink and user which is monitored the events in a sensor network. Most of the network architectures assume that sensor nodes are stationary. Some application are required the mobility of sinks or cluster-heads (gateways). Routing messages from or to moving nodes is more challenging since route stability becomes an important optimization factor, in addition to energy, bandwidth etc. The sensed event can be either dynamic or static depending on the application.

Node Deployment: It is an important issue to deployment of sensor nodes in topological manner. This is application dependent and affects the performance of the routing protocol. The deployment is either deterministic or self-organizing as already mentioned above.

Node Capabilities: Depending on the application of the sensor network, the data delivery model to the sink can be continuous, event-driven, query-driven and hybrid [4,5]. In the continuous delivery model, each sensor sends data periodically. In event-driven and query-driven models, the transmission of data is triggered when an event occurs or a query is generated by the sink. Some networks apply a hybrid model using a combination of continuous, event-driven and query-driven data delivery. The routing protocol is highly influenced by the data delivery model, especially with regard to the minimization of energy consumption and route stability. For instance, it has been concluded in [6] that for a habitat monitoring application where data is continuously transmitted to the sink, a hierarchical routing protocol is the most efficient alternative. This is due to the fact that such an application generates significant redundant data that can be aggregated on route to the sink, thus reducing traffic and saving energy.

V. WIRELESS SENSOR NETWORKS VS. TRADITIONAL WIRELESS NETWORKS

There are many existing protocol, techniques and concepts from traditional wireless network, such as cellular network, mobile ad-hoc network, wireless local area network and Bluetooth, are applicable and still used in wireless sensor network, but there are also many fundamental differences which lead to the need of new protocols and techniques [2].

There are many existing protocol, techniques and concepts from traditional wireless network, such as cellular network, mobile ad-hoc network, wireless local area network and Bluetooth, are applicable and still used in wireless sensor network, but there are also many fundamental differences which lead to the need of new protocols and techniques. Some of the most important characteristic differences are summarized below:

Number of nodes in wireless sensor network is much higher than any traditional wireless network. Possibly a sensor network has to scale number of nodes to thousands. Moreover a sensor network might need to extend the monitored area and has to increase number of nodes from time to time. This needs a highly scalable solution to ensure sensor network operations without any problem.

Due to large number of sensor nodes, addresses are not assigned to the sensor nodes. Sensor networks are not address-centric; instead they are data-centric network. Operations in sensor networks are centered on data instead of individual sensor node. As a result sensor nodes require collaborative efforts.

Sensor nodes mainly use a broadcast communication paradigm, whereas most ad hoc networks are on point-to-point communications. Sensor nodes are much cheaper than nodes in ad hoc networks.

Wireless sensor networks are environment-driven. While data is generated by humans in traditional networks, the sensor network generate data when environment changes. As a result the traffic pattern changes dramatically from time to time. Sensor networks are mainly used to collect information while MANETs (Mo-bile Adhoc Networks) are designed for distributed computing rather than information gathering.

ISSUES OF OLD ARTICLES

Routing protocol in wireless sensor network

IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 15, NO. 2, SECOND QUARTER 2013

Energy-Efficient Routing Protocols in WirelessSensorNetworks: A Survey
Nikolaos A. Pantazis, Stefanos A. Nikolidakis and Dimitrios D. Vergados, Senior Member, IEEE

During the recent years, many energy efficient routing protocols have been proposed for WSNs. In the above paper author mention the following energy efficient routing protocol for wireless sensor network

.

Data-centric protocols

In many applications of sensor networks, it is not feasible to assign global identifiers to each node due to the sheer number of nodes deployed. Such lack of global identification along with random deployment of sensor nodes makes it hard to select a specific set of sensor nodes to be queried. Therefore, data is usually transmitted from every sensor node within the deployment region with significant redundancy. Since this is very inefficient in terms of energy consumption, routing protocols that will be able to select a set of sensor nodes and utilize data aggregation during the relaying of data have been considered. This consideration has led to data-centric routing, which is different from traditional address-based routing where routes are created between addressable nodes managed in the network layer of the communication stack. In data-centric routing, the sink sends queries to certain regions and waits for data from the sensors located in the selected regions. Since data is being requested through queries, attribute-based naming is necessary to specify the properties of data. SPIN [5] is the first data-centric protocol, which considers data negotiation between nodes in order to eliminate redundant data and save energy. Later, Directed Diffusion [1] has been developed and has become a breakthrough in data-centric routing. Then, many other protocols have been proposed either based on Directed Diffusion or following a similar concept. In this section, these protocols are described in details.

Flooding and Gossiping: Flooding and gossiping [7] are two classical mechanisms to relay data in sensor networks without the need for any routing algorithms and topology maintenance. In flooding, each sensor receiving a data packet broadcasts it to all of its neighbors and this process continues until the packet arrives at the destination or the maximum number of hops for the packet is reached. On the other hand, gossiping is a slightly enhanced version of flooding where the receiving node sends the packet to a randomly selected neighbor, which picks another random neighbor to forward the packet to and so on. Although flooding is very easy to implement, it has several drawbacks, see figures 6.1 redrawn from [5]. Such drawbacks include *implosion* caused by duplicated messages sent to same node, *overlap* when two nodes sensing the same region send similar packets to the same neighbor and *resource blindness* by consuming large amount of energy without consideration for the energy constraints [8]. Gossiping avoids the problem of implosion by just selecting a random node to send the packet rather than broadcasting. However, this cause delays in propagation of data through the nodes.

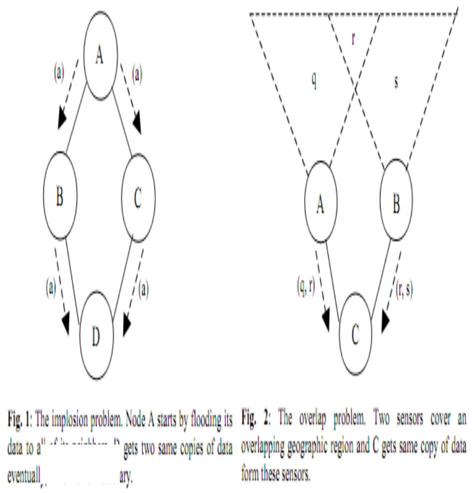

Fig 6.1 Flooding & Gossiping.

Sensor Protocols for Information via Negotiation: (SPIN) [5] is among the early work to pursue a data-centric routing mechanism. The idea behind SPIN is to name the data using highlevel descriptors or meta-data. Before transmission, meta-data are exchanged among sensors via a data advertisement mechanism, which is the key feature of SPIN. Each node upon receiving new data, advertises it to its neighbors and interested neighbors, i.e. those who do not have the data, retrieve the data by sending a request message. SPIN's meta-data negotiation solves the classic problems of flooding such as redundant information passing, overlapping of sensing areas and resource blindness thus, achieving a lot of energy efficiency. There is no standard meta-data format and it is assumed to be application specific, e.g. using an application level framing. There are three messages defined in SPIN to exchange data between nodes. These are: ADV message to allow a sensor to advertise a particular meta-data, REQ message to request the specific data and DATA message that carry the actual data. Fig. 6.2 redrawn from [8], summarizes the steps of the SPIN protocol.

One of the advantages of SPIN is that topological changes are localized since each node needs to know only its single-hop neighbors. SPIN gives a factor of 3.5 less than flooding in terms of energy dissipation and meta-data negotiation almost halves the redundant data. However, SPIN’s data advertisement mechanism cannot guarantee the delivery of data. For instance, if the nodes that are interested in the data are far away from the source node and the nodes between source and destination are not interested in that data, such data will not be delivered to the destination at all. Therefore, SPIN is not a good choice for applications such as intrusion detection, which require reliable delivery of data packets over regular intervals.

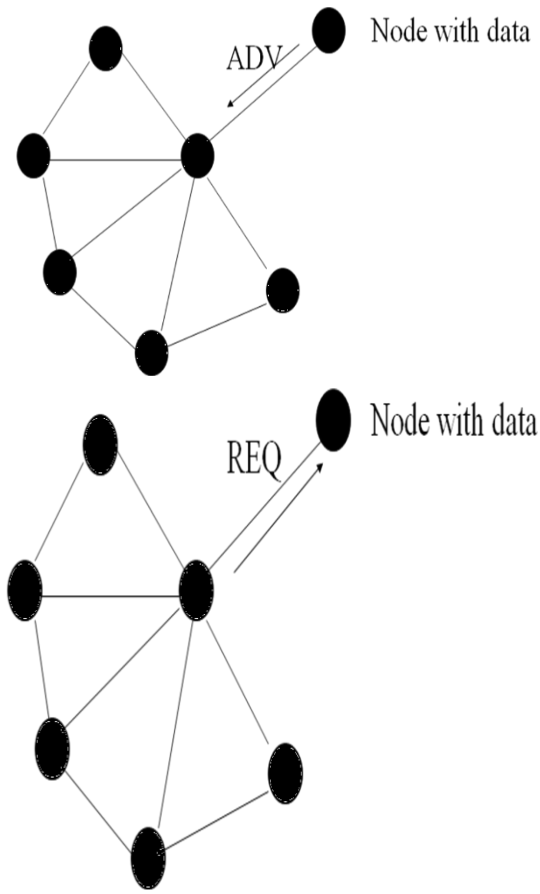

Fig. 6.2: SPIN Protocol.

Directed Diffusion: Directed Diffusion [8][9] is an important milestone in the data-centric routing research of sensor networks. The idea aims at diffusing data through sensor nodes by using a naming scheme for the data. The main reason behind using such a scheme is to get rid of unnecessary operations of network layer routing in order to save energy. Direct Diffusion suggests the use of attribute-value pairs for the data and queries the sensors in an on demand basis by using those pairs. In order to create a query, an interest is defined using a list of attribute-value pairs such as name of objects, interval, duration, geographical area, etc. The interest is broadcast by a sink through its neighbors. Each node receiving the interest can do caching for later use. The nodes also have the ability to do in-network data aggregation, which is modeled as a minimum Steiner tree problem [3]. The interests in the caches are then used to compare the received data with the values in the interests. The interest entry also contains several gradient fields. A gradient is a reply link to a neighbor from which the interest was received. It is characterized by the data rate, duration and expiration time derived from the received interest's fields. Hence, by utilizing interest and gradients, paths are established between sink and sources. Several paths can be established so that one of them is selected by reinforcement. The sink resends the original interest message through the selected path with a smaller interval hence reinforces the source node on that path to send data more frequently.

Path repairs are also possible in Directed Diffusion. When a path between a source and the sink fails, a new or alternative path should be identified. For this, Directed Diffusion basically reinitiates reinforcement by searching among other paths, which are sending data in lower rates. Ganesan et al. [2] suggest employing multiple paths in advance so that in case of a failure of a path, one of the alternative paths is chosen without any cost for searching for another one. There is of course extra overhead of keeping these alternative paths alive by using low data rate, which will definitely use extra energy but more energy can be saved when a path fails and a new path should be chosen.

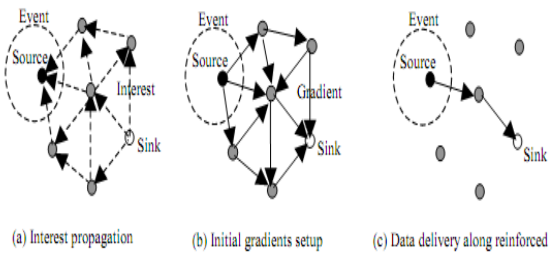

Fig 6.3 Direct Diffusion Protocol Phases.

Energy-aware routing: Shah et al. [9] proposed to use a set of sub-optimal paths occasionally to increase the lifetime of the network. These paths are chosen by means of a probability function, which depends on the energy consumption of each path. Network survivability is the main metric that the approach is concerned with. The approach argues that using the minimum energy path all the time will deplete the energy of nodes on that path. Instead, one of the multiple paths is used with a certain probability so that the whole network lifetime increases. The protocol assumes that each node is addressable through a class-based addressing which includes the location and types of the nodes. There are 3 phases in the protocol:

1) Setup phase: Localized flooding occurs to find the routes and create the routing tables. While doing this, the total energy cost is calculated in each node. For instance, if the request is sent from node N_i to node N_j, N_j calculates the cost of the path as follows:

$$\mathbf{C_{Nj,Ni} = Cost(N_i) + Metric(N_j,N_i)}$$

Here, the energy metric used captures transmission and reception costs along with the residual energy of the nodes. Paths that have a very high cost are discarded. The node selection is done according to closeness to the destination. The node assigns a probability to each of its neighbors in routing (forwarding) table (FT) corresponding to the formed paths. The probability is inversely proportional to the cost. N_j then calculates the average cost for reaching the destination using the neighbors in the forwarding fable (FT_j) using formula. This average cost for N_j is set in the cost field of the request and forwarded.

2) Data Communication Phase: Each node forwards the packet by randomly choosing a node from its forwarding table using the probabilities.

3) Route maintenance phase: Localized flooding is performed infrequently to keep all the paths alive.

The described approach is similar to Directed Diffusion in the way potential paths from data sources to the sink are discovered. In Directed Diffusion, data is sent through multiple paths, one of them being reinforced to send at higher rates. On the other hand, Shah et al. select a single path randomly from the multiple alternatives in order to save energy. Therefore, when compared to Directed Diffusion, it provides an overall improvement of 21.5% energy saving and a 44% increase in network lifetime. However, such single path usage hinders the ability of recovering from a node or path failure as opposed to Directed Diffusion. In addition, the approach requires gathering the location information and setting up the addressing mechanism for the nodes, which complicate route setup compared to the Directed Diffusion.

Rumor routing: Rumor routing [6] is another variation of Directed Diffusion and is mainly intended for contexts in which geographic routing criteria are not applicable. Generally Directed Diffusion floods 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 number of events is small and number of queries is large. Rumor routing is between event flooding and query flooding. The 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.

Gradient-Based Routing: Schurgers et al. [7] have proposed a slightly changed version of Directed Diffusion, called Gradient-based routing (GBR). The idea is to keep the number of hops when the interest is diffused through the network. Hence, each node can discover the minimum number of hops to the sink, which is called height of the node. The difference between a node's height and that of its neighbor is considered the gradient on that link. A packet is forwarded on a link with the largest gradient.

The authors aim at using some auxiliary techniques such as data aggregation and traffic spreading along with GBR in order to balance the traffic uniformly over the network. Nodes acting as a relay for multiple paths can create a data combining entity in order to aggregate data. On the other hand, three different data spreading techniques have been presented:

• Stochastic Scheme: When there are two or more next hops with the same gradient, the node chooses one of them at random.
• Energy-based scheme: When a node's energy drops below a certain threshold, it increases its height so that other sensors are discouraged from sending data to that node.
• Stream-based scheme: The idea is to divert new streams away from nodes that are currently part of the path of other streams.

The data spreading schemes strives to achieve an even distribution of the traffic throughout the whole network, which helps in balancing the load on sensor nodes and increases the network lifetime. The employed techniques for traffic load balancing and data fusion are also applicable to other routing protocols for enhanced performance. Through simulation GBR has been shown to outperform Directed Diffusion in terms of total communication energy.

Constrained anisotropic diffusion routing (CADR) [8] is a protocol, which strives to be a general form of Directed Diffusion. Two techniques namely information-driven sensor querying (IDSQ) and constrained anisotropic diffusion routing (CADR) are proposed. The idea is to query sensors and route data in a network in order to maximize the information gain, while minimizing the latency and bandwidth. This is achieved by activating only the sensors that are close to a particular event and dynamically adjusting data routes.

The major difference from Directed Diffusion is the consideration of information gain in addition to the communication cost. In CADR, each node evaluates an information/cost objective and routes data based on the local information/cost gradient and end-user requirements. The information utility measure is modeled using standard estimation theory.

Although COUGAR provides a network-layer independent solution for querying the sensors, it has some drawbacks: First of all, introducing additional query layer on each sensor node will bring extra overhead to sensor nodes in terms of energy consumption and storage. Second, in-network data computation from several nodes will require synchronization, i.e. a relaying node should wait every packet from each incoming source, before sending the data to the leader node. Third, the leader nodes should be dynamically maintained to prevent them from failure.

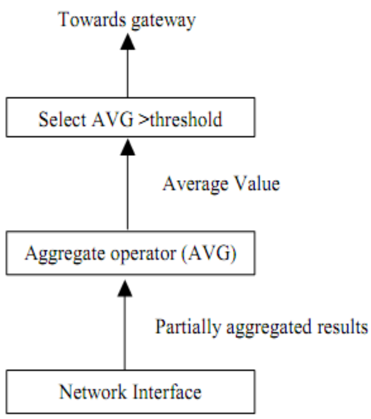

Fig. 5: Query plan at a leader node: The leader node gets all the readings, calculates the average and if it is greater than a threshold sends it to the gateway (sink).

Fig 6.4 COUGAR.

ACQUIRE: A fairly new data-centric mechanism for querying sensor networks is ACtive Query forwarding In sensor nEtworks (ACQUIRE) [3]. As in [4], the approach views the sensor network as a distributed database and is well-suited for complex queries which consist of several sub queries. The querying mechanism works as follows: The query is forwarded by the sink and each node receiving the query, tries to respond partially by using its pre-cached information and forward it to another sensor. If the pre-cached information is not up-to-date, the nodes gather information from its neighbors within a look-ahead of *d* hops. Once the query is being resolved completely, it is sent back through either the reverse or shortest-path to the sink.

One of the main motivations for proposing ACQUIRE is to deal with one-shot, complex queries or data where a response can be provided by many nodes. Since, the data-centric approaches such as Directed Diffusion uses flooding-based query mechanism for continuous and aggregate queries; it would not make sense to use the same mechanism for one-shot complex queries due to energy considerations. ACQUIRE mechanism provides efficient querying by adjusting the value of parameter *d.* Note that if *d* is equal to network size, then the protocol behaves similar to flooding. On the other hand, the query has to travel more hops if *d* is too small.

Hierarchical protocols

Similar to other communication networks, scalability is one of the major design attributes of sensor networks. A single-tier network can cause the gateway to overload with the increase in sensors density. Such overload might cause latency in communication and inadequate tracking of events. In addition, the single-gateway architecture is not scalable for a larger set of sensors covering a wider area of interest since the sensors are typically not capable of long-haul communication. To allow the system to cope with additional load and to be able to cover a large area of interest without degrading the service, networking clustering has been pursued in some routing approaches.

The main aim of hierarchical routing is to efficiently maintain the energy consumption of sensor nodes by involving them in multi-hop communication within a particular cluster and by performing data aggregation and fusion in order to decrease the number of transmitted messages to the sink. Cluster formation is typically based on the energy reserve of sensors and sensor's proximity to the cluster head [2]. LEACH [4] is one of the first hierarchical routing approaches for sensors networks. The idea proposed in LEACH has been an inspiration for many hierarchical routing protocols [6][2][10], although some protocols have been independently developed [1][5]. We explore hierarchical routing protocols in this section.

Low-Energy Adaptive Clustering Hierarchy (LEACH)

IEEE Proceedings of the Hawaii International Conference on System Sciences, January 4-7, 2000, Maui, Hawaii.
Energy-Efficient Communication Protocol for Wireless Microsensor Networks Wendi RabinerHeinzelman, AnanthaChandrakasan, and HariBalakrishnan Massachusetts Institute of Technology

In this paper author present an energy efficient protoconLEACH which is one of the most popular hierarchical routing algorithms for sensor networks. The idea is to form clusters of the sensor nodes based on the received signal strength and use local cluster heads as routers to the sink. This will save energy since the transmissions will only be done by such cluster heads rather than all sensor nodes. Optimal number of cluster heads is estimated to be 5% of the total number of nodes.

All the data processing such as data fusion and aggregation are local to the cluster. Cluster heads change randomly over time in order to balance the energy dissipation of nodes. This decision is made by the node choosing a random number between 0 and 1. The node becomes a cluster head for the current round if the number is less than the predefined threshold.

LEACH achieves over a factor of 7 reduction in energy dissipation compared to direct communication and a factor of 4-8 compared to the minimum transmission energy routing protocol. The nodes die randomly and dynamic clustering increases lifetime of the system. LEACH is completely distributed and requires no global knowledge of network. However, LEACH uses single-hop routing where each node can transmit directly to the cluster-head and the sink. Therefore, it is not applicable to networks deployed in large regions. Furthermore, the idea of dynamic clustering brings extra overhead, e.g. head changes, advertisements etc., which may diminish the gain in energy consumption.

PEGASIS & Hierarchical-PEGASIS: Power-Efficient GAthering in Sensor Information Systems (PEGASIS) [10] 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 Fig. 6 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.

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 to 300% for different network sizes and topologies. Such performance gain is achieved through the elimination of the overhead caused by dynamic

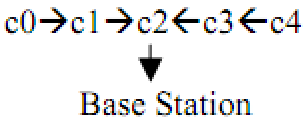

Fig 6.5 Chaining in PEGASIS.

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.

Hierarchical-PEGASIS [2] is an extension to PEGASIS, which aims at decreasing the delay incurred for packets during transmission to the base station and proposes a solution to the data gathering problem by considering energy × delay metric. In order to reduce the delay in PEGASIS, simultaneous transmissions of data messages are pursued. To avoid collisions and possible signal interference among the sensors, two approaches have been investigated. The first approach incorporates signal coding, e.g. CDMA. In the second approach only spatially separated nodes are allowed to transmit at the same time.

The chain-based protocol with CDMA capable nodes, constructs a chain of nodes, that forms a tree like hierarchy, and each selected node in a particular level transmits data to the node in the upper level of the hierarchy. This method ensures data transmitting in parallel and reduces the delay significantly. Since the tree is balanced, the delay will be in O(lg N) where N is the number of nodes.

Threshold sensitive Energy Efficient sensor Network protocol (TEEN) [6] 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. The model is depicted in Fig.2.6, which is redrawn from [6].

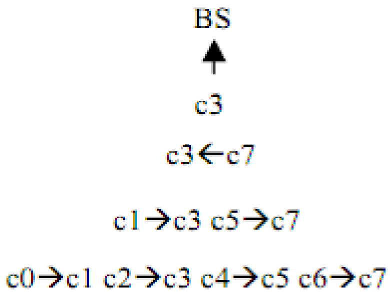

Fig 6.6 Data gathering in a chain based binary scheme.

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 value of that attributes 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.

The Adaptive Threshold sensitive Energy Efficient sensor Network protocol (APTEEN) [5] is an extension to TEEN and aims at both capturing periodic data collections and reacting to time-critical events. The architecture is same as in TEEN. When the base station forms the clusters, the cluster heads broadcast the attributes, the threshold values, and the transmission schedule to all nodes. Cluster heads also perform data aggregation in order to save energy.

APTEEN supports three different query types: historical, to analyze past data values; one-time, to take a snapshot view of the network; and persistent to monitor an event for a period of time. Simulation of TEEN and APTEEN has shown them to outperform LEACH [4]. The experiments have demonstrated that APTEEN's performance is between LEACH and TEEN in terms of energy dissipation and network lifetime. TEEN gives the best performance since it decreases the number of transmissions. The main drawbacks of the two approaches are the overhead and complexity of forming clusters in multiple levels, implementing threshold-based functions and dealing with attribute-based naming of queries.

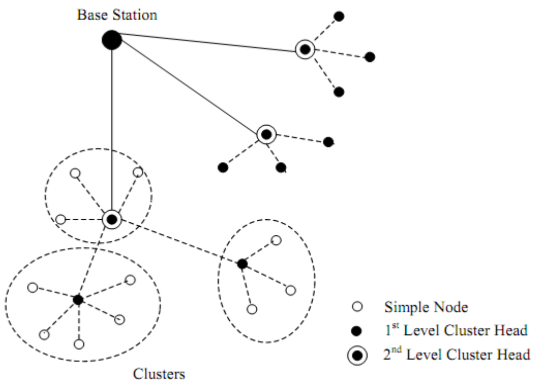

Fig 6.7 Hierarchical Clustering in TEEN & APTEEN

IMPROVE V-LEACH

IEEE 2012 Third International Conference on Advanced Computing & Communication Technologies

An EXTENED VICE-CLUSTER SELECTION APPROACH TO IMPROVE V LEACH PROTOCOL IN WSN

Mrs. Asha Ahlawat, MsVineetaMalik , Department of electronics and communication, Hindu college of engineering Sonepat, India

In the above paper author completely analyzed the typical clustering Routing Protocol-LEACH and its deficiencies and proposed improved v-leach. The work to be done in improved v-leach protocol on selection of vice cluster head. The Vice Cluster head is that alternate head that will work only when the cluster head will die. And author makes comparison of LEACH protocol and improved V-LEACH protocol. From the simulation results, author can draw a number of conclusions first: the number of alive nodes is more than the original leach. Second, the number of dead nodes is less than the original leach protocol. The network lifetime is increased as compare to LEACH.

SEP PROTOCOL: We study the impact of heterogeneity of nodes, in terms of their energy, in wireless sensor networks that are hierarchically clustered. In these networks some of the nodes become cluster heads, aggregate the data of their cluster members and transmit it to the sink. We assume that a percentage of the population of sensor nodes is equipped with additional energy resources—this is a source of heterogeneity which may result from the initial setting or as the operation of the network evolves. We also assume that the sensors are randomly (uniformly) distributed and are not mobile, the coordinates of the sink and the dimensions of the sensor field are known. We show that the behavior of such sensor networks becomes very unstable once the first node dies, especially in the presence of node heterogeneity. Classical clustering protocols assume that all the nodes are equipped with the same amount of energy and as a

VI. CONCLUSIONS

Energy efficiency of WSNs is a vital point to be discussed because of their wide application. The LEACH protocol is considered to be a basis for all hierarchical protocols proposed in the literature. It has many merits like load balancing, energy efficiency and self-organization. But it has some demerits like poor scalability for very large network areas and it is not considering the residual energy of individual sensor nodes. Hence, to overcome the demerits many researchers are being still proposing the modified versions of LEACH protocol. In this article, we have reviewed some of the state of art LEACH based protocols. It has been found that there is a scope of improvement in energy efficient hierarchical clustering algorithms for real time applications.

REFERENCE

[1]. J. Kulik, W. R. Heinzelman, and H. Balakrishnan, "Negotiation-based protocols for disseminating information in wireless sensor networks," Wireless Networks, Volume: 8, pp. 169-185, 2002.
[2]. C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed diffusion: a scalable and robust communication paradigm for sensor networks," Proceedings of ACM MobiCom '00, Boston, MA, 2000, pp. 56-67.
[3]. A. Manjeshwar and D. P. Agarwal, "TEEN: a routing protocol for enhanced efficiency in wireless sensor networks," In 1st International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing, April 2001.

[4]. A. Manjeshwar and D. P. Agarwal, "APTEEN: A hybrid protocol for efficient routing and comprehensive information retrieval in wireless sensor networks," Parallel and Distributed Processing Symposium., Proceedings International, IPDPS 2002, pp. 195-202.

[5]. W. Heinzelman, A. Chandrakasan and H. Balakrishnan, "Energy-Efficient Communication Protocol for Wireless Microsensor Networks," Proceedings of the 33rd Hawaii International Conference on System Sciences (HICSS '00), January 2000.

[6]. SundeepKarthikeyanVaidynathan, Sayantansur and Sinha. Data aggregation techniques in sensor networks. Technical Report,OSU-CISRC-11/04-TR60, 2004.

[7]. D. Agrawal N. Shrivastava, C. Buragohain and S. Suri. Medians and beyond: new aggregation techniques for sensor networks. Proceedings of the 2nd international conference on Embedded networked sensor systems, pages 239{249, 2004. ACM Press.75 Bibliography

[8]. XiuliRen and Haibin Yu1. Security mechanisms for wireless sensor networks. IJCSNS International Journal of Computer Science and Network Security, VOL.6(No.3):100{107, March 2006.

[9]. S. Setia S. Zhu and S. Jajodia. Leap: efficient security mechanisms for large scale distributed sensor networks. Proceedings of the 10th ACM conference on Computer and communications security, pages 62-72, 2003. ACM Press.

[10]. Y. Xu, J. Heidemann, 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, pp. 70-84.

Vikram Pratap Singh Thakur, et. al. "A Review Article on an Effective Routing Algorithm Based On Optimization in Wireless Sensor Networks." *International Journal of Engineering Research and Applications (IJERA)*, vol.10 (08), 2020, pp 39-49.