International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2020): 7.803

Energy Efficient Sensory Data Collection in Wireless Sensor Networks

Liji Varghese

Lecturer, Department of Computer Engineering, SCMS College of Polytechnics, Kerala, India

Abstract: ***Wireless Sensor Networks consist of numerous nodes with sensing, computing and wireless communication capabilities. When WSNs are utilized in safety-critical or highly-reliable applications, two-timing constraints are considered: real-time constraints and network lifetime constraints. WSNs security is required due to it's sensitive information transmission and utilized in a wide range of application like military sensing and tracking, health monitoring, data acquisition in hazardous environments and habitat monitoring. Wireless Sensor network applications involve a group of isolated urban area consisting of sensor nodes monitoring environmental parameters. Our proposed protocol aims at minimizing the general network overhead and energy cost using multi hopping data retrieval process which always ensures sensible energy consumption among various sensor nodes and more network lifetime. This is often achieved through building efficient cluster structures which consist of sensor nodes that can route their measured data to thier assigned cluster head. Energy efficiency is achieved using mobile sinks.***

Keywords: Cluster Head, Cluster Structures, Energy Consumption, Security

1. Introduction

Wireless sensor networks could easily envision a wide range of real-world WSN-based applications from sensor-based environmental monitoring, home automation, health care, and security class of applications. We are witnessing new research challenges related to the design of algorithms and network protocols that will enable the development of sensor-based applications. A wireless sensor network has sensor nodes capable of collecting information from the environment and communicating with each other via wireless transceivers[9]. The collected data are going to be delivered to at least one or more sinks, generally via multi-hop communication. The sensor nodes are expected to work with low batteries and are often deployed to not-easily-accessible in large quantities. It is difficult to replace the batteries of the sensor nodes. On the opposite hand, the sink is usually rich in energy. The researchers are going for the efficient utilization of the energy to prolong the network lifetime sensor energy since it is the most precious resource in the WSN[4]. The communications within the WSN have the many-to-one property therein data from an outsized number of sensor nodes tend to be concentrated into a couple of sinks. To save energy for distant sensor nodes from the sinks, multi-hop routing is generally needed so that the nodes near a sink can be burdened with relaying a large amount of traffic from other nodes.

Sensor nodes are limited resources in terms of power, processor, and memory, and low-bandwidth and bandwidth connections. Limited battery power is used to operate sensory nodes and it is very difficult to replace or refill them when the nodes die[2]. This will affect network performance. Energy-saving and harvesting increase the life of the network. To increase the range of communication and reduce energy consumption, we need to save the energy of

hearing areas. Sensors nodes are used to collect data and wish all nodes to work continuously and transmit data as long as possible. This address deals with the life problem of wireless network networks. Node sensors use their power while transmitting data, receiving, and transmitting packets. Therefore, designing algorithms for routes that extend the life until the end of the first battery are important reasons to consider. Our goals in reducing the overall network overtime and in increasing data performance have ensured the use of power between SNs and longevity. Many methods that exploit the flow of the sink in data collection on WSNs have been suggested in recent years. In a single-hop connection, we can reduce power consumption, however, due to delays in high data delivery. In the second solution, this delay is low but the power consumption due to multi hop connections is very high.

Many applications of wireless sensor networks are considered to handle critical situations where data retrieval time is critical [3], i.e., bringing each location's information as quickly as possible to the base station becomes a critical issue.

It is important to ensure that the information can be successfully obtained from the base station for the first time instead of being transferred again. In wireless parts of the network data, collection and road construction are challenging tasks due to their powerful and unique structures. Many router agreements are made, but among those processes are grouped operations that are energy-efficient, fast, and extend the life of the network. In the event of receiving events, the nodes are idle and active at the time the event takes place[10]. The sensors node periodically sends collection data to the base station. Traffic is an important problem in compiling network data, and on the other hand, synchronizing sleep and wakefulness are important network problems for event access. Recent years have seen the emergence of WSNs as a new data-gathering paradigm, in which a large number of sensors spread across the field of surveillance and extract data of interest by studying real-world events in the physical environment.

2. Characteristics

Our proposed protocol aims to reduce the overall network usage and power consumption. It is associated with the process of retrieving large amounts of data while ensuring balanced power consumption between SNs and long network life. This is achieved by constructing clusters of structures containing nodes that members submit their measured data to the head of their assigned group (CH). Combining has proven to be an effective way to plan a network in the context above. In addition to gaining power efficiency, the merger reduces channel collisions and packet collisions [6], which has led to network development under greater load. Benefits of power consumption between the lives of a Sensor that ensures an increase. Enables limited power consumption across WSN by building exploitative cluster structures. It also reduces data overload. Power consumption becomes a very important factor in WSN because the network needs to operate at the expected time. Power consumption becomes a very important factor in WSN because the network needs to operate at the expected time. Lowering data packets is transferred to the data sink via multi-hop transmission between sensors [10]. Due to the nature of the multi-hop channels, the packets have to undergo multiple transmissions before accessing the data sink. As a result of multi-hop, a lot of energy is used to transfer data along the way. Instead of reducing the power consumption in the transmission path does not mean that it extends the life of the network as some popular sensors along the way may lose power faster than others, which can cause unequal power consumption throughout the network.

3. Network Architecture

Wireless mesh architecture is the first step in providing high-performance and dynamic high bandwidth networks in a particular coverage area. Wireless network infrastructure construction is a router network eliminating the installation between nodes [4]. It is made up of peer-to-peer radio devices that do not need to be plugged into a cable port like traditional WLAN (AP) points. The Mesh design supports signal strength by breaking long distances into a series of short hops.

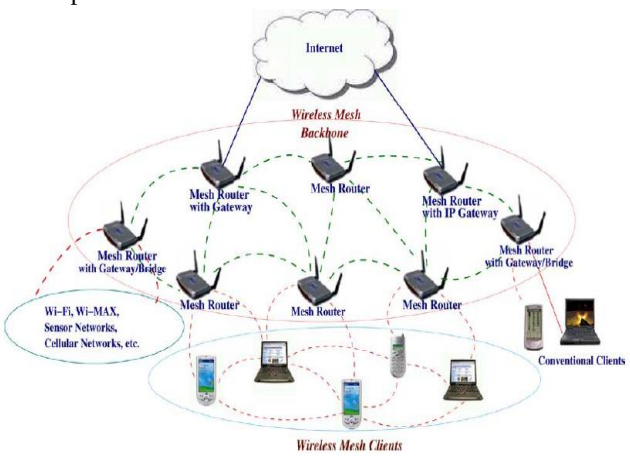

Figure 1: Wireless Mesh Architecture

Medium channels not only amplify signals but collectively make transfer decisions based on their network knowledge, which means creating a route. Such a design with careful design can provide high bandwidth spectral efficiency, and economic benefits over the cover area. Wireless networks have a stable structure without the occasional failure of nodes or the addition of new nodes. The traffic method, compiled by a large number of end-users, is constantly changing[5]. Almost every road connected to a network mechanical network is forwarded to or from the gate, while in connecting networks or networks with customer spaces traffic flows between two nodes. There are various types of wireless networks used to attract various communications. They are

1) Infrastructure Networks
2) Rapidly Deployable Networks
3) Hybrid Networks

3.1 Infrastructure Networks

Infrastructure Networks contain special nodes called access points (APs), which are connected via existing networks. APs are special in the sense that they can interact with wireless nodes as well as with the existing wired network. The other wireless nodes, also known as mobile stations (STAs), communicate via APs. The APs also act as bridges with other networks. In this structure, mesh routers create infrastructure, where the dashed and solid lines show wireless links and cables, respectively. The wireless mesh network is a backbone infrastructure that can be built using a variety of radio technologies, space-based routers that create a self-configuring mechanism, live links between them [7]. With function, mesh routers can be connected to the Internet. This approach, also called infrastructure meshing, provides the backbone for standard clients and enables WMN connectivity through existing wireless networks, through gate/bridge operation on mesh routers. Ordinary clients with an Ethernet interface can connect to mesh routers via Ethernet links. For regular clients with the same radio technology as mesh routers, they can communicate directly with mesh routers. When using different radio technologies, clients must connect to their channels with Ethernet connections on mesh routers. Client meshing provides peer-to-peer networks between client devices [2]. In this type of architecture, client nodes form a real network to perform configuration and configuration tasks and provide end-user applications to customers.

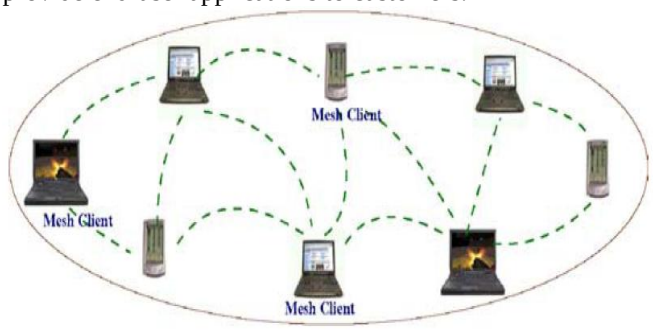

Figure 2: Wireless mesh network clients

So that mesh router is not needed. Wireless mesh network clients are usually built using the same type of radio on devices. Therefore, the Client wireless mesh network is similar to a normal ad network. However, the requirements for end-user devices are increasing compared to the meshing

of infrastructure, because in client wireless mesh network end users have to perform additional tasks such as routing and configuration.

3.2 Rapidly Deployable Networks

In emergency response times, where the basic communication infrastructure is completely dismantled, is a critical and challenging task. In such a situation, rapidly deployable networks are needed to enable first responders to interact with disaster survivors, each other, and the control room. These networks operate under challenging conditions, such as power constraints and establishing a network back haul; further, the network must be easy to deploy, operate, and maintain. To mobilize the smooth transit of rescue teams for providing emergency services in disaster situations, a number of disaster management schemes or rapid deployment systems have been proposed in the literature that mainly focus on emergency communication in order to connect first responders to the control server[3].They have developed an energy efficient routing protocol that limits the number of duplicate messages transmission to improve the data delivery ratio and extend the operating time of battery-powered devices.

The protocol reduces duplicate messages by finding recurring contacts and generates a routing table that uses recurring contacts to transmit a message to a destination. By finding repeated contacts and creating a routing table that utilizes these repeated contacts to send a message to a destination, the proposed protocol considerably reduces the number of control and operation management messages. Owing to reduction in message transmissions, their protocol improved the overall network energy consumption[1], while maintaining a high delivery rate. In this system to help military officers in critical situations, such as war conditions or attacks in a gangster area. In military warfare, a robust communication system is required so that the military head can communicate with the soldiers and relay the information easily. A mobile robot is utilized to carry and deploy the nodes at the scene of incident. However, nodes have restricted ranges and can be damaged as the robot moves around snags. The proposed system has communication limitations in situations where no line of sight will be available, such as in urban area.

3.3 Hybrid Networks

This structure is a combination of infrastructure and mesh network. Mesh clients can access the network through mesh routers and connect directly with other clients with spaces. While the infrastructure provides connectivity to other Sensory networks, capabilities provide advanced connectivity and integration within wireless mesh network [WMN]. The features of wireless mesh networks are described below, where hybrid constructs are considered. As it contains all the benefits of wireless networks. It supports network connectivity and can create, live and organize itself. Wireless networks are multi-hop but have wireless/core infrastructure provided by mesh routers[2]. Mesh routers have minimal mobility and create a dedicated and dedicated router, which greatly reduces the customer load of mesh and other end nodes. End node traffic is easily supported by wireless infrastructure. Mesh routers cover a wide range of networks, including both wireless and wireless. Therefore, many types of network access are available on WMNs. Power barriers are different for mesh routers and mesh clients. It also works with other wireless networks.

4. Communication in wireless sensor Networks

Through wireless sensor networks (WSN), we can acquire the various interesting event information around sensor nodes through multihop communications. In WSN, there are two types of applications, that is, event or query based. Commonly, in these application, the value on each sensor node is very sensitive to delay or latency. So, it is strongly required to deliver data to sink node within the deadline since data received after the deadline is not acceptable at all in WSN[6]. The good example of application demanding real-time communication in WSN includes tracking of moving object and intrusion detection.However, compared to typical networks, it is very difficult to achieve real-time communication in WSN. Severe constraints such as limited computing power and narrow bandwidth are not suitable to provide real-time communication accordingly. So, a number of important issues and research challenges have to be addressed to provide real-time communication in WSN[4]. Based on this demand, this special issue is planned to contribute to advances in real-time communications in WSN. In order to guarantee latency forunpredictable on-demand communications, a root node controls the transmission timing of high-priority packets,while other nodes autonomously decide what channel to use and when to transmit packets to a neighbor. In the proposed scheme, packet priority is determined in accordance with application requirements. The proposed scheme operates over a MAC layer and does not rely on any specific MAC protocol.

5. Security Requirements in Wireless Sensor Networks

The Wireless Sensor Network contains autonomous sensors distributed locally to monitor global environmental conditions. The development of wireless nerve networks was encouraged by the use of the military as a precaution on the battlefield. Wireless Sensor Networks (WSN) are installed in critical areassuch as surveillance, airports, military applications so protecting wireless nerve networks is a very difficult task. The following are the security requirements for networks.

5.1 Confidentiality

A privacy requirement is required to ensure that sensitive information is properly protected and is not disclosed to unauthorized third parties.

The purpose of privacy helps to protect information that flows between the network's sensors or between the sensors and the channel's channel from exposure, as the enemy with the appropriate equipment can listen to the communication. By listening silently, the enemy may hear sensitive information such as hearing data and traffic information.

Depending on the sensitivity of the stolen data, the enemy can cause serious damage because it can use information to detect many illegal intentions which means offenses, fraud [10]. For example, competitors can use data to produce a better product i.e. a sensor security monitoring app.

In addition, by stealing tracking information the enemy could enter its own network nodes in an attempt to hear all communications. If we consider eavesdrop adoption as a network level threat [3], then a local level threat could be a negative threat to the enemy. Encrypted nodes are a major threat to privacy purposes because the enemy may steal sensitive data stored on nodes such as cryptographic keys used to encrypt the connection.

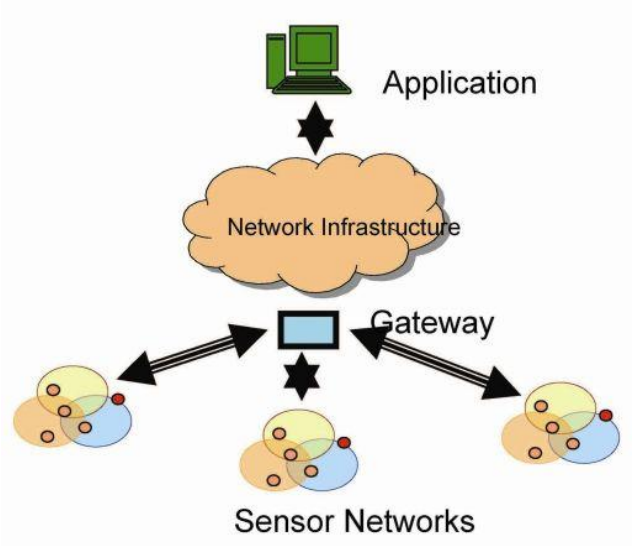

Figure 3: Confidentiality in sensor networks

5.2 Authentication

As with traditional systems, verification strategies ensure the identity of the participants in the communication, thus separating legitimate users from the participants.

In the case of sensor networks, it is important that each sensor node and base station have the ability to ensure that the received data is actually sent by a trusted sender and not the enemy who has deceived legitimate sources in receiving false data. If such a case took place and false information was provided on the network, then the network's behavior would have been predictable and many times it would not have come out as expected [9].

The purpose of authenticity is important to achieve in the consolidation of spaces. Integration involves classification according to a particular attribute such as location, hearing data etc and that each cluster usually has a cluster head which is a node that joins its cluster and the entire sensor network (i.e. communication between different clusters is done through cluster heads). In these cases, where consolidation is required, there are two verification cases to be investigated; first, it is important to ensure that the nodes contained in each cluster will only exchange data with authorized nodes contained and trusted by the specified cluster (based on a specific verification process). Alternatively, if nodes within a collection receive data from unreliable nodes within the current node community and continue to process it, the expected data from that collection will be based on false data and may cause damage[11]. The second condition of verification involves communication between the heads of the councils of each group; communication should only be established by group heads who can prove their identity No malicious node should be able to act as the header of the group and communicate with the official header of the collection, send false information or retrieve modified data.

5.3 Integrity

Moving on to the integrity objective, there is the danger that information could be altered when exchanged over insecure networks. Lack of integrity could result in many problems since the consequences of using inaccurate information could be disastrous, for example for the healthcare sector where lives are endangered.

Integrity controls must be implemented to ensure that information will not be altered in any unexpected way. Many sensor applications such as pollution and healthcare monitoring rely on the integrity of the information to function with accurate outcomes; it is unacceptable to measure the magnitude of the pollution caused by chemicals waste and find out later on that the information provided was improperly altered by the factory that was located nearby the monitored lake[6]. Therefore, there is urgent need to make sure that information is traveling from one end to the other without being intercepted and modified in the process.

5.4 Freshness

Many other attacks have been made on sensory networks to attack messages where the enemy can capture messages exchanged between locations and repeat them over time to create confusion on the network. The purpose of data updating ensures that the messages are new, which means they are compliant with the message order and have not been reused. To achieve innovation, network agreements must be designed to identify duplicate packets and dispose of them to prevent potential interference.

5.5 Secure Management

Management is required for all programs built from multiple sources and sensitive information is handled. In the case of sensory networks, we need secure management at the base station level; as sensory connections keep in the base station, issues such as distribution of keys to sensor nodes in order to establish encryption and transmission information require secure management [1]. In addition, integration requires secure management as well, as each group of nodes can add a large number of nodes that need authentication to each other and exchange information securely. In addition, the interaction of each sensor network can change rapidly and rapidly. Therefore, secure group management policies are required to add and remove members and validate data in node groups.

5.6 Availability

Availability ensures that services and information can be accessed at the time that they are required. In sensor networks, there are many risks that could result in loss of availability such as sensor node capturing and denial of service attacks. Lack of availability may affect the operation of many critical real-time applications like those in the healthcare sector that require a 24/7 operation that could even result in the loss of life. Therefore, it is critical to ensure resilience to attacks targeting the availability of the system and find ways to fill in the gap created by the capturing or disablement of a specific node by assigning its duties to some other nodes in the network.

5.7 Quality of Service

Quality of Service objective is a bigheadache to security. And when we are speaking about sensor networks with all the limitations they have, quality of service becomes even more constrained. Security mechanisms must be lightweight so that the overhead caused for example by encryption must be minimized and not affect the performance of the network. Performance and quality in sensor networks involve the timely delivery of data to prevent for example propagation of pollution and the accuracy with which the data reported match what is actually occurring in their environment.

Applications of Wireless Sensor Networks

- Fire detection
- Water quality monitoring
- landslide detection
- Air pollution monitoring
- Data center monitoring

FacebookTwitter

6. Review of Different Phases

6.1 Cluster Formation Phase

Cluster heads will be specialized nodes with power or a standard node depending on the algorithm and usage [3]. Here the base station is the head of the cluster that performs integration functions such as data integration and data compression to reduce the amount of transmission to the base station (or sink) thus saving energy. Composition-based algorithms are believed to be the most effective algorithm for WSNs.

Improve bandwidth consumption by reducing friction Work is currently underway on energy efficiency in WSNs which will lead to the selection of cluster heads. Setting up a small hop-count transfer. To navigate the Multi-hop route, packets must undergo multiple transmissions before accessing the data sink[6]. Reducing the use of power utilizing transmission does not mean that it extends the lifespan of the network to other sensors along the way. The problem with static precision is that when a node transfers data continuously, that node will lose a lot of power. It can cause node failure.

To use a strong node. If the previous node is switched on by the hop down node then the power loss of the node should be very small.

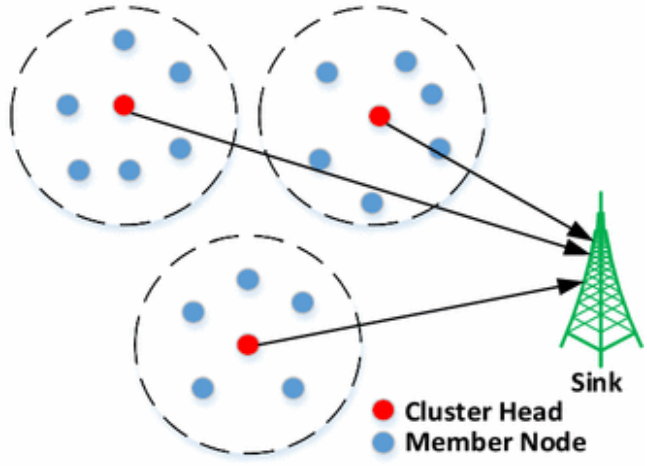

Figure 4: Cluster Formation Phase

6.2 Rendezvous node attachment for cluster head

The RNs' selection process commences immediately afterward the information needed for the execution of this phase.CHs located far from the MS trajectories do not have any RNs within transmission range It is noted that our approach typically requires a single MS trip to collect the information needed to execute the setup phase[1]. All these phases complete in reasonably short period of time As soon as the set up phase finalizes, sensory data collected at CHs from their attached cluster members are forwarded toward the RNs following an intercluster overlay graph.

6.3 Data Forwarding to Rendezvous Nodes

The data accumulated at individual source nodes aresent to local Cluster Head (CHs). CHs perform data processing to remove spatial-temporal data redundancy, which is likely to exist since cluster members are located maximum two hops away[8]. CHs then forward filtered data toward remote CH they are attached to. Alongside the intercluster path, a second-level of data filtering may apply. In the case that multiple RNs exist in that cluster, data are not equally distributed among them. Instead, the CH favors the data delivery by the most suitable RN[7]. Data distribution among RNs should ensure that each RN will be able to accommodate its assigned data, i.e., to deliver all its buffered data and not experience an outage.

6.4 Communication between Rendezvous node and Mobile Sinks

The data accumulated at individual source nodes are sent to local Cluster Head (CHs). CHs perform data processing to remove spatial-temporal data redundancy, which is likely to exist since cluster members are located maximum two hops away. CHs then forward filtered data toward remote CH they are attached to. Alongside the intercluster path, a second-level of data filtering may apply. In the case that multiple RNs exist in that cluster, data are not equally distributed among them[4]. Instead, the CH favors the data delivery by the most suitable RN. Data distribution among RNs should ensure that each RN will be able to accommodate its assigned data, i.e., to deliver all its

buffered data and not experience an outage.

6.5 Selection of sensor in Rendezvous node

This selection largely determines network lifetime. RNs lie within the range of traveling sinks and their location depends on the position of the CH and the sensor field with respect to the sinks trajectory. Suitable RNs are those that remain within the MS's range for relatively longtime[3], in relatively short distance from the sink's trajectory and have sufficient energy supplies in practical deployments A large number of RNs implies that the latter will compete for the wireless channel contention as soon as the mobile robot appears in range, thereby resulting in low data throughput and frequent outages.A small number of RNs implies that each RN is associated with a large group of sensors[1]. Hence, RNs will be heavily used during data relays, their energy will be consumed fast and they will be likely to experience buffer overflows.

7. Conclusion

Energy efficiency is one of the important issues in wireless sensor networks. So to overcome this issue in this paper we are using mobile sinks. It provide uniform load balancing and also the hotspots around the sink changes through which it achieves uniform energy consumption. The output can be simulated using Network Simulator -2 which is an open source simulation tool. Another major advantage is security. It is difficult for attackers to locate and chase mobile sinks to get the sensitive information.

References

[1] Chris Townsend and Steven Arms. Wireless Sensor Network: Principles and Applications. Sensor Magazine, February, 2004.
[2] R. Szewczyk, A. Mainwaring, J. Anderson and D. Culler. An Analysis of a Large Scale Habit Monitoring Application. In SenSys'04, 2004.
[3] G. Tolle, J. Polastre, R. Szewczyk, N. Turner, K. Tu, S. Burgess, D. Gay, P. Buonadonna, W. Hong, T. Dawson, and D. Culler. A Macroscope in the Redwoods. In SenSys'05, November 2005.
[4] N. Xu, S. Rangwala, K. K. Chintalapudi, D. Ganesan, A. Broad, R. Govindan, and D. Estrin. A Wireless Sensor Network for Structural Monitoring. In SenSys'04, 2004.
[5] T. He and et. al. VigilNet: An Integrated Sensor Network System for Energy-Efficient Surveillance. ACM Transactions on Sensor Networks, Vol. 2(No. 1): Page 1 – 38, February 2006.
[6] Aditya Singh Mandloi and Vineeta Choudhary, "Study of Various Techniques for Data Gathering in WSN", ISROSET-IJSRNSC, Vol-1, Issue-2, pp (12-15), Jul – Aug 2013
[7] N. Li and J. C. Hou. FLSS: A fault-tolerant topology control algorithm for wireless networks. In Proceedings of the ACM International Conference on Mobile Computing and Networking (MobiCom), Philadelphia, Pennsylvania, September 2004.
[8] X. Li, I. Stojmenovic, and Yu Wang. Partial Delaunay triangulation and degree limited localized Bluetooth scatternet formation. IEEE Transactions on Parallel and Distributed Systems, 15(4):350–361, April 2004.
[9] N. Li and J. C. Hou. FLSS: A fault-tolerant topology Control algorithm for wireless networks. In Proceedings of the ACM International Conference on Mobile Computing and Networking (MobiCom), Philadelphia, Pennsylvania, September 2004.
[10] Handbook of Sensor Networks: Algorithms and Architectures, Edited by I. Stojmenovic´ ISBN 0-471-68472-4 Copyright # 2005 John Wiley & Sons, Inc.
[11] V. Rodoplu and T. H. Meng. Minimum energy mobile wireless networks, IEEE Journal on Selected Areas in Communications, 17(8):1333–1344, August 1999.