© 2017 IJSRSET | Volume 3 | Issue 8 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

Routing Protocols in Wireless Networks New Security Methodology

Rakesh Kumar Singh, Pinki Singh, Deepak Chikara
Department of Computer Science and Engineering, IIMT college of Engineering, Greater Noida, India

ABSTRACT

Advances in wireless sensor network (WSN) technology has provided the availability of small and low-cost sensor nodes with capability of sensing various types of physical and environmental conditions, data processing, and wireless communication. The self-organizing network which is Mobile ad hoc network (MANET) its established automatically via wireless connections by a combination of portable nodes without the support of a centralized management or static infrastructure. The portable nodes redirect packets among these nodes, enabling connection between nodes outside the range of wireless transmission hop by hop capabilities are necessary. Finally, the proposed algorithm depended on the Dynamic Source Routing (DSR) to remove malicious nodes, minimum spanning tree for routing path plus coding-encryption technique of a chaos based adaptive arithmetic for encrypting, compression plus decompression, decrypt a message. In this paper, we give a survey of routing protocols for Wireless Sensor Network and compare their strengths and limitations.

Keywords : Wireless Sensor Networks, Routing Protocols, Cluster Head

I. INTRODUCTION

Wireless sensor network (WSN) is widely considered as one of the most important technologies for the twenty-first century [1]. In the past decades, it has received tremendous attention from both academia and industry all over the world. A WSN typically consists of a large number of low-cost, low-power, and multifunctional wireless sensor nodes, with sensing, wireless communications and computation capabilities [2,3]. These sensor nodes communicate over short distance via a wireless medium and collaborate to accomplish a common task, for example, environment monitoring, military surveillance, and industrial process control [4]. The basic philosophy behind WSNs is that, while the capability of each individual sensor node is limited, the aggregate power of the entire network is sufficient for the required mission.

In the portable ad hoc networks every nodes provided by a receiver plus transmitter. This wireless receiver and transmitter enable the nodes at the same radio communication range to contact with each other. Habitually nodes participate with the same physical media; they transmit and collect signals at the same frequency band, and follow the same step sequence or broadcasting code Sensor nodes are battery-powered and are expected to operate without attendance for a relatively long period of time. In most cases it is very difficult and even impossible to change or recharge batteries for the sensor nodes. WSNs are characterized with denser levels of sesensor node deployment, higher unreliability of sensor nodes, and sever power, computation, and memory constraints. Thus, the unique characteristics and constraints present many new challenges for the development and application of WSNs.

Due to the severe energy constraints of large number of densely deployed sensor nodes, it requires a suite of network protocols to implement various network control and management functions such as synchronization, node localization, and network security. The traditional routing protocols have several shortcomings when applied to WSNs, which are mainly due to the energy-constrained nature of such networks [4]. For example, flooding is a technique in which a given node broadcasts data and control packets that it has received to the rest of the nodes in the network. This process repeats until the destination node is reached. Note that

this technique does not take into account the energy constraint imposed by WSNs. As a result, when used for data routing in WSNs, it leads to the problems such as implosion and overlap [9,12]. Given that flooding is a blind technique, duplicated packets may keep circulate in the network, and hence sensors will receive those duplicated packets, causing an implosion problem. Also, when two sensors sense the same region and broadcast their sensed data at the same time, their neighbors will receive duplicated packets. To overcome the shortcomings of flooding, another technique known as gossiping can be applied [10]. In gossiping, upon receiving a packet, a sensor would select randomly one of its neighbors and send the packet to it. The same process repeats until all sensors receive this packet. Using gossiping, a given sensor would receive only one copy of a packet being sent. While gossiping tackles the implosion problem, there is a significant delay for a packet to reach all sensors in a network. Furthermore, these inconveniences are highlighted when the number of nodes in the network increases.

A large number of research activities have been carried out to explore and overcome the constraints of WSNs and solve design and application issues. In this paper various routing protocols for wireless sensor network are discussed and compared. Section 2 of the paper discusses the network characteristics and design objectives. In Sections 3, the network design challenges and routing issues are described. In Section 4, various routing protocols are discussed and compared. Finally, Section 5 concludes the survey.

II. SECURE ROUTING

Protected routing protocols overcome malevolent nodes that be able to obstruct the accurate operation of a routing protocol by adjusting routing information, via imitating other nodes and by inventing false routing information. This Protected routing protocols of ad hoc networks are either combinations of security mechanisms within the existing protocols or entirely novel independently protocols. In general, the proposed secure routing protocols was classified into two classes, routing protocols which use hash chains and routing protocols that require predefined dependence relationships in order to operate [1].

1. hash chains is A one-way hash function H(.)to be more secure in routing protocol is to follow these properties:
2. 1-H(.) can take a message of arbitrary length as input and produce a message digest of a fixed-length output.
3. Given x, it is hard to compute H−1 (y) = x given y. However, it is easy to compute H(x) = y.
4. Given x, its arithmetically not practicable to determine x'≠ x such that H(x') = H(x) [3].

2.1 Network Characteristics

As compared to the traditional wireless communication networks such as mobile ad hoc network (MANET) and cellular systems, wireless sensor networks have the following unique characteristics and constraints:

Dense sensor node deployment: Sensor nodes are usually densely deployed and can be several orders of magnitude higher than that in a MANET.

Battery-powered sensor nodes: Sensor nodes are usually powered by battery and are deployed in a harsh environment where it is very difficult to change or recharge the batteries. Severe energy, computation, and storage constraints: Sensors nodes are having highly limited energy, computation, and storage capabilities.

Self-configurable: Sensor nodes are usually randomly deployed and autonomously configure themselves into a communication network. Unreliable sensor nodes: Since sensor nodes are prone to physical damages or failures due to its deployment in harsh or hostile environment.

Data redundancy: In most sensor network application, sensor nodes are densely deployed in a region of interest and collaborate to accomplish a common sensing task. Thus, the data sensed by multiple sensor nodes typically have a certain level of correlation or redundancy.

Application specific: A sensor network is usually designed and deployed for a specific application. The design requirements of a sensor network change with its application. Many-to-one traffic pattern: In most sensor network applications, the data sensed by sensor nodes flow from multiple source sensor nodes to a particular sink, exhibiting a many-to-one traffic pattern.

Frequent topology change: Network topology changes frequently due to the node failures, damage, addition, energy depletion, or channel fading.

2.2 Network Design Objectives

Most sensor networks are application specific and have different application requirements. Thus, all or part of the following main design objectives is considered in the design of sensor networks:

Small node size: Since sensor nodes are usually deployed in a harsh or hostile environment in large numbers, reducing node size can facilitate node deployment. It will also reduce the power consumption and cost of sensor nodes.

Low node cost: Since sensor nodes are usually deployed in a harsh or hostile environment in large numbers and cannot be reused, reducing cost of sensor nodes is important and will result into the cost reduction of whole network.

Low power consumption: Since sensor nodes are powered by battery and it is often very difficult or even impossible to charge or recharge their batteries, it is crucial to reduce the power consumption of sensor nodes so that the lifetime of the sensor nodes, as well as the whole network is prolonged.

Scalability: Since the number sensor nodes in sensor networks are in the order of tens, hundreds, or thousands, network protocols designed for sensor networks should be scalable to different network sizes.

Reliability: Network protocols designed for sensor networks must provide error control and correction mechanisms to ensure reliable data delivery over noisy, error-prone, and time-varying wireless channels.

Self-configurability: In sensor networks, once deployed, sensor nodes should be able to autonomously organize themselves into a communication network and reconfigure their connectivity in the event of topology changes and node failures.

Adaptability: In sensor networks, a node may fail, join, or move, which would result in changes in node density and network topology. Thus, network protocols designed for sensor networks should be adaptive to such density and topology changes.

Channel utilization: Since sensor networks have limited bandwidth resources, communication protocols designed for sensor networks should efficiently make use of the bandwidth to improve channel utilization.

Fault tolerance: Sensor nodes are prone to failures due to harsh deployment environments and unattended operations. Thus, sensor nodes should be fault tolerant and have the abilities of self-testing, self-calibrating, self-repairing, and self-recovering.

Security: A sensor network should introduce effective security mechanisms to prevent the data information in the network or a sensor node from unauthorized access or malicious attacks.

QoS support: In sensor networks, different applications may have different quality-of-service (QoS) requirements in terms of delivery latency and packet loss. Thus, network protocol design should consider the QoS requirements of specific applications.

III. Network Design Challenges and Routing Issues

The design of routing protocols for WSNs is challenging because of several network constraints. WSNs suffer from the limitations of several network resources, for example, energy, bandwidth, central processing unit, and storage [11,13]. The design challenges in sensor networks involve the following main aspects [4,11,13]:

Limited energy capacity: Since sensor nodes are battery powered, they have limited energy capacity. Energy poses a big challenge for network designers in hostile environments, for example, a battlefield, where it is impossible to access the sensors and recharge their batteries. Furthermore, when the energy of a sensor reaches a certain threshold, the sensor will become faulty and will not be able to function properly, which will have a major impact on the network performance. Thus, routing protocols designed for sensors should be as energy efficient as possible to extend their lifetime, and hence prolong the network lifetime while guaranteeing good performance overall.

Sensor locations: Another challenge that faces the design of routing protocols is to manage the locations of the sensors. Most of the proposed protocols assume that the sensors either are equipped with global positioning system (GPS) receivers or use some localization technique to learn about their locations.

Limited hardware resources: In addition to limited energy capacity, sensor nodes have also limited processing and storage capacities, and thus can only perform limited computational functionalities. These hardware constraints present many challenges in software development and network protocol design for sensor networks, which must consider not only the energy constraint in sensor nodes, but also the processing and storage capacities of sensor nodes.

Massive and random node deployment: Sensor node deployment in WSNs is application dependent and can be either manual or random which finally affects the performance of the routing protocol. In most applications, sensor nodes can be scattered randomly in an intended area or dropped massively over an inaccessible or hostile region. If the resultant distribution of nodes is not uniform, optimal clustering becomes necessary to allow connectivity and enable energy efficient network operation.

Network characteristics and unreliable environment: A sensor network usually operates in a dynamic and unreliable environment. The topology of a network, which is defined by the sensors and the communication links between the sensors, changes frequently due to sensor addition, deletion, node failures, damages, or energy depletion. Also, the sensor nodes are linked by a wireless medium, which is noisy, error prone, and time varying. Therefore, routing paths should consider network topology dynamics due to limited energy and sensor mobility as well as increasing the size of the network to maintain specific application requirements in terms of coverage and connectivity.

Data Aggregation: Since sensor nodes may generate significant redundant data, similar packets from multiple nodes can be aggregated so that the number of transmissions is reduced. Data aggregation technique has been used to achieve energy efficiency and data transfer optimization in a number of routing protocols.

Diverse sensing application requirements: Sensor networks have a wide range of diverse applications. No network protocol can meet the requirements of all applications. Therefore, the routing protocols should guarantee data delivery and its accuracy so that the sink can gather the required knowledge about the physical phenomenon on time.

Scalability: Routing protocols should be able to scale with the network size. Also, sensors may not necessarily have the same capabilities in terms of energy, processing, sensing, and particularly communication. Hence, communication links between sensors may not be symmetric, that is, a pair of sensors may not be able to have communication in both directions. This should be taken care of in the routing protocols.

IV. Routing Protocols in WSN

Routing in wireless sensor networks differs from conventional routing in fixed networks in various ways. There is no infrastructure, wireless links are unreliable, sensor nodes may fail, and routing protocols have to meet strict energy saving requirements [5]. Many routing algorithms were developed for wireless networks in general. All major routing protocols proposed for WSNs may be divided into seven categories as shown in Table 1. We review sample routing protocols in each of the categories in preceding sub-sections.

Table 1: Routing Protocols for WSNs

Category	Representative Protocols
Location-based Protocols	MECN, SMECN, GAF, GEAR, Span, TBF, BVGF, GeRaF
Data-centric Protocols	SPIN, Directed Diffusion, Rumor Routing, COUGAR, ACQUIRE, EAD, Information-Directed Routing, Gradient-Based Routing, Energy-aware Routing, Information-Directed Routing, Quorum-Based Information Dissemination, Home Agent Based Information Dissemination
Hierarchical Protocols	LEACH, PEGASIS, HEED, TEEN, APTEEN
Mobility-based Protocols	SEAD, TTDD, Joint Mobility and Routing, Data MULES, Dynamic Proxy Tree-Base Data Dissemination
Multipath-based Protocols	Sensor-Disjoint Multipath, Braided Multipath, N-to-1 Multipath Discovery
Heterogeneity-based Protocols	IDSQ, CADR, CHR
QoS-based protocols	SAR, SPEED, Energy-aware routing

4.1 Location-based Protocols

In location-based protocols, sensor nodes are addressed by means of their locations. Location information for sensor nodes is required for sensor networks by most of the routing protocols to calculate the distance between two particular nodes so that energy consumption can be estimated. In this section, we present a sample of location-aware routing protocols proposed for WSNs.
Geographic Adaptive Fidelity (GAF): GAF is an energy-aware routing protocol primarily proposed for MANETs, but can also be used for WSNs because it favors energy conservation. The design of GAF is motivated based on an energy model that considers energy consumption due to the reception and transmission of packets as well as idle (or listening) time when the radio of a sensor is on to detect the presence of incoming packets. GAF is based on mechanism of turning off unnecessary sensors while keeping a constant level of routing fidelity (or uninterrupted connectivity between communicating sensors). In GAF, sensor field is divided into grid squares and every sensor uses its location information, which can be provided by GPS or other location systems to associate itself with a particular grid in which it resides. This kind of association is exploited by GAF to identify the sensors that are equivalent from the perspective of packet forwarding.

As shown in Figure 1, the state transition diagram of GAF has three states, namely, discovery, active, and sleeping. When a sensor enters the sleeping state, it turns off its radio for energy savings. In the discovery state, a sensor exchanges discovery messages to learn about other sensors in the same grid. Even in the active state, a sensor periodically broadcasts its discovery message to inform equivalent sensors about its state. The time spent in each of these states can be tuned by the application depending on several factors, such as its needs and sensor mobility. GAF aims to maximize the network lifetime by reaching a state where each grid has only one active sensor based on sensor ranking rules. The ranking of sensors is based on their residual energy levels. Thus, a sensor with a higher rank will be able to handle routing within their corresponding grids. For example, a sensor in the active state has a higher rank than a sensor in the discovery state. A sensor with longer expected lifetime has a higher rank.

Coordination of Power Saving with Routing: Span is a routing protocol also primarily proposed for MANETs, but can be applied to WSNs as its goal is to reduce energy consumption of the nodes. Span is motivated by the fact that the wireless network interface of a device is often the single largest consumer of power. Hence, it would be better to turn the radio off during idle time. Although Span does not require that sensors know their location information, it runs well with a geographic forwarding protocol. Span helps sensors to join a forwarding backbone topology as coordinators that will forward packets on behalf of other sensors between any source and destination. When used with a geographic forwarding protocol, Span's election rule requires each sensor to advertise its status (i.e., coordinator or non-coordinator), its neighbors, and its coordinators. Furthermore, when it receives a packet, a coordinator forwards the packet to a neighboring coordinator if any, which is the closest to the destination or to a non-coordinator that is closer to the destination.

Trajectory-Based Forwarding (TBF): TBF is a routing protocol that requires a sufficiently dense network and the presence of a coordinate system, for example, a GPS, so that the sensors can position themselves and estimate distance to their neighbors. The source specifies the trajectory in a packet, but does not explicitly indicate the path on a hop-by-hop basis. Based on the location information of its neighbors, a forwarding sensor makes a greedy decision to determine the next hop that is the closest to the trajectory fixed by the source sensor. Route maintenance in TBF is unaffected by sensor mobility given that a source route is a trajectory that does not include the names of the forwarding sensors. In order to increase the reliability and capacity of the network, it is also possible to implement multipath routing in TBF where an alternate path is just another trajectory. TBM can be used for implementing networking functions, for example, flooding, discovery, and network management. TBF can also be used for resource discovery. Another interesting application of TBF is securing the perimeter of the network.

Geographic Random Forwarding (GeRaF): GeRaF was proposed by Zorzi and Rao , which uses geographic routing where a sensor acting as relay is not known a priori by a sender. There is no guarantee that a sender will always be able to forward the message toward its ultimate desti destination, that is, the sink. This is the reason that GeRaF is said to be best-effort forwarding.

GeRaF assumes that all sensors are aware of their physical locations, as well as that of the sink. Although GeRaF integrates a geographical routing algorithm and an awake-sleep scheduling algorithm, the sensors are not required to keep track of the locations of their neighbors and their awake-sleep schedules. When a source sensor has sensed data to send to the sink, it first checks whether the channel is free in order to avoid collisions. If the channel remains idle for some period of time, the source sensor broadcasts a request-to-send (RTS) message to all of its active (or listening) neighbors. This message includes the location of the source and that of the sink. Note that the coverage area facing the sink, called forwarding area, is split into a set of Np regions of different priorities such that all points in a region with a higher priority are closer to the sink than any point in a region with a lower priority. When active neighboring sensors receive the RTS message, they assess their priorities based on their locations and that of the sink. The source sensor waits for a CTS message from one of the sensors located in the highest priority region. For GeRaF, the best relay sensor the one closest to the sink, thus making the largest advancement of the data packet toward the sink. In case that the source does not receive the CTS message, implies that the highest priority region is empty. Hence, it sends out another RTS polling sensors in the second highest priority region. This process continues till the source receives the CTS message, which means that a relay sensor has been found. Then, the source sends its data packet to the selected relay sensor, which in turn replies back with an ACK message. The relay sensor will act in the same way as the source sensor in order to find the second relay sensor. The same procedure repeats until the sink receives the sensed data packet originated from the source sensor. It may happen that the sending sensor does not receive any CTS message after sending Np RTS messages. This means that the neighbors of the sending sensor are not active. In this case, the sending sensor backs off for some time and retries later. After a certain number of attempts, the sending sensor either finds a relay sensor or discards the data packet if the maximum allowed number of attempts is reached.

Minimum Energy Communication Network (MECN): MECN is a location-based protocol for achieving minimum energy for randomly deployed ad hoc networks, which attempts to set up and maintain a minimum energy network with mobile sensors. It is self-reconfiguring protocol that maintains network connectivity in spite of sensor mobility. It computes an optimal spanning tree rooted at the sink, called minimum power topology, which contains only the minimum power paths from ach sensor to the sink. It is based on the positions of sensors on the plane and consists of two main phases, namely, enclosure graph construction and cost distribution. For a stationary network, in the first phase (enclosure graph construction), MECN constructs a sparse graph, called an enclosure graph, based on the immediate locality of the sensors. An enclosure graph is a directed graph that includes all the sensors as its vertex set and whose edge set is the union of all edges between the sensors and the neighbors located in their enclosure regions. In other words, a sensor will not consider the sensors located in its relay regions as potential candidate forwarders of its sensed data to the sink. In the second phase (cost distribution), non-optimal links of the enclosure graph are simply eliminated and the resulting graph is a minimum power topology. This graph has a directed path from each sensor to the sink and consumes the least total power among all graphs having directed paths from each sensor to the sink. Each sensor broadcasts its cost to its neighbors, where the cost of a node is the minimum power required for this sensor to establish a directed path to the sink.

While MECN is a self-reconfiguring protocol, and hence is fault tolerant (in the case of mobile networks), it suffers from a severe battery depletion problem when applied to static networks. MECN does not take into consideration the available energy at each sensor, and hence the optimal cost links are static. In other words, a sensor will always use the same neighbor to transmit or forward sensed data to the sink. For this reason, this neighbor would die very quickly and the network thus becomes disconnected. To address this problem, the enclosure graph and thus the minimum power topology should be dynamic based on the residual energy of the sensors.

Small Minimum-Energy Communication Network (SMECN): SMECN is a routing protocol proposed to improve MECN, in which a minimal graph is characterized with regard to the minimum energy property. This property implies that for any pair of sensors in a graph associated with a network, there is a minimum energy-efficient path between them; that is, a path that has the smallest cost in terms of energy consumption over all possible paths between this pair of

sensors. Their characterization of a graph with respect to the minimum energy property is intuitive. In SMECN protocol, every sensor discovers its immediate neighbors by broadcasting a neighbor discovery message using some initial power that is updated incrementally. Specifically, the immediate neighbors of a given sensor are computed analytically. Then, a sensor starts broadcasting a neighbor discovery message with some initial power p and checks whether the theoretical set of immediate neighbors is a subset of the set of sensors that replied to that neighbor discovery message. If this is the case, the sensor will use the corresponding power p to communicate with its immediate neighbors. Otherwise, it increments p and rebroadcasts its neighbor discovery message.

4.2 Data Centric Protocols

Data-centric protocols differ from traditional address-centric protocols in the manner that the data is sent from source sensors to the sink. In address-centric protocols, each source sensor that has the appropriate data responds by sending its data to the sink independently of all other sensors. However, in data-centric protocols, when the source sensors send their data to the sink, intermediate sensors can perform some form of aggregation on the data originating from multiple source sensors and send the aggregated data toward the sink. This process can result in energy savings because of less transmission required to send the data from the sources to the sink. In this section, we review some of the data-centric routing protocols for WSNs.

Sensor Protocols for Information via Negotiation (SPIN): SPIN protocol was designed to improve classic flooding protocols and overcome the problems they may cause, for example, implosion and overlap. The SPIN protocols are resource aware and resource adaptive. The sensors running the SPIN protocols are able to compute the energy consumption required to compute, send, and receive data over the network. Thus, they can make informed decisions for efficient use of their own resources. The SPIN protocols are based on two key mechanisms namely negotiation and resource adaptation. SPIN enables the sensors to negotiate with each other before any data dissemination can occur in order to avoid injecting non-useful and redundant information in the network. SPIN uses meta-data as the descriptors of the data that the sensors want to disseminate. The notion of meta-data avoids the occurrence of overlap given sensors can name the interesting portion of the data they want to get. It may be noted here that the size of the meta-data should definitely be less than that of the corresponding sensor data. Contrary to the flooding technique, each sensor is aware of its resource consumption with the help of its own resource manager that is probed by the application before any data processing or transmission. This helps the sensors to monitor and adapt to any change in their own resources.

There are two protocols in the SPIN family: SPIN-l (or SPIN-PP) and SPIN-2 (or SPIN-EC). While SPIN-l uses a negotiation mechanism to reduce the consumption of the sensors, SPIN-2 uses a resource-aware mechanism for energy savings. Both protocols allow the sensors to exchange information about their sensed data, thus helping them to obtain the data they are interested in. SPIN-l is a three-stage handshake protocol by which the sensors can disseminate their data. This protocol applies for those networks using point-to-point transmission media (or point-to-point networks), in which two sensors can communicate exclusively with each other without interfering with other sensors. SPIN-BC improves SPIN-PP by using one-to-many communication instead of many one-to-one communications. It is a three-stage handshake protocol for broadcast transmission media, where the sensors in a network communicate with each other using a single shared channel. SPIN-2 differs from SPIN-l in that it takes into account the residual energy of sensors. If the sensors have plenty of energy, SPIN-2 is identical to SPIN-l, and hence has the same three stages. However, when a sensor has low residual energy, it controls its participation in a data dissemination process. While the family of SPIN protocols applies to lossless networks, it can be slightly updated to apply to lossy or mobile networks.

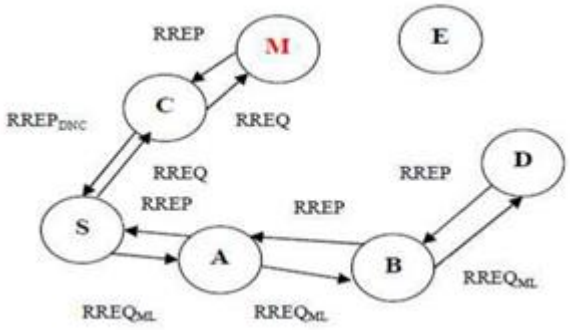

Figure 1. Route discovery process of AODV

Directed Diffusion: Directed diffusion is a data-centric routing protocol for sensor query dissemination and processing. It meets the main requirements of WSNs such as energy efficiency, scalability, and robustness. Directed diffusion has several key elements namely data naming, interests and gradients, data propagation, and reinforcement. A sensing task can be described by a list of attribute-value pairs. At the beginning of the directed diffusion process, the sink specifies a low data rate for incoming events. After that, the sink can reinforce one particular sensor to send events with a higher data rate by resending the original interest message with a smaller interval. Likewise, if a neighboring sensor receives this interest message and finds that the sender's interest has a higher data rate than before, and this data rate is higher than that of any existing gradient, it will reinforce one or more of its neighbors.

Rumor Routing: Rumor routing is a logical compromise between query flooding and event flooding app schemes [32]. Rumor routing is an efficient protocol if the number of queries is between the two intersection points of the curve of rumor routing with those of query flooding and event flooding. Rumor routing is based on the concept of agent, which is a long-lived packet that traverses a network and informs each sensor it encounters about the events that it has learned during its network traverse. An agent will travel the network for a certain number of hops and then die. Each sensor, including the agent, maintains an event list that has event-distance pairs,

The Ad-Hoc Demand Distance Vector (AODV)

This algorithm also can be called a pure on-demand route acquisition system; Nodes does not give false data to active paths either share or exchange information about the routing table nor keep this information. Additional, a node does not have to maintain and discover a route to another node until the communicate between two nodes needed, the fig-1- below shown the routing discover process unless the former node which is an intermediate routing station provides its services to maintain communication between two other nodes[5].

The importance connectivity of the local mobile node makes each mobile node uses multiple techniques to become more aware of neighboring nodes, one of these technique includes local broadcasts known as hello messages (not system-wide). The routing tables are designed to optimize response time of the nodes within the neighborhood to local movements, and due to the requests of new routes, this technique provides fast response time. The primary objectives of the algorithm are:

1. Discovery packets were broadcasting when it needed only.
2. To differentiate between management of local connectivity and maintenance of general topology.
3. To distribute information to mobile nodes that needs the information about changes in local connectivity.

Energy-Aware Data-Centric Routing (EAD): EAD is a novel distributed routing protocol, which builds a virtual backbone composed of active sensors that are responsible for in-network data processing and traffic relaying. In this protocol, a network is represented by a broadcast tree spanning all sensors in the network and rooted at the gateway, in which all leaf nodes' radios are turned off while all other nodes correspond to active sensors forming the backbone and thus their radios are turned on. Specifically, EAD attempts to construct a broadcast tree that approximates an optimal spanning tree with a minimum number of leaves, thus reducing the size of the backbone formed by active sensors. EAD approach is energy aware and helps extend the network lifetime. The gateway plays the role of a data sink or event sink, whereas each sensor acts as a data source or event source.

4.3 Hierarchical Protocols

Many research projects in the last few years have explored hierarchical clustering in WSN from different perspectives [2]. Clustering is an energy-efficient communication protocol that can be used by the sensors to report their sensed data to the sink. In this section, we describe a sample of layered protocols in which a network is composed of several clumps (or clusters) of sensors. Each clump is managed by a special node, called cluster head, which is responsible for coordinating.

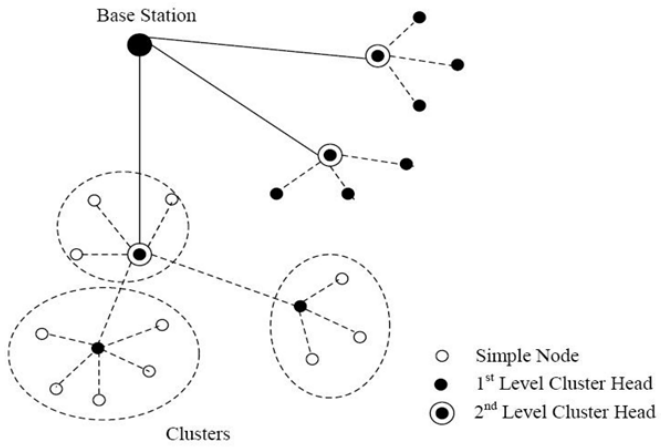

Figure 2. Cluster-based Hierarchical Model

As shown in Figure 2, a hierarchical approach breaks the network into clustered layers . Nodes are grouped into clusters with a cluster head that has the responsibility of routing from the cluster to the other cluster heads or base stations. Data travel from a lower clustered layer to a higher one. Although, it hops from one node to another, but as it hops from one layer to another it covers larger distances. This moves the data faster to the base station. Clustering provides inherent optimization capabilities at the cluster heads. In this section, we review a sample of hierarchical-based routing protocols for WSNs.

Low-energy adaptive clustering hierarchy (LEACH): LEACH is the first and most popular energy-efficient hierarchical clustering algorithm for WSNs that was proposed for reducing power consumption. In LEACH, the clustering task is rotated among the nodes, based on duration. Direct communication is used by each cluster head (CH) to forward the data to the base station (BS). It uses clusters to prolong the life of the wireless sensor network. LEACH is based on an aggregation (or fusion) technique that combines or aggregates the original data into a smaller size of data that carry only meaningful information to all individual sensors. LEACH divides the a network into several cluster of sensors, which are constructed by using localized coordination and control not only to reduce the amount of data that are transmitted to the sink, but also to make routing and data dissemination more scalable and robust. LEACH uses a randomize rotation of high-energy CH position rather than selecting in static manner, to give a chance to all sensors to act as CHs and avoid the battery depletion of an individual sensor and dieing quickly. The operation of LEACH is divided into rounds having two phases each namely (i) a setup phase to organize the network into clusters, CH advertisement, and transmission schedule creation and (ii) a steady-state phase for data aggregation, compression, and transmission to the sink.

LEACH is completely distributed and requires no global knowledge of network. It reduces energy consumption by (a) minimizing the communication cost between sensors and their cluster heads and (b) turning off non-head nodes as much as possible . 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. While LEACH helps the sensors within their cluster dissipate their energy slowly, the CHs consume a larger amount of energy when they are located farther away from the sink. Also, LEACH clustering terminates in a finite number of iterations, but does not guarantee good CH distribution and assumes uniform energy consumption for CHs.

Power-Efficient Gathering in Sensor Information Systems (PEGASIS): PEGASIS is an extension of the LEACH protocol, which 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). The data is gathered and moves from node to node, aggregated and eventually sent to the base station. The chain construction is performed in a greedy way. Unlike LEACH, PEGASIS avoids cluster formation and uses only one node in a chain to transmit to the BS (sink) instead of using multiple nodes. A sensor transmits to its local neighbors in the data fusion phase instead of sending directly to its CH as in the case of LEACH. In PEGASIS routing protocol, the construction phase assumes that all the sensors have global knowledge about the network, particularly, the positions of the sensors, and use a greedy approach. When a sensor fails or dies due to low battery power, the chain is constructed using the same greedy approach by bypassing the failed sensor. In each round, a randomly chosen sensor node from the chain will transmit the aggregated data to the BS, thus reducing the per round energy expenditure compared to LEACH.

Simulation results showed that PEGASIS is able to increase the lifetime of the network twice as much the lifetime of the network under the LEACH protocol. Such performance gain is achieved through the elimination of the overhead caused by dynamic cluster formation in LEACH and through decreasing the number of transmissions and reception by using data aggregation. Although the clustering overhead is avoided, PEGASIS still requires dynamic topology adjustment since a sensor node needs to know about energy status of its neighbors in order to know where to route its data. Such topology adjustment can introduce significant overhead especially for highly utilized networks.

Hybrid, Energy-Efficient Distributed Clustering (HEED): HEED extends the basic scheme of LEACH by using residual energy and node degree or density as a metric for cluster selection to achieve power balancing. It operates in multi-hop networks, using an adaptive transmission power in the inter-clustering communication. HEED was proposed with four primary goals namely (i) prolonging network lifetime by distributing energy consumption, (ii) terminating the clustering process within a constant number of iterations, (iii) minimizing control overhead, and (iv) producing well-distributed CHs and compact clusters. In HEED, the proposed algorithm periodically selects CHs according to a combination of two clustering parameters. The primary parameter is their residual energy of each sensor node (used in calculating probability of becoming a CH) and the secondary parameter is the intra-cluster communication cost as a function of cluster density or node degree (i.e. number of neighbors). The primary parameter is used to probabilistically select an initial set of CHs while the secondary parameter is used for breaking ties. The HEED clustering improves network lifetime over LEACH clustering because LEACH randomly selects CHs (and hence cluster size), which may result in faster death of some nodes. The final CHs selected in HEED are well distributed across the network and the communication cost is minimized. However, the cluster selection deals with only a subset of parameters, which can possibly impose constraints on the system. These methods are suitable for prolonging the network lifetime rather than for the entire needs of WSN.

Threshold Sensitive Energy Efficient Sensor Network Protocol (TEEN): TEEN [42,43] is a hierarchical clustering protocol, which groups sensors into clusters with each led by a CH. The sensors within a cluster report their sensed data to their CH. The CH sends aggregated data to higher level CH until the data reaches the sink. Thus, the sensor network architecture in TEEN is based on a hierarchical grouping where closer nodes form clusters and this process goes on the second level until the BS (sink) is reached. TEEN is useful for applications where the users can control a trade-off between energy efficiency, data accuracy, and response time dynamically. TEEN uses a data-centric method with hierarchical approach. Important features of TEEN include its suitability for time critical sensing applications. Also, since message transmission consumes more energy than data sensing, so the energy consumption in this scheme is less than the proactive networks. However, TEEN is not suitable for sensing applications where periodic reports are needed since the user may not get any data at all if the thresholds are not reached.

Adaptive Periodic Threshold Sensitive Energy Efficient Sensor Network Protocol (APTEEN): APTEEN [44] is an improvement to TEEN to overcome its shortcomings and aims at both capturing periodic data collections (LEACH) and reacting to time-critical events (TEEN). Thus, APTEEN is a hybrid clustering-based routing protocol that allows the sensor to send their sensed data periodically and react to any sudden change in the value of the sensed attribute by reporting the corresponding values to their CHs. The architecture of APTEEN is same as in TEEN, which uses the concept hierarchical clustering for energy efficient communication between source sensors and the sink. APTEEN supports three different query types namely (i) historical query, to analyze past data values, (ii) one-time query, to take a snapshot view of the network; and (iii) persistent queries, to monitor an event for a period of time. APTEEN guarantees lower energy dissipation and a larger number of sensors alive.

Energy Efficient Homogenous Clustering Algorithm for Wireless Sensor Networks: Singh et al. [3] proposed homogeneous clustering algorithm for wireless sensor network that saves power and prolongs network life. The life span of the network is increased by ensuring a homogeneous distribution of nodes in the clusters. A new cluster head is selected on the basis of the residual energy of existing cluster heads, holdback value, and nearest hop distance of the node. The homogeneous

algorithm makes sure that every node is either a cluster head or a member of one of the clusters in the wireless sensor network. In the proposed clustering algorithm the cluster members are uniformly distributed, and thus, the life of the network is more extended. Further, in the proposed protocol, only cluster heads broadcast cluster formation message and not the every node. Hence, it prolongs the life of the sensor networks. The emphasis of this approach is to increase the life span of the network by ensuring a homogeneous distribution of nodes in the clusters so that there is not too much receiving and transmitting overhead on a Cluster Head.

4.4 Mobility-based Protocols

Mobility brings new challenges to routing protocols in WSNs. Sink mobility requires energy-efficient protocols to guarantee data delivery originated from source sensors toward mobile sinks. In this section we discuss sample mobility-based routing protocols for mobile WSNs.

Joint Mobility and Routing Protocol: A network with a static sink suffers from a severe problem, called energy sink-hole problem, where the sensors located around the static sink are heavily used for forwarding data to the sink on behalf of other sensors. As a result, those heavily loaded sensors close to the sink deplete their battery power more quickly, thus disconnecting the network. This problem exists even when the static sink is located at its optimum position corresponding to the center of the sensor field To address this problem, a mobile sink for gathering sensed data from source sensors was suggested. In this case, the sensors surrounding the sink change over time, giving the chance to all sensors in the network to act as data relays to the mobile sink and thus balancing the load of data routing on all the sensors. Under the shortest-path routing strategy, the average load of data routing is reduced when the trajectories of the sink mobility correspond to concentric circles (assuming that the sensor field is a circle). Another category of mobility trajectories is to move the sink in annuli. However, such movement can be viewed as a weighted average over the movements on a set of concentric circles. In particular, the optimum mobility strategy of the sink is a symmetric strategy in which the trajectory of the sink is the periphery of the network. The trajectory with a radius equal to the radius of the sensor field maximizes the distance from the sink to the centre of the network that represents the hot spot.

Data MULES Based Protocol: Data MULE based was proposed to address the need of guaranteeing cost-effective connectivity in a sparse network while reducing the energy consumption of the sensors [46]. It is a three-tier architecture based on mobile entities, called mobile ubiquitous LAN extensions (MULE). The MULEs architecture has three main layers. The bottom layer contains static wireless sensors that are responsible for sensing an environment. The top layer includes WAN connected devices and access points/central repositories for analyzing the sensed data. These access points communicate with a central data warehouse enabling them to synchronize the collected data, identify redundant data, and acknowledge the receipt of the data sent by the MULEs for reliable data transmission. The middle layer has mobile entities (MULEs) that move in the sensor field and collect sensed data from the source sensors when in proximity deliver them to those access points when in close range. The MULE architecture helps the sensors save their energy as much as possible and thus extend their lifetime. Since the sensors directly communicate with the MULEs through short-range paths, they deplete their energy slowly and uniformly. In addition, the MULE architecture has low infrastructure cost. Because of the direct communication between the source sensors and the MULES, there is no routing overhead that would drain the energy of the sensors. MULE architecture is fault tolerant and very robustness and scalable. However, if a MULE fails, it will degrade the performance of a sparse network for decreasing its data success rate and increasing its latency. For time-critical applications, the MULE architecture may introduce an undesirable delay in reporting the sensed data of the source sensors and thus may not be practical. One way to solve this problem is to equip the MULEs with an always-on connection so that they act as mobile sinks (i.e., MULEs and access points).

Scalable Energy-Efficient Asynchronous Dissemination (SEAD): SEAD is self-organizing protocol, which was proposed to trade-off between minimizing the forwarding delay to a mobile sink and energy savings. SEAD considers data dissemination in which a source sensor reports its sensed data to multiple mobile sinks and consists of three main components namely dissemination tree (d-tree) construction, data

dissemination, and maintaining linkages to mobile sinks. It assumes that the sensors are aware of their own geographic locations. Every source sensor builds its data dissemination tree rooted at itself and all the dissemination trees for all the source sensors are constructed separately. SEAD can be viewed as an overlay network that sits on top of a location-aware routing protocol, for example, geographical forwarding.

Dynamic Proxy Tree-Based Data Dissemination: A dynamic proxy tree-based data dissemination framework [48] was proposed for maintaining a tree connecting a source sensor to multiple sinks that are interested in the source. This helps the source disseminate its data directly to those mobile sinks. In this framework, a network is composed of stationary sensors and several mobile hosts, called sinks. The sensors are used to detect and continuously monitor some mobile targets, while the mobile sinks are used to collect data from specific sensors, called sources, which may detect the target and periodically generate detected data or aggregate detected data from a subset of sensors. Because of target mobility, a source may change and a new sensor closer to the target may become a source. Each source is represented by a stationary source proxy and each sink is represented by a stationary sink proxy. The source and sink proxies are temporary in the sense that they change as the source sensors change and the sinks move. A source will have a new source proxy only when the distance between the source and its current proxy exceeds a certain threshold. Likewise, a sink will have a new sink proxy only when the distance between the sink and its current proxy exceeds a certain threshold. The design of such proxies reduces the cost of pushing data to and querying data from the source and sinks proxies.

4.5 Multipath-based Protocols

Considering data transmission between source sensors and the sink, there are two routing paradigms: single-path routing and multipath routing. In single-path routing, each source sensor sends its data to the sink via the shortest path. In multipath routing, each source sensor finds the first k shortest paths to the sink and divides its load evenly among these paths. In this section, we review a sample of multipath routing protocols for WSNs.

Disjoint Paths: Sensor-disjoint multipath routing is a multipath protocol that helps find a small number of alternate paths that have no sensor in common with each other and with the primary path. In sensor-disjoint path routing, the primary path is best available whereas the alternate paths are less desirable as they have longer latency. The disjoint makes those alternate paths independent of the primary path. Thus, if a failure occurs on the primary path, it remains local and does not affect any of those alternate paths. The sink can determine which of its neighbors can provide it with the highest quality data characterized by the lowest loss or lowest delay after the network has been flooded with some low-rate samples. Although disjoint paths are more resilient to sensor failures, they can be potentially longer than the primary path and thus less energy efficient.

Braided Paths: Braided multipath is a partially disjoint path from primary one after relaxing the disjointedness constraint. To construct the braided multipath, first primary path is computed. Then, for each node (or sensor) on the primary path, the best path from a source sensor to the sink that does not include that node is computed. Those best alternate paths are not necessarily disjoint from the primary path and are called idealized braided multipaths. Moreover, the links of each of the alternate paths lie either on or geographically close to the primary path. Therefore, the energy consumption on the primary and alternate paths seems to be comparable as opposed to the scenario of mutually ternate and primary paths. The braided multipath can also be constructed in a localized manner in which case the sink sends out a primary-path reinforcement to its first preferred neighbor and alternate-path reinforcement to its second preferred neighbor.

N-to-1 Multipath Discovery: N-to-1 multipath discovery is based on the simple flooding originated from the sink and is composed of two phases, namely, branch aware flooding (or phase 1) and multipath extension of flooding (or phase 2). Both phases use the same routing messages whose format is given by {mtype, mid, nid, bid, cst, path}, where mtype refers to the type of a message. This multipath discovery protocol generates multiple node-disjoint paths for every sensor. In multihop routing, an active per-hop packet salvaging strategy can be adopted to handle sensor failures and enhance network reliability.

subset of sensors need to be active when there are interesting events to report in some parts of the network. The choice of a subset of active sensors that have the most useful information is balanced by the communication cost needed between those sensors. Useful information can be sought based on predicting the space and time interesting events would take place. In IDSQ protocol, first step is to select a sensor as leader from the cluster of sensors. This leader will be responsible for selecting optimal sensors based on some information utility measure.

Cluster-Head Relay Routing (CHR): CHR routing protocol uses two types of sensors to form a heterogeneous network with a single sink: a large number of low-end sensors, denoted by L-sensors, and a small number of powerful high-end sensors, denoted by H-sensors. Both types of sensors are static and aware of their locations using some location service. Moreover, those L-and H-sensors are uniformly and randomly distributed in the sensor field. The CHR protocol partitions the heterogeneous network into groups of sensors (or clusters), each being composed of L-sensors and led by an H-sensor. Within a cluster, the L-sensors are in charge of sensing the underlying environment and forwarding data packets originated by other L-sensors toward their cluster head in a multihop fashion. The H-sensors, on the other hand, are responsible for data fusion within their own clusters and forwarding aggregated data packets originated from other cluster heads toward the sink in a multihop fashion using only cluster heads. While L-sensors use short-range data transmission to their neighboring H-sensors within the same cluster, H-sensors perform long-range data communication to other neighboring H-sensors and the sink. Neighbors and uses geographic forwarding to find the paths. In addition, SPEED strive to ensure a certain speed for each packet in the network so that each application can estimate the end-to-end delay for the packets by dividing the distance to the sink by the speed of the packet before making the admission decision. Moreover, SPEED can provide congestion avoidance when the network is congested. The routing module in SPEED is called Stateless Geographic Non-Deterministic forwarding (SNFG) and works with four other modules at the network layer. The beacon exchange mechanism collects information about the nodes and their location. Delay estimation at each node is basically made by calculating the elapsed time when an ACK is received from a neighbor as a response to a transmitted data packet. By looking at the delay values, SNGF selects the node, which meets the speed requirement. If it fails, the relay ratio of the node is checked, which is calculated by looking at the miss ratios of the neighbors of a node (the nodes which could not provide the desired speed) and is fed to the SNGF module. When compared to Dynamic Source Routing (DSR) and Ad-hoc on-demand vector routing (AODV) , SPEED performs better in terms of end-to-end delay and miss ratio. Moreover, the total transmission energy is less due to the simplicity of the routing algorithm, i.e. control packet overhead is less, and to the even traffic distribution. Such load balancing is achieved through the SNGF mechanism of dispersing packets into a large relay area SPEED does not consider any further energy metric in its routing protocol. Therefore, for more realistic understanding of SPEED's energy consumption, there is a need for comparing it to a routing protocol, which is energy-aware.

Energy-Aware QoS Routing Protocol: In this QoS aware protocol for sensor networks, real-time traffic is generated by imaging sensors. The proposed protocol extends the routing approach in [62] and finds a least cost and energy efficient path that meets certain end-to-end delay during the connection. The link cost used is a function that captures the nodes' energy reserve, transmission energy, error rate and other communication parameters. In order to support both best effort and real-time traffic at the same time, a class-based queuing model is employed. The queuing model allows service sharing for real-time and non-real-time traffic. The protocol finds a list of least cost paths by using an extended version of Dijkstra's algorithm and picks a path from that list which meets the end-to-end delay requirement. Simulation results show that the proposed protocol consistently performs well with respect to QoS and energy metrics, however, it does not provide flexible adjusting of bandwidth sharing for different links.

V. CONCLUSION

Mobile Ad hoc Network requires the high level of security as compare to the regular wired networks Security issues which is neglected while designing routing protocols for ad-hoc networks. Through DSR protocol, it is easier to infract the security of wireless ad-hoc network. DSR protocol is susceptible to various attacks including Black hole and Gray hole.The ultimate

objective behind the routing protocol design is to keep the sensors operating for as long as possible, thus extending the network lifetime. The energy consumption of the sensors is dominated by data transmission and reception. Therefore, routing protocols designed for WSNs should be as energy efficient as possible to prolong the lifetime of individual sensors, and hence the network lifetime.

In this paper, we have surveyed a sample of routing protocols by taking into account several classification criteria, including location information, network layering and in-network processing, data centricity, path redundancy, network dynamic.

Two important related research directions should receive attention from the researcher namely the design of routing protocols for duty-cycled WSNs, and three-dimensional (3D) sensor fields when designing such protocols. Although most of research work on WSNs, in particular, on

routing, considered two-dimensional (2D) settings, where sensors are deployed on a planar field, there are some situations where the 2D assumption is not reasonable and the use of a 3D design becomes a necessity the data compression is also an issue for several reasons in Authentication and Non-repudiation refer to the inability to deny the performance of some action falsely. The DSR scheme is depends on the idea to distribute a secret through multiple independent paths while it is transmitted across the network.

VI. REFERENCES

[1]. "21 ideas for the 21st century", Business Week, Aug. 30 1999, pp. 78-167.

[2]. "Ivan Stojmenovic and Stephan Olariu. Data-centric protocols for wireless sensor networks. In Handbook of Sensor Networks, Chapter 13, pages 417–456. Wiley, 2005.

[3]. "Christopher Ho, Katia Obraczka, Gene Tsudik, and Kumar Viswanath, "Flooding for reliable multicast in multi-hop ad hoc networks", In Proceedings of the 3rd International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications (DIAL-M'99), 1999, pp. 64–71.

[4]. "Ming Liu, Jiannong Cao, Guihai Chen, and Xiaomin Wang, "An Energy-Aware Routing Protocol in Wireless Sensor Networks", Sensors 2009, vol. 9, pp. 445-462.

[5]. "Luis Javier García Villalba, Ana Lucila Sandoval Orozco, Alicia Triviño Cabrera, and Cláudia Jacy Barenco Abbas, "Routing Protocol in Wireless Sensor Networks", Sensors 2009, vol. 9, pp. 8399-8421.

[6]. "E. Zanaj, M. Baldi, and F. Chiaraluce, "Efficiency of the Gossip Algorithm for Wireless Sensor Networks", In Proceedings of the 15th International Conference on Software, Telecommunications and Computer Networks (SoftCOM), Split–Dubrovnik, Croatia, September, 2007.

[7]. "Jamal Al-Karaki, and Ahmed E. Kamal, "Routing Techniques in Wireless Sensor Networks: A Survey", IEEE Communications Magazine, vol 11, no. 6, Dec. 2004, pp. 6-28.

[8]. "I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A Survey on Sensor Network", IEEE Communication Magazine, vol. 40, no. 8, Aug. 2002, pp. 102-114.

[9]. "Kemal Akkaya and Mohamed Younis, "A Survey on Routing Protocols for Wireless Sensor Networks", Ad hoc Networks, vol. 3, no. 3, May 2005, pp. 325-349.

[10]. Yipin Sun, Rongxing Lu, Xiaodong Lin, Jinshu Su and Xuemin (Sherman) Shen, "NEHCM: A Novel and Efficient Hash-chain based Certificate Management Scheme for Vehicular Communications".

[11]. F. Bevitelli, E. Di Cola, L. Fortuna and F. Itnlia, "Multilayer Chaotic Encryption for Secure Communications in Packet Switching Networks" , CommunicationTechnology Proceedings, 2000. WCC - ICCT 2000. International Conference on 21-25 Aug. 2000

[12]. Jun Zheng and Abbas Jamalipour, "Wireless Sensor Networks: A Networking Perspective", a book published by A John & Sons, Inc, and IEEEE, 2009.

[13]. S. Misra et al. (eds.), Guide to Wireless Sensor Networks, Computer Communications and Networks, DOI: 10.1007/978-1-84882-218-4 4, Springer-Verlag London Limited 2009.