

## Chapter 2

# RFIDs and WSNs

**Abstract** This chapter presents in-depth knowledge about the two technologies i.e. RFID and WSN. The characterization, working principles and applications of these technologies are discussed in a useful manner.

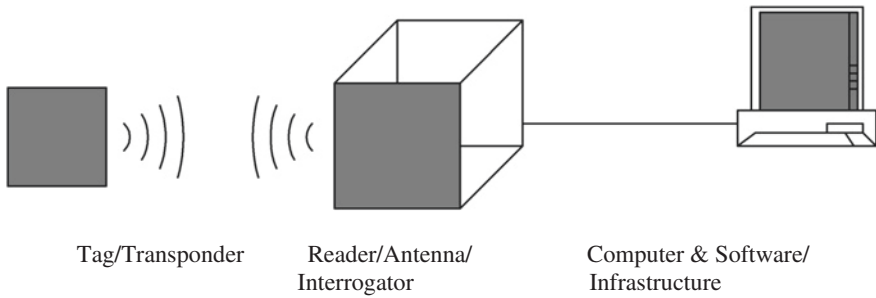
**Keywords** Tags • Reader • Routing

### 2.1 Radio Frequency IDentification (RFID)

The computing technology is expected to interact with the physical environment through small wireless and communication devices in future. In this regard, the RFID (Radio Frequency Identification) is one of the most promising technologies for influencing the real and virtual world. RFID has the ability to identify and track the objects with its unique code and provides information about the presence or absence of the object. RFID technology is implied separately in a number of applications like asset monitoring, public transportation, supply chain, controlling building access etc.

The history of RFID can be tracked as far back as the 1920s with the birth of radar systems (the word radar is an acronym for radio detection and ranging). The development of the technology, a combination of radar and radio broadcast technology, is messy and convoluted but there is consensus that it developed from the work carried out during WW2 to identify enemy aircraft, known as ‘Identification: Friend or Foe’ (IFF) systems [1]. The radio frequency part of RFID is the communication medium between tags and readers. With passive RFID tags, radio frequency is also used to deliver power to the tag, as they do not have on-board power systems [2].

RFID systems are designed to be asymmetric: readers are expensive and power hungry, whilst tags are cheap and require comparatively low levels of energy [3].



**Fig. 2.1** Overview of a RFID system [4]

In addition, there are three key elements that need to be borne in mind while discussing RFID systems: energy source (which determines if a tag is passive or active), frequency and memory (Fig. 2.1).

### 2.1.1 Frequency

The RFID operating frequencies band is divided into four major classes: “like Low Frequency (LF) 125–134 kHz, High Frequency (HF) 13.56 MHz, Ultra High Frequency (UHF) 315–433 MHz, 865–956 MHz” and 2.45 GHz and Microwave Frequency 2.45 GHz [5]. Based on these frequency bands, the communication range greatly depends upon factors like “the operating environment, the detail of the antenna design and the available system power” [6]. RFID is fundamentally based on wireless communication, making use of radio waves, which form part of the electromagnetic spectrum (i.e. frequencies from 300 kHz to 3 GHz). RFID operates in unlicensed spectrum space, sometimes referred to as ISM (Industrial, Scientific and Medical) but the exact frequencies that constitute ISM may vary depending on the regulations in different countries (Table 2.1).

### 2.1.2 Tag-Reader Communication

Tag-reader communication is handled by common procedures often specified in RFID standards such as the “ISO 15693 and ISO 18000-3 for HF or the ISO 18000-6 and EPC for UHF” [7]. Tag-reader communication process is initiated by the reader once it is powered on. The reader broadcasts signals at a special frequency band. The corresponding tags within the reader’s range will absorb the signal energy to power up their internal integrated circuits. The tags then respond to the reader after decoding the signal as valid and continue RF transaction indicating its presence.

**Table 2.1** RFID operating frequencies and associated characteristics [1]

Band	Frequency	RFID frequency (typical)	Read range (approx)	Transfer rate of data	Characteristics	Applications
Low frequency	30–300 kHz	125–134 kHz	<0.5 m	Less than 1 kbit/s	Short-range, low data transfer rate, penetrates water but not metal	Animal ID car immobilizer
High frequency	3–30 MHz	13.56 MHz	Up to 1.5 m	Approximately 25 kbit/s	Higher ranges, reasonable data rate (similar to GSM phone), penetrates water but not metal	Smart labels contact-less travel cards access and security
Ultra high frequency	300 MHz–3 GHz	433 MHz or 865–956 MHz 2.45 GHz	Up to 100 m for 433 MHz and 0.5–5 m for 865–956 MHz	For 433–956; 30 kbit/s For 2.45; 100 kbit/s	Long ranges, high data transfer rate, concurrent read of <100 items, cannot penetrate water or metals	Specialist animal tracking
Microwave	2–30 GHz	2.45 GHz	Up to 10 m	Up to 100 kbit/s	Long range, high data transfer rate, cannot penetrate water or metal	Logistics moving vehicle toll

## 2.2 RFID System Components

An RFID system has two main components: the RF reader (known also as the base-station or interrogator) and the RF tag (or transponder). When RFID tags are attached to physical objects they enable those objects to identify themselves to RFID readers through the use of radio frequency communication [8].

### 2.2.1 Tag

An RFID tag (also referred to as a “transponder, smart tag, smart label, or radio barcode”) has a unique identification number (ID) and memory that is designed to store certain unique information (such as “manufacturer name, product type, and environmental factors including temperature, humidity, etc”.) about the physical object to which the tag is attached, the size of which varies between 32 bits and 32,000 bytes. This tag attached to any physical object can be read and/or written wirelessly with the help of a reader to ascertain its identity, position, or state. The tag consists of a “silicon chip or an integrated circuit” and an antenna. The silicon chip holds an inimitable recognition number and the antenna can launch and take delivery of radio waves. These two components are typically attached to a smooth plastic card which can then be attached to any substantial object. The physical size of a tag can be quite small, thin (like a grain of rice) and can be easily embedded in items like plastic cards, tickets, clothing labels, books, etc [9].

### 2.2.2 Reader

The reader also refers to as interrogator or scanner may have a number of antennas that accounts the process of sending and receiving RF data to and from tags wirelessly [10]. The readers may be deployed stationary or as mobile to notify or energize the tags to “wake it up”. The reader is a hand-held or fixed unit that can interrogate nearby RFID tags and obtain their ID numbers using radio frequency (RF) communication (i.e. the process does not require contact). When a passive tag is within range of a reader, the tag’s antenna absorbs the energy being emitted from the reader, directs the energy to ‘fire up’ the integrated circuit on the tag, which then uses the energy to beam back the ID number and any other associated information.

## 2.3 Types of Tags

RFID tags have been classified into a number of categories based on the power source, memory type and wireless communication signal. Each of these classifications is mentioned below [11].

### ***2.3.1 Tags by the Power Source***

Based on power source, Liu et al. [12] classified RFID tags into three major classes: “active tags, passive tags, and semi-passive (semi-active) tags”.

#### **2.3.1.1 Active Tags**

These tags contain their own power resource that supplies power to the radio transceiver and on-board circuitry. These tags have more processing power than rest of tags. These tags can communicate with readers in a distance of 100 m or more. They can respond to low power signal from RFID reader than other tags. Due to its advanced processing power, these tags can also be set for incorporated sensors for reporting environmental factors such as temperature, humidity etc. Active tags have a significant amount of memory than passive tags and are best suited for environment where a number of tags need to be read simultaneously. However, these tags are relatively expensive than the passive/semi-passive ones and have a finite battery life which must be replaced periodically [13].

#### **2.3.1.2 Passive Tags**

A passive tag does not use any power source of its own. It utilizes the same signal for appending information as a power source and contains a low power integrated circuit. This integrated circuit is attached to an antenna. With the help of this antenna, the tag collects electromagnetic energy from the reader transmitted signal which induces a current in the tag antenna. This current wakes up the tag circuit that reflects a piece of energy reverse to the transceiver adding information to the reflected signal with the help of modulation. These tags have power only when in communication with an RFID reader. Generally, the low power constraint restricts these tags to a short read range up to 3 m or less. This restriction also results in small amount of memory which can store manufacturer unique data in the range of 64 bits. However, these tags have much longer life cycle because they require energy only for its processing operations which is utilized from the received signal. These kinds of tags are cheaper than powered tags because of their nominal involved circuitry. These types of tags are more suitable for applications of individual products such as super markets checkouts and smart cards.

#### **2.3.1.3 Semi-passive Tags**

Semi-passive tags are set with energy source to sustain information in the tags or energized some supplementary tasks. This category of tags utilizes the radio waves of source as a power source for their communication like other passive tags. This

category of tags has more reliability and larger communicating range than pure passive tags because more power is available for other purposes. Nevertheless, its life cycle gets reduced due to its dependence on battery source and results in an expensive range than other passive tags. Generally, the terms “Semi-passive” and “Semi-active” are used interchangeably in literatures.

### ***2.3.2 Tags by the Memory Type***

Another classification of RFID tags is based on memory type, tags with read/write memory, and tags with read-only memory.

#### **2.3.2.1 Read Only Tags**

RFID tag with read/only memory is programmed once by the manufacturers and cannot be modified thereafter. As limited size of static information can be stored so these tags are easy to integrate with a data collection system. Usually, these devices are cheaper than others.

#### **2.3.2.2 Read/Write Tags**

This class of tags performs both types of memory operations. The information on the memory can be altered dynamically after the manufacturing process. These tags can store larger amount of information (usually in the range of 32–128 kbytes) than Read-only tags but are quite expensive and are not suitable for application of inexpensive-items.

### ***2.3.3 Tags by the Wireless Communication Signal***

Another classification of RFID tags is based on the technique of wireless signal used for exchange of information among the two nodes of communication. i.e. (Near field RFID and Far field RFID) [14].

## **2.4 Routing in WSNs**

The process of determining a path from source to destination when a data transmission request is made, called routing. In WSNs, network-layer is the layer which is responsible for routing of all the data. In particular case when the sink

node is away or does not lie in the range of source node, multi-hop routing technique is applied and their packets are relayed by intermediate sensor nodes. The solution lies in implementing the routing tables. Routing table comprises lists which have the information about node options, as destination of any packet. It is function of the routing algorithm along with routing protocol's support for their creation and maintenance.

### ***2.4.1 Routing Challenges and Design Issues***

Different constraints and objectives have been considered for WSN depending on the different architectures, applications and designs. Though the analysis of the routing-protocol performance is diligently associated with the architectural model yet the considerable limitations are [15]:

- **Network dynamics:** Sensor nodes are supposed to be stationary in maximum sensor networks, because the configurations with mobile sensor nodes are very few in numbers. Sometimes the mobility support of sinks or cluster head is very essential. The other important factor is route optimization stability, in addition to bandwidth, energy constraints etc. The transfer of routing messages between mobile nodes is more challenging. Thus, depending on particular application, the sensed event may be either dynamic or static.
- **Node deployment:** The deployment of node is application specific and performance of routing protocol is highly dependent on it. The deployment of node is either self-organizing or deterministic. In situations where deployment is deterministic, the placement of sensors is done manually and the routing paths for data transmission are predetermined. When nodes are deployed in the self-organizing manner, an ad-hoc infrastructure is created by scattering the nodes. The other factors affecting the performance and energy efficiency is position of the sink or cluster-head. When the nodes are not distributed uniformly, optimal clustering becomes an urgent issue for efficient operation of the power system.
- **Energy considerations:** While an infrastructure is created, setting up process of the routes is greatly under effect of energy constraints. Subsequently, the power of transmission of wireless radio is relative to square of the distance or higher than that sometimes when obstacles are present, lesser energy will be consumed in multi-hop routing than direct communication. Nevertheless, multi-hop routing leads major overhead for medium access control and topology management. The performance of direct routing would be well enough if all the nodes lie close enough to the sink. Sensors are dispersed over an interested area, randomly most of the time, and multi-hop routing becomes inevitable.
- **Data delivery models:** The transmission of data from source to the sink can be uninterrupted, driven by some event, hybrid and driven by some query. It is highly dependent on the application scenario of the sensor network. Considering the uninterrupted model for data delivery, data is sent by each

sensor periodically. In query-driven and event-driven models, thus whenever an event occurs or the sink generates some query, the transmission of data is activated. Sometimes a hybrid model is applied by sensors by combining continuous, query-driven and event-driven delivery of data. The choice of routing protocol used is highly inclined by the model for delivering data, particularly when reduction of route stability and energy consumption is under consideration.

- **Data aggregation/fusion:** Multiple nodes can produce similar types of packets which are aggregated to minimize the transmission. Substantial amount of redundant data is generated by sensor nodes for this purpose. The aggregation of data is the process of data combination from various sources by using different functions.
- **Node capabilities:** In a sensor network, different functionalities can be linked with the sensor nodes. A sensor node is very application specific, thus a node can be devoted to a certain special task such as sensing of data, relaying and collection of data. The usage of these functionalities all at once on a single node might make the energy of that node drained very quickly.

### 2.4.2 Routing Objectives

There are some of the applications of sensor network which require just the successful data delivery between a source node and a destination node. Nevertheless, there are some of the applications where more assurance is required. These are the requirements in real-time for maximizing the life time of network and for delivering the data [16].

- **Non-real time delivery:** It is essential for all routing protocols to consider the guarantee of data delivery. In clear meanings, if there exists a routing path between the interactive nodes, the routing protocol should always find it. This property of precision can be proven in a way which is more recognized, while the performance evaluating parameter is the data delivery ratio.
- **Real-time delivery:** Some of the sensor network application scenarios deal with in-time data delivery so they require in-time delivery of that message, if failed to do that, the message becomes useless and it might losses informative content after the time limit. Hence, thorough control of network's delay is the key objective of these routing protocols. The time constraint message delivery ratio is the parameter for evaluating the performance of these protocols.
- **Network life Span:** The applications where the sensor nodes in the network must run as long as possible, this objective is crucial. The protocols which are concerned about network lifetime, by considering the remaining energy levels, try to balance the energy consumption among the nodes equally. Though,



like every other sensor node application, the network lifetime parameter is also application dependent. Maximum routing protocols deal with the assumption that every node is important equally and one of the parameter they use is the time, until the first node drains off, and the energy consumed by nodes on average, as another parameter. If nodes are not equally important, then the time until the last or high-priority nodes die can be a reasonable metric [17, 18].

### ***2.4.3 Characteristics of Routing Protocols***

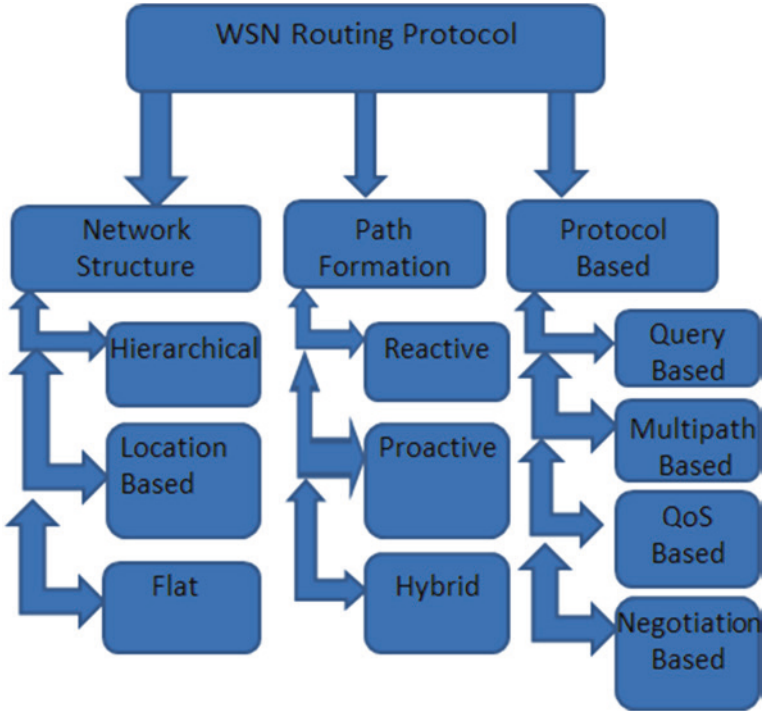
Generally, wireless sensor routing protocols are:

- Capable of collecting data.
- Application dependent.
- Data centric.
- Capable of optimizing energy consumption.

## **2.5 Routing Techniques in Wireless Sensor Networks**

WSN Routing Protocols can generally be classified in three ways, according to the way of routing paths are established, the network structure, the protocol operation. Figure 2.2 shows the WSN routing protocols classification.

There can be three ways for the establishment of a routing path, namely proactive, reactive or hybrid. Routing protocols capable of calculating all the routes before they are really needed and then store these routes in a routing table of each node, is proactive routing protocol. Whenever there is a change in routing path, the change must be circulated through the entire network. Since a WSN may consist of several hundreds or thousands of sensor nodes, each sensor node is keeping the routing table, it could be huge in size and therefore proactive protocols [19] are not much suitable for sensor networks. Reactive protocols [19] calculate routes if they are needed. Hybrid protocols use a combination of these two ideas. But in general, considering the network structure, the routing in networks of sensors can be divided into categories described as hierarchical-based routing, flat-based routing and location-based routing. In hierarchy-based routing, however, nodes play different roles in the network. In the flat routing, all nodes have the same role. In the location-based routing, the positions of the sensor nodes are operated for routing data in the network. Furthermore, these protocols can be classified into query-based, multipath-based, QoS-based, negotiation-based or coherent-based routing techniques depending on the protocol operation.



**Fig. 2.2** Classification of WSN routing protocols

### 2.5.1 Flat Routing

Assigning individual identifiers to every node in a network is not feasible due to higher density of sensor nodes present in a network for wide variety of applications. Thus random deployment of sensor nodes in a network with no global identifiers makes selection of set of sensor nodes, difficult for a query. Therefore, within a deployment area data transmitted from sensor node is generally in redundant form. This realization helped in emergence of data-centric routing [20].

### 2.5.2 Hierarchical Protocols

Scalability is one of the key design attributes of sensor networks. Due to the reason that the sensors cannot communicate over longer distances, there is no scalable architecture for single gateway sensors. In order to cope with extra load on a network, some approaches have adopted aggregation procedure which maintain the service and enable the network to cover large area of deployed interests.

Hierarchical routing works in two layers, Cluster-heads are selected on the first layer and second layer is used for routing the information. Hierarchical protocols maximize the overall system lifetime, scalability, and energy efficiency [21].

### ***2.5.3 Location-Based Protocols***

For geographically deployed sensor networks, exact location information of sensors is very important. It enables the distance calculation between two particular nodes in order to estimate the energy consumption and thus total energy of the network. Typically, two techniques have been used in the literature to find the location, one is by using Global Positioning System (GPS) and other is by finding the coordinates of the nodes in the neighborhood. Due to unavailability of some addressing system for sensor networks such as assigning IP addresses to individual sensors and their spatial deployment in a region, the location information may be accessed which is useful in routing data efficiently with energy consideration [21].

### ***2.5.4 Multipath Routing Protocols***

Several ways are used to maximize the performance of a network. On failure of the primary link between the source and the destination, there is another way which measured fault tolerance (resilience) of a protocol. This can be increased by maintaining multiple paths between the source and the destination. This increases the cost of the energy consumption and the generation of traffic. Alternative paths are kept alive by sending periodic messages. Therefore, the reliability can be increased [21].

### ***2.5.5 Query Based Routing Protocols***

A REQ (request for data) meta-data has been propagated by destination nodes through the network and a node with requested data returns the data to the node. The forwarded data is then matched with the query to initiative query. Generally, local languages are used to describe the queries, or languages having high-level queries [21].

### ***2.5.6 Negotiation Based Routing Protocols***

High-level data descriptors are used eliminate duplicate data transmissions, via negotiation. Communicating decisions are made depending on the available resources. Using

flooding for data dissemination for providing implosion and overlapping between the sent data is the motivation behind this. The consumption of energy is increased and more processing is required to send the same data to different sensor nodes. Thus, removal of duplicate information and prevention of redundant data is the main idea of the negotiation based routing in sensor networks [21].

### ***2.5.7 QoS-Based Routing Protocols***

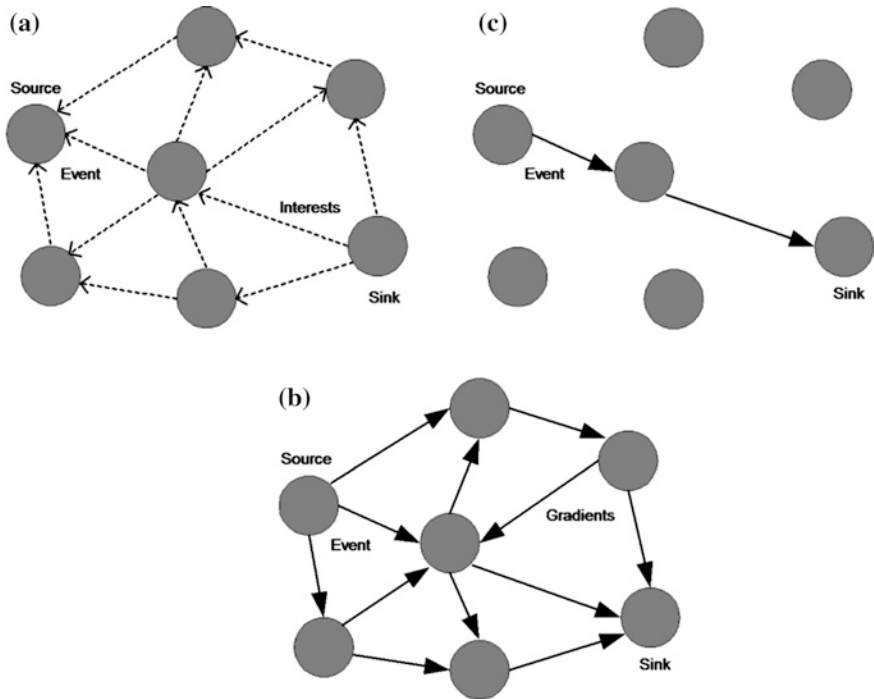
Quality of Service (QoS) parameters, such as delay, power, and bandwidth is satisfied upon delivery of data to the base station, the network has a balance between energy consumption and data quality [21].

## **2.6 Routing Protocols for WSN**

One of the most important and efficient routing protocols of WSNs is Directed Diffusion (DD). It is a typical data-centric protocol for WSN which laid the essential foundation for routing design of wireless network and is leading the way in data centric protocol design. In next section DD and another routing protocol ACQUIRE is discussed in detail. ACQUIRE is an efficient query based routing protocol especially designed for energy aware efficient routing in WSNs.

### ***2.6.1 Directed Diffusion Protocol***

Direct Diffusion [22] is a data centric protocol. It is the first protocol proposed for wireless sensor networks scenarios that works better than the flooding techniques. It consists of several elements: interests, data messages, gradients, and reinforcements. First, request is sent by the sink node by sending data interest. The message of interest is a query, which specifies that the user wants its neighbors to name the data. Data is named using attribute-value pairs and is information is collected or processed. Interests are flooded throughout the network. This data may be an event which is a brief description of the phenomenon detected. Whenever a node receives an interest, it will check if this interest already exists or it's new. If it is a new interest, the sensor node set up a gradient to the sender to "draw" the data down which corresponds to the interest. Each pair of neighboring nodes establishes a gradient in the other. After creating step gradient, the source node starts sending data corresponding to the related interests of the sink. The data is generally distributed to all its neighbors' gradient. The events are propagated to the initiators of interest along a variety of paths gradient. The sensor networks reinforce some of these paths. The reinforcing pattern is usually designed for the minimum or maximum packet delay received during a certain period of time as shown in Fig. 2.3.



**Fig. 2.3** Direct diffusion; **a** propagation of interest, **b** initial gradient setup, **c** data delivery [22]

Directed Diffusion tasks are named using attribute-value pairs. For the naming scheme based on the value attributes, a range of values is associated with each attribute. Some other choices are also available for attribute-value pair arrangement and naming systems. Somehow, the choice of naming scheme and arrangement can affect the performance of diffusion by affecting the appearance of the task.

The interest is usually introduced into the network through sink. For each active task, the sink periodically broadcasts an interest in all of its neighbors. Since in the sensor network it is highly inconvenient to locate the sources accurately, interest must necessarily be distributed over a wider section of the network. Accordingly, if the selected sink has data rate that is initially high, the energy consumption could be high due to the wider distribution of sensor data. The desired higher flow rate data may be obtained by reinforcement.

The interest is trivial state and sink is responsible for updating it periodically. Periodic interest propagated by sinks is necessary because there is a fair chance that it might not be received. To overcome this problem, the same interest is simply re-sent by the sink, thus increasing timestamp attribute. Each node is responsible for maintaining a cache of interests. Each item in the cache is related as a separate interest. Interest contains information about the immediate previous hop only so, the state of interest related to the number of distinct active interests. Few

fields are associated with interests in cache. A timestamp field shows the timestamp of the last corresponding interest received. A gradient field contains a data rate requested by the corresponding neighbor range, and the derivative of interest and a duration field attribute and derived from the timestamp expires, to attributes of interest. The duration field indicates the approximate life of the gradient and interest. Data is propagated by gradients. For event-triggered applications, every gradient contains a type gradient instead of a data rate gradient. There are two types of gradient: Exploratory gradient and Data gradient. Exploratory gradients are for the path setup and repair while gradients data for sending actual data. Gradient type by default is exploratory.

On receiving interest, a node first checks its availability in cache. If there is no corresponding interest, the node creates an entry of interest and each field of the entry in the interest is determined. This entry contains a single gradient towards the neighbor whose interest was received, with the rate specified event data. Thus, it is necessary to distinguish individual neighbors. Then the timestamp fields and duration is updated by node. Expired gradient will be removed from the entry of interest, but not all gradients will expire at the same time.

When an interest is received, a node may decide to refer the interest in a subset of its neighbors. To its neighbors, this interest seems to come from the sending node, although a distant well may be the true origin. With such a completely local interaction, interest is distributed across the network. Interests However, all receipts are sent again. Using the cache of interest, a node can delete a received interest if it has recently re-sent a corresponding interest. In general, there are several possible choices for the neighbors to return the interest.

The best alternative in a simple way would be retransmitting the same interest of all neighbors, like flooding the interest. Since interest is flooded, gradients are established by all nodes. Unlike simplified in Fig. 2.3b description, each pair of neighboring nodes establishes a gradient towards each other. Since there is no information about sink in received interest, when a node receives an interest, node is unable to find out that if the interest is delivered to the node because it is in the form of loop, also that the interest is delivered using a different path, or the same interest is newly generated from another sink. Such bidirectional gradients can cause a node to receive a copy of events of low data rate from each of its neighbors. However, this technique can enable fast recovery paths or reinforcing the empirical failure best ways and do not incur persistent loops.

### ***2.6.2 Low Energy Adaptive Clustering Hierarchical Protocol (LEACH)***

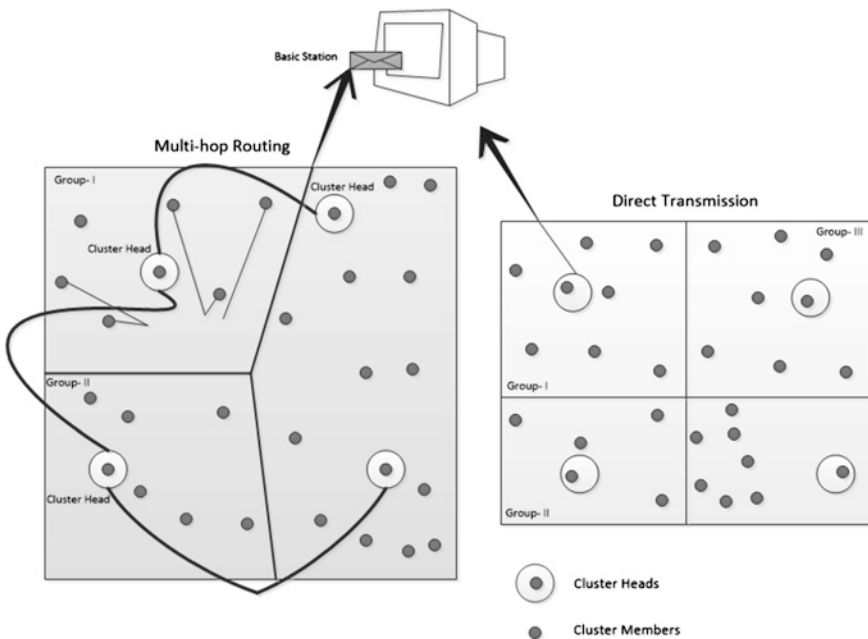
LEACH protocol is the most widely used protocol [23] and can be described as a combination of multi-hop routing and cluster architecture. The sensors with LEACH protocol work by forming cluster-heads and cluster members among the group. The communication between clusters, cluster-head and base stations

are done by multi-hop routing. The operations that are conducted in the protocol LEACH is divided into two phases, the setup phase and the steady state phase.

In the setup phase, all of the sensors within a network get together make groups in some region of the cluster. They communicate with each other by exchanging short messages. One sensor node can act as a cluster head at a time and is capable of communicating to all other remaining sensors. Primarily, similar type of sensors depending on the signal strength of messages sent by the cluster heads chooses to form clusters. Interested sensors meet again at the head of the cluster when they send a signal indicating their acceptance to join as a response. Thus, this is the end of setup phase. The group leader can decide the optimal number of cluster members, it can handle or requires.

Before entering the first phase, parameters such as relative computation cost and network topology are taken into consideration. A TDMA schedule is applied to all members of the cluster group to send messages to the cluster head and cluster head to the base station. Figure 2.4 shows two phases of a sensor in a LEACH protocol, all sensors formed as members of the cluster head and the cluster heads in the second phase of ammunition perform data transmission to the sink in a multi-hop structure. A direct transmission system is also provided below.

As soon as a cluster head is selected for a region, all the sensed and collected data is sent using TDMA slots allotted to the cluster head. Then this data is compressed and transmitted to base station by cluster head, which completes the



**Fig. 2.4** LEACH operation showing set-up, steady state phases using multi-hop, also showing direct transmission [23]

second phase, called the **Steady State Phase**. Once the steady-state finishes the data transmission to the sink, the whole process comes to an end and a new search for the forming of cluster heads for a region and new cluster-member formation begins.

Since the network is distributed, there is a possibility that all the sensors might not be too close or at equal distance to the cluster head, so the cost of energy consumption by the farther sensor is not equal to the cost of energy consumption by the nearest node. In order to minimize this, procedure of cluster heads formation is rotated among all the nodes in the cluster. LEACH minimizes global energy usage by distributing the load of the network to all the nodes or cluster members at different intervals.

The data sent by all the cluster heads in a network is received at base station in compressed format. An important point is that the cluster heads which are away from base station, cannot send their data to base station directly therefore, they forward their data to nearest cluster heads and they eventually forwards the information to the base station, forming a multi-hop routing network. Making cluster head responsible for forwarding the data improves lifetime of network by improving the lifetime of sensors [24].

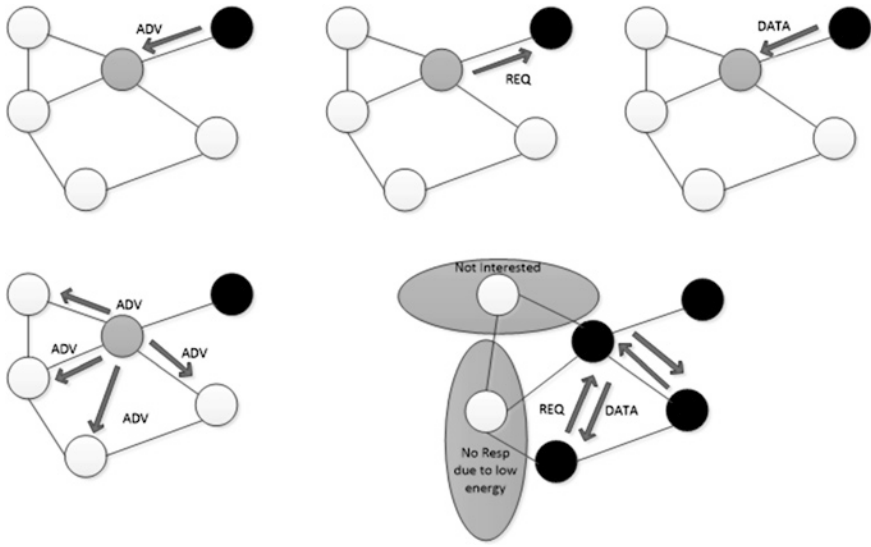
### ***2.6.3 Sensor Protocol for Information via Negotiation (SPIN)***

Distribution of data became the main motivation behind developing SPIN. Dissemination or distribution of data is the process of collecting the observations from all the deployed sensors in a network, treating every sensor as sink node. Life time of the sensors is made prolonged by sensibly controlling consumption of energy during computation and communication. SPIN was proved better protocol by removing drawbacks in the sophisticated protocols like: overlapping, implosion and resource blindness [23]. These issues of flooding and resource blindness were solved by using negotiations and resource adaptation.

SPIN uses three types of messages for transmitting data, also known as Meta data before data transmission among the neighbors in the network. First the interest is propagated when a node sends this meta-data to its neighboring node. Since information is exchanged by using meta-data, it helps the node to choose particular type of data from particular node, saving the energy. While sharing data directly between two nodes might result in greater energy consumption. Nodes cannot respond to all the data messages sent by all other nodes because of the changing topology or network structure.

Characteristics of shared information are described in meta-data. The size of meta-data is made smaller than the original data and it should be distinct from other data types. Meta-data are application-specific and they always consider their geographic location or a unique ID while communicating with the neighbor nodes. Three types of meta-data messages are exchanged between the nodes:





**Fig. 2.5** Five stages of SPIN showing the three-way handshaking [23]

**ADV:** This type of meta-data is used when a SPIN node has something new to exchange it with other neighbouring nodes in the network. So, this is advertisement meta-data.

**REQ:** This is the request meta-data and any node interested in exchanging new information, sent this type of message to the node having this new interest or information.

**DATA:** The actual data that has to be shared between two nodes which are involved in exchange.

Considering the scenario that a node A has gone through update and it needs to forward this new information to other neighboring nodes in a network. For this purpose first message it send is an ADV message to the nearest neighbors, containing required fields describing data type computation and communication type etc. Only interested nodes will respond in this updated information will send REQ message to source node as a response. On receiving REQ message, the source node transmits the requested information to interested node. This is how the data dissimilates (Fig. 2.5).

#### 2.6.4 Active Query Forwarding In sensor Networks Protocol (ACQUIRE)

ACQUIRE [23] is a data centric, query-based protocol. Recently ACQUIRE has appeared as a technique that is energy efficient and highly scalable query-based

protocol for use in real-world sensor networks. The motivation behind ACQUIRE is the injection of active queries into the network that are capable of triggering when local updates are performed similar to COUGAR [25], it considers the network as a distributed database. The query is sent by the sink and each node that receives the query by processing the existing information. After that it forwards the query to a neighboring sensor. If the existing information in the node needs to be updated, the node looks for the information from the neighbors who are at most  $d$  hops far away.

ACQUIRE, when comes to compare with other alternative routing protocols seems to beats all other strategies, keeping its parameters values optimum. The reason behind that performance would be that it is especially designed for complex, one-shot queries, even when the other schemes too are enhanced with cached updates. In particular, optimal ACQUIRE performs many orders of magnitude better than flooding-based schemes (such as Directed Diffusion) for such queries in large networks. Energy consumption can be reduced to 60 % by using ACQUIRE with optimum settings and parameters (Fig. 2.6).

The traditional flooding-based techniques must be taken as overview in order to know mechanism of ACQUIRE better. Two main stages are clearly separated in those techniques, which are response gathering stage and dissemination stage. Several copies of queries in the form of interests for named data are flooded in the network first. Nodes carrying data relevant to those queries respond. For non-persistent queries, the costs lined with queries are dominated by flooding. Similarly, in the process of aggregation data is collected in suboptimal way as a result of duplicate responses, causing increased energy cost.

On the other hand, query and response stages are not separated in ACQUIRE. The querier node generates an active, one shot, rather complex query, carrying

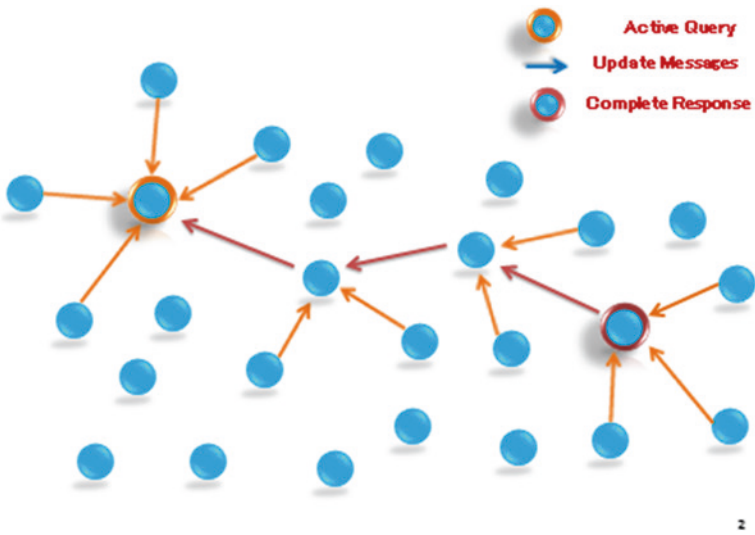


Fig. 2.6 Working of ACQUIRE protocol

multiple sub-queries capable of corresponding to different interests. The query generated is then forwarded to other neighboring nodes following certain sequence. The updates received by all nodes are then utilized by active node at each intermediate step, within  $d$  hop distance in order to resolve it partially. Whenever a node receives an active query, it triggers for updates if it is holding old/expired information. First active node tries to resolve the query partially with information it is already holding, then it forwards the remaining unresolved query to another node randomly selected within  $d$  hop distance. The choice of node can be either way by random walk or directed intelligently based on other information. Hence as the active complex query moves through the network, it keeps getting “smaller” as pieces of it become resolved gradually, until it reaches a node which has every information to resolve it completely. The forwarded query becomes a complete response at this point where it is resolved completely and it is forwarded back to source node as complete rote.

ACQUIRE protocol is therefore well-suited for complex, one-shot queries for replicated data. When it comes to discuss persistent queries, flooding based techniques can work better than ACQUIRE because of their low cost of interest flooding rate.

### 2.6.5 Geographical Adaptive Fidelity Protocol (GAF)

It locates network nodes and makes the best use of them for better fidelity. All nodes use a location-identification technique lie within the network, together with its nearest neighbors by using information location systems like GPS. In GAF, all nodes are commanded according to the networks also called the virtual networks. All network nodes are divided into the virtual networks and all nodes that are under the same grid coordinate with each other to see who will enter a state of sleep and for how long. Load balancing is performed and a single node will not get drawn with the work of others. It can also be very simple to define virtual networks and all the nodes in the window A can communicate with all nodes in Bare adjacent window. Sleep time decided or information depends on the application and system.

There are three state variances in GAF, i.e. discovery, active and sleep. At start all nodes begin with the discovery state. Radio of the node is turned on and starts sending discovery messages to find the adjacent its nodes in same network. Each discovery message is a collection of certain parameters, e.g:

**Node State:** Discovery, Active or Sleeping

**Node ID:** The node itself or its current location

**Grid ID:** Each node in a network utilizes its location information gathered from GPS and the size of its grid in order to query its grid id

**(*enat*):** Estimated node active time, this is the node lifetime. This is the total remaining energy in the node.

These parameters such as node move to discovery mode, which sets the time  $T_d$  (Time Discovery) and send discovery messages to all its neighbors in the network. After transmitting a message to this discovery, it enters the active state. This may include sleep mode if there are other nodes in the network, corresponding to the processing of fidelity before falling in the active state. In active mode, the node sets the timeout value  $T_a$  showing the remaining time that the node is intended to remain in an active state. During the active state, the node retransmits the message to the discovery of a certain time interval  $T_d$  and enters sleep mode if it detects another node, which corresponds to a node or a node of higher rank, which can handle the communication and routing. The three types of state processing is represented in Fig. 2.7, which states performance of the node during discovery, active and sleep state [26].

Sleeping state of a node can be achieved from discovery state or the active state. Prior to the sleeping state, all the timers like  $T_a$  and  $T_d$  are cancelled and radio is put down to power off.

The node completes time frame  $T_s$  to return to the discovery state, which is application or system input.

GAF follows a load-balancing mechanism to maintain a constant communication medium or routing path between the nodes. This is done to make the nodes in the grid work efficiently and to analyze the nodes increase in lifetime. This is dependent on the assumption that all nodes in a specific grid are equal and no node is completely used; this is repeated till all the nodes are died out. There is possibility of nodes available in a pool with more energy resources or in other words with higher ranks. To deal with these nodes there is slot available so that they may handle some other process among other nodes. This is the case where nodes are commanded to shift back to discovery state after the completion of active state

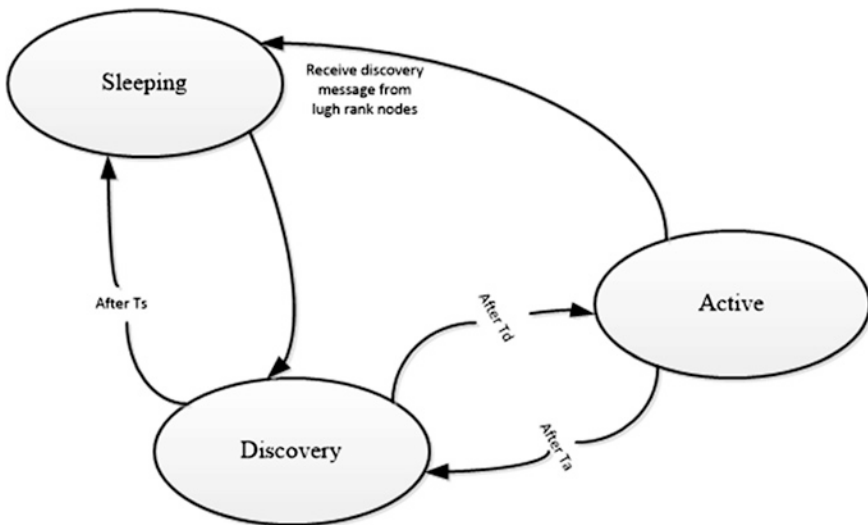


Fig. 2.7 Showing three state transitions in geographic adaptive fidelity [26]

time interval  $T_a$ . Timer  $T_a$  is settled at *enat* and discovery message advertisement is started. Timer  $T_s$  is set to sleeping time which is again equal to *enat*, i.e. the sleeping time.

### 2.6.6 Dynamic Source Routing (DSR)

Dynamic Source Routing protocol is one of the reactive protocols. It states the way for all nodes in a network to find a route to multiple destinations in the grid. Overall overhead of network bandwidth is minimized using DSR. DSR does not broadcast routing updates periodically. Battery power is also saved by stopping the periodic large routing update messages broadcast. In case of failure however there is an option available at MAC layer to inform the routing protocol [23, 26].

Following are properties of Dynamic source routing:

1. DSP takes advantage of saving space in nodes memory by avoiding the up-to date routing information in intermediate nodes.
2. No periodic update messages broadcast saves network bandwidth.
3. Battery is also saved by avoiding periodic updates in DSR.
4. Information is gathered by sniffing the routes in received packets.
5. Piggybacking new request allow unidirectional communication to the source node.
6. Interface address filtering turned off in order to scan all packets. This allows the interface to run in a promiscuous mode free environment. An intruder can sniff to all the information in the packets for some valuables such as credit card information and passwords.

**Route Discovery:** DSR stores all known routes in a cache. RREQ is used by the source node to broadcast messages to start conversation between nodes. Other nodes search their own cache in order to find the route to source node as soon as they receive RREQ. RREQ is forwarded in case of route unavailability and current node address is stored in sequence of hops. RREQ propagation is a recursive process and kept on broadcast till the destination is available by itself. In this scenario a RREP is unicasted to the source node. RREP packet contents itself contain hops sequence in the grid to reach the destination [23, 26] (Fig. 2.8).

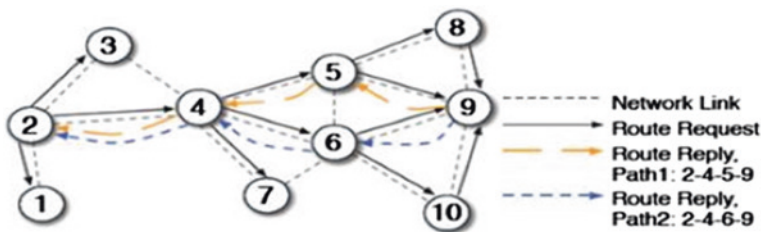


Fig. 2.8 DSR route discovery for target node [27]

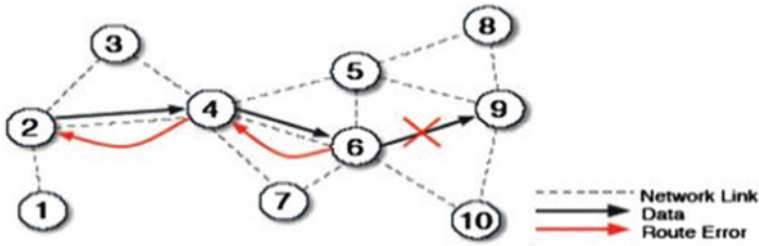


Fig. 2.9 DSR maintenance for error route [27]

*Route Maintenance:* Error packet is generated and sent to source node in case of an invalid path discovery. The sent route does not contain the hop that has error in the path and it is removed from the memory i.e. cache of host. All related hop routes also are deleted (Fig. 2.9).

## References

1. Ward M (2006) RFID: Frequency, standards, adoption and innovation. JISC Technol Stand Watch. Available at <http://www.jisc.ac.uk/techwatch>
2. Zhang Y, Yang LT, Chen J (eds) (2009) RFID and sensor networks: architectures, protocols, security and integrations, pp 511–536
3. [http://www.rfidc.com/docs/introductiontorfid\\_technology.html](http://www.rfidc.com/docs/introductiontorfid_technology.html). Accessed 20 Apr 2010
4. [http://www.aimglobal.org/technologies/rfid/what\\_is\\_rfid.asp](http://www.aimglobal.org/technologies/rfid/what_is_rfid.asp). Accessed 20 Apr 2010
5. Dressen D (2004) Considerations for RFID technology selection. Atmel Appl J (Corporate Communication: Atmel Corporation)
6. <http://en.wikipedia.org/wiki/File:Sensornode.svg>. Accessed 20 Apr 2010
7. Laran (2004) RFID: a basic introduction to RFID technology and its use in the supply chain
8. <http://en.wikipedia.org/wiki/File:WSN.svg> Accessed 20 Apr 2010
9. Beiwei Z, Kunyuan H, Yunlong Z (2010) Network architecture and energy analysis of the integration of RFID and wireless sensor network. In: Proceedings of Chinese control and decision conference
10. Liu H, Bolic M, Nayak A, Stojmenovi I (2009) Integration of RFID and wireless sensor networks. Bentham Science Publishers, Sharjah
11. Ilie-Zudor E, Kemeny Z, Egri P, Monostori P (2006) The RFID technology and its current applications. In: Proceedings of the modern information technology in the innovation processes of the industrial enterprises-MITIP, pp 29–36
12. Liu H, Bolic M, Nayak A, Stojmenovi I (2008) Taxonomy and challenges of the integration of RFID and wireless sensor networks. IEEE Netw 26–32
13. Thompson D (2006) RFID technical tutorial. J Comput Sci Col 21(5):8–9
14. Sung J, Sanchez Lopez T, Kim D (2007) The EPC sensor network for RFID and WSN integration infrastructure. In: Proceedings of the fifth IEEE international conference on pervasive computing and communications, 618–621
15. Akyildiz IF, Su W, Sankarasubramaniam Y, Cayirci E (2002) A survey on sensor networks. IEEE Commun Mag
16. Mitsugi J, et al (2007) Architecture development for sensor integration in the EPC global network. Auto-ID labs white paper

17. Cheekiralla S, Engels DW (2005) A functional taxonomy of wireless sensor network devices. In: Proceedings of the 2nd international conference on broadband network, vol 2, no 3–7, pp 949–956
18. Heinzelman WB, Chandrakan AP, Blakrishnan H (2002) An application-specific protocol architecture for wireless microsensor networks. *IEEE Trans Wirel Commun* 1(4):660–670
19. Lee CKL, Lin XH, Kwok YK (2003) A multipath ad hoc routing approach to combat wireless link insecurity, vol 1, pp 448–452
20. Al-Karaki JN, Kamal AE (2004) Routing techniques in wireless sensor networks: a survey. *IEEE Wirel Commun* 11:6–28
21. Krishnamachari B, Estrin D, Wicker S (2002) Modeling data centric routing in wireless sensor networks. *IEEE INFOCOM*, New York
22. Intanagonwiwat C, Govindan R, Estrin D (2000) Directed diffusion: a scalable and robust communication paradigm for sensor networks. In: Proceedings of the 6th annual ACM/IEEE international conference on mobile computing and networking (MobiCom\_00), Boston, MA
23. Sadagopan N, Krishnamachari B, Helmy A (2005) Active query forwarding in sensor networks. *Ad Hoc Netw* 3(1):91–113
24. Zhao J, Erdogan AT, Arslan T (2005) A novel application specific network protocol for wireless sensor networks. *IEEE Reference number* 0-7803-8834-8/05
25. Yao Y, Gehrke J (2002) The cougar approach to in-network query processing in sensor networks. In: *SIGMOD*
26. Stemm M, Katz RH (1997) Measuring and reducing energy consumption of network interfaces in hand-held devices. *IEICE Trans Commun (Special Issue on Mobile Computing)*
27. Ullah M (2009) Evaluation of routing protocols in wireless sensor networks. Master's thesis

RFID-WSN Integrated Architecture for Energy and Delay-Aware Routing

A Simulation Approach

Ahmed, J.; Siyal, M.Y.; Tayyab, M.; Nawaz, M.

2015, XII, 89 p. 36 illus., 22 illus. in color., Softcover

ISBN: 978-981-287-413-9