Contents lists available at Science-Gate

International Journal of Advanced and Applied Sciences

Journal homepage: http://www.science-gate.com/IJAAS.html

Routing protocols from wireless sensor networks to the internet of things: An overview

Salem Belhaj [1, 2, *], Sofian Hamad [1]

[1]Computer Science Department, Faculty of Science, Northern Border University, Arar, Saudi Arabia
[2]Computer Science Department, University of Tunis /Ecole Nationale Supérieur des Ingénieurs de Tunis, Tunis, Tunisia

ARTICLE INFO

Article history:
Received 23 April 2018
Received in revised form
10 July 2018
Accepted 10 July 2018

Keywords:
Routing
WSNs
IoT

ABSTRACT

This article examined the state-of-the-art overview of the most relevant routing protocols that have been proposed as part of constrained networks, including Wireless Sensor Networks (WSNs) and the Internet of Things (IoTs). This category of network will be one of the main parts of the future global network. Therefore, achieving satisfactory performance on constrained networks is a current research challenge, especially at the routing level. In this vision, the classification of routing protocols in sensor networks is established and the current state of standardization in the area of the Internet of Things is updated. In addition, a comparison of the described protocols is discussed for each class of algorithms. Finally, some technological challenges and some emerging lines of recent research on resource-constrained routing approaches for WSNs and IoTs are briefly discussed.

1. Introduction

Historically, the trend of Internet-based technology has shifted from the classic web to social networks, then to ubiquitous computing and ultimately cloud computing. Currently, there is a need for data-on-demand, which implies an emerging trend for the exchange of information between users and devices (Kortuem et al., 2010). Therefore, future Internet-based applications involve distributed smart objects communicating autonomously.

A WSN typically comprises a number of autonomous, low-power, spatially distributed, mobile or stationary Sensor Nodes (SNs) or motes, ranging theoretically from two to several thousand, that communicate together to transmit data to the Base Station (BS), without using pre-existing infrastructure. Note that SNs can be deployed randomly or deterministically, in an area where data collection is desired.

Smart sensors are small devices, with limited resources and cheaper than traditional sensors. These sensors can sense, collect and measure physical or environmental properties such as pressure, humidity, chemical vapor, signal, lighting, vibration, motion, and pollutants, etc. (Akyildiz et al., 2002). Then, the collected data is transmitted to a central device (for example a computer or a portable terminal). A SN can have different sizes and prices, depending on its performance. Size, accuracy and cost constraints result in corresponding constraints on SN resources such as energy, memory, processing capacity and bandwidth.

Research and development of routing algorithms in WSNs were initially driven by defense applications. Today, research on WSNs and IoTs has been very dynamic and has attracted growing interest from the scientific, military and industrial communities. Their applications and commercial potential are increasing every day and are very promising. This interest is due, among other things, to the recent progress and convergence of Micro-electromechanical Systems (MEMS) technology that has favored the development of fully integrated, energy-efficient, cost-effective, small, easy-to-use, accurate, scalable and smart sensors.

The primary design goal of a routing algorithm operating in the context of WSNs is to minimize power consumption and thereby extend network lifetime. To achieve this goal, most components of a SN, including the radio, must be in low-power sleep mode and reactivated only when transmitting or receiving information (Romer and Mattern, 2004).

WSNs have proven their effectiveness in many military applications such as battlefield surveillance,

* Corresponding Author.
Email Address: Salem.Belhaj@nbu.edu.sa (S. Belhaj)
https://doi.org/10.21833/ijaas.2018.09.009

target tracking radar (Arora et al., 2004), and the intelligence services (Đurišić et al., 2012). Their use is also found in remote environmental monitoring such as monitoring of air pollution (Yi et al., 2015). In addition, they have been widely deployed in health care monitoring such as blood glucose testing (Alemdar and Ersoy, 2010). Another important area of their application is the agriculture, such as low-cost greenhouse monitoring (Srbinovska et al., 2015). They are also used for monitoring, detection and real-time management of disasters such as forest fires (Aslan et al., 2012), landslides (Ramesh, 2014) and earthquakes (Faulkner et al., 2011). Besides, WHANs (Wireless Home Automation Networks) (Gomez and Paradells, 2010) to monitor and control smart home management applications.

The devices of the IoTs sense environmental conditions using sensor networks, which serve as hands and feet for the IoTs, without which it can neither advance nor operate. Indeed, sensors are the bridge that connects the physical world to the digital-world through the transmission of sensed physical values across the network to the end-user.

Far from being exhaustive, our survey focuses on the main techniques that have marked the evolution of routing in wireless sensor networks as well as the evolution of IoTs standards. On the other hand, this survey can help the reader to choose the most appropriate routing algorithm. In addition, our research helps to update the state-of-the-art, including a list of key protocols that have marked the evolution of this line of research.

This manuscript is organized as follows: In the next section, a state-of-the-art on routing protocols in WSNs is established. In section 3, a comparison between WSNs and other adhoc networks is discussed. In section 4, routing techniques in WSNs are classified, analyzed and discussed based on sample protocols. In section 5, the current state of lower layer normalization for IoTs is queried. In section 6, some future challenges and some lines of research for routing in WSNs and IoTs are given. Finally, in section 7, the conclusions drawn from this research are announced.

2. Related works

The growing interest in WSNs has motivated the development of associated protocols. The literature presents a large number of surveys dealing with routing in sensor networks. Among them, several general surveys (Akyildiz et al., 2002; Tilak et al., 2002; Yick et al., 2008; Rawat et al., 2014) have studied the design, characteristics, physical constraints of SNs, applications and communication protocols in all layers of the protocol stack. While other surveys are more specific to certain aspects, such as clustering (Abbasi and Younis, 2007; Liu, 2012), the Mac layer (Demirkol et al., 2006; Yadav et al., 2009), energy-based routing (Anastasi et al., 2009; Pantazis et al., 2013; Ogundile and Alfa, 2017), multipath routing (Radi et al., 2012; Tarique et al., 2009), Wireless Multimedia Sensor Networks (WMSN) (Darabi et al., 2008; Ehsan and Hamdaoui, 2012), Mobile Agent in WSNs (Chen and Gonzalez, 2007) and routing protocols (Al-Karaki and Kamal, 2004; Akkaya and Younis, 2005; Goyal and Tripathy, 2012), as our current research.

In 2002, the authors of Akyildiz et al. (2002) presented one of the first surveys into potential applications and factors that influence design issues in sensor networks. They discuss the physical constraints of the SNs and proposed protocols for all network layers. The authors summarize their survey with potential research directions for WSNs. Nevertheless, given the date of the survey, the article does not take into account the recent routing protocols that appeared after the paper.

In 2004, the authors of Al-Karaki and Kamal (2004) presented a review of the literature on WSNs routing protocols. The article presents about 25 routing protocols classified into two main categories, namely network structure and protocol operation. The first category contains three classes, namely flat, hierarchical and location-based. The second routing class has four protocol families, based on multipath, query, negotiation, and QoS. In addition, the authors analyzed the difficulties encountered in designing a routing protocol for WSNs. Furthermore, they presented a detailed comparison of these routing algorithms, indicating the benefits and drawbacks of each protocol, and attempted to identify the design trade-offs between energy and overhead savings.

Akkaya and Younis (2005) examined about 22 routing algorithms for sensor networks and classified them into three categories: data-centric, hierarchical, and location-based. Their survey work involves routing in WSNs, where other QoS requirements are taken into account.

Yick et al. (2008) established a top-down approach to several applications and insights into various aspects of wireless sensor networks. It describes their challenges and classifies them into three categories: (i) underlying platform and operating system, (ii) network services, provisioning and deployment, and (iii) protocol stack. The authors also examined five categories of wireless sensor networks, namely terrestrial, underground, submarine, multimedia, and mobile networks. Furthermore, they presented the research development of the categories mentioned in the literature.

Anastasi et al. (2009) focused on the power consumption of a typical SN. First, the authors decomposed the energy consumption of the components of a conventional SN and divide it into four parts: a sensing subsystem, a local computation subsystem comprising a microcontroller and a memory, a transmission radio subsystem and a power supply unit. They provide the basics of energy conservation and discuss architecture-based solutions, power outages and mobility-based to minimize power consumption in WSNs. In addition, the authors introduced a systematic and in-depth taxonomy through which they categorized energy-saving systems based on duty cycling, data

management, and mobility. They also stressed the importance of conserving the energy consumed by the SN component, as in the data transmission phase, and that the radio energy consumption is greater than that due to sampling or processing.

Biradar et al. (2009) presented the design issues of WSNs as well as a classification of routing algorithms based on their characteristics and the mechanisms used to increase the longevity of the network. However, they do not provide enough details about the algorithms discussed, nor any direct comparison between them. The authors of Yadav et al. (2009) presented the design challenges of energy-efficient MAC algorithms for wireless sensor networks. In fact, they describe about 12 network access protocols for WSNs, highlighting their strengths and weaknesses. However, they also do not discuss detailed comparison of the described algorithms. In 2012, a classification of routing approaches for WMSNs and some energy-aware routing techniques are presented in Ehsan and Hamdaoui (2012), where the performance issue of each technique is highlighted. The authors describe the design challenges of this routing class, followed by the limitations of existing methods designed for non-multimedia content.

In 2013, an extensive survey of energy-efficient routing approaches for wireless sensor networks is presented by Pantazis et al. (2013). They classified more than 57 routing algorithms into four schemas. Various energy-efficient and energy-balanced routing algorithms have been examined and have been put forward to study their performance and thus compare the different energy-aware routing approaches for WSNs. Rawat et al. (2014) provided an overview of WSNs, indicating their scope and challenges. The authors reviewed major research, test beds, standards, platforms, as well as WSN techniques. In addition, they described the current events in the WSN research, which examine the possible interaction between WSNs and other emerging technologies such as mobile robots, cloud sensors, IoT and so on. The authors explained how this synergy would help WSNs achieve the right potential. Their survey is concluded with open research orientations.

3. WSNs versus Adhoc networks

Although several routing algorithms have been proposed in the context of traditional adhoc networks, they do not prove to be well suited to WSNs. Indeed, these wireless networks, such as MANETs, VANETS, Wireless Mesh Networks (WMNs), or WSNs are characterized by their adhoc nature and share certain characteristics such as limited resources. Nevertheless, wireless sensor networks may be more constrained than other adhoc networks for the following reasons:

- A high SN deployment density, because in a WSN, the number of SNs can be many times greater than the number of nodes in other adhoc networks. Therefore, the routing protocols must support long distance transmissions, regardless of the network extent.
- Absence of global identification in sensor networks due to the large number of sensors and therefore the large amount of overhead incurred.
- WSNs are primarily used to collect information, which implies that data flows from multiple sources converge to a central node, while other adhoc networks are intended for distributed processing rather than data collection.
- SNs require careful management of resources due to their harsh constraints in terms of energy, computing capacity, and memory.
- The design requirements for a wireless sensor network are application dependent.
- The topology of a WSN rarely changes because the nodes are mostly stationary after deployment.
- In WSNs, the high probability of unwanted redundancy in the collected data must be exploited by routing protocols for better utilization of energy and bandwidth.

4. Routing in wireless sensor networks

4.1. Data-centric approaches

It is difficult to assign a global identifier to each SN of a WSN because of the large number of SNs that may exist. This lack of global identification has prompted reflection on a new concept of Data-Centric (DC) routing, dissimilar from traditional address-based routing. This concept is based on attribute-value pair naming of all data generated by SNs. In data-centric routing, the BS sends queries to certain regions of the network and waits for sensor responses in those picked regions. Because data is requested through queries, depending on certain attributes, attribute addressing is required to specify data properties. Unlike traditional end-to-end (e2e) routing, the DC routing approach eliminates redundancy, minimizes transmission, saves energy, and increases network longevity.

Early DC routing searches, such as SPIN (Heinzelman et al., 1999) and directed diffusion (Intanagonwiwat et al., 2000), have saved energy by negotiating data between nodes to eliminate redundancy. These two algorithms motivated the appearance of several other algorithms based on a similar idea (Braginsky and Estrin 2002; Yao and Gehrke, 2002; Sadagopan et al., 2003).

4.2. Classification of routing algorithms in WSNs

The classification of the different routing approaches that exist in the context of WSNs is described by Fig. 1.

4.3. Network structure

The network structure describes the characteristics of a network in relation to the roles

played by its nodes. In other words, all the nodes are equal, or some are privileged.

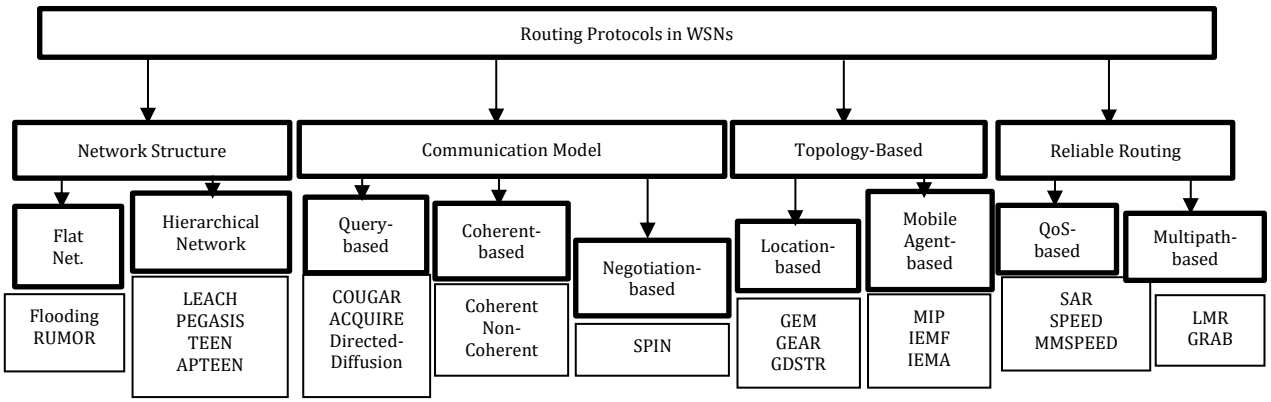

Fig. 1: Classification of routing algorithms in WSNs

4.3.1. Flat-based routing

In the absence of hierarchy, all network nodes are considered equal and have identical roles or functionality. The flat network architecture has several benefits, including a minimal additional overhead for the management of the communication infrastructure between the SNs.

Flooding

It is a simple reactive mechanism that can be used for routing in sensor networks (Lim and Kim, 2001); its maintenance is not pricey and its methods are not complex. In case of flooding, the incoming packets copies are broadcast on each link except the one through which the packets arrived. Although this method clogs the network with a huge amount of unnecessary traffic, it remains an extremely robust routing mechanism, as long as there is a possible route from the source to the destination. As for the delivery of the packets, it is guaranteed as soon as possible.

Nevertheless, flooding has several disadvantages, namely:

- Implosion: Duplicate messages are broadcast on the same SN in this state.
- Overlay: If two SNs share the same area of observation, they can both experience the same stimuli at the same time. Consequently, neighboring SNs receive duplicate messages.
- Blindness of resources: The algorithm does not take into account all available energy resources. Indeed, an effective energy algorithm must consider the amount of energy available at all times.

Furthermore, flooding consumes a lot of energy, because for each packet, all the nodes of the broadcast domain will receive it and will transmit it to their neighbors, which leads to a very short lifetime of the network.

Rumor routing (RR)

It involves a logical trade-off between flood event notifications and flood queries (Braginsky and Estrin, 2002). It is primarily intended for networks where Geographic Routing (GR) criteria are not applicable. As the Fig. 2 illustrates, the RR protocol creates paths leading to each event in the network, as opposed to event flooding that creates a network-wide gradient field. Thus, following the generation of a query, it can cross the network randomly until it finds a node on the path to the event. Once the path to the event is found, it can be directly routed to the event. Otherwise, if the path to the event cannot be discovered, the application may attempt to resubmit the request or flood it in the worst case. The Rumor mechanism is useful for providing queries to events in large networks. Moreover, this protocol is designed to be adaptable to the needs of the application, for example to support distribution rates and successful repair paths. In addition, it is able to elegantly deal with node failures by linearly degrading its throughput based on the number of failed nodes.

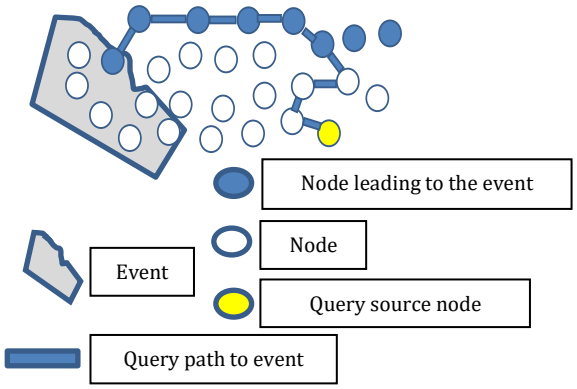

Fig. 2: Query source looks for a path to the event. Once it finds a node on the path, it is directly routed to the event (redrawn from Braginsky and Estrin (2002))

4.3.2. Hierarchical-based routing

Also known as cluster routing methods, which are designed to conserve energy by organizing nodes into clusters, so that cluster heads (CHs) aggregate and reduce transmitted data to save power; there is a hierarchy of nodes of low and high energy. The lower-level nodes transmit data to higher-level nodes, resulting in a balance of the network's energy structure. As such, a node with high residual energy commits to acts as a CH for data processing and

transmission, while low-energy nodes can be used to perform near-target sensing. The CH provides coordination of intra-cluster activities as well as inter-cluster information delivery, which contributes to the network's overall scalability, lifetime, and energy-efficient routing in sensor networks. Cluster routing is an effective way to optimize power consumption in a cluster, aggregate and merge data to reduce the number of messages forwarded to the base station. Some problems can occur with such a hierarchical network structure, as the nodes around the BS will exhaust their batteries faster than others. In addition, the dark parts of the network are a problem where some parts of the network become inaccessible. Indeed, if the only node that connects one region of the network to the rest fails, this region will be isolated.

Cluster routing is primarily a dual-layer routing, where one layer is used to select CHs while the other layer is for routing. This generates two routing families: a dynamic hierarchy schema where clusters are dynamically formed and a static hierarchy schema where clusters are formed statistically; remain unchanged throughout the lifetime of the network.

Low-energy adaptive clustering hierarchy (LEACH)

It is a distributed cluster routing algorithm for micro-wireless sensor networks (Heinzelman et al., 2000). LEACH divides the WSN into multiple clusters of sensors, on the one hand to reduce the amount of data transferred to the BS, and on the other hand to make the routing and dissemination of data more efficient. In the configuration phase, some of the nodes declare themselves as CHs, which gather data from neighboring sensors compressing them and transmitting the aggregated data to the base station. The CH role swivels between the SNs in the same cluster to evenly distribute the power consumption among them. Each SN determines whether it will become a CH in the current rotation, if it becomes one for a period, it cannot be one again for N iterations, where N is the desired percentage of CHs. Subsequently, the probability that a node becomes a CH at each rotation depends on the amount of its remaining energy. This CHs rotation results in balanced power consumption at all nodes, extending the longevity of the WSN. In the stable state phase, each node joins the nearest CH. Then, the CH plans for each node of its cluster when it will transmit its data. Nevertheless, the algorithm uses a single-hop routing in which each SN can transmit directly to the CH and the sink. As a result, it is not appropriate for WSNs deployed in large areas. In addition, dynamic clustering can result in additional overhead, which can decrease the gain in power consumption.

Power-Efficient Gathering in Sensor Information Systems (PEGASIS)

This protocol is an enhanced version of LEACH (Lindsey and Raghavendra, 2002). Instead of forming multiple clusters, PEGASIS forms chains from SNs using a greedy algorithm. It is assumed that all SNs have a global view of the network. Thus, the construction of the chain will begin from the furthest SN to the nearest SN. If a SN dies, the chain is rebuilt in the same way to bypass the missing SN. The BS can calculate this chain and broadcast it to all SNs. Thus, each SN communicates only with its close neighbor to transmit and receive data. In addition, only one SN is selected in this chain to send to the base station, thus reducing the amount of energy consumed. Thereby, the collected data moves from one SN to the other, aggregated and then sent to the base station.

In general, the PEGASIS protocol is more efficient than LEACH (Pantazis et al., 2013). Indeed, the transmission distance for most SNs is reduced. However, the PEGASIS protocol suffers from a major problem, namely redundant data transmission. The main cause of this problem is the lack of considering the location of the BS with respect to the remaining energy of the SNs, when one of them is chosen as the head node.

Threshold sensitive Energy Efficient sensor Network protocol (TEEN)

It is a hierarchical algorithm designed to be sensitive to sudden changes in sensed attributes such as motion (Manjeshwar and Agrawal, 2001). Reactivity is of great importance for real-time applications, where the WSN operates in a reactive mode.

For the TEEN protocol, the CH broadcasts two threshold values to its cluster nodes: the hard threshold and the soft threshold. The hard threshold is an absolute value for the sensed attribute, beyond which the SN must activate its issuer and report to its CH. The soft threshold is a small modification in the value of the sensed attribute, which activates the node issuer to transmit. Nodes are constantly sensing their environment. The first time a parameter of the set of attributes reaches its hard threshold value, the node activates its issuer and sends the sensed data.

Adaptive Threshold sensitive Energy Efficient sensor Network (APTEEN)

This is an enhancement of the TEEN protocol, which aims to collect periodic data and respond to events with time constraints (Manjeshwar and Agrawal, 2002). Note that both TEEN and APTEEN protocols share the same architecture. As soon as the BS forms the clusters, the CHs broadcast the attributes, the threshold values, and the transmission schedule to all the nodes. Then, the CHs aggregate the data to save power. APTEEN supports different types of queries: history, to parse past values of data; once, to take an instant view of the network; and persistent to supervise an event for a while. The main advantage of APTEEN over TEEN is that SNs consume less energy. However, its major drawbacks are its complexity and long delays.

4.3.3. Comparison of routing schemas based on the network structure

The results of the simulation in Lim and Kim (2001) show that Flooding has a delivery rate of up to 100 %. The Rumor protocol successfully provides 98.1 % of all queries and can achieve significant savings on flooding event (Braginsky and Estrin, 2002).

The LEACH protocol reduces the total number of transmissions compared to direct communication. In addition, the first node of the network lacks power at 230 seconds and all SNs die at 700 seconds.

APTEEN's performance lies between those of TEEN and LEACH in terms of power consumption and network longevity (Manjeshwar and Agrawal, 2002). TEEN only transmits time-constrained data while continuing to sense the environment. On the other hand, APTEEN has a periodic data transmission to overcome the disadvantages of TEEN.

In the following, Table 1 compares the protocols belonging to the network structure class, which may be useful for the reader. In addition, the advantages and disadvantages of each protocol of this routing scheme are briefly summarized.

Table 1: Comparison of routing protocols based on network structure

Protocols	Class.	Scalability	Mobility	Overhead	Power-Usage	Advantages	Disadvantages
Flooding	Flat	Limited	Low	High	High	Simple and robust mechanism.	Implosion.
Rumor	Flat	Good	Low	Low	Low	Manage node failures, which degrade linearly its throughput based on the number of failed nodes.	Can send duplicate messages to the same node.
LEACH	Hierar	Good	Fixed BS	High	High	Low energy, ad-hoc, distributed protocol.	Does not apply to networks deployed in large areas and dynamic clustering incurs additional overhead.
TEEN	Hierar	Good	Fixed BS	High	High	Performs well under conditions such as sudden changes in sensed attributes.	A lot of energy consumption and overhead in case of large WSN.
APTEEN	Hierar	Good	Fixed BS	High	High	Low energy consumption.	Long delay.
PEGASIS	Hierar	Good	Fixed BS	Low	Max	The transmission distance for most SNs is reduced.	The BS location does not take into account the energy of the nodes when one of them is selected as the head node. Redundant data transmission.

4.4. Communication model

The communication model adapted in a routing algorithm is associated with the way the protocol acts to route the packets. Protocols in this family can provide a higher data volume for a given amount of energy. Similarly, in terms of dissemination rate and use of energy, algorithms in this category can achieve quasi-theoretical performance in P2P and broadcast networks. The problem with this kind of algorithms is that they do not guarantee the delivery of the data.

In this class, the main characteristic of such algorithms is the way of making a routing decision, without relying primarily on the structure of the network. Thereby, a negotiation-based technique, where the nodes negotiate together before the data is transmitted, is considered to convey the information between two ends. The best-known protocols belonging to this class are presented below.

4.4.1. Negotiation-based routing

Sensor Protocols for Information via Negotiation (SPIN) (Heinzelman et al., 1999; Kulik et al., 2002) are some of the first efforts to implement a data-centric routing mechanism. The family of SPIN algorithms is mainly founded on two principles:

- In order to perform efficiently and save power, the SNs need to exchange the data they already have and the data they still have to receive, instead of sending all the data.
- The nodes of a WSN need to closely supervise and adapt quickly to changes in their own energy resources in order to extend the lifetime of the network.

The basic principle of SPIN protocols is to assign a high-level name to their data using descriptors or metadata, in order to fully describe the data collected and to conduct metadata negotiations prior to data transmission (Ben-Othman and Yahya, 2010). Nodes use metadata-based negotiations to reduce redundant data sent over the network because neighboring nodes have similar data. It is therefore necessary to share only the data that other nodes do not have. The semantics of the metadata format is not defined in SPIN and depends on the application. Practically, if a node has data, it starts by announcing, by sending an ad packet, that it has detected an event or is receiving data. On the other hand, if another node has received the ad packet and is interested in this data, it will forward a request packet and upon its receipt, the node will transmit the actual data in the data packet. Thus, SPIN is considered a three-step algorithm because the communication between nodes is based on three kinds of messages: ADV is used to announce new data, REQ to request data and DATA is the message

itself. The SPIN protocol is scalable in the sense that each node needs to know only its immediate neighbors, therefore any modification of the topology would be local. Otherwise, the main disadvantage of this protocol is that it does not guarantee the delivery of data. In fact, take the case where an interested node is very far from the advertisement, so this interested node will not receive any data if the nodes between these two nodes are not interested by this data.

4.4.2. Query-based routing

In such routing protocols, data exchange is done through queries and replies. The receiving nodes send a request message over the entire network and only those nodes having the required data reply. For example, the destination node propagates a request for the sensed data from another node on the network; the node holding these data replies with the data that matches the query (Sadagopan et al., 2005). Usually, these queries are represented using a high-level query language or a natural language.

Directed Diffusion (DD)

It uses caching and data processing techniques to reduce energy consumption; the aggregation of data (for example, deleting duplicates) is done en route. The DD algorithm consists of the following key elements (Intanagonwiwat et al., 2000):

- Naming: The sensing task is described using a listing of attribute-value pairs, where the attributes can be the data type, the transmission interval, the duration, and so on.
- Interests and Gradients: The description of the task indicates an interest for the data corresponding to the attributes. This data is sent in response to the interest. As the interest spreads throughout the WSN, the gradients from the source to the BS are configured, for example, according to the requirements of interest. Each node of the network maintains a cache of interest, where each element is particularly interesting. When the source has interesting data, it transmits the data along the path of the gradient of interest.
- Data Propagation: When a SN detects a target, it looks in its cache of interest for a corresponding entry. Thereby, if it finds one, it calculates the highest rate of events requested among all its outgoing gradients.
- Reinforcement: Events begin to flow to the initiators of interests on several paths. The WSN reinforces one or more of these paths.

Note that DD cannot be used for complex queries because of energetic reasons. In fact, DD evenly uses a flood-based query technique for continuous and aggregated queries.

COUGAR

It sees the WSN as a large distributed database (Yao and Gehrke, 2002). The principle of this protocol is to use declarative queries for the sensed data generated by the sensors, to summarize the processing of the queries from the functions of the network layer. This protocol uses data aggregation in the WSN to save more energy. It provides independent network-layer interfaces for the data query, where an additional query layer, located in the upper layers, supports abstraction. It integrates the architecture of the sensor database, where a leader is selected from the sensor nodes to aggregate and transfer data to the BS.

The advantage of this approach is that it renders a network computing capability providing energy efficiency in such situations where huge amounts of data are generated. However, COUGAR has some disadvantages, namely, adding a query layer on each SN can add additional overhead, which implies costs in terms of power consumption and storage. On the other hand, the complexity of the synchronization during network data processing and the dynamic maintenance of leading nodes to avoid failures.

Active query forwarding in sensor networks (ACQUIRE)

It has been proposed in Sadagopan et al. (2003) as a query technique for WSNs. Based on the same principle as COUGAR, this protocol sees the network as a distributed database, where complex queries can be subdivided into multiple sub-queries. The base station transmits a request that will be retransmitted by each node receiving the request. Meanwhile, each SN attempts to partially respond to the request using its cache, and then forwards it to another SN. If the cached information is not up-to-date, the nodes collect information from their neighbors. Thus, ACQUIRE can handle complex queries by allowing many nodes to participate in the responses.

The ACQUIRE protocol is well suited to unique and complex response requests that can be executed by many nodes. To select the next node for the transmission of the query, the algorithm selects it randomly or according to the satisfaction of the maximum potential query.

4.4.3. Coherent and non-coherent data processing routing

In sensor networks, the routing algorithm that initiates data processing at the SN level is proposed in Sohrabi et al. (2000). This algorithm has two variants:

- Coherent Data Processing Routing: This variant is a power saving technique where only the minimum processing is performed by the SN. The Timestamp, the duplicate deletion is the task performed in the minimal processing. After that, the data is transmitted to the aggregators.
- Non-Coherent Data Processing Routing: In this variant (Jolly and Latifi, 2006), the SNs process the raw data locally before sending them to the other SNs for additional processing by the so-called

aggregators. This routing mechanism comprises three data processing steps:

(i) the detection of targets, consists of the detection of events, the collection and pre-processing of their information,
(ii) the declaration of membership, the SN chooses to participate to a collaborative function and announces this intention to all the neighbors and
(iii) the election of the central node, which is selected to perform more accurate information processing.

4.4.4. Comparison of routing schemas of the communication model

The DD and COUGAR algorithms select the least power consuming path, while the ACQUIRE protocol selects the shortest path to minimize power consumption. Moreover, Directed Diffusion is more scalable than COUGAR and ACQUIRE.

In the following, Table 2 provides a comparison of routing protocols based on the communication model class in terms of certain metrics, which may be useful for the reader. In addition, the advantages and disadvantages of each protocol of this routing scheme are briefly summarized.

Table 2: Comparison of routing protocols based on communication model

Protocols	Class.	Scalabili.	Mobility	Overhead	Power-Usage	Advantages	Disadvantages
SPIN	Negotia.	Ltd.	No	Low	Ltd.	Reduce redundant data.	Does not guarantee delivery of data.
Directed Diffusion	Query-based	Ltd.	Ltd.	Low	Ltd.	Extends the network lifetime.	Cannot be used for streaming data or event-driven applications.
COUGAR	Flat	Ltd.	No	High	Ltd.	Provides energy efficiency when a large amount of data is generated.	Overhead, complexity of synchronization in calculating network data
ACQUIRE	Query-based	Ltd.	Ltd.	Low	Low	Ideal for one-time and complex response requests provided by multiple nodes.	Flooding.

4.5. Topology-based routing

The basic idea behind topology-based routing algorithms is that each network node retains the topology information on which the protocol is based. The different routing protocols adapting this approach can be further classified as follows.

4.5.1. Location-based routing

In this class of routing algorithms, the SNs are addressed through their locations, which can be the signal strength if the nodes are close to one another. In the case of remote nodes, the relative coordinates of the SNs can be extracted by means of exchange between neighboring nodes. This kind of protocol recognizes the effect of physical distances and the geographic distribution of SNs as important as the performance of the WSN.

The location-based approach is founded on two main assumptions:

- Each node knows the positions of its network neighborhood.
- The source is supposed to know the destination position.

The localized query broadcasting mechanism in geo-sensitive WSNs uses the existing query routing tree and does not imply additional communication channels. This type of algorithm requires the periodic exchange of HELLO messages between the nodes to allow neighbors to learn their positions. The location-based routing mechanism is interesting because it works without using a routing table.

The main drawbacks of location-based protocols are:

- Efficiency counts on the balance between geographical distribution and the appearance of traffic.
- Any performance dependence on the traffic load that counteracts neglect of distance can occur in the event of an overload.
- Their scalability is limited in the case of mobile nodes.

Geographic and energy aware routing (GEAR)

This protocol does not use greedy algorithms, like other GR approaches, to route packets to the desired destination (Yu et al., 2001). Instead, it uses energy-sensitive and geo-sensitive neighbor selection heuristics to route queries to the target region in a WSN. The main features of GEAR are:

- When a neighbor is near the destination, GEAR selects the best next hop node from all the closest neighbors to the destination.
- A hole exists when all the neighbors are far away. GEAR then chooses the best next hop node that reduces the cost for that neighbor.

The main benefit of this protocol is that each SN is aware of its own location and its residual energy, as well as localizations of its neighbors and their residual energy, thanks to a simple Hello protocol. In addition, it tries to balance the power consumption between the nodes and thus increase the longevity of the network.

Graph embedding for routing (GEM)

It is a routing algorithm that attempts to tag SNs in a unique and distributed way (Newsome and Song, 2003). Messages are routed by knowing only the tags of their immediate neighbors. In this protocol, virtual coordinates are used rather than actual coordinates.

The main advantage of GEM is that it efficiently carries messages over the WSN, although each SN needs to know only the tags of its neighbors. In addition, it is robust in the case of dynamic networks, shows good performance against voids and obstacles, and easily adapts to the size and density of the network. While its weakness lies in the overload of the SNs located at low levels of the routing tree.

Greedy distributed spanning tree routing (GDSTR)

It transfers packets using a simple greedy forwarding as much as possible. This protocol can find the optimal routes while generating little control traffic (Leong et al., 2006). The main contribution of this approach is the proposal of a new type of spanning tree, called a hull tree that looks like a spanning tree where a convex hull is associated with each node. This convex hull shelters the locations of all its descending nodes in the tree. Hull trees are constructed through the aggregation of convex hull information, which can be used to avoid unproductive paths; rather, they are able to cross a reduced sub-tree formed only of nodes with convex hulls, which include the destination node.

The GDSTR protocol has several advantages among which it is simple, easy to understand and to implement. Furthermore, it offers a shorter path and a shorter hop length than other GR protocols. Although it requires only one shaft for accuracy, it uses robustness to give it more transfer choices.

The first disadvantage of GDSTR compared to other GR approaches is its problem with local dead ends, where greedy transmission fails. The most of existing GR protocols plan the node connectivity graph, and then use the right-hand rule to bypass the resulting faces to handle dead ends. The GDSTR protocol manages this situation differently, it routes to a spanning tree until it reaches a node where greedy transfer can resume.

4.5.2. Mobile agent-based routing

In the majority of cases, the specific nature of the WSN application requires SNs to have multiple functionalities. As a result, it is not practical for the SNs to load all the necessary applications into the main memory and execute them, because of limited memory constraints.

The development of Mobile Agent (MA) systems is a very dynamic research focus for wireless sensor networks (Chen and Gonzalez, 2007). MA systems consist mainly of an autonomous and intelligent computer program called a MA, which migrates between the SNs of a WSN to perform a task, depending on the environmental conditions. MA systems use migration codes to facilitate the redeployment of flexible applications, local processing, and collaborative processing of signals and information. This can provide the network with new features such as additional flexibility, as opposed to traditional client-server communications in WSNs.

Thus, a MA-based routing protocol is used in sensor networks to route data from the sensed area, which is an area of interest, to the destination. In Chen and Gonzalez (2007), the design problem of a MA in a WSN is presented, and decomposed into four components: architecture, itinerary planning, middleware system design, and agent cooperation.

In most cases, the application of MA systems in wireless sensor networks can result in reduced bandwidth consumption and network flexibility. Nevertheless, finding the optimal route is NP-hard (Wu et al., 2004) and a lot of effort is underway.

Multi-agent itinerary planning (MIP)

It was introduced in Chen et al. (2009). In most cases, Single Agent-Based Itinerary Planning (SIP) algorithms are developed and executed on MA systems. Nevertheless, the use of large-scale SIP algorithms can result in high delays and load imbalance. In such cases, the use of a MIP algorithm may be justified.

The main idea of the algorithm suggested in Chen et al. (2009) is to distribute the impact factor of each source on the other sources. Consider the example of a network with K source nodes; each source will receive (K-1) impact factors from other sources plus one of itself. Then, the cumulative impact factor is calculated and the location of the source with the largest cumulative impact factor is chosen.

Itinerary energy minimum for first-source-selection (IEMF) and itinerary energy minimum algorithm (IEMA)

IEMF has been proposed in Chen et al. (2011), as well as its iterative version, the IEMA algorithm. In addition to the choice of the first source node, the IEMA protocol tries to optimize to a certain extent the remaining route. On the other hand, the IEMF offers high-energy efficiency with a low delay. However, by limiting the use to a single agent to perform all tasks, the protocol is not scalable with a high number of sources to visit.

4.5.3. Comparison of topology-based routing schemas

The results of the simulation in Leong et al. (2006) show that the GDSTR protocol routes packets over shorter paths than other protocols, and is therefore likely to deliver packets faster and with less radio resources consumption.

The GEAR protocol performs better than the Flooding protocol as indicated in Yu et al. (2001). Indeed, it realizes energy balance by adopting an alternative path; thus, it increases from 25% to 45% the length of the path on all delivered packets.

For a small number of sources, simulation results in Chen and Gonzalez (2007) show that MIP's power consumption is higher than that of SIP protocols. Nevertheless, this protocol is designed to be used with a large number of sources. Thereby, based on the results of 40 sources, the power consumption of the MIP protocol is much better than that of the SIP protocols.

In the following, Table 3 gives a comparison of the topology-based routing protocols. In addition, the advantages and disadvantages of each protocol of this routing scheme are briefly summarized.

Table 3: Comparison of topology-based routing protocols

Protocols	Class.	Scalabili.	Mobility	Overhead	Power-Usage	Advantages	Disadvantages
GDSTR	Location	Ltd.	No	High	Low	Finds the optimal routes while generating little control traffic.	Overhead costs.
GEM	Location	Good	Ltd.	Low	High	Messages are efficiently routed across the network, while each node needs to know only its neighbors tags.	Overloads nodes located at low levels of the tree.
GEAR	Location	Ltd.	Ltd.	MOD	Ltd.	Tries to balance the power consumption and thus increases the network lifetime.	Periodic table exchange.
MIP	Mobile-Agent based	Ltd.	Good	Low	Low	Consume less power in case of large number of network nodes.	High delay.
IEMF/IEMA	Mobile-Agent based	Ltd.	Good		High	Aims to optimize to a certain extent the remaining route.	Non-scalable with a large number of source nodes to visit.

4.6. Reliable routing

Algorithms in this class are more resistant to routing failures, either by performing load-balancing routes, or by satisfying quality of service metrics, such as delay, and throughput. However, network nodes may suffer from overloading the routing tables on each SN. This class of algorithms can be further subdivided into two subclasses, described below.

4.6.1. Multipath-based routing

This type of routing protocol generates many routing paths to the sink node instead of one, as a fault-tolerance mechanism. Only one path is chosen from all constructed paths, usually based on the remaining energy. Multipath routing has the benefit of performing load balancing, in addition to resisting routing failures (Tarique et al., 2009). Therefore, there is a trade-off between the reliability of the network and the traffic load associated with maintaining alternative paths. Performance evaluations of multipath routing protocols can show that they have lower routing overhead, lower e2e delay, and easier congestion than single-path routing protocols. There are many routing protocols for WSNs that belong to this schema, the most important of which are described below.

Label-based multipath routing (LMR)

This protocol broadcasts a control message across the WSN in search of an alternative path (Hou et al., 2004). Meanwhile, labels are assigned to the paths that the message traverses; they are used for segmented backup path search if a disjoint path is not feasible. This protocol is designed to use only localized information to discover disjoint alternative paths or multiple segments to protect the working path, which can be achieved through flooding.

Once the nodes of the work path have strengthened one of their links, they broadcast a label message to their neighbors. The reinforcement and label messages take an integer, called a label, which is incremented at each work node, which must store this value under its own label. Label messages are transmitted to the source along all the paths traversed by the exploratory messages. A node receiving two or more label messages will only transfer the one with the smallest label value. The idea is to ensure that the label message of the node closest to the sink is as far away as possible, so that disjoint paths can be discovered.

Label information can reduce the routing overhead and the configuration time of the backup path. However, to find alternative paths, LMR involves overhead, a flooded label message, a label reinforcement message, and an exploratory backup message.

GRAdient broadcast (GRAB)

It is specifically designed for robust data delivery to handle unreliable nodes and fallible wireless links (Ye et al., 2005). The GRAB protocol manages a cost field through the propagation of advertising packets (ADVs). As soon as a node receives an ADV packet containing the cost of the sender, it updates its cost by adding the cost of its link with the sender. It then compares the resulting cost with that previously recorded and the lowest cost is adopted. If it gets a lower cost than the old one, it broadcasts an ADV packet containing this new cost. The protocol controls the width of the band by the amount of credit carried in each data packet, which allows the sender to adjust the robustness of the data delivery.

The advantage of this protocol is to rely on the collective efforts of several nodes for robust data delivery, without relying on individual nodes. Whereas, sending redundant data causes additional overhead.

4.6.2. QoS-based routing

In this routing family, the network must balance power consumption and QoS (Akkaya and Younis, 2005). In particular, whenever a sink requests data from SNs in the WSN, the transmission must satisfy a QoS level of metrics such as delay and throughput, when supplying data to the base station. QoS-based routing is typically accomplished by reserving resources in a connected communication that satisfies the QoS requirements for each connection. In the following, the most important protocols of this class are discussed.

Sequential assignment routing (SAR)

It is one of the first routing mechanisms for wireless sensor networks that introduced the notion of quality of service into routing decisions (Sohrabi et al., 2000). This algorithm builds trees based on single-hop neighbors from the sink taking into account the routing decision factors: the quality of service metrics, the energy resources on each path, and the priority level of each packet. Once these trees are built, several paths from the sink to the sensors are formed; one of them is chosen based on energy resources and QoS on the path. To avoid a single path failure, a multipath policy is used as well as a localized path restoration procedure. Recovery following a failure is achieved by applying the consistency of the routing table between the nodes upstream and downstream of each path.

SPEED

It is a quality of service based routing algorithm for sensor networks, which provides e2e soft real-time guarantees, helping to avoid congestion as it occurs (He et al., 2003). It consists of the following components (Fig. 3).

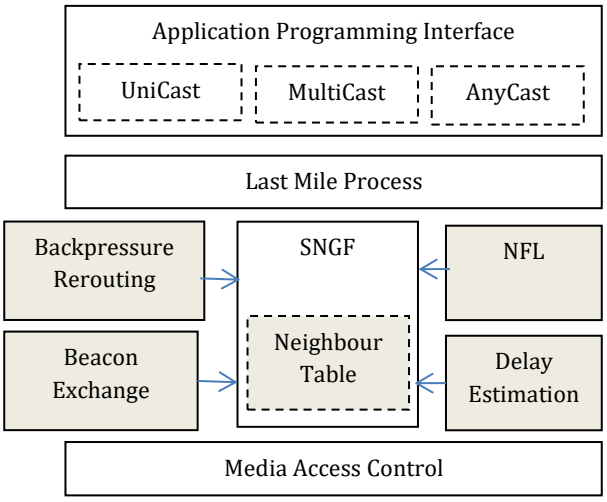

Fig. 3: The architecture of SPEED

As illustrated in Fig. 3, SPEED's routing module is Stateless Non-Deterministic Geographic Forwarding (SNGF), which is responsible for finding the next hop node that can support the desired delivery speed on the WSNs. The Neighbor-hood Feedback Loop (NFL) and Backpressure Rerouting are two modules that can reduce or divert traffic in case of congestion. The Beacon Exchange module gathers information about the nodes and their position so that SNGF can perform GR. The Delay Estimation module is used to detect congestion, by estimating the delay at each node through the calculation of the elapsed time between the trans-mission of a data packet and the reception of the corresponding acknowledgment. The Last-Mile process is intended to support three types of real-time communication: unicast, multicast and anycast. The NFL module is responsible for providing the relay ratio, which is calculated by examining the missing ratios of the node's neighbors (the nodes that did not provide the desired speed) and is sent to the SNGF. Finally, the Backpressure-Rerouting module is used to avoid voids, when a node cannot find the next hop, and eliminate congestion by returning messages to sources to pursue new paths.

SPEED is more efficient than DSR and AODV, in terms of e2e delay and loss rates. In addition, the total transmission energy is less because of the simplicity of the routing protocol that is to say that the overhead of the control packet is less. Such load balancing is performed by the SNGF packet dispersion technique in a large relay area. SPEED responds to transient congestion in the most stable way. However, in case of heavy congestion, its energy consumption is slightly higher, mainly because it provides more packets at destination than other protocols. Nevertheless, SPEED does not take into account the power consumption in its routing algorithm.

Multi-path and multi-SPEED (MMSPEED)

It is a routing protocol developed for a probabilistic guarantee of quality of service in wireless sensor networks. While most QoS-based routing algorithms focus on timeliness or reliability, MMSPEED supports both (Felemban et al., 2006).

MMSPEED provides an e2e QoS with a local decision on each intermediate node without recovery and maintenance of the e2e path. Localized estimation errors are corrected using dynamic compensation.

The distinguishing feature of MMSPEED is its ability to provide e2e requirements in a localized manner, which is desirable for the scalability and adaptability of large scale WSNs. Moreover, it can provide differentiated quality of service in the areas of reliability and speed. On the other hand, it consumes more power due to computation of packet routing, longer frame overhead, and long redundant paths (Darabi et al., 2008). This additional power consumption significantly reduces network lifetime.

4.6.3. Comparison of reliable routing schemas

SAR retains several paths between the nodes and the BS (Sohrabi et al., 2000), providing fault-tolerance and easy recovery. On another side, the algorithm suffers from the need to maintain the

tables at each SN, which may be heavy especially when the number of nodes is huge.

The e2e delay for the SPEED varies from 10ms to 140ms (He et al., 2003). It also manages to deliver 95% of its packets to destination. Besides, the MMSPEED can provide a differentiation of service in the area of reliability and the two flow groups of the simulation can satisfy their own reliability requirements up to 20 flows (Felemban et al., 2006). In addition, MMSPEED can result in higher power consumption due to more calculations that are complex and a longer frame.

QoS-based routing protocols can provide energy-efficient routing with guaranteed QoS, as long as the nodes are not mobile.

The LMR protocol is effective with local multicast and reduces the average number of messages (Hou et al., 2004). For a network of 400 nodes, in case of unicast, the maximum number of overhead packets is 500, whereas in case of multicast; the maximum number of overhead packets is 4500.

In the following, Table 4 provides a comparison of the reliable routing protocols. In addition, the advantages and disadvantages of each protocol of this routing scheme are briefly summarized.

Table 3: Comparison of reliable routing protocols

Protocols	Class.	Scalabili.	Mobility	Overhead	Power-Usage	Advantages	Disadvantages
SAR	QoS-based	Ltd.	No	High	Low	Low energy consumption. Maintains several paths to the destination.	Maintenance of tables at each SN, especially when the number of nodes is huge.
SPEED	QoS-based	Ltd.	No	Less	Low	Good performance in terms of e2e delay and miss ratio.	Does not perform well in case of heavy congestion.
MMSPEED	QoS-based	Ltd.	No			Provide differentiated QoS in the area of reliability and significantly improve the effective capacity of a WSN.	In a high-load network, the e2e delay requirements cannot be met.
LMR	Multi-path-based	Good	Good	High		Label information may reduce the routing overhead and the configuring time of the backup path.	May have additional overhead to discover alternate paths.

5. Current state of standardization for IoTs protocols

Standardization is a major prerequisite for achieving interoperability. This is of particular interest for IoTs and WSN, because common access to devices, sensors, and software components leading to new cross-domain applications is the primary focus of IoTs.

Since the IETF began its work on IoT-related technologies, IPv6 has been chosen as the best solution. Nevertheless, among the biggest challenges in deploying IPv6 sensing devices is effectively use low power and low bandwidth. In order to meet these challenges, several standards bodies, such as the IETF and the IEEE, have taken the initiative to standardize protocols for constrained networks; the most important of them are presented below.

5.1. IEEE 802.15.4 standard

This is the most relevant communication standard for WSNs. It has been standardized by the IEEE 802.15 Working Group for communication devices operating in Low-Rate Wireless Personal Area Networks (LR-WPANs), approved by ANSI in 2017. As shown in Fig. 4, the IEEE 802.15.4 standard specifies the physical layer and the media access layer for short-range radio frequency communication in WPAN with low energy consumption, low complexity, and low cost. The basic standard was published in 2003 and the revisions in 2006, 2011 and 2015. This standard forms the basis for other standards such as ZigBee.

For the distribution of network nodes, The IEEE 802.15.4 standard supports two kinds of network topologies, namely peer-to-peer and star topology, as illustrated by Fig. 5. The star topology is preferred in the case of a small coverage area and low delay is required for the application. While the peer-to-peer topology is more appropriate for a large coverage area with no delay constraint.

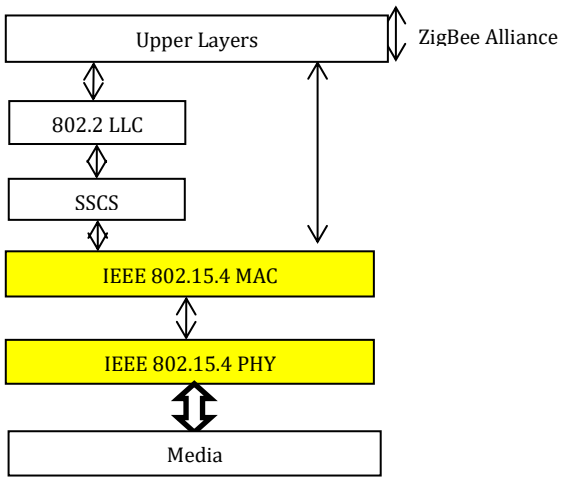

Fig. 4: IEEE 802.15.4 protocol stack. Upper layers: ZigBee, 6LowPAN (redrawn from Buratti et al. (2009))

5.2. Bluetooth low energy (BLE)

The latest version, adopted by the Bluetooth Special Interest Group (SIG) in December 2016, is Bluetooth5 (BLE, 2016), whose new features focus mainly on IoTs. BLE technology (BLE, 2016) allows a new low-cost Bluetooth for smart devices to run longer, with an improved communication range. Compared to traditional Bluetooth, BLE operates the same 2.45 GHz ISM band, but uses different channels.

Bluetooth 5 provides, for BLE, options that can double the speed at 2 Mbps burst at the expense of the range, or up to four times the range at the expense of throughput, and multiply by eight the streaming capability, by increasing the packet lengths. These features, along with enhanced interoperability and coexistence with other wireless technologies, continue to drive IoTs forward.

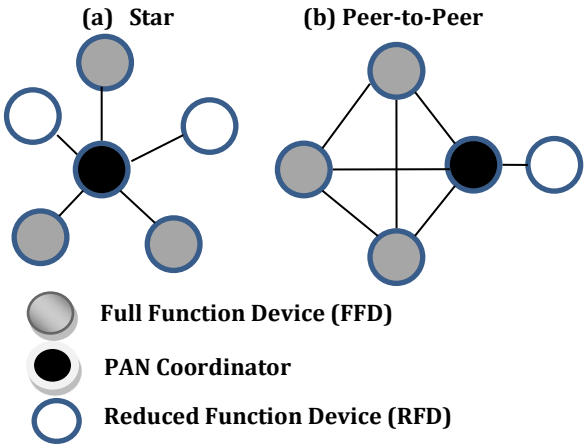

Fig. 5: The IEEE 802.15.4 network topologies: (a) star topology and (b) peer-to-peer topology

5.3. IEEE 802.15.4a- ultra wideband (UWB)

It is a radiofrequency communication technology in which the information is periodically transferred by a series of very short pulses (Porcino and Hirt, 2003). The Ultra Wideband is a proposed technology for the IEEE 802.15.4a that provides an alternative physical layer for the LR-WPANs and is an amendment to the IEEE 802.15.4a standard. The benefits of UWB include spectral efficiency, the ability to transmit high data rates with low energy, high measurement accuracy, localization capability, and the ability to manage multipath environments. Nevertheless, UWB is not suitable for long-distance communications or for measuring hazardous area data due to high-energy pulses. The Radio-UWB pulse (Dardari et al., 2009) based on ultra-short waveforms is a promising technology for WSNs.

5.4. ZigBee

It is a low-cost, low power wireless communication standard used to create WPAN and managed by Zigbee Alliance (ZigBee, 2017). Its main contribution is to provide mesh capabilities for the IEEE 802.15.4 standard by adding network and security layers and an application framework. Zigbee covers different areas of application such as home automation, healthcare, lighting management and telecommunication services. Generally, to deploy Zigbee, additional equipment such as a Zigbee coordinator and a Zigbee router are required in addition to the Zigbee device. The ZigBee node requires an IEEE 802.15.4 / IP gateway to establish communication with an IP network. Therefore, ZigBee is well suited for wireless sensor network applications that do not require interfacing with IP devices. Nevertheless, the latest ZigBee IP specification relies on IPv6 and CoAP (IEEE, 2015; IETF, 2018).

5.5. 6LoWPAN (IPv6 over low power wireless personal area networks)

The 6LoWPAN standard has been defined (RFC 4944) (Montenegro et al., 2007) by the IETF to adapt IPv6 to IEEE 802.15.4 networks, and thus extend IPv6 to IoTs. The 6LowPAN Working Group [6lowpan] is working on IPv6 optimization on networks using IEEE 802.15.4; in particular, it explains how to deploy IPv6 on the MAC layer and the physical layer of IEEE 802.15.4. The benefits of this approach are the ability to reuse existing IPv6 technology infrastructures. In addition, the transmission of IPv6 packets over IEEE 802.15.4 links ensures interoperability with other IP devices. IP for Smart Objects (IPSO) Alliance (Dunkels and Vasseur, 2008) promotes the use of 6LowPAN and integrated IP solutions in smart objects. This protocol provides an adaptation layer, a new packet format and address management, to allow these devices to enjoy all the advantages of IP communication. Since IPv6 packet sizes are larger than the IEEE 802.15.4 frame size, an adaptation layer is interposed between the MAC layer and the network layer to optimize IPv6 on IEEE 802.15.4. The adaptation layer provides mechanisms for IPv6 header compression, fragmentation and reassembly, enabling the sending of IPv6 packets on IEEE 802.15.4 networks. However, this type of network is originally designed for computing devices with higher processing capacity and higher memory resources that are poorly suited to IoTs, and there is still a lot of research to develop to achieve better performance.

5.6. Routing protocol for low power and lossy networks (RPL)

RPL is the new standard routing protocol proposed by the IETF via the ROLL working group (Winter et al., 2012). It is a distance-vector routing algorithm for low power and lossy networks (LLNs) using IPv6. It aims to support ubiquitous sensing applications in the future framework of IoTs.

RPL supports three types of traffic patterns, including point-to-point (P2P), point-to-multipoint (P2MP) and multipoint-to-point (MP2P). The RPL nodes are connected without a loop, thus building a destination-oriented acyclic graph (DODAG) by exchanging distance vectors. RPL tries to avoid routing loops by calculating the position of a node, called rank, relative to others. This rank decreases if a node approaches the root and increases in the opposite direction. By broadcasting the routing constraints, the DODAG root filters the nodes that do not satisfy the constraints and selects the optimal path according to the metrics.

In the steady state phase, on a path to the root DODAG, each SN in the sensor network has identified

a stable set of parents, as well as one of them as a preferred parent. Each router transmits the primary source of routing control information, which is DODAG Information Object (DIO) messages, using the local link multicast, indicating its respective rank in the DODAG. After receiving a few DIO messages, the router calculates its own rank so that it is greater than the rank of each parent, and then starts sending DIO messages. Thereby, the formation of DODAG begins at the root and progressively extends to the entire network.

RPL offer a technique for broadcasting information about the dynamically formed network topology. Broadcasting of such information generates a minimal configuration in the nodes, allowing them to function primarily autonomously.

It should also be mentioned that RPL could operate on nodes with limited power and memory capabilities. The protocol dynamically adjusts the sending rate of routing control messages that will be generated frequently only if the network is in an unstable state. In addition, the protocol allows the use of source routing when P2MP is needed, which reduces memory overhead on the intermediate nodes. Although the current version of RPL has provided many useful features, such as support for multiple links, there is still room for improvement to achieve the aforementioned ambitious goal.

6. Future directions and challenges for routing in WSNs and IoTs

As we have seen in this article, emerging technologies such as WSNs and IoTs expose various technological challenges that are not met by classic adhoc networks. This requires the design of new algorithms to meet these challenges of constrained-networks. Current research has improved the performance of many aspects of WSNs and IoTs, such as node deployment, data aggregation and network lifetime.

6.1. Future challenges in WSNs routing

For a medium and long-term view, some of the research challenges and interesting opportunities on the WSN are presented, as well as some future research orientations are indicated.

6.1.1. Deployment, management and auto-reconfigurability

The sensors become miniaturized, multi-parameter and easier to design than before. Although sensors can be produced with very low power consumption and are localized, their deployment and management, for example to replace faulty nodes, can sometimes be difficult. The goal is to add new nodes to replace defective SNs in the deployment domain, as well as the ability to remove nodes from the network, or the flexibility of a SN to be reconfigured dynamically, without affecting the normal operation of the WSN. In addition, the combination of sensors and actuators capable of acting on the environment opens new perspectives to the wireless sensor network concept. Thus, sensor networks not only forward the sensing information of a particular environment, but also act to control it through actuators. This involves the automatic design of online control-command and signal processing for state estimation.

6.1.2. QoS requirements

QoS is an increasingly important issue in WSN applications. Thus, it is still a need to develop routing protocols for WSNs that will provide a high level of QoS for both application and end-users. However, the data-centric nature of the WSN makes it difficult to describe the QoS. Besides, the QoS requirements in WSNs are application-specific. Whereas conventional networks use QoS metrics such as loss rate and bandwidth, WSNs use metrics such as residual energy, network sensing coverage and network longevity. It is therefore important that researchers focus on developing routing algorithms for WSNs that will provide guaranteed minimum QoS to upper layers. Thereby, designing a proper QoS-based routing protocol for WSN is a still open research problem. However, the provision of quality-of-service in sensor networks is very difficult because of their limited resources, difficult conditions in the deployment domains, deployment of random nodes, and high interdependence between quality-of-service properties. In addition, future research should address quality-of-service issues involving heterogeneous constrained networks.

6.1.3. Sensor mobility

The nodes of a WSN are supposed to be static, whereas today an increasing interest is granted to the applications supporting the mobility of the sensors, as for example in the applications of the telemedicine where the mobile sensors are attached to the patient, and must send the collected data to the physician. In such cases, the routing requirements differ with each environment; more research is needed to handle such situations.

6.1.4. Sharing resources in heterogeneous WSNs

Most previous research on WSNs assumes that it consists of homogeneous components. A difficult issue is to make the best use of shared resources in heterogeneous WSNs. In addition, the SNs of a sensor network can be shared by several applications with different goals. Thus, with the rise of the use of sensor networks, it is necessary to design algorithms capable of effectively serving multiple applications simultaneously, by ensuring a fast context change and without affecting the operation of the network.

6.1.5. Multilayered protocol design

A multilayered protocol design methodology for resource- constrained networks is a promising area of research. In fact, several cross-layer models are available in sensor networks, but their attention is limited on traditional OSI model layers (physical, etc.). While future multilayered research should focus on layer merging and layer collaboration to save energy, improve network performance and extend its lifetime. The design and development of effective modeling techniques and the successful exploitation of multilayer interactions is an open research topic.

6.1.6. Network security

In addition to power consumption, another critical factor in WSNs is the network security, which must be provided to protect against interceptions and malicious behavior. Sensor network security in is a persistent research problem that includes cryptographic methods, key management mechanisms, intrusion detection, secure routing algorithms, secure data aggregation, privacy and trust management. Although there are several proposed secure algorithms for the data-link and network layers, any vulnerability can be exploited at any layer of the protocol stack. Thereby, it is necessary to secure all layers without negligence. Ensuring the safety of a wireless sensor network in a continuous, cost-effective and energy-efficient manner is a dynamic problem of open research. Other security-related concerns in sensor networks that need to be addressed include, but are not limited to, energy security, data consistency and authentication, data encryption, QoS security assessment, etc.

6.2. Future challenges in IoTs routing

Previously, the IETF's efforts to develop WSNs-specific solutions were presented and some opportunities and challenges related to the practice of current IoTs standards were summarized. From a technological point of view, IoTs are not based solely on industrial innovations to promote network convergence, but also on fundamental academic innovations to enhance technical design. The Internet-of-Things domain is growing rapidly and dynamically, in addition to everything that is focused on merging new technologies, such as IoTs cloud systems (Truong and Dustdar, 2015).

6.2.1. Convergent networks

The future infrastructure of the Internet-of-Things will be available everywhere in our daily lives (household appliances, smart cities, etc.). Given the growing number of IoTs standards and the coexistence of different wireless communication technologies, such as ZigBee and Wi-Fi, it becomes necessary to design compatible heterogeneous technologies to reach converged networks, allowing routing protocols to converge to a new topology when changes occur. For example, ZigBee officially publishes its specification to show compatibility with IETF standards.

6.2.2. Green IT

Integrating WSNs into the automation of the IoTs and its implementation to enable green computing have been a major concern in recent years and will remain so for the coming years. By leveraging local radio resources, different wireless communication technologies can cooperate to provide effective and environmentally friendly communications. The use of recyclable materials in the manufacture of electronic components could be the ideal solution for ensuring green computing.

6.2.3. Energy balancing network

One of the main goals of designing an energy-efficient routing protocol for sensor networks is the balancing of energy in terms of the power consumed by the sensors. In other words, routing protocols must minimize network power consumption by choosing not only routes with a minimum number of hops, but also routes that extend network lifetime.

7. Conclusion

This article has presented basic concepts and recent research directions on routing approaches in sensor networks and the Internet of Things. It should be noted that this overview is far from being exhaustive. In fact, we have only discussed successful protocols that have marked the evolution of this line of research. The subject of routing protocols in a constrained environment is always open and continuously growing. In particular, in the field of IoTs, which is attracting increasing interest, as has been demonstrated.

Therefore, more in-depth studies are needed to develop an appropriate routing algorithm that will increase the lifetime of WSNs, while improving the power consumption of SNs on the network while ensuring efficient data distribution. In addition, further efforts are needed to standardize protocols for the future of the Internet of Things to ensure interoperability and convergence of networks.

However, several open research questions need to be investigated further. Firstly, it is emphasized that energy efficiency is still a major concern for research communities on WSNs and IoTs, in addition to scalability, mobility, QoS, security and virtualization.

Acknowledgment

The authors gratefully acknowledge the approval and the support of for this research study by the

grant no. (SCI-2017-1-7-F-7170) from the Deanship of Scientific Research at Northern Border University, Arar, KSA.

References

Abbasi AA and Younis M (2007). A survey on clustering algorithms for wireless sensor networks. Computer Communications, 30(14-15): 2826-2841.

Akkaya K and Younis M (2005). A survey on routing protocols for wireless sensor networks. Ad Hoc Networks, 3(3): 325-349.

Akyildiz IF, Su W, Sankarasubramaniam Y, and Cayirci E (2002). Wireless sensor networks: A survey. Computer Networks, 38(4): 393-422.

Alemdar H and Ersoy C (2010). Wireless sensor networks for healthcare: A survey. Computer Networks, 54(15): 2688-2710.

Al-Karaki JN and Kamal AE (2004). Routing techniques in wireless sensor networks: A survey. IEEE Wireless Communications, 11(6): 6-28.

Anastasi G, Conti M, Di Francesco M. and Passarella A (2009). Energy conservation in wireless sensor networks: A survey. Ad Hoc Networks, 7(3): 537-568.

Arora A, Dutta P, Bapat S, Kulathumani V, Zhang H, Naik V, and Choi YR (2004). A line in the sand: A wireless sensor network for target detection, classification, and tracking. Computer Networks, 46(5): 605-634.

Aslan YE, Korpeoglu I, and Ulusoy Ö (2012). A framework for use of wireless sensor networks in forest fire detection and monitoring. Computers, Environment and Urban Systems, 36(6): 614-625.

Ben-Othman J and Yahya B (2010). Energy efficient and QoS based routing protocol for wireless sensor networks. Journal of Parallel and Distributed Computing, 70(8): 849-857.

Biradar RV, Patil VC, Sawant SR, and Mudholkar RR (2009). Classification and comparison of routing protocols in wireless sensor networks. Special Issue on Ubiquitous Computing Security Systems, 4: 704-711.

BLE (2016). Bluetooth core specification. Bluetooth Low Energy. Available online at: https://www.bluetooth.com/specifications/bluetooth-core-specification

Braginsky D and Estrin D (2002). Rumor routing algorthim for sensor networks. In the 1st ACM International Workshop on Wireless Sensor Networks and Applications, ACM, Atlanta, Georgia, USA: 22-31.

Buratti C, Conti A, Dardari D, and Verdone R (2009). An overview on wireless sensor networks technology and evolution. Sensors, 9(9): 6869-6896.

Chen M and Gonzalez S (2007). Applications and design issues for mobile agents in wireless sensor networks. IEEE Wireless Communications, 14(6): 20-26.

Chen M, Gonzalez S, Zhang Y, and Leung VC (2009). Multi-agent itinerary planning for wireless sensor networks. In the International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness, Springer, Berlin, Heidelberg, Germany: 584-597.

Chen M, Yang LT, Kwon T, Zhou L, and Jo M (2011). Itinerary planning for energy-efficient agent communications in wireless sensor networks. IEEE Transactions on Vehicular Technology, 60(7): 3290-3299.

Darabi S, Yazdani N, and Fatemi O (2008). Multimedia-aware MMSPEED: A routing solution for video transmission in WMSN. In the 2nd International Symposium on Advanced Networks and Telecommunication Systems, IEEE, Mumbai, India: 1-3.

Dardari D, Conti A, Ferner U, Giorgetti A, and Win MZ (2009). Ranging with ultrawide bandwidth signals in multipath environments. Proceedings of the IEEE, 97(2): 404-426.

Demirkol I, Ersoy C, and Alagoz F (2006). MAC protocols for wireless sensor networks: A survey. IEEE Communications Magazine, 44(4): 115-121.

Dunkels A and Vasseur JP (2008). IP for smart objects. Technical Report, Internet Protocol for Smart Objects (IPSO) Alliance, White Paper 1. Available online at: http://www.ipso-alliance.org/wp-content/media/why_ip.pdf

Đurišić MP, Tafa Z, Dimić G, and Milutinović V (2012). A survey of military applications of wireless sensor networks. In the Mediterranean Conference on Embedded Computing, IEEE, Bar, Montenegro: 196-199.

Ehsan S and Hamdaoui B (2012). A survey on energy-efficient routing techniques with QoS assurances for wireless multimedia sensor networks. IEEE Communications Surveys and Tutorials, 14(2): 265-278.

Faulkner M, Olson M, Chandy R, Krause J, Chandy KM, and Krause A (2011). The next big one: Detecting earthquakes and other rare events from community-based sensors. In the 10th International Conference on Information Processing in Sensor Networks, IEEE, Chicago, USA: 13-24.

Felemban E, Lee CG, and Ekici E (2006). MMSPEED: Multipath Multi-SPEED protocol for QoS guarantee of reliability and. Timeliness in wireless sensor networks. IEEE Transactions on Mobile Computing, 5(6): 738-754.

Gomez C and Paradells J (2010). Wireless home automation networks: A survey of architectures and technologies. IEEE Communications Magazine, 48(6): 92-101.

Goyal D and Tripathy MR (2012). Routing protocols in wireless sensor networks: A survey. In the Second International Conference on Advanced Computing and Communication Technologies, IEEE, Rohtak, Haryana, India: 474-480.

He T, Stankovic JA, Lu C, and Abdelzaher T (2003). SPEED: A stateless protocol for real-time communication in sensor networks. In the 23rd International Conference on Distributed Computing Systems, IEEE, Providence, Rhode Island, USA: 46-55.

Heinzelman WR, Chandrakasan A, and Balakrishnan H (2000). Energy-efficient communication protocol for wireless microsensor networks. In the 33rd annual Hawaii International Conference on System Sciences, IEEE, Maui, USA.

Heinzelman WR, Kulik J, and Balakrishnan H (1999). Adaptive protocols for information dissemination in wireless sensor networks. In the 5th annual ACM/IEEE International Conference on Mobile Computing and Networking, ACM, Seattle, Washington, USA: 174-185.

Hou X, Tipper D, and Kabara J (2004). Label-based multipath routing (LMR) in wireless sensor networks. In the 6th International Symposium on Advanced Radio Technologies, Boulder, USA: 113-118.

IEEE SA (2015). IEEE Std 802.15.4-2015 (Revision of IEEE Std 802.15.4-2011) - IEEE standard for low-rate wireless networks. IEEE Standard Association. Available online at: https://standards.ieee.org/findstds/standard/802.15.4-2015.html

IETF (2018). IPv6 over Low power WPAN (6lowpan). Available online at: https://datatracker.ietf.org/wg/6lowpan/about/

Intanagonwiwat C, Govindan R, and Estrin D (2000). Directed diffusion: A scalable and robust communication paradigm for sensor networks. In the 6th Annual International Conference on Mobile Computing and Networking, ACM, Boston, Massachusetts, USA: 56-67.

Jolly V and Latifi S (2006). Comprehensive study of routing management in wireless sensor networks-Part-I. In the International Conference on Wireless Networks, Las Vegas, USA: 37-44.

Kortuem G, Kawsar F, Sundramoorthy V, and Fitton D (2010). Smart objects as building blocks for the internet of things. IEEE Internet Computing, 14(1): 44-51.

Kulik J, Heinzelman W, and Balakrishnan H (2002). Negotiation-based protocols for disseminating information in wireless sensor networks. Wireless Networks, 8(2/3): 169-185.

Leong B, Liskov B, and Morris R (2006). Geographic routing without planarization. In the 3rd Symposium on Networked Systems Design and Implementation, San Jose, USA, 6: 1-25.

Lim H and Kim C (2001). Flooding in wireless ad hoc networks. Computer Communications, 24(3-4): 353-363.

Lindsey S and Raghavendra CS (2002). PEGASIS: Power-efficient gathering in sensor information systems. In the IEEE Aerospace Conference Proceedings, IEEE, Big Sky, USA, 3: 3-3.

Liu X (2012). A survey on clustering routing protocols in wireless sensor networks. Sensors, 12(8): 11113-11153.

Manjeshwar A and Agrawal DP (2001). TEEN: A routing protocol for enhanced efficiency in wireless sensor networks. IEEE Int'l Parallel and Distributed Processing Symposium, San Francisco, USA.

Manjeshwar A and Agrawal DP (2002). APTEEN: A hybrid protocol for efficient routing and comprehensive information retrieval in wireless sensor networks. In the IEEE Int'l Parallel and Distributed Processing Symposium, Fort Lauderdale, Florida, USA.

Montenegro G, Kushalnagar N, Hui J, and Culler D (2007). Transmission of IPv6 packets over IEEE 802.15.4 networks. RFC4944. Available online at: http://tools.ietf.org/html/rfc4944

Newsome J and Song D (2003). GEM: Graph EMbedding for routing and data-centric storage in sensor networks without geographic information. In the 1st International Conference on Embedded Networked Sensor Systems, ACM, Los Angeles, California, USA: 76-88.

Ogundile OO and Alfa AS (2017). A survey on an energy-efficient and energy-balanced routing protocol for wireless sensor networks. Sensors, 17(5): 1-5.

Pantazis NA, Nikolidakis SA, and Vergados DD (2013). Energy-efficient routing protocols in wireless sensor networks: A survey. IEEE Communications Surveys and Tutorials, 15(2): 551-591.

Porcino D and Hirt W (2003). Ultra-wideband radio technology: Potential and challenges ahead. IEEE Communications Magazine, 41(7): 66-74.

Radi M, Dezfouli B, Bakar KA, and Lee M (2012). Multipath routing in wireless sensor networks: survey and research challenges. Sensors, 12(1): 650-685.

Ramesh MV (2014). Design, development, and deployment of a wireless sensor network for detection of landslides. Ad Hoc Networks, 13: 2-18.

Rawat P, Singh KD, Chaouchi H, and Bonnin JM (2014). Wireless sensor networks: A survey on recent developments and potential synergies. The Journal of Supercomputing, 68(1): 1-48.

Romer K and Mattern F (2004). The design space of wireless sensor networks. IEEE Wireless Communications, 11(6): 54-61.

Sadagopan N, Krishnamachari B, and Helmy A (2003). The ACQUIRE mechanism for efficient querying in sensor networks. In the 1st IEEE International Workshop on Sensor Network Protocols and Applications, IEEE, Anchorage, AK, USA: 149-155.

Sadagopan N, Krishnamachari B, and Helmy A (2005). Active query forwarding in sensor networks. Ad Hoc Networks, 3(1): 91-113.

Sohrabi K, Gao J, Ailawadhi V, and Pottie GJ (2000). Protocols for self-organization of a wireless sensor network. IEEE Personal Communications, 7(5): 16-27.

Srbinovska M, Gavrovski C, Dimcev V, Krkoleva A, and Borozan V (2015). Environmental parameters monitoring in precision agriculture using wireless sensor networks. Journal of Cleaner Production, 88: 297-307.

Tarique M, Tepe KE, Adibi S, and Erfani S (2009). Survey of multipath routing protocols for mobile ad hoc networks. Journal of Network and Computer Applications, 32(6): 1125-1143.

Tilak S, Abu-Ghazaleh NB, and Heinzelman W (2002). A taxonomy of wireless micro-sensor network models. ACM SIGMOBILE Mobile Computing and Communications Review, 6(2): 28-36.

Truong HL and Dustdar S (2015). Principles for engineering IoT cloud systems. IEEE Cloud Computing, 2(2): 68-76.

Winter T, Thubert P, Brandt A, Hui J, Kelsey R, Levis P, Pister K, Struik R, Vasseur JP, and Alexander R (2012). RPL: IPv6 routing protocol for low-power and lossy networks. RFC6550. Available online at: http://tools.ietf.org/html/rfc6

Wu Q, Rao NS, Barhen J, Iyenger SS, Vaishnavi VK, Qi H, and Chakrabarty K (2004). On computing mobile agent routes for data fusion in distributed sensor networks. IEEE Transactions on Knowledge and Data Engineering, 16(6): 740-753.

Yadav R, Varma S, and Malaviya N (2009). A survey of MAC protocols for wireless sensor networks. UbiCC Journal, 4(3): 827-833.

Yao Y and Gehrke J (2002). The cougar approach to in-network query processing in sensor networks. ACM Sigmod Record, 31(3): 9-18.

Ye F, Zhong G, Lu S, and Zhang L (2005). Gradient broadcast: A robust data delivery protocol for large scale sensor networks. Wireless Networks, 11(3): 285-298.

Yi WY, Lo KM, Mak T, Leung KS, Leung Y, and Meng ML (2015). A survey of wireless sensor network based air pollution monitoring systems. Sensors, 15(12): 31392-31427.

Yick J, Mukherjee B, and Ghosal D (2008). Wireless sensor network survey. Computer Networks, 52(12): 2292-2330.

Yu Y, Govindan R, and Estrin D (2001). Geographical and energy-aware routing: a recursive data dissemination protocol for wireless sensor networks. Technical Report, UCLA Computer Science Department, Los Angeles, California, USA.

ZigBee (2017). ZigBee Alliance. Available online at: http://www.zigbee.org