

Routing in Wireless Sensor Networks for Surveillance of Airport Surface Area

Juliette Garcia Alviz, Alain Pirovano, Mickaël Royer

▶ **To cite this version:**

Juliette Garcia Alviz, Alain Pirovano, Mickaël Royer. Routing in Wireless Sensor Networks for Surveillance of Airport Surface Area. Nets4, 13th International Workshop on Communication Technologies for Vehicles, Nets4Aircraft and UAV session, May 2018, Madrid, Spain. pp. 27-38 / ISBN 978-3-319-90370, 10.1007/978-3-319-90371-2_3 . hal-01785107

HAL Id: hal-01785107

https://enac.hal.science/hal-01785107

Submitted on 31 May 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Routing in Wireless Sensor Networks for Surveillance of Airport Surface Area

Juliette Garcia, Alain Pirovano, and Mickaël Royer

ENAC/Telecom/ReSCo/Université de Toulouse
juliette.garcia@recherche.enac.fr,alain.pirovano@enac.fr,mickael.royer@enac.fr

Abstract. The surveillance of airport surface area is a crucial operation for the safety of passengers and the airport itself. Even if this method have shown its limits, today the airports keep employing visual inspection. Some technology radar based systems are available but they are still very expensive and do not cover exhaustively the needs. In this paper, we present the first part of a research work that aims to propose a surface surveillance method based on wireless sensor networks (WSN). To the best of our knowledge, this is an unexplored alternative. However, considering their low cost and their ability to ensure surveillance in other domains like agriculture, WSNs surely represent an interesting solution in airports. Our research focuses on the definition of a suitable routing protocol for WSN in the context of airport surface surveillance. We present in this article some properties about the context of airport surveillance and then a brief description and classification of the most popular routing protocols for WSN. Finally we identify a routing protocol for WSN that, as the most suitable for the considered context, could be used as reference in the next steps of our research works.

Keywords: WSN, routing protocols, Airport Surface Area Surveillance

1 Introduction

A WSN is a collection of spatially dispersed devices equipped with sensors, which are strategically deployed to monitor the environment. Sensors periodically gather and transfer data via wireless communication to a central node where data are collected and processed. The central node is known as the sink. WSNs have recently been employed in a variety of applications, including road traffic control, home automation, battlefield surveillance, environment monitoring, among several others. One of the characteristics of WSNs, that have made them popular in the last years, is that sensors are cheap and can be easily deployed with very low impact on their environment. In addition, sensor nodes can be deployed in short time and the network topology can be easily modified, tailored or scaled. Even, under inclement weather conditions these allow high precision of data gathering. In WSN applications, the area of interest is often larger than the communication range of the sensor nodes. Therefore, to reach

the sink, a sensor may use other ones as relays. The path to the sink that each data package should follow is defined by a routing protocol. This set of rules is a core element in the functioning of any WSN. If the routing protocol is properly designed, data will arrive to the destination on time and sensors will be efficiently used. Otherwise, various undesired phenomena such as excessive delays, unnecessary energy consumption and excessive data replication, may appear. Unfortunately, the construction of an effective routing protocol for WSN is by no means an easy task due to the inherent complexities of this type of networks and the number of properties and parameters that have to be taken into account. A suitable management of network resources (e.g., sensor nodes storage capacity, processing capability and energy), and a proper schedule for data transfer in case of segmented networks, are just some of the main challenges.

In this paper, we emphasize on the selection of suitable routing protocols for WSN for Airport Surface Area Surveillance (ASAS). To the best of our knowledge, this subject has not been addressed in the literature. Our main purpose at this point is to identify one or some routing protocols that are the most appropriate for application in ASAS. To do so, we study some popular routing protocols found in the literature and we classify them according to a set of criteria that allows us to determine which ones are more suitable for the application in airports. The Fig. 1 shows an example of the application we will investigate.

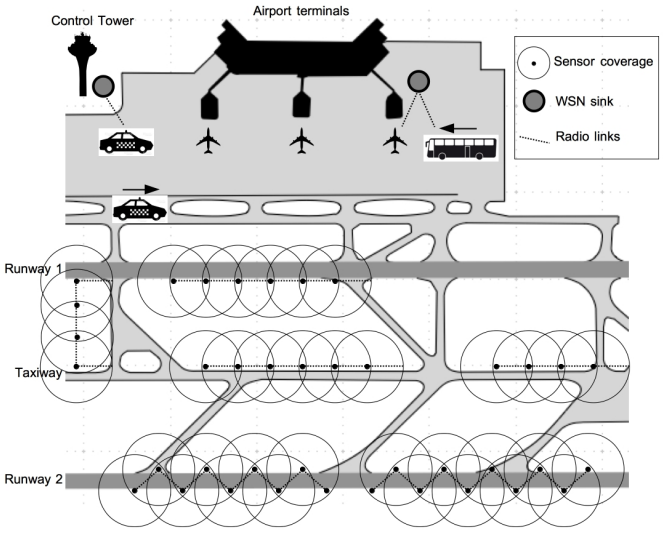


Fig. 1. Airport Surface Area Surveillance WSN-based

The rest of the paper is organized as follows: Firstly Section 2 delves into the concept and application of Airport Surface Area Surveillance. Then, we state and explain which types of data have to be collected and the properties of our

environment. Section 3 provides a brief review of most popular routing protocols for WSN and their classification. Section 4 discusses the most suitable routing protocols for WSN applied to ASAS. Finally, Section 5 concludes the paper and gives some potentials further steps in this research work.

2 Airport Surface Area Surveillance (ASAS)

2.1 Overview and Principles

The airport surface area surveillance is a crucial aspect for the safety of passengers and the preservation of airports integrity. It encompasses a set of strategies used to monitor and control operations in both, movement areas (taxiways and runways) and non-movement areas (aprons and aircraft parking spots). ASAS procedures in movement areas are oriented to accident prevention and short term decision making (e.g. detect and remove objects from the runway). And procedures in non-movement areas focus on short term, less critical decision making (e.g. detect excessive noise levels and intervene).

Some unfortunate past events have put in evidence the need for rigorous ASAS procedures. Along the history, the presence of objects in the runways has caused major economic and human losses associated to minor and fatal aircraft accidents. One of the most popular ones was the Air France Concorde 4590 Flight accident occurred in 2000. During the taking off, one of the tires of the aircraft serving the flight exploded and the aircraft got fire. Two minutes after, the aircraft crashed. An exhaustive investigation revealed that the accident was attributed to a titanium piece (about 3 cm wide and 43 cm long) that had fallen off in the runway from a plane that took off some minutes previously.

Nevertheless airports continue performing regular self-inspections proceeded by ground personnel that go over the runway. The objective is to ensure that these areas are free from FOD (Foreign Object Damage), animals, and so on [1]. However, even full-conscious, reasoning humans are prone to errors due to fatigue, limited visibility among other factors that can prevent them to locate a FOD for instance. In addition, visual inspections are time consuming and no take-offs or landings can be conducted in parallel. Thus, only a few daily inspections are the typical mark for airports adopting the visual method. Alternative technology-based methods have emerged in recent years. They offer the possibility of conducting more accurate and frequent inspections. However these technologies have only received the attention of a few major airports in the world, due to their cost. The system based on WSN, that we seek to propose, aims to provide the advantages of the automated, technology-based methods, at an affordable cost.

2.2 Interviews with Airport Managers and Air Traffic Controllers

We have conducted interviews with some actors (airport manager and controllers) that could be the future users of our solution. After a short presentation

of our project, during the interviews we seek to determine: (i) the way ASAS are currently being conducted, (ii) expected improvements in ASAS by adoption of WSNs, and (iii) main types of relevant data for ASAS (attributes of interest to be measured). This section is devoted to the discussion of the information collected during the interviews regarding the aspects mentioned above.

How ASAS is currently being conducted According to the interviewees, nowadays ASAS is mainly and more exclusively done by visual inspection. One of the main limitations of this practice is that airport regular operations (landings, take-offs, taxiing, etc) need to be stopped during inspections. But with the continuous increasing air traffic, the inspections must be performed as quickly as possible but with effectiveness. In addition, gathered data may contain errors (for instance, due to human fatigue). A few alternative technologies in contrast to visual inspection have emerged in the recent years. Most of them focused on automated runway scanning (ARS) [1]. These technologies use millimeter wave radars to continuously scan runway surfaces and their installation requires a relatively heavy work. The interviewees stated those alternatives are in most cases unacceptable due to their high cost. On the other hand, an interview disclosed by [1] in 2011 to 50 airports around the world concluded that only 6% of airports in the sample were implementing continuous surface surveillance using technology-based methods. The study also suggested the high cost of such technologies as a potential reason for the low statistic.

Expected improvements of ASAS by Adoption of WSN Most expectations, from the application of WSN for ASAS, point to three major angles:

- Precision and accuracy: WSNs are expected to enhance the quality of data gathered through the strategic deployment of high precision sensors near critical sensing spots. This way, imprecisions in the data associated to human factors and inaccuracies resulting from lack of closeness during data gathering, could be virtually eradicated.
- Knowledge on spatial components of attributes: WSNs will allow the transition from one/a few to multiple sensing spots. This is expected to dramatically improve the awareness about conditions in airport surface area. Environmental data could be translated into surface or temperature plots, providing traffic controllers with wide spatial information about attributes of interest through an intuitive display for instance.
- Natural coupling with airport operations: WSNs are intended to integrate gently with the daily functioning of airports. Sensing will be conducted by a collection of small devices. These could be conveniently located at several points while keeping closeness to the critical sensing spots, without perturbing regular operations. On the other hand, as explained later the dedicated WSN will certainly result in several segmented ones. Hence, each segmented WSN could opportunistically use airport ground vehicles/personnel as data mules, exploiting their regular displacements to transmit information among

isolated parts of the network. It has also to be underline here that as our solution will be based on wireless links and autonomous sensors and therefore its installation and deployment are expected to be easy.

Main types of relevant data for ASAS The interviewing process also gave us the possibility to list the most relevant type of data that could be monitored with WSNs (see Table 1). The list includes several environmental conditions related to temperature, noise, pollution and visibility that may be considered as non critical. The list includes another subclass of type of data that are sensitive and critical for the safety. Some of these which may justify a brief explanation for the sake of clarity. Taxiway flow rate refers to the number of aircraft that make use of each taxiway during a day of operation. Similarly, apron visit rate and aircraft parking spot visit rate refer to the number of aircraft that make use of each apron and parking spot during a day of operation, respectively. We may also define the state of runway safety lights, which will be a binary variable indicating if each safety light is properly functioning or not, and taxiway misselection, that will indicate if some aircraft went through the wrong taxiway. As critical data we consider also those related with detection of FOD, animals, and intrusion.

Hence, we classified each attribute in the table as critical and non-critical. The classification of attributes in these categories provides insights on the required particularities of the routing protocol for this application. We will go deeper into this in Section 4.

Table 1. Attributes of interest for the airports

Attribute	Critical	Non-critical
Numerical		
Pavement temperature	x	x
Noise	x	x
Pollution (NO_2, CO, SO_2)		x
Water/snow height	x	x
Taxiway flow rate		x
Apron visit rate		x
Aircraft parking spot visit rate		x
Categorical		
Presence of animals/foreign object	x	
State of runway safety lights	x	
State of the road	x	x
Taxiway misslecion	x	x

2.3 Environment and network properties

Finally some last points that may be important to define a suitable routing protocol are related to the network topology and its properties. As shown in

the Fig. 1, two main recurring properties can be stated. Firstly, considering the wide area of an airport, the WSNs should be segmented in several subnetworks. In these cases, a recommended method, to ensure the reachability between each segmented WSN and the sink, is based on the use of vehicles as data mules. These latter will collect data and bring them to the sink. In airport, the data mule role could be played by the existing vehicle or even the arriving aircraft in an opportunistic way. Secondly, as the infrastructure of a typical airport shows geometric shapes, the WSNs topologies are expected to have this same property.

3 Routing Protocols in WSN

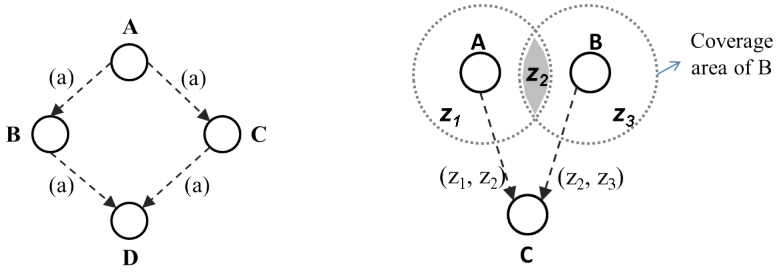
This section is devoted to describe some popular routing protocols used in WSN and propose a classification intended to select an appropriated routing protocol for a given application.

3.1 Overview of Popular Routing Protocols for WSN

Before describing some routing protocols, we detail two simple strategies for forwarding data that do not require a routing algorithm. For that reason, these strategies, in our criterion, are not considered as protocols. These are flooding and gossiping strategy.

Flooding strategy This is the first strategy created to transfer information between the sensor nodes and the sink. A sensor, every time it senses data, transmits it to all its neighbor nodes and, in turn, these neighbors transmit it to its neighbor nodes, until data reach the destination [2]. It has three critical drawbacks:

- Implosion: which occurs when a node receives duplicated or redundant data. The Fig. 2(a) shows this problem. Here, node A floods its data (a) to its neighbors B and C. In turn, these nodes send a copy of it on to its common neighbor D. As result, it produces resource wastes by sending redundant data to the same node.
- Overlap: which occurs when two sensors sense an overlapping spatial region. The Fig. 2(b) illustrates that sensor A and B cover an overlapping geographic region, named z_2. When these sensors flood their data to node C, C will receive duplicated data of z_2 region. Again, this strategy produces redundant data and then resource wastes.
- Resource blindness: this strategy does not consider the available energy in each node for taking decisions. The non-consideration of energy resources may lead to wrong or unfeasible decisions in the routing process.



(a) Implosion (b) Overlap

Fig. 2. Drawbacks in flooding strategy

Gossiping strategy It is a slightly enhanced version of flooding. Instead of sending data to all its neighbors, a sensor node sends data to only one randomly selected neighbor node, which selects another random neighbor node, until the data reach the destination [2]. This strategy reduces the implosion problem. However, this could lead to increase the latency to forward the data to the sink.

The following protocols improve the drawbacks of the previous strategies:

SPIN (Sensor protocols for information via negotiation) It is a family of protocols that aims to overcome the problems of implosion, overlap and resource blindness presented in flooding strategy [2].

To overcome implosion problem SPIN adopts a negotiation process. For that, it uses three types of messages: advertisement (ADV), request (REQ) and data (DATA). A node, which collects data, will send an ADV to all its neighbors with meta-data fields which describe the collected information. Their neighbors will specify with a REQ if they are interested in this data. Only the neighbors which confirm their interest for the information will receive the data. This prevents a node from receiving redundant information.

On the other hand, to overcome overlap problem, SPIN uses meta-data descriptors which precise in particular the portion of the region that it collects. Thus, if a node notices, in the received ADV, that it has already received data from a certain part of a region, it indicates in REQ in which parts it is interested.

Finally, this protocol allows the sensor nodes to check their resources before data transmission. Using it, the nodes may be aware of its available energy to make suitable decisions.

Directed diffusion In this protocol, the sink is the one who makes information queries. Sensors whose features match with a query will be called sources of information and only these ones can send data. This protocol seeks to determine a single path between the sink and the sources of information [2]. The protocol operates in three stages:

- Spreading interests: the sink sends an interest message to each of its neighbors and these resend it only to its neighbors that have not received it yet. This message specifies a set of the attributes that are of interest to the sink.
- Set up gradients: each node, that receives the interest, stores a gradient that contains the previous node which sent to it the interest and its own data rate. The nodes that never receive an interest will have a null gradient. The source sends the data to all the neighbors with a gradient different than null (possibly it sends along multiple paths), toward the sink.
- Path reinforcement: after the sink starts receiving data, it selects the path with low delay based in the data rate of each sensor node. Once a single path is chosen, the sink requests data at a higher rate.

GEAR (Geographic and Energy Aware Routing) It is an improvement of Directed Diffusion protocol. The main idea is to use geographic information (e.g. provided by GPS) to restrict the number of interests sent in Directed Diffusion to an certain region rather than to send interests to the whole network [3].

Rumor routing It is another variation of Directed Diffusion and is mainly used in the cases in which geographic routing techniques are not applicable. Directed Diffusion floods the query to the entire network. However, in some cases the sink requires a bit amount of data and thus the use of flooding is unnecessary. An alternative is to flood the events. For that, once an event occurs, a package (called agent) is sent to "spread rumors about the location of the source". While it is moving, it builds the shortest path to such event. Then, when the sink requests information about the event, its query moves blindly through the network until it stumbles upon a sensor node visited by the agent. The query can take advantage of the path provided by the agent that will drive to the source of information for the shortest path. Once the query arrives to the source, data is sent using the path used by the query [2].

LEACH (Low-Energy Adaptive Clustering Hierarchy) This protocol uses an aggregation strategy, the setup of groups of sensors (cluster) for reducing the redundant information that arrives to the sink [2]. To build these clusters, it works in rounds. Each round consists of two stages:

- Setup stage: in this stage, some random cluster heads (CH) are selected. The CHs are the only nodes that can receive, aggregate and send information to the sink. The remaining nodes must seek the closer CH and join to its cluster.
- Transmission stage: the sensor nodes send collected data to its corresponding CH. And finally, the CHs send aggregated data to the sink.

This way, the route created for each node is always composed of 2 hops. The first hop is the selected CH and the second hop is the sink.

PEGASIS (Power Efficient Gathering in Sensor Information Systems) In this protocol, nodes are organized into a chain, using a greedy algorithm. So that, each node sends to and receives from only one of its neighbors. In each round, a random node, called leader, is selected. Then, sensor nodes sense data and send it to its closer neighbor and, in turn, this latter forwards it to its closer neighbor, until the data can reach a leader node. The leader node aggregates data and send it to the sink [4]. This protocol seeks that all the nodes become leader, at least one time, to balance their energy.

TEEN (Threshold sensitive Energy Efficient sensor Network protocol) This protocol is based on cluster formation. It uses a hierarchical structure similar to LEACH, but it proposes an additional level between the CHs and the sink, named second level of CH. This second level aims to extend network coverage. Thus, the route is composed by 3 hops. The first hop is the first level CH, the second one is the second level CH and third one is the sink.

On the other hand, this protocol was one of the first protocols, for WSN, performed for data transfer based on events [4]. This means that sensor nodes send only when a sensed attribute overpasses a given threshold. This protocol manages two thresholds:

- Hard threshold (HT): this is the minimum value beyond which the node sends data to its CH.
- Soft threshold (ST): once the HT is reached, it is possible to test it. This is a change in the value of the sensed attribute which triggers the sending of data from sensor nodes to its CH.

Thefore, HT aims to reduce the number of transmissions by sending only data in the range of the interest and ST aims to reduce the number of transmissions by avoiding sending non-significant changes.

This protocol is suitable for time-critical applications. However it is not suitable for applications where periodic reports are needed because user may not get any data if thresholds are not reached.

APTEEN (Adaptive Threshold sensitive Energy Efficient Network protocol) This protocol is an extension of TEEN. It considers the transfer of information not only based on events that exceed limits but also periodically. For that, this protocol handles a variable that counts the time. If the elapsed time exceeds a fixed duration, the sensors, even if the sensed data has not exceeded a threshold, must send it. In this way, data is collected periodically and based on events [4].

RPL (Routing Protocol for Low-power and Lossy Networks) This protocol is the only one which is standardized by the IETF (Internet Engineering Task Force) group. It organizes the WSN as a Directed Acyclic Graph (DAG) rooted at the sink. A DAG is a directed graph with no cycles.

This protocol is supported in the exchange of local messages. The objective function of each node is a measure of its cost to reach the sink. The route to the nodes is built starting from the sink. The sink sends a local message to its neighbors to join the DAG. Each node compares the current value of its objective function with the value of the objective function currently used. If this is convenient for the node, it chooses it as his parent, that is, the next hop to reach to the sink. The neighbor nodes will repeat this process until all the nodes are attached to the DAG. The resulting graph minimizes the cost of routes from sink to all the nodes [5]. This way, the sensor nodes can send data to sink by just forwarding the packet to its immediate parent.

3.2 Classification of Routing Protocols for WSN

To determine the suitable routing protocols for a given application, we classify the solutions according to relevant properties which can be split into two categories:

- Linked to the Context: properties which are directly associated to the specific context and constrain the routing solution. The context contains some characteristics associated with the network and with the handling of the required data.
- Linked to the Algorithm: properties independent to the context, which has to be fixed during the design of the algorithm to optimize the efficiency of the solution.

Linked to the Context

Data collect mode It defines when each node should send data to the sink. It can be:

- Periodic: sensor nodes send data to the sink at a fixed rate.
- Event-based: the system works based on a set of predefined target events, such as the exceeding of a given threshold in a sensed attribute. Sending information only occurs when a target event occurs.
- Query-based: the system uses requests of information generated by the sink. Each time a query is generated, relevant sensor nodes react and send the requested information.
- Hybrid: the system combines some of the three rules described above.

Topology of the network In our classification, it states if every nodes is able to communicate with any other node or not. Depending of the terrain and the location of data which has to be collected, a network can be:

- Fully connected: every node is able to communicate with each other via direct or multi-hop communication.
- Segmented: some nodes are not able to communicate with other nodes in the network.

Maximum number of hops This refers to the maximum number of hops allowed between any node and the sink. Sometimes, the size and the geometric configuration of the terrain may enforce a known or unknown number of hops to transfer data from some nodes to the sink. According to it, the number of hops can be:

- Limited: the route is composed of a fixed number of hops to reach the sink.
- Unlimited: the route can be composed of any number of hops to reach the sink.

Linked to the algorithm

Redundancy control mechanism Sensed information is often replicated in two ways: (i) implosion and (ii) overlap (see Flooding strategy in Section 3.1). Redundancy control mechanisms are strategies to reduce the amount and impacts of information redundancy.

- Data centric: collected information is temporarily stored in sensors as named data. When information is sent, it is tagged with details about the sensor node that collected it and some attributes related to the data such as the time of measurement. As the messages travel through the network, sensor nodes cross reference the tag of each incoming message with the tags of the data that they already know, and they reject all redundant message.
- Aggregation: some nodes, strategically located over the network, get the responsibility of aggregating information and eliminating redundancies.
- Position centric: when a sensor node has something to transfer, instead of sharing the information with all the neighbors, it builds a route based on its spatial location. This mechanism is often applied in networks with mobile sensor nodes, where locations are determined by GPS.

Route generation scheme It defines when the routes are computed. It can be:

- Proactive: all routes are computed before they are required and then, they are periodically updated.
- Reactive: routes are computed each time a sensor node needs to send data to the sink.
- Hybrid: uses a combination of the proactive and reactive schemes.

Performance metric It is the objective to be optimized in the construction of the routes. Most common ones are:

- Latency: time elapsed from the sending of message by a sensor node to its delivery at the sink.
- Energy: amount of energy invested in the transfer.

Table 2 contains the protocols, described in section 3.1, categorized according the classification proposed in this section. In this table, the property P1 corresponds to data collect mode, P2 to topology of the network, P3 to maximum number of hops, P4 to redundancy control mechanism, P5 to route generation scheme and P6 to performance metric.

Table 2. Classification of routing protocols

Routing protocol	Linked to the context			Linked to the Algorithm		
	P1	P2	P3	P4	P5	P6
SPIN	P	Fc	Unlim	Dc	Re	Energy
Directed diffusion	Q	Fc	Umlim	Dc	Re	Delay
EAR	Q	Fc	Umlim	Lc	Re	Delay
Rumor routing	Q, E	Fc	Umlim	Dc	Hybrid	Delay
LEACH	P	Fc	Two	Agg	Pro	Energy
PEGASIS	P	Fc	Unlim	Agg	Pro	Energy
TEEN	E	Fc	Three	Dc, Agg	Re	Energy
APTEEN	P, E	Fc	Three	Dc, Agg	Pro, Re	Energy
RPL	P	Fc	Unlim	Dc	Pro	Hops, delay

P: periodic, Q: query-based, E: event-based, Fc: full connected, Unlim: Unlimited, Dc: data-centric, Agg: aggregation, Lc: location-centric, Re: reactive, Pro: proactive

4 Suitable Routing Protocols for WSN dedicated to Airport Surface Area Surveillance

Up to now, we have highlighted the concept of ASAS in Section 2 and introduced some popular routing protocols in Section 3. This section is dedicated to select one or some routing protocols that seem suitable for the ASAS context at this point of the study. To achieve this objective, we use the classification introduced earlier and the special features of ASAS problematic.

Data collect mode Based on the information provided in Table 1, two types of data collect mode are required for an airport surveillance case:

- Event-based: presence of animals/intruders, pavement temperature, state of runway safety lights and all the attributes categorized as critical.
- Periodic: pollution, pavement temperature, taxiways flow rate.

All the routing protocols which are not exclusively based on query comply with this constraint.

Network topology As explained in section 2.3, a WSN deployed for the surveillance of an airport should be segmented in subnetworks. This implies the use of data mules or mobile sinks. So far, none of the reviewed protocols has been designed for this kind of topology. Nevertheless, some additional improvements have already been developed to incorporate the use of data mules in the routing protocols. These developments have been carried out by RPL [6] or LEACH [7].

Maximum number of hops The geometry of an airport platform implies some specific constraints for the WSN. For instance, some groups of nodes will follow runways, meaning that the topology will be linear. Thus, some paths between the sensor nodes and the data mules might contain a lot of hops. Therefore, only solutions that support unlimited number of hops can work in this context.

According to this, there is not a reviewed routing protocol that fits to all the properties of the ASAS case. However, some of them are close, particularly RPL that complies with the data collect mode, unlimited number of hops and can be enhanced to support data mules or mobile sinks. Moreover, RPL is the only protocol that has been standardized and indeed it is often used as reference by the research community. That's why, we start studing more deeply RPL as a potential solution of routing protocol in the context of ASAS based on WSN.

5 Conclusions and Further Works

In this paper, we provided a brief description of what is being done in the ASAS and the potential benefits of WSN applied in ASAS. We also provided a description and classification of the most popular routing protocols for WSN available in the literature. Our classification allowed us to identify that RPL is a routing protocol with potential to be implemented for ASAS, but that requires important changes. The main obstacle for implementation of RPL is that it is not suitable for segmented networks, which may often be the case of WSNs in airports. At this point, we will continue reviewing the state of the art about the use of data mule in WSN and work in RPL improvements to make it totally suitable for the ASAS case in WSN.

References

1. C Daniel Prather. *Current Airport Inspection Practices Regarding FOD (foreign Object Debris/damage)*, volume 26. Transportation Research Board, 2011.
2. Kemal Akkaya and Mohamed Younis. A survey on routing protocols for wireless sensor networks. *Ad hoc networks*, 3(3):325–349, 2005.
3. Yan Yu, Ramesh Govindan, and Deborah Estrin. Geographical and energy aware routing: A recursive data dissemination protocol for wireless sensor networks. 2001.
4. Shio Kumar Singh, MP Singh, and DK Singh. A survey of energy-efficient hierarchical cluster-based routing in wireless sensor networks. *International Journal of Advanced Networking and Application (IJANA)*, 2(02):570–580, 2010.
5. Nicola Accettura, Luigi Alfredo Grieco, Gennaro Boggia, and Pietro Camarda. Performance analysis of the rpl routing protocol. In *Mechatronics (ICM), 2011 IEEE International Conference on*, pages 767–772. IEEE, 2011.
6. Veena Safdar, Faisal Bashir, Zara Hamid, Hammad Afzal, and Jae Young Pyun. A hybrid routing protocol for wireless sensor networks with mobile sinks. In *Wireless and Pervasive Computing (ISWPC), 2012 7th International Symposium on*, pages 1–5. IEEE, 2012.
7. Saeid Mottaghi and Mohammad Reza Zahabi. Optimizing leach clustering algorithm with mobile sink and rendezvous nodes. *AEU-International Journal of Electronics and Communications*, 69(2):507–514, 2015.