Surveillance of sensitive fenced areas using duty-cycled wireless sensor networks with asymmetrical links

Ali Benzerbadj, Bouabdellah Kechar, Ahcène Bounceur, Mohammad Hammoudeh

PII: S1084-8045(18)30114-0

DOI: 10.1016/j.jnca.2018.03.027

Reference: YJNCA 2108

To appear in: *Journal of Network and Computer Applications*

Received Date: 3 August 2017

Revised Date: 6 March 2018

Accepted Date: 22 March 2018

Please cite this article as: Benzerbadj, A., Kechar, B., Bounceur, Ahcè., Hammoudeh, M., Surveillance of sensitive fenced areas using duty-cycled wireless sensor networks with asymmetrical links, *Journal of Network and Computer Applications* (2018), doi: 10.1016/j.jnca.2018.03.027.

Surveillance of Sensitive Fenced Areas Using Duty-Cycled Wireless Sensor Networks With Asymmetrical Links

Ali Benzerbadj[a,b,*], Bouabdellah Kechar[a], Ahcène Bounceur[b], Mohammad Hammoudeh[c]

[a] *Research Laboratory in Industrial Computing and Networks (RIIR), Department of Computer Science, Faculty of Exact and Applied Sciences, University of Oran 1 Ahmed Ben Bella, P.O. Box 1524 El M'Naouer, Oran, Algeria*
[b] *Université de Bretagne Occidentale, Lab-STICC UMR CNRS 6285, 20 Avenue Victor Le Gorgeu, 29238 Brest Cedex 3, France*
[c] *School of Computing, Mathematics & D.T., Manchester Metropolitan University, U.K*

Abstract

This paper presents a cross-layer communication protocol for Wireless Sensor Network (WSN) enabled surveillance system for sensitive fenced areas, e.g., nuclear/oil site. Initially, the proposed protocol identifies the boundary nodes of the deployed WSN to be used as sentinel nodes, i.e., nodes that are always in active state. The remaining nodes are used as duty-cycled relay nodes during the data communication phase. The boundary nodes identification process and data routing are both performed using an enhanced version of the Greedy Perimeter Stateless Routing (GPSR) protocol, which relies on a Non Unit Disk Graph (N-UDG) and referred to as GPSR over Symmetrical Links (GPSR-SL). Both greedy and perimeter modes of GPSR-SL forward data through symmetrical links only. Moreover, we apply the Mutual Witness (MW) fix to the Gabriel Graph (GG) planarization, to enable a correct perimeter routing on a N-UDG. Simulation results show that the proposed protocol achieves higher packet delivery ratio by up to 3.63%, energy efficiency and satisfactory latency when compared to the same protocol based on the original GPSR.

Keywords: Radio Irregularity, Link Asymmetry, Network Boundary Nodes,

*Corresponding author
Email address: `ali.benzerbadj@univ-brest.fr` (Ali Benzerbadj)

GPSR, Network Lifetime, Reliable Geographical Routing Protocol

1. Introduction

Wireless Sensor Networks (WSNs) are a class of wireless ad hoc networks. They consist of a set of battery-powered sensor nodes with limited hardware resources, i.e., memory, processing, radio range and bandwidth. Nowadays, they are extensively used in several domains such as military, health, environment, transport and agriculture etc. [1, 2, 3]. Their mission is to collect information from the physical world and to send it, through multihop communication, to a sink node that is connected to a remote decision system.

Surveillance is an attractive domain in which WSNs are increasingly used. However, surveillance applications require an energy-efficient and reliable design. On one hand, the monitoring scheme should be energy-aware in order to extend the network lifetime and, therefore, the duration of the surveillance mission. Indeed, batteries of sensor nodes can not be easily replaced due to the nature of such mission, which requires discretion and even stealth operation, the harsh environment in which the network is deployed or the scale of the deployment. On the other hand, the routing of the messages, from the source nodes, where the intrusion is detected towards the sink node, should be performed reliably to reduce data loss and ensure a high protection of the monitored area.

In this paper, we address the surveillance of sensitive fenced areas, e.g., oil or nuclear site, using WSNs with asymmetrical links. Asymmetrical links are the consequence of radio irregularity phenomenon [4]. It arises from multiple factors, such as antenna and medium type, and is accentuated by environmental factors such as obstacles, e.g., buildings, hills or mountains, and weather conditions.

To address the requirements of monitoring sensitive fenced areas, we propose a duty-cycled WSN protocol that is based on algorithms which rely on realistic assumptions about radio and consequently on their resulting Non-Unit Disk connectivity Graph (N-UDG), to route packets to the sink node. This protocol first identifies the nodes located on the fence of the sensitive area, called

Sentinel Nodes (SNs), using an algorithm based on a variant of the Greedy Perimeter Stateless Routing protocol (GPSR) termed GPSR over Symmetrical Links(GPSR-SL). SNs are maintained in active state throughout the duration of the surveillance mission. When an intrusion occurs, the SN that detects the intrusion generates an Alert Message (AM) and sends it towards the sink node. To save energy, the remaining network nodes, referred to as Duty-Cycled Relay Nodes (DC-RNs), are duty-cycled and used as relay nodes during the routing process of AMs. The duty cycling is done asynchronously [5, 6] using a Medium Access Control (MAC) protocol similar to B-MAC [7]. Secondly, the proposed surveillance protocol ensures a reliable routing process of AMs by the use of GPSR-SL, which enables reliable geographic routing on a N-UDG [8, 9, 10, 11]. Indeed, an AM is forwarded through symmetrical links only, using greedy, perimeter or a combination of the two routing modes allowed by GPSR-SL. Moreover, in order to overcome the perimeter routing failure resulting from the failure of the planarization algorithms [12, 13] when they are executed on a N-UDG, we use the Mutual Witness (MW) fix [12, 14].

The remainder of the paper is structured as follows. Section 2 presents the related work. Section 3 provides the targeted WSN system model and assumptions of the current study. Section 4 presents an overview of the original GPSR protocol. Section 5 details the GPSR-SL protocol. Section 6 describes the proposed surveillance protocol. Section 7 presents the simulation results. Finally, Section 8 concludes this paper.

2. Related Work

Energy saving and routing of AMs towards the sink are two key issues in the design of WSNs-based surveillance systems employed to secure sensitive fenced areas and international borders. Indeed, given that sensor devices are energy-constrained, energy conservation ensures the extension of the network lifetime and consequently the longevity of the surveillance mission. Furthermore, reporting of event detection to the sink must be done reliably to reduce false positives and true negatives. In this section, survey energy saving mechanisms and routing protocols used in such systems.

Kim et al. [15] proposed a WSN-based Fence surveillance System (WFS). The latter is expanded to connect and control network camera, Unmanned Ground Vehicles (UGV) and Unmanned Aerial Vehicles (UAV) in order to improve system accuracy. WFS is organized in three parts, ground and fence sensors, base station and subsystems (UAV and UGV). To achieve energy saving in the ground/fence WSN, the authors employed a sleep/awake mechanism for CPU, RF module and sensor modules. Furthermore, they utilized a hierarchical routing protocol to report the result of the collaborative detection performed by ground and fence sensors to the base station. WFS exhibits interesting features such as adaptation to dynamic changes of network topology and low power consumption. However, none of these features was verified experimentally, in simulation or test bed.

In [16], Sun et al. introduced BorderSense which is a 3-layered WSN architecture for border patrol systems (long strip-like monitoring area). It combines various types of sensors such as UGV/UAV, unattended ground/underground sensors and camera sensors, to improve the detection accuracy of border patrol systems. The main contribution of this paper is to describe a framework to deploy and operate BorderSense. The authors did not consider means of energy savings such as sleep/awake cycle or transmission power control to save energy in ground/underground WSNs. As regards the routing of multimodal data between the sensors of different layers when suspicious events are detected, they outlined communication protocols from literature on the basis of which they proposed communication solutions to enable a cooperative intrusion detection between the three layers of BorderSense. These proposed solutions were not evaluated, performance evaluation of BorderSense was left for future work.

Rothenpieler et al. [17] presented FlegSens which is a surveillance system for critical areas, e.g., borders or private properties. The system uses only simple passive infrared sensors for trespass detection. FlegSens's major focus is to ensure integrity and authenticity of AMs in the presence of an attacker who may even compromise a certain number of sensor nodes in the WSN. To extend the network lifetime, authors use a duty cycling protocol at the link layer to manage the duty cycles of nodes and minimize communications end-to-end delay. Furthermore, they used a flooding mechanism at the network layer to communicate detection of a trespasser towards a dedicated gateway. Flooding-based algorithms are not scalable, energy inefficient and do not ensure reliable delivery of AM.

An approach to mitigate the hole problem in WSNs-based surveillance applications is proposed in [18]. Holes are the result of intentional destruction of sensor nodes or death due to batteries depletion. Simulation results show that this sensor redeployment based mitigation approach extends the network lifetime and keeps its sensing quality above a certain threshold. The effect of three main factors on the sensing quality and the network lifetime are studied:

- density of the deployment
- intruder interarrival
- redeployment.

The authors have not considered the effect of asymmetrical links on the sensing quality and the network lifetime.

In [19], the performance of Ad hoc On Demand Distance Vector (AODV), Dynamic Source Routing (DSR) and Optimized Link State Routing (OLSR) protocols are compared in WSNs-based border surveillance applications. The comparison is made using delay, traffic load, packet loss, and energy consumption metrics. Simulation results have shown that DSR performs better than AODV and OLSR for a network with limited number of nodes. However, one of the drawbacks of DSR is that it relies on a network connectivity graph with symmetrical links. In fact, when a node knows a route to the destination, it sends a unicast Route REPly packet (RREP) to the source node via the reverse path of that it has learnt during the Route REQuest (RREQ) packets broadcast phase.

Bellazreg et al. [20] proposed a border surveillance system based on a heterogeneous WSN deployed along the border in the form of a thick line. The authors described a deployment strategy and a routing technique to ensure a good quality of coverage and efficient data exchange. However, the study focused on coverage and connectivity without giving any attention to energy consumption or reliability of links.

In [21], Hammoudeh et al. proposed a border-surveillance system based on Linear WSNs (LWSNs). Their system, based on flat and modular architecture, comprises a set of Basic Sensor Nodes (BSNs) which collaborate to detect and report events to a Monitoring Tower (MT) that is connected to a remote decision center. A cross layer communication protocol, referred to as Levels Division Graph (LDG), is designed to meet the requirements of LWSNs-based applications in terms of energy efficiency and end-to-end delay. LDG adjusts dynamically BSNs transmission power based on their network level, which is proportional to their distance from the MT, to achieve energy savings. Moreover, the authors proposed a mechanism of sleep/awake cycle to save more energy and reduce end-to-end delay. Furthermore, link selection in LDG algorithm is based on a cost metric which includes residual energy of the parent in the data routing tree, distance to reach it and the quality of the link between the two nodes. The latter is provided by the MAC layer based on the Received Signal Strength Indicator. The study did not specify how can a BSN reach a MT in the existence of asymmetrical links.

It is clear from the literature survey that there is no real attempt to address the link asymmetry issue, which has a negative impact on the performance of higher layer protocols. The deployment of WSNs in real environment necessitates new protocols that take into account this phenomenon to meet the requirements of WSNs-based surveillance applications including PDR, latency and energy consumption.

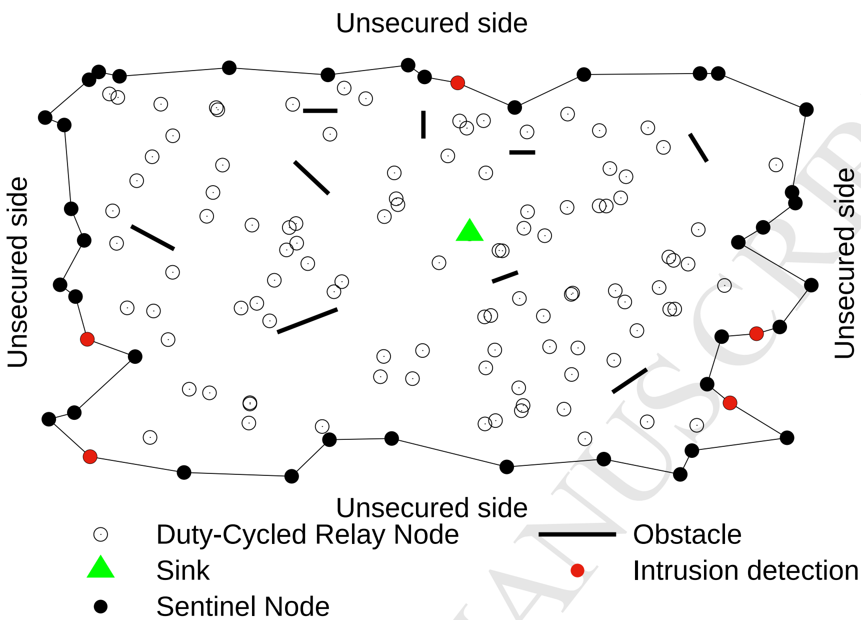


Figure 1: Surveillance model based on a Duty-Cycled WSN.

3. Network Model and Assumptions

We consider a static WSN, composed of N sensor nodes and one resource-rich sink, as depicted in Figure 1. Nodes are deployed uniformly at random to monitor a fenced sensitive area. We assume that the terrain is not obstacle free. Each node is aware of its own position, obtained through a Global Positioning System (GPS) or a localization approach [22, 23, 24, 25, 26]

The transmission ranges of nodes are irregular due to multiple factors, including, antenna and medium type, obstacles and weather conditions. Therefore, links between nodes may be asymmetrical and voids may be present in the network. We remind that voids may also exist due initial deployment irregularities.

In this study, the path loss between two nodes, which is due the distance between a Transmitter-Receiver (T-R) pair and to the presence of fading factors, is predicted using the log-normal shadowing model as defined in [27]:

$$PL(d) = PL(d_0) + 10 \times n \times log_{10}(\frac{d}{d_0}) + X_\sigma \quad (1)$$

where $PL(d)$ is the path loss in dB at the T-R distance d in meters, $PL(d_0)$ is the path loss in dB at a reference distance d_0 in meters, X_σ is a zero-mean Gaussian distributed random variable in dB with standard deviation σ in dB, and n is the path loss exponent. n indicates at which rate the path loss increases with the T-R distance. Table 1 shows the value of n in different environments. σ represents the shadowing effect. We note that in this study we do not consider the temporal variation of the path loss. If P_t is the transmitted power at T-R distance d, the received power $P_r(d)$ is expressed as follows:

$$P_r(d)[dBm] = P_t[dBm] - PL(d)[dB] \quad (2)$$

Table 1: Path loss exponent for different environments [27].

Environment	n
Free space	2
Urban area cellular radio	2.7 to 3.5
Shadowed urban cellular radio	3 to 5
In building line-of-sight	1.6 to 1.8
Obstructed in building	4 to 6
Obstructed in factories	2 to 3

The real connectivity graph of the network is noted as $G(V, E)$, where V represents the set of nodes and E is the set of edges representing connectivity between nodes. An edge (A, B), i.e., $A \rightarrow B$, exists between nodes A and B if and only if a message sent by A can reach B. We indicate the set of neighbors of a node u by $\mathcal{N}(u)$ and its set of neighbors that belong to its Gabriel Graph (GG) [28] by $\mathcal{N}_g(u)$. A GG is a planar graph, i.e., a graph in which no two edges cross. It is built from the initial network connectivity graph using either Algorithm 1 or Algorithm 2. We remind that a packet is forwarded over a GG, when using the perimeter mode of GPSR-SL protocol.

The neighborhood discovery stage takes place once sensor nodes have been initially deployed. Then, the identification phase of SNs starts. At the end of this phase, the duty cycle[1] of DC-RNs (nodes that have not been identified as SNs) is set to a value less than one and the surveillance process begins. Thus, when an intruder attempts to cross the network boundary, an AM is generated by the SN having detected the intrusion and forwarded towards the sink through symmetrical links using GPSR-SL. At the access level, we use an asynchronous contention-based MAC protocol (similar to B-MAC protocol) with a retransmission mechanism.

4. An Overview of the GPSR Protocol

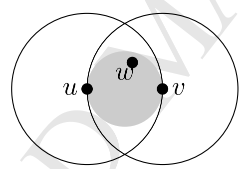


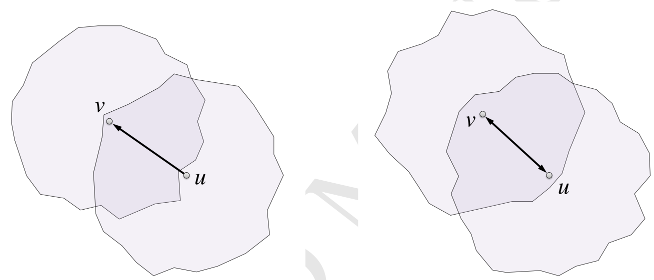
Figure 2: How to build GG [28]: when the network connectivity graph is modeled using UDG, the edge $uv \notin$ GG if there is a witness w in the shaded circle of diameter uv (see Algorithm 1).

The Greedy Perimeter Stateless Routing (GPSR) protocol is a well-known geographic routing protocol for wireless networks [28]. To forward a packet, GPSR combines a greedy routing method on the initial UDG and a perimeter routing. This perimeter routing is called face routing and it runs on a planar subgraph such as GG, which is built from the initial UDG as shown in Figure 2. Using the greedy routing, a node sends a packet to its geographically closest neighbor to the destination. Greedy forwarding fails when a packet reaches a node that has no neighbors closer to the destination than itself, due to the presence of voids in the network. This is known as the local maximum problem.

[1] $duty\ cycle = \frac{activity}{activity+sleep}$

In that case, the packet is routed using the perimeter mode, which forwards the packet to its final destination based on the well-known right hand rule [29], counter-clockwise along the faces of the planar subgraph that intersect with the line between the source and the final destination. Greedy mode resumes when the packet reaches a node that is closer to the final destination than the node that has initiated the perimeter mode.

Greedy and perimeter routing of GPSR are designed to work on a UDG, where links between nodes are symmetrical. Therefore, when the connectivity graph of the WSN is modeled as a N-UDG, they suffer from a number of problems.



(a) Asymmetrical link due to the radio irregularity (u can hear v but not vice versa).

(b) Symmetrical link (u can hear v and vice versa).

Figure 3: Radio irregularity gives rise to link asymmetry.

When using the greedy mode, the link between the forwarding node and the selected next neighbor may be asymmetric due the to the radio irregularity phenomenon as shown in Figure 3(a). Thus, the forwarding node will never receive an ACK from that neighbor even if it will try to retransmit the packet. Therefore, it drops the packet after a certain number of tries. Obviously, this leads to a waste of energy due to retransmissions, and to a low PDR in the case where the packet has been effectively lost. On the other hand, the link between the forwarding node and the next neighbor may be bidirectional, as depicted by Figure 3(b), but it may experience a high path loss. In this case, the packet will be likely lost due to the unreliability of the link or it will be necessary to retransmit it. This situation leads to reduction in PDR as well as increase in energy consumption and end-to-end delay.

As for the perimeter mode, it suffers from the failure of planarization algorithms. It has been shown that in presence of radio irregularity, these algorithms produce a subgraph that is a partitioned planar, planar with asymmetric links or not planar at all in which crossing edges are still present [12, 13]. These three pathologies lead to the failure of the perimeter routing. To overcome this routing failure on a N-UDG, several fixes have been proposed such as Mutual Witness (MW) [12], Cross-Link Detection Protocol (CLDP) [14], Lazy Cross-link Removal (LCR) [10] and Greedy Distributed Spanning Tree Routing (GDSTR) [30].

Algorithm 1 GG algorithm

Require: $\mathcal{N}(u)$.

Ensure: Edge (u, v) belongs to Gabriel Graph or not.

```
while v ∈ N(u) do
  while w ∈ N(u) do
    if (w = v) then
      continue {go to next node}
    else
      {m is the middle of the segment uv}
      if (distance(m,w) < distance(m,v)) then
        N_g(u) ← N_g(u) − {v}
        break {leave the current loop}
      end if
    end if
  end while
end while
```

Algorithm 2 GG algorithm with MW fix

Require: $\mathcal{N}(u)$.

Ensure: Edge (u, v) belongs to the Gabriel Graph of the node u or not.

while $v \in \mathcal{N}(u)$ **do**
  while $w \in \mathcal{N}(u)$ **do**
    if $(w = v)$ **then**
      continue {go to next node}
    else
      {m is the middle of the segment uv}
      if $((w \in \mathcal{N}(u)) \wedge (w \in \mathcal{N}(v)))$ **then**
        if (distance(m,w) $<$ distance(m,v)) **then**
          $\mathcal{N}_g(u) \leftarrow \mathcal{N}_g(u) - \{v\}$
          break {leave the current loop}
        end if
      end if
    end if
  end while
end while

Table 2: The structure of a Hello packet broadcasted by a node NI.

Field	Full name
NI	Node Identifier
NP	Node Position
NS	Neighbors Set (all nodes from which it can hear)

Table 3: Neighbor table of a node u.

Field	Full name
NGI	NeiGhbor Identifier
NGP	NeiGhbor Position
SYM	1 if the link $(u \rightarrow NGI)$ is symmetrical else 0
STATUS	1 if SN, else 0

5. Description of GPSR-SL Protocol

The Greedy Perimeter Stateless Routing over Symmetrical Links (GPSR-SL) is a variant of the original GPSR described in Section 4, which is suitable for N-UDG. The original GPSR has been modified as follows.

Firstly, we have added a link symmetry detection mechanism [31] which allows each sensor node to identify its symmetrical neighbors. During the neighborhood discovery stage, a node broadcasts its identifier, its position and its Neighbor Set (SN), i.e., all nodes from which it can hear, as shown by the structure of a Hello packet in Table 2. On the reception of a Hello packet, a node fills its neighbor table, as shown in Table 3, and checks whether its own identifier belongs to NS included in the Hello packet received. If it is the case, it marks the link, between itself and the node from which it receives the Hello packet, as symmetrical (SYM = 1). Otherwise, the link is marked as asymmetrical (SYM = 0)

Secondly, we have modified the greedy and perimeter modes of the original GPSR as described in Sections 5.1 and 5.2 respectively.

5.1. Greedy routing

Algorithm 3 Greedy routing of GPSR-SL.

Require: a packet p, $\mathcal{N}(u)$.

Ensure: next hop v if it exists, otherwise returns -1.

$d \leftarrow$ distance(u, p.SP)
$v \leftarrow -1$
while $w \in \mathcal{N}(u)$ **do**
  if link(u,w) is symmetrical **then**
    if distance(w, p.SP) $< d$ **then**
      $d \leftarrow$ distance(w, p.SP))
      $v \leftarrow w$
    end if
  end if
end while
return v

The greedy mode of the GPSR-SL forwards a packet based on two criteria, the distance and the link symmetry, as shown in Algorithm 3. The forwarding node chooses among its neighbors with whom it has a symmetrical link, the one that is geographically closest to the sink. Given that each node saves the coordinates of all its 1-hop neighbors in its neighbor table and the sink coordinates are included in the AM to forward (see Table 4), the forwarding node is indeed able to identify its geographically closest neighbor to the sink among its neighbors with which it has a symmetrical link. We remind that link symmetry detection is done during the neighborhood stage.

5.2. Perimeter routing

Unlike the greedy routing which is executed on the initial connectivity graph, the perimeter routing must be executed on a planar subgraph that is built from the initial graph, by removing crossing edges using planarization algorithms, e.g., GG planarization. These algorithms fail to produce a planar subgraph when the underlying network connectivity graph is a N-UDG [12, 13]. This

Table 4: Header fields of a packet p (NET layer) [28].

Field	Full name
PK	Packet Kind (AM or BDP)
FM	Forwarding Mode (Greedy or Perimeter)
SI	Sink Identifier
SP	Sink Position
PH	Previous Hop Identifier
I-NPF	Identifier of the Node where packet entered Perimeter mode for the First time
P-NPF	Position of the node having identifier I-NPF
LFP	Position of the point on the line between the source and destination packet entered current face
FE	First Edge traversed on current face

failure gives rise consequently to a perimeter routing failure. Several fixes have been proposed to overcome the failure of these algorithms, namely Mutual Witness (MW) [12], Cross-Link Detection Protocol (CLDP) [14], Lazy Cross-link Removal (LCR) [10] and Greedy Distributed Spanning Tree Routing (GDSTR) [30]. Among these proposed fixes, we have chosen to implement the MW fix due to its high message-efficiency [10] and ease of implementation. We remind that the MW fix applied to GG planarization is not enough to obtain a "safe" planar subgraph.

Perimeter routing of GPSR-SL runs on a planar subgraph obtained using GG planarization algorithm to which we apply the MW fix. The MW states that a node u eliminates the link (u, v) from the initial graph if there exists at least one witness, visible both to u and v, in the shaded circle of diameter uv depicted in Figure 2. In our case, this is achieved when nodes broadcast their neighboring tables (their NS), during the neighborhood discovery phase described in section 5, in order to identify the symmetrical links.

Every time a node u has to forward a packet, using the perimeter mode, to a node v among its neighbors with which it has a symmetrical link, it checks if the edge (u, v) belongs to its GG or not. If it belongs, the node v it becomes a candidate to be the next hop. Then, among all these candidate nodes, the next hop is chosen using the well-known right hand rule [28]. If the chosen edge (u, v) intersects with the line between the node where the AM enters the perimeter mode for the first time and the sink node, GPSR-SL protocol moves to the next face of the GG and continues the routing of the AM on that face.

6. GPSR-SL based surveillance protocol

In this section, we present the cross-layer surveillance protocol dedicated to the surveillance of sensitive fenced areas. Initially, the proposed protocol identifies the Network Boundary Nodes (NBNs) to be used as SNs during the surveillance process. Then, it ensures the routing of AMs generated by SNs, until the sink.

6.1. Identification of NBNs

When the neighborhood discovery stage ends, the sink node begins the discovery of NBNs through the creation and sending of a Border Discovery Packet (BDP) to a Fictitious Destination (FD). The latter is a sensor node which is disconnected from all other nodes of the WSN. We remind that the algorithm of identification of NBNs is inspired by the algorithm described in [32].

As illustrated in Figure 4, the sink projects its 2-D location on the four lines delimiting the deployment field, i.e., the fences of the monitored area. Then, it selects the closest point to itself among the obtained four points, to be the FD. Secondly, the sink creates a BDP (see Table 4), and sends it towards the FD using GPSR-SL protocol. Initially, the Forwarding Mode (FM) field of BDP is set to *Greedy*. As shown in Algorithm 4, each time the BDP is forwarded using the perimeter mode, the forwarder node identifies itself as SN and broadcasts this information to its neighbors. When the BDP returns back to the node where it is entered in the Perimeter mode for the First time (NPF), the discovery stage

Algorithm 4 The proposed communication protocol.

Require: a packet p, $\mathcal{N}(u)$, $\mathcal{N}_g(u)$.

Ensure: the forwarding of a packet p to a next hop v and the identification of NBNs.

```
if p.FM = “Greedy” then
    v ← greedy(p)
    if v = −1 then
        v ← perimeter(p)
    end if
else {FM = “Perimeter”}
    if dist(u, p.SP) < dist(p.P-NPF, p.SP) then
        p.FM ← “Greedy”
        v ← greedy(p)
        if v = −1 then
            v ← perimeter(p)
        end if
    else
        v ← perimeter(p)
    end if
end if
if v ≠ −1 then
    forwarding p to v
    if (p.FM = “Perimeter” and p.PK = “BDP”) then
        u identifies itself as SN and informs its neighbors.
    end if
else
    routing failure at node u
end if
```

of SNs stops. In fact, when the BDP returns back to that node (NPF), it is confirmed that all SNs have been identified, because the FD is disconnected from all other nodes and therefore the BDP will never reach it. Finally, the radio of the DC-RNs is duty cycled and the surveillance process is initialized.

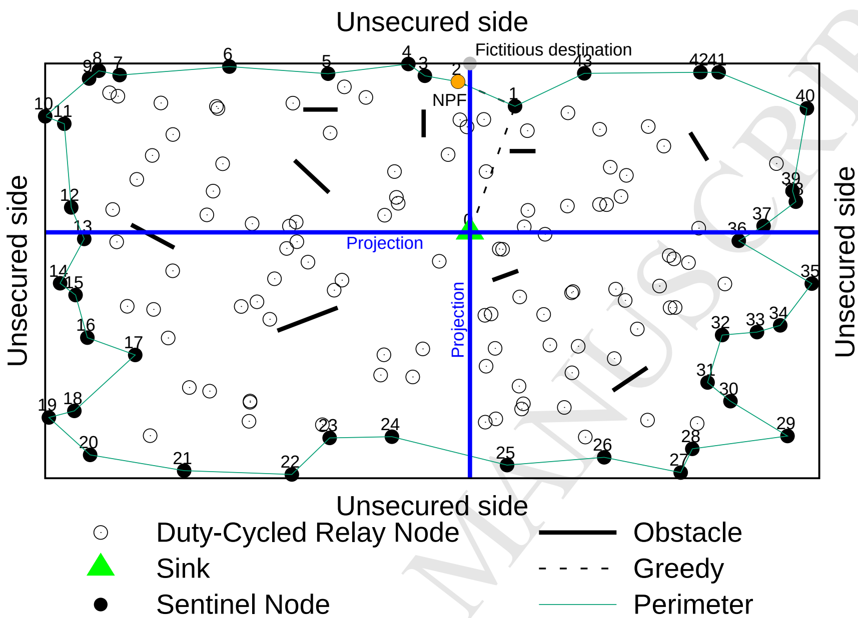


Figure 4: Network boundary nodes identification.

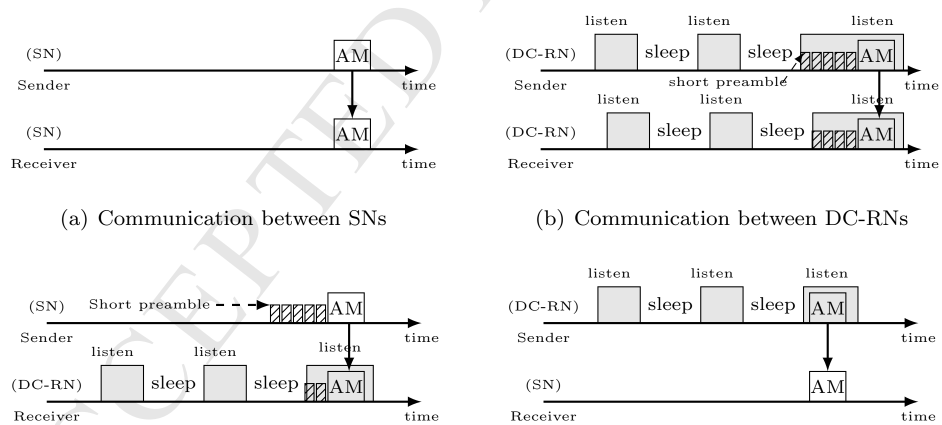
In the example shown in Figure 4, the sink node greedily sends a BDP to node 1, which is geographically the closest node to the FD represented with a gray color. Then, node 1 sends the BDP to its neighbor, node 2, which is the closest neighbor to the FD. Node 2 has no neighbors closest to the FD than itself. This node represents a local maximum, in which the BDP enters the perimeter mode for the first time.

Node 2, which is also called (NPF), changes the FM of BDP to *Perimeter* and forwards it to node 3, using the right hand rule. The BDP makes a complete tour counter-clockwise until reaching the node where it has entered the perimeter mode for the first time (NPF), namely node 2. At this moment, we are sure that all NBNs have been discovered.

6.2. Alert Message routing

Upon detecting an intrusion, the SN generates an AM and sends it towards the sink using a multi-hop routing protocol, as described by the network-layer Algorithm 4. The next hop is given by GPSR-SL protocol using, either greedy or perimeter mode. The greedy mode is executed on the initial network connectivity graph. It attempts to forward the AM, over symmetrical links, to the neighbor geographically closest to the sink.

As for perimeter mode, it requires a planar subgraph to forward the AM. In this study, we have used GG planarization algorithm to which we apply the MW fix (see Algorithm 2), to build a planar subgraph of the underlying initial network connectivity graph. We remind that the MW states that a node u eliminates the link (u, v) from the initial graph if there exists at least one witness, visible both to u and v, in the shaded circle of diameter uv depicted in Figure 2. The forwarding of the AM is done over the GG subgraph obtained, using the perimeter mode of GPSR-SL described in Section 5.2.



(a) Communication between SNs

(b) Communication between DC-RNs

(c) Communication between SN and DC-RN

(d) Communication between DC-RN and SN

Figure 5: Communication between two nodes at the access level (MAC layer) according to the status of the receiver node.

At the access level, the AM is sent using an asynchronous contention based MAC protocol (similar to B-MAC [7]). The communication between two nodes

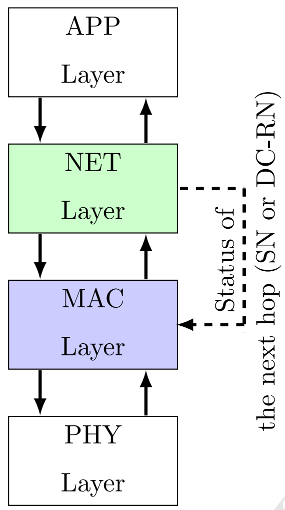


Figure 6: Illustration of the cross-layer design used.

is done based on the status of the destination node (SN or DC-RN) as depicted in Figure 5. In fact, if the receiver is a DC-RN, the sender transmits a series of short preambles, lasting as long as the sleep period of the receiver before sending the AM as shown in Figure 5(b) and Figure 5(c). However, in the case where the destination is a SN, the sender saves energy by transmitting the AM directly, since SN is always in active state; this is illustrated in Figure 5(a) and Figure 5(d).

The information about the status of the receiver is obtained by the MAC layer of the sender through a cross layer design which enables an interaction between the network and the MAC layers as shown in Figure 6. We recall that when a node identifies itself as SN during the NBNs identification stage, it broadcasts its status to its neighbors which store this information in their neighbor table (at the network layer).

7. Performance Evaluation

The performance of the presented surveillance protocol is evaluated through simulation under the Castalia simulator [33], which is based on the OMNeT++

platform [34]. We use three metrics, namely energy consumption, PDR and end-to-end delay to compare the performance of our GPSR-SL surveillance protocol with the GPSR surveillance protocol. We note that the interference management model implemented in Castalia simulator have been used in order to manage collisions in the network. The interference model is based on the Signal to Interference plus Noise Ratio (SINR) metric. In fact, when a sensor node receives several signals sent by multiple sources or due to the multi-path phenomenon, it accepts the one with the higher SINR. All results are averaged over 100 runs of 120 second simulated time each. We note that we vary the network topology during each simulation run, by varying the path loss between nodes, while the number and positions of the nodes remain unchanged. We remind that the path loss between two nodes is predicted using Equation (1) given in Section 3. Its variation is obtained by the variation of the shadowing effect represented by the zero-mean Gaussian distributed random variable with standard deviation σ, X_σ. Table 5 summarizes the most important parameters of the simulation.

7.1. Performance metrics

- Energy: Is the overall energy consumed during the simulation duration, computed according to the energy model provided by the Castalia simulator.
- PDR: Represents the ratio of the number of packets received by the sink to the number of packets generated by source nodes.
- Average End-to-end delay: Is the average elapsed time between the time of sending an alert by a source node and the time of arrival of this alert to the sink.

7.2. Results analysis

7.2.1. Effect of varying the length of the duty cycle

Figure 7 highlights the PDR according to the variation of the duty cycle length. Results show that the proposed surveillance protocol achieves higher

Table 5: Simulation parameters.

Parameter	Value
Simulation time	120 seconds
Terrain (not obstacle free)	$90\ m \times 90\ m$
Number of nodes	150
Network Topology per simulation run	100 (at each simulation run, the number and positions of the nodes are kept constant while the path loss between nodes varies)
Average number of NBNs	44
Average number of Alert Messages (AMs) sent	4.69, 9.19, 15.98
Deployment	Random
Number of sinks	1 (always in active state)
Battery capacity	18720 Joules
Propagation model	Log-normal shadowing
n	2.4
σ	4.0 dB
Radio	CC2420
Data rate	250 kbps
Radio sensitivity	$-95\ dBm$
TX power	0 dBm
Power consumption	TX: 57.42 milliWatt RX: 62 milliWatt
Network Layer	GPSR-SL, GPSR
MAC Layer	Tunable MAC (B-MAC like protocol)
Listen period	10 milliseconds
Number of retransmissions	0
Duty Cycle of SNs	1
Duty Cycle of DC-RNs	Ranging from 0.1 to 1.0 by step of 0.1
Interference management	Enabled

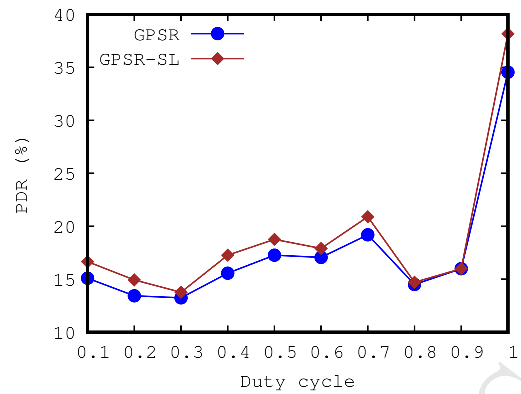
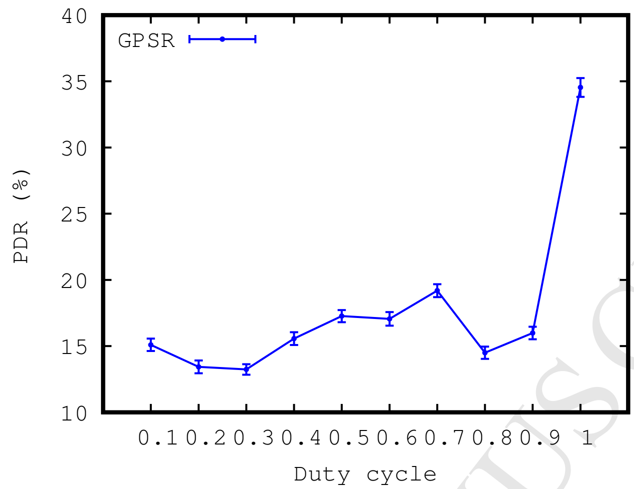


Figure 7: PDR according to the duty cycle (average number of AMs over the 100 simulations = 4.69, deployment area = $90m \times 90m$, total number of nodes = 150).

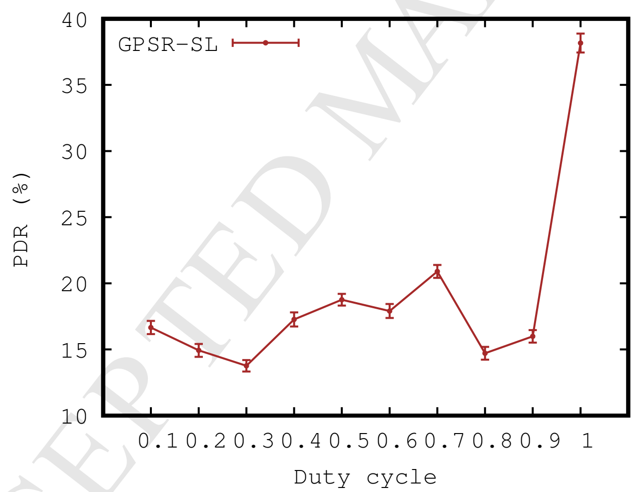
PDR when compared to the original GPSR. The PDR is improved under the different duty cycle lengths considered. The improvement is 1.32% on average. It reaches 3.63% when all the nodes of the network are maintained in active state. The high PDR allowed by the proposed protocol is the direct consequence of the use of reliable links, i.e., symmetrical links to forward the AMs. It is also due to the use of the MW fix, which enhances the performance of the perimeter routing on a N-UDG.

Figure 8 shows PDR plots with error bars, corresponding respectively to GPSR and GPSR-SL. We note that we have used a 99.73% confidence interval, i.e., 99.73% of simulation values fall within three standard deviations of the mean ($3^*\sigma$).

Figure 9 shows that GPSR-SL achieves energy conservation when compared to GPSR. Indeed, despite the fact that the PDR achieved by GPSR-SL is higher than that of the GPSR, the total energy consumption in the network when using GPSR-SL is almost the same than that resulting from the use of GPSR. The main reason is that GPSR-SL forwards AMs through symmetrical links, which are more reliable than asymmetrical links used by original GPSR. The waste of energy resulting from the use of GPSR is mainly due to the fact that packets are lost when they are forwarded through asymmetrical links. This re-



(a)



(b)

Figure 8: PDR with error bars according to the duty cycle (average number of AMs over the 100 simulations = 4.69, deployment area = 90m x 90m, total number of nodes = 150)

sult shows that GPSR-SL is able to achieve the same PDR as GPSR at lower energy expenditure. This makes GPSR-SL more suitable for long-term surveillance applications, which require low energy consumption in order to extend the

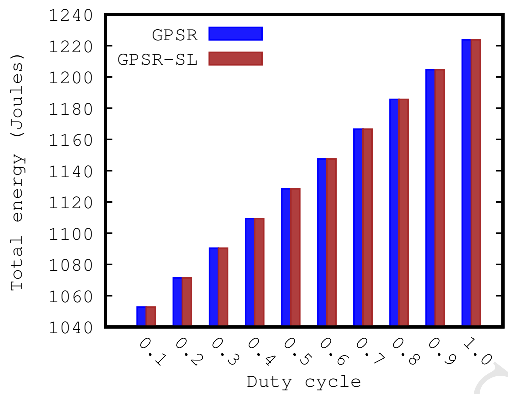


Figure 9: Total energy consumed according to the duty cycle (average number of AMs over the 100 simulations = 4.69, deployment area = $90m \times 90m$, total number of nodes = 150).

network lifetime and operate reliably.

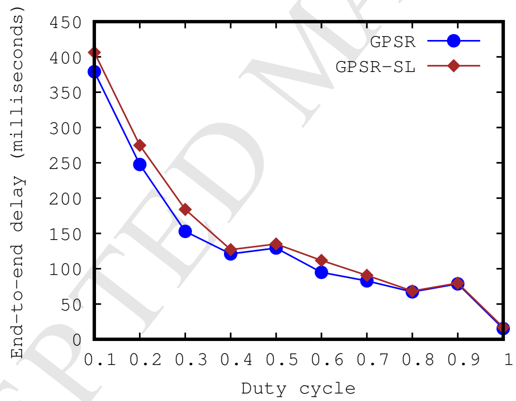


Figure 10: Average End-to-end delay according to the duty cycle, (average number of AMs over the 100 simulations = 4.69, deployment area = $90m \times 90m$, total number of nodes = 150).

Figure 10 shows the average end-to-end delay generated by the two studied protocols. It is observed in the figure that GPSR-SL achieves a reasonable average end-to-end delay under the different duty cycle, compared to GPSR. The slight difference ($\in$ [0.96 ms, 30.99 ms]) is due to the fact that the link between the forwarding node and the node geographically closest to the sink is generally not symmetrical. Therefore, the shortest path will not always be chosen by GPSR-SL leading to an increase in the hops traveled by an AM to reach the sink.

400 *7.2.2. Effect of increasing of the number of AMs*

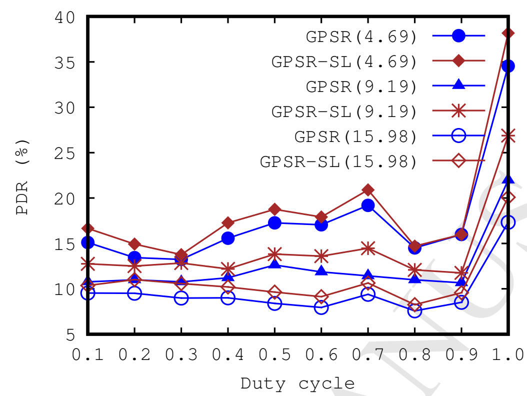


Figure 11: PDR according to the number of AMs, deployment area = $90m \times 90m$, total number of nodes = 150).

As depicted in Figure 11, the PDR achieved by GPSR and GPSR-SL decreases under the different duty cycle lengths considered, when the number of AMs increases. This is due to the interference resulting from the increase of concurrent transmissions. However, GPSR-SL achieves a higher PDR than GPSR,
405 since AMs are forwarded through symmetrical links which are more resilient to interference. This is a very interesting result since in surveillance applications, it is common for several intruders to cross the secured area at the same time (see Figure 1) from different places. Thus, several AMs will be generated and sent simultaneously towards the sink. In this case, our surveillance protocol based
410 on GPSR-SL will be able to forward more AMs to the sink. This is of prime importance in the process of monitoring of a sensitive area since it allows the remote decision system to react to a maximum number of AMs.

Figures 12 and 13, represent respectively the results of the two other metrics considered in this study. As can be seen in Figure 12, the total energy consumed
415 in the network, when using either GPSR or GPSR-SL, is almost the same. This

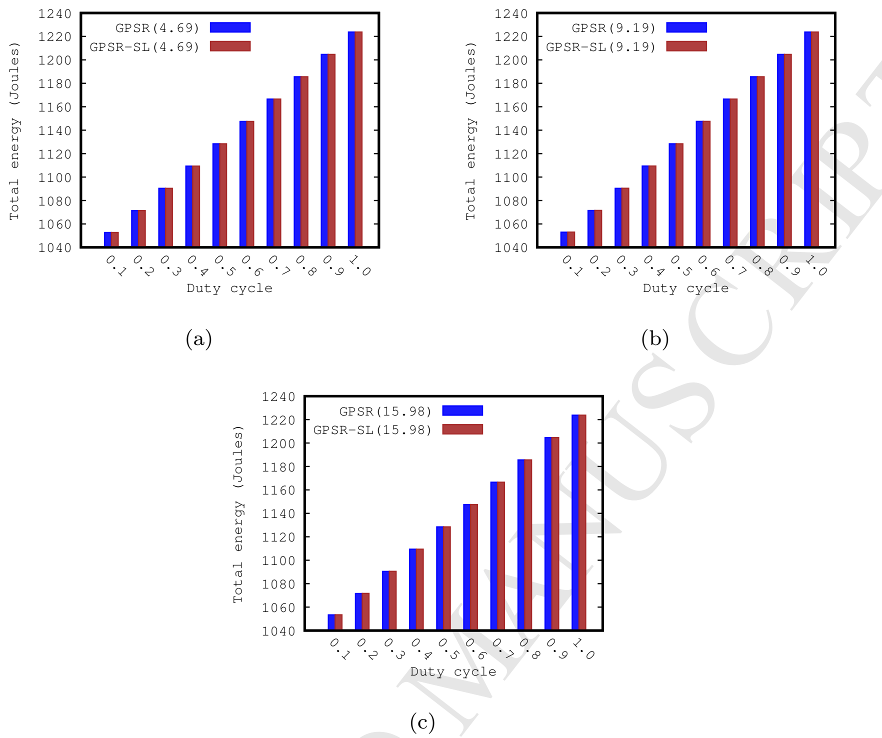


Figure 12: Total energy consumed according to the number of AMs, deployment area = $90m \times 90m$, total number of nodes = 150).

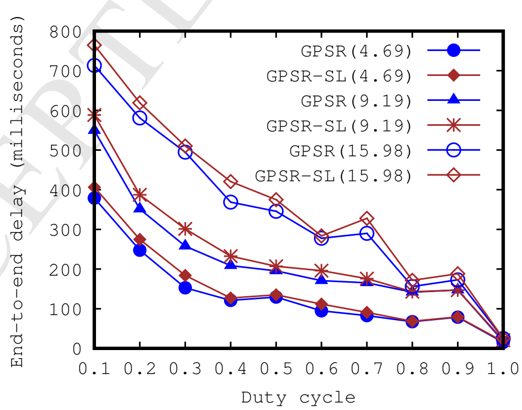


Figure 13: End-to-end delay according to the number of AMs, deployment area = $90m \times 90m$, total number of nodes = 150).

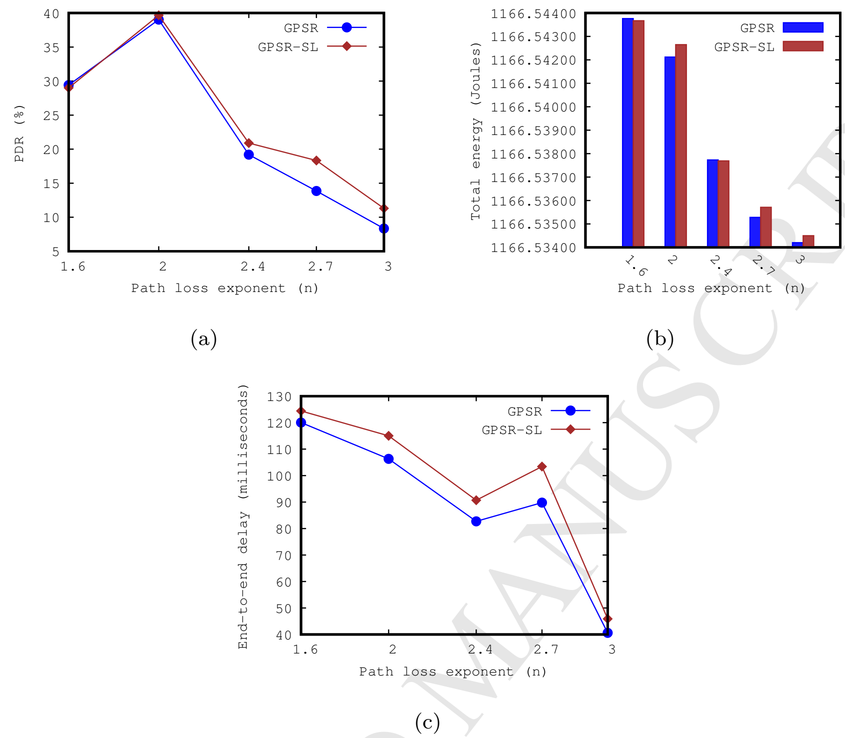


Figure 14: Simulation results of the three considered metrics, according to the path loss exponent (deployment area = $90m \times 90m$, total number of nodes = 150, duty cycle = 0.7 (70%), average number of AMs over the 100 simulations = 4.69).

confirms our analysis of energy consumption in Section 7.2.1. The end-to-end delay for both protocols increases also since nodes will increasingly (when AMs increase, as depicted in Figure 13) delay their transmissions due to interference created by the simultaneous transmissions. We notice that as can be seen in Figure 13, GPSR-SL achieves a reasonable end-to-end delay, compared to its rival GPSR.

7.2.3. Effect of varying the path loss exponent

Figure 14 (a) highlights the PDR according to the variation of the path loss exponent (n). The results show that GPSR_SL achieves a higher PDR when compared to the original GPSR. Figures 14(b) and 14(c) show respectively the effectiveness of GPSR-SL in terms of energy consumption and latency when it is compared to GPSR. Indeed, our proposed protocol enables energy efficiency and satisfactory latency. For example, for $n = 2.7$ the PDR_{GPSR_SL}= 18.34%, the energy consumed is 1166.53571 Joules and the latency is 103.40 milliseconds, while PDR_{GPSR}=13.86%, the energy consumed is 1166.53528 Joules and the latency is 89.8 milliseconds.

7.2.4. Effect increasing of the network density

Table 6: PDR achieved by GPSR_SL according to the duty cycle and number of sensor nodes.

Duty Cycle	PDR(GPSR_SL$_{(150)}$)	PDR(GPSR_SL$_{(250)}$)
0.7 (70%)	20.90%	20.67%
1.0 (100%)	38.17%	36.81%

As shown in Table 6, the increase of the number of sensor nodes leads to the decrease of PDR achieved by GPSR_SL, for the two considered values of the duty cycle (0.7 (70%)) and (1.0 (100%)). This can be explained as follows. When the network becomes dense, nodes are closer to each other and consequently links are more reliable. In such case, GPSR_SL maximizes the average hop count traversed by an AM. Indeed, GPSR_SL will choose short symmetrical links. Therefore the risk of collision and interference increases. The solution is to forward the AMs based on the trade-off between hop count and the quality of links (symmetrical links with the lowest path loss) in order to further reduce packet loss and retransmissions.

Table 7: PDR achieved by GPSR according to the duty cycle and number of sensor nodes.

Duty Cycle	PDR(GPSR$_{(150)}$)	PDR(GPSR$_{(250)}$)
0.7 (70%)	19.19%	18.29%
1.0 (100%)	34.54%	34.92%

As for GPSR (See Table 7), the variation is likely due to the increase of the node degree, i.e., $N(u)$ becomes more important and therefore a node u has much more candidate neighbors for the next hop. The new candidates for the next hop may be a factor of increase or decrease of PDR. We remind that the increase of the number of sensor nodes has no significant impact on the average hop count generated by GPSR since it continues to select the long distance links regardless of the node density (favors neighbors closer to the destination).

8. Conclusion and Future Work

This paper presents a surveillance cross-layer protocol for monitoring sensitive fenced areas under realistic terrain constraints, such as obstacles, and other unpredictable fading factors, e.g., interference, which lead to the radio irregularity phenomenon. The key point of the proposed GPSR-SL surveillance protocol is that it is based on algorithms, which take into account radio irregularities, by modeling the WSN connectivity-graph as a N-UDG. Experimental evaluation demonstrates the effectiveness of GPSR-SL in terms of PDR, energy consumption and end-to-end delay when it is compared to its rival GPSR. Indeed, the results show that the proposed protocols enables a high PDR without increasing energy consumption and while maintaining application-acceptable end-to-end delay compared to GPSR.

As an extension of the current work, we plan to make the NBNs identification algorithm robust against NBNs failures. We also plan to forward the AMs based on the trade-off between hop count and the quality of links (symmetrical links with the lowest path loss) in order to further reduce packet loss and retransmission rate. Another possible extension, to enhance both the PDR and the algorithm used for the identification of the network boundary nodes; this can be achieved through the enhancement of the performance of the perimeter mode of GPSR-SL by implementing other more efficient fixes of the planarization algorithms. Finally, we plan to secure the forwarding process of an AM towards the sink and the protocol robustness against malicious attacks such as jamming.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, Wireless sensor networks: a survey, Computer networks 38 (4) (2002) 393–422.

[2] P. Rawat, K. D. Singh, H. Chaouchi, J. M. Bonnin, Wireless sensor networks: a survey on recent developments and potential synergies, The Journal of Supercomputing 68 (1) (2014) 1–48.

[3] J. Yick, B. Mukherjee, D. Ghosal, Wireless sensor network survey, Computer networks 52 (12) (2008) 2292–2330.

[4] G. Zhou, T. He, S. Krishnamurthy, J. A. Stankovic, Models and solutions for radio irregularity in wireless sensor networks, ACM Transactions on Sensor Networks (TOSN) 2 (2) (2006) 221–262.

[5] P. Huang, L. Xiao, S. Soltani, M. W. Mutka, N. Xi, The evolution of mac protocols in wireless sensor networks: A survey, IEEE communications surveys & tutorials 15 (1) (2013) 101–120.

[6] P. Suriyachai, U. Roedig, A. Scott, A survey of mac protocols for mission-critical applications in wireless sensor networks, IEEE Communications Surveys & Tutorials 14 (2) (2012) 240–264.

[7] J. Polastre, J. Hill, D. Culler, Versatile low power media access for wireless sensor networks, in: Proceedings of the 2nd international conference on Embedded networked sensor systems, ACM, 2004, pp. 95–107.

[8] M. Z. Zamalloa, K. Seada, B. Krishnamachari, A. Helmy, Efficient geographic routing over lossy links in wireless sensor networks, ACM Transactions on Sensor Networks (TOSN) 4 (3) (2008) 12.

[9] F. Kuhn, R. Wattenhofer, A. Zollinger, Ad hoc networks beyond unit disk graphs, Wireless Networks 14 (5) (2008) 715–729.

[10] Y.-J. K. R. Govindan, B. Karp, S. Shenker, Lazy cross-link removal for geographic routing, in: Proceedings of the 4th international conference on Embedded networked sensor systems, ACM, 2006, pp. 112–124.

[11] L. Barriere, P. Fraigniaud, L. Narayanan, J. Opatrny, Robust position-based routing in wireless ad hoc networks with irregular transmission ranges, Wireless Communications and Mobile Computing 3 (2) (2003) 141–153.

[12] Y.-J. Kim, R. Govindan, B. Karp, S. Shenker, On the pitfalls of geographic face routing, in: Proceedings of the 2005 joint workshop on Foundations of mobile computing, ACM, 2005, pp. 34–43.

[13] K. Seada, A. Helmy, R. Govindan, Modeling and analyzing the correctness of geographic face routing under realistic conditions, Ad Hoc Networks 5 (6) (2007) 855–871.

[14] Y.-J. Kim, R. Govindan, B. Karp, S. Shenker, Practical and robust geographic routing in wireless networks, in: Proceedings of the 2nd international conference on Embedded networked sensor systems, ACM, 2004, pp. 295–296.

[15] Y. Kim, J. Kang, D. Kim, E. Kim, P. K. Chong, S. Seo, Design of a fence surveillance system based on wireless sensor networks, in: Proceedings of the 2nd International Conference on Autonomic Computing and Communication Systems, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2008, p. 4.

[16] Z. Sun, P. Wang, M. C. Vuran, M. A. Al-Rodhaan, A. M. Al-Dhelaan, I. F. Akyildiz, Bordersense: Border patrol through advanced wireless sensor networks, Ad Hoc Networks 9 (3) (2011) 468–477.

[17] P. Rothenpieler, D. Krüger, D. Pfisterer, S. Fischer, D. Dudek, C. Haas, A. Kuntz, M. Zitterbart, Flegsens-secure area monitoring using wireless

sensor networks, Proceedings of the 4th Safety and Security Systems in Europe.

[18] R. Kosar, I. Bojaxhiu, E. Onur, C. Ersoy, Lifetime extension for surveillance wireless sensor networks with intelligent redeployment, Journal of network and computer applications 34 (6) (2011) 1784–1793.

[19] H. Sharei-Amarghan, A. Keshavarz-Haddad, G. Garraux, Routing protocols for border surveillance using zigbee-based wireless sensor networks, in: International Conference on Computer Networks, Springer, 2013, pp. 114–123.

[20] R. Bellazreg, N. Boudriga, S. An, Border surveillance using sensor based thick-lines, in: Information Networking (ICOIN), 2013 International Conference on, IEEE, 2013, pp. 221–226.

[21] M. Hammoudeh, F. Al-Fayez, H. Lloyd, R. Newman, B. Adebisi, A. Bounceur, A. Abuarqoub, A wireless sensor network border monitoring system: Deployment issues and routing protocols, IEEE Sensors Journal.

[22] J. Hightower, G. Borriello, Location systems for ubiquitous computing, Computer 34 (8) (2001) 57–66.

[23] A. Boukerche, H. A. Oliveira, E. F. Nakamura, A. A. Loureiro, Localization systems for wireless sensor networks, wireless Communications, IEEE 14 (6) (2007) 6–12.

[24] N. Bulusu, J. Heidemann, D. Estrin, Gps-less low-cost outdoor localization for very small devices, Personal Communications, IEEE 7 (5) (2000) 28–34.

[25] G. Han, H. Xu, T. Q. Duong, J. Jiang, T. Hara, Localization algorithms of wireless sensor networks: a survey, Telecommunication Systems 52 (4) (2013) 2419–2436.

[26] A. Savvides, C.-C. Han, M. B. Strivastava, Dynamic fine-grained localization in ad-hoc networks of sensors, in: Proceedings of the 7th annual in-

ternational conference on Mobile computing and networking, ACM, 2001, pp. 166–179.

[27] T. S. Rappaport, et al., Wireless communications: principles and practice, Vol. 2, prentice hall PTR New Jersey, 1996.

[28] B. Karp, H.-T. Kung, Gpsr: Greedy perimeter stateless routing for wireless networks, in: Proceedings of the 6th annual international conference on Mobile computing and networking, ACM, 2000, pp. 243–254.

[29] Y.-J. Kim, R. Govindan, B. Karp, S. Shenker, Geographic routing made practical, in: Proceedings of the 2nd conference on Symposium on Networked Systems Design & Implementation-Volume 2, USENIX Association, 2005, pp. 217–230.

[30] B. Leong, B. Liskov, R. Morris, Geographic routing without planarization., in: NSDI, Vol. 6, 2006, p. 25.

[31] G. Zhou, T. He, S. Krishnamurthy, J. A. Stankovic, Impact of radio irregularity on wireless sensor networks, in: Proceedings of the 2nd international conference on Mobile systems, applications, and services, ACM, 2004, pp. 125–138.

[32] M. Aissani, S. Bouznad, A. Hariza, S. Allia, An effective mechanism for handling open voids in wireless sensor networks, in: Proceedings of the 5th International Conference on Sensor Technologies and Applications, 2011, pp. 24–29.

[33] Castalia, An OMNeT-based simulator for low-power wireless networks, https://github.com/boulis/Castalia (last visited on 04.01.2018).

[34] OMNeT++, Discrete Event Simulator, `http://www.omnetpp.org` (last visited on 04.01.2018).

Biography

Ali Benzerbadj is an assistant professor in the department of Mathematics and Computer Science-Institute of Sciences -University Center of Ain Témouchent, Algeria. He received a M.S degree (Magister) in Computer Science (Option : CAO/IAO & Simulation) from the University of Oran 1 Ahmed Ben Bella, Algeria, in 2012. He is a PhD candidate at final stage (Cotutelle between the University of Oran 1 and the University of Western Brittany (UBO), France). His current research interests include routing and MAC protocols in Ad-hoc Networks under realistic assumptions about radio.

Biography

Kechar Bouabdellah (kechar.bouabdellah@univ-oran.dz) is an associate Professor in the Department of Computer Science at Oran 1 Ahmed Ben Bella University, Algeria where he received his Ph.D. in 2010. He has authored several journal publications, refereed conference publications and book chapters. He has been a member of the technical program and organizing committees of several international IEEE/ACM conferences and workshops. He also serves as a referee of renowned journals such as IEEE Transactions on computers, IEEE Communications Magazine, IEEE Systems Journal and South African Journal of Science. His current research interests include IoT and big data technologies, mobile wireless sensor/actuator networks, Zigbee/IEEE 802.15.4 technologies deployment, Vehicular ad-hoc networks, vehicular sensor networks and heterogeneous wireless networks, with special emphasis on radio resource management techniques, performance modelling, provisioning QoS and practical societal and industrial applications. He has supervised and co-supervised several undergraduate graduate students in these areas. He has co-founded in 2011 the laboratory of industrial computing and networking (RIIR). He is currently head of a research team on wireless sensor networks and their societal and industrial applications.

Biography

Ahcene Bounceur is an associate professor (HDR and qualified for professorship) of Computer Science and Operations Research at the University of Brest (UBO). He is a member of the Lab-STICC Laboratory. He received a Ph.D. in Micro and Nano electronics at Grenoble INP, France in 2007. He received the M.S. degrees from ENSIMAG, Grenoble, France in 2003. From April 2007 to August 2008, he was a postdoctoral fellow at TIMA Laboratory. From September 2007 to August 2008, he was with Grenoble INP, where he was a temporary professor. He has obtained the 3rd place of the Annual IEEE Test Technology Technical Council (TTTC-IEEE) Doctoral Thesis Contest, Berkeley, May 2007. His current research activities are focused on : Tools for simulation of Wireless Sensor Networks (WSN) dedicated to Smart-cities and IoT, parallel models for accelerating simulations and predicting/testing parameters in WSNs, sampling methods for data mining and Big Data. He is the coordinator of the ANR project PERSEPTEUR and a partner of the eHealth project SUIDIA.

Biography

Dr Mohammad Hammoudeh is a Senior Lecturer in Computer Networks and Security in the School of Computing, Math and Digital Technology at the Manchester Metropolitan University. He received his Ph.D. in Computer Science from the University of Wolverhampton in 2009, his MSc (Distinction) in Advanced Distributed Systems from the University of Leicester in 2007, his BSc (Hons) in Computer Communications from the Arts, Sciences & Technology University in Lebanon in 2004, and a DipCompSci in Computer Information Systems in 2002. He is the co-founder and member of the FUture Networks and Distributed Systems research Group (FUNDS). He is the founder and head of the MMU IoT Lab. His research interests are in highly decentralised algorithms, communication, and cross-layered solutions to wireless sensor networks. He also has research interests in pervasive and mobile computing, specifically in Internet of Things. He has been researching and publishing work that focuses on big sensory data mining and visualisation. All his research projects are interdisciplinary, applied to real life problems. Latterly, his research focus is on the system design of distributed intelligent systems and their application within large-scale wireless sensor networks, including smart cities, border security and monitoring, flood detection and control, as well as waste tracking and management.


Mathemat
echnolog