Dissimulation-based and load-balance-aware routing protocol for request and event oriented mobile wireless sensor networks

Bournane Abbache, Sofiane Aissani, Mawloued Omar, Farah-Sarah Ouada, Nawel Yessad, Mohamed Azni, Abdelkamel Tari

To cite this version:

HAL Id: hal-03033814
https://hal.science/hal-03033814
Submitted on 1 Dec 2020
Dissimulation-based and load-balance-aware routing protocol for request and event oriented mobile wireless sensor networks

Bournane Abbache(1), Sofiane Aissani(1), Mawloud Omar(2), Farah-Sarah Ouada(1), Nawel Yessad(1), Mohamed Azni(1), and Abdelkamel Tari(1)

(1) Laboratoire d'Informatique Médicale, Faculté des Sciences Exactes
Université de Bejaia, 06000 Bejaia, Algérie.

(2) Unité de Recherche LaMOS, Faculté des Sciences Exactes
Université de Bejaia, 06000 Bejaia, Algérie.

Abstract

Mobile Wireless Sensor Network (MWSN) is a set of interconnected mobile sensor devices forming a dynamic network without a fixed administration. MWSN is used in various domains, such as disaster detection, medical systems, military applications, vehicular communications, and in other sensitive applications. Compared to the classical sensor networks, MWSNs involve an additional constraint consisting of the topology change frequency caused by the mobility of sensor devices. This influences highly the energy consumption and consequently the network reliability. In this paper, we take in charge this important issue and we contribute by the proposition of an efficient and energy-aware routing protocol. The proposed protocol operates for both request and event oriented MWSN applications. It introduces the sensor device mobility history in order to build-up stable routing paths, and incorporates a novel technique of dissimulation in order to exchange the mobility control messages without overhead. We have evaluated the performances of the proposed protocol through simulations, in which it provides effective results in terms of energy consumption and load-balancing.

Keywords: MWSN, Routing, Mobility, Dissimulation, Energy.
1. Introduction

The broad spectrum of Wireless Sensor Network (WSN) applications is already observable, especially in the emergent communication technologies such as the Internet of things and smart cities. WSNs are highly deployed in various domains of application such as fire detection, pollution supervising, industrial machine monitoring, medical remote diagnostics, military applications, etc. Nevertheless, WSN has specific characteristics, arising not negligible constraints, where the sensor devices are often deployed in inaccessible areas making them non-rechargeable. Unfortunately, their limited resources in terms of power, bandwidth, memory and processing, make the protocols used in conventional networks inappropriate. The protocols intended for WSN must be lightweight, with a low load of computation and communication overhead. The latter requirements allow saving implicitly the energy consumption, and consequently prolong the network lifetime.

Mobile Wireless Sensor Networks (MWSNs) extend the range of applications for other promising domains. Some of the applications, such as monitoring and tracking systems, require mobile sensor devices or sensor devices deployed on mobile agents. Mobility management in such networks becomes a challenging requirement. Network pre-configuration is insufficient, because links can be created or broken due to the mobility of sensor devices. The movement of the latter involves recurrent network topology changes and partitioning. There are also some other challenges [25, 24] addressed with the sink mobility.

To address the problem of routing, several solutions have been designed in the context of MWSNs. Most of them are based on the sensor devices location information or on the network flooding with control messages in order to determine the routing paths. Unfortunately, they present drawbacks, particularly in the energy consumption due to the communication load and GPS (Global Positioning System) overhead. As the classical WSNs, mobile sensor devices have a limited computation capacity, bandwidth and energy resource, and require lightweight routing solutions. They should guarantee efficient data delivery with respect to a low control transmission load in order to maximize the network lifetime. The energy consumption and the load-balancing [1] should be also addressed, which makes the routing protocol design more challenging. This paper addresses the latter issues and contributes with the following:

- An efficient and energy-aware routing protocol is proposed with mobility support.
- The proposed protocol is adapted to meet both request and event oriented MWSN applications.
- The proposed protocol takes in charge the sensor devices mobility history in order to select the most stable routing paths.
• The proposed protocol takes in charge the sensor devices signal strength and the number of times they are involved in routing to select the optimal routing paths increasing the network lifetime.

• The proposed protocol incorporates a novel technique of data dissimilation in order to exchange, without overhead, the mobility control messages.

The remaining of this paper is structured as follows. In Section 2 we review the literature. In Section 3 we present the detailed description of the proposed protocol. In Section 4 we analyze its performances with comparison to concurrent protocols. Finally, we conclude this paper in Section 5.

2. Related work

In the literature, various routing protocols have been proposed to meet the mobility requirements in the context of sensor networks. For more detail about the state-of-the-art please refer to [20, 21]. In this section, we review some relevant and recent routing protocols, which we classify into predictable and unpredictable mobility based protocols (cf. Figure 1).

![Figure 1: Classification of existing routing protocols in MWSNs](image)

2.1. Unpredictable mobility based protocols

In this category of protocols, several parameters are integrated in the data communication process with the aim to select the more stable next hop in order to take in charge the frequent network topology changing. The parameters are incorporated in the routing decision, such as the mobility speed and the localization information (e.g., signal strength and GPS). In what follows, we give a description of each protocol belonging to this category.

In [18], Intanagonwiwat et al. have proposed one of the most popular routing protocols, called Directed-Diffusion, which is adapted to both static and mobile sensor networks. Following this protocol, the sink broadcasts the request in the network. Upon receiving the request, the destination node returns back the required data using the best reverse routing path.
In [8], Umar et al. have proposed a State-Aware Link Maintenance Approach (SALMA). The protocol combines both reactive and proactive routing, namely Dynamic Source Routing (DSR) [16] and Optimized Link State Routing (OLSR) [17]. It uses DSR for the initial routes discovery and OLSR for the routes maintenance with the aim to avoid delayed data communication. The protocol introduces the sensor devices activeness in the network operations, where it divides them into three categories: aware and active sensor devices, aware but not performing the data transfer, and idle and do not keep any routing information.

In [9], Majid et al. have proposed an Energy efficient and Balanced Energy consumption Cluster based Routing Protocol (EBECRP) for the under water sensor networks. The aim of EBECRP is to improve the stability period, the network lifetime, and to reduce the load of the sensor devices, which are near to the sink. EBECRP is based on cluster-based architecture with mobile sinks, which change their positions frequently.

In [2], Saleh et al. have proposed a Multi-Aware Query Driven (MAQD) routing protocol based on a "neuro-fuzzy" inference system for MWSNs. The main purpose of MAQD is to route efficiently the data packets from specific/all mobile sensor devices based on a query delivered to the sink. MAQD considers four types of awareness: long-life-aware, delay-aware, total power cost, and shortest path. Based on the selected awareness type, a fuzzy inference system selects the proper routing path. MAQD operates in three phases: routes discovery phase, data reply phase and route maintenance phase.

In [15], Cugola and Migliavacca have proposed a Context and Content-Based Routing protocol (CCBR) designed for multisink-based MWSNs. CCBR is based on flat architecture with sensor devices mobility. It introduces a probabilistic receiver-based approach to route the data packets. Each sensor device decides forwarding the packets autonomously or loosely collaborating with other devices by keeping the routing information updated.

In [10], Hayes and Ali have proposed a Location-Aware Sensor Routing protocol (LASeR) for MWSNs. LASeR is based on a flat architecture with mobility of sensor devices. The routing uses location information to divide the monitored area into several circular areas with index locations. The principle of routing is based on the gradient. If the location index indicates that the packet comes from a node farther from the well, then it will be transferred. This inherently creates diversity of routes. If one of the routes were to fail, there would be others available to deliver the packet. LASeR provides reliable packet transmission. However, it floods the network during data transmission, furthermore duplication of data and reception overload by the receiver.

In [22], Hayes and Ali have proposed RASeR (Robust Ad-hoc SEnsor Routing), which is an improvement of [23]. It uses a technique of blind transmission to route the packets to the receiver. Both protocols use a MAC GTDMA (Global Time Division Multiple Access) to deal with the problem of gradient maintenance in a dynamic topology without having to flood the
network. However, instead of using data encapsulation, the packets are limited to a single piece of data. The authors propose a new packet structure, which reduces the storage size.

2.2. Predictable mobility based protocols

The protocols belonging to this category are based on mobility model that has specific rules to manage the sensor devices mobility. The mobility models that fall into this category can be random mobility and predefined mobility. In the former class, the mobile sensor devices move in a random direction that is changed periodically. In the second class, the mobile sensor devices depend on a specific movement direction [1]. In what follows, we give a description of each protocol belonging to this category.

In [4], Padmavati and Trilok have proposed LEACHDistance-M, where the selection of CHs (Cluster-Heads) is based on the upper threshold distance, lower threshold distance, residual energy and least mobility. LEACHDistance-M operates in two phases: the setup and the steady-state. In the first phase, a CH is elected and non-CHs are associated with that CH based on the maximum residual energy. The non-CH sensor devices compute the total residual energy of the CH’s cluster and select a sensor device as CH that has the maximum sum of residual energy. In the second phase, the non-CH sensor devices send the data to their CH, which aggregates and forwards them to the sink.

In [6], Ali et al. have proposed a Mobile Sink based Data Gathering Protocol (MSDGP). The sensor devices with more energy and amount of data are selected as CHs. The motivation behind the cluster formation is to extend the network lifetime by reducing the communication overhead. The data is stored unless the mobile sink comes within the transmission range of the CHs and requests for the aggregated data. Once the request is received, the CHs forward the data to the mobile sink.

In [5], Sharma et al. have proposed a rendezvous-based routing protocol for MWSNs. The protocol is based on flat architecture and focuses on the rendezvous region creation in the middle of the network followed by a tree construction within that region. The protocol introduces two different data transmission modes. In the first mode, the tree is directed toward the sink and the source sensor device transmits the data to the sink through this tree by selecting the closest backbone-tree. In the second mode, the source sensor device gets the sinks location from the tree and transmits the data directly to the sink. The source sensor device retrieves the sink location from the nearest backbone-tree sensor device.

In [7], Akbar et al. have proposed a Balanced Energy-Efficient Network Integrated Super Heterogeneous (BEENISH), improved BEENISH (iBEENISH), and some improvements including mobility for heterogeneous MWSNs. The protocol is a proactive and cluster-based architecture. It considers several energy sensor device levels and selects the CHs on the basis of residual energy and the average network energy in order to dynamically vary the CH selection.
mobile sink stops on its location and directly gathers data from sensor devices in order to avoid long-distance communication.

In [3], Burgos et al. have proposed a Leader-Based protocol for Routing (LBR) in MWSNs. The protocol is based on the leader sensor device election and the spanning tree construction by considering the sink mobility. It uses a measure of the link quality to maintain a reconfigurable spanning tree in the network graph. Two alternative variants of LBR have been implemented, namely LBR1 and LBR2. LBR1 uses a reactive and asynchronous forwarding mechanism to propagate leader election messages. LBR2 is based on periodic communication pattern.

2.3. An overall comparison and our contributions

The reviewed protocols are compared in Table 1 on the basis of multiple parameters, which includes the network architecture, path establishment, multipath and mobility support. For more information about the protocol details, kindly refer to its corresponding reference presented in the first column.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Architecture</th>
<th>Path establishment</th>
<th>Multipath</th>
<th>Mobility</th>
</tr>
</thead>
<tbody>
<tr>
<td>[18]</td>
<td>Flat</td>
<td>Reactive</td>
<td>Yes</td>
<td>Fully</td>
</tr>
<tr>
<td>[8]</td>
<td>Flat</td>
<td>Hybrid</td>
<td>Yes</td>
<td>Sensor devices</td>
</tr>
<tr>
<td>[9]</td>
<td>Cluster-based</td>
<td>Proactive</td>
<td>No</td>
<td>Sink</td>
</tr>
<tr>
<td>[15]</td>
<td>Flat</td>
<td>Proactive</td>
<td>Yes</td>
<td>Sensor devices</td>
</tr>
<tr>
<td>[5]</td>
<td>Flat</td>
<td>Hybrid</td>
<td>No</td>
<td>Sink</td>
</tr>
<tr>
<td>[7]</td>
<td>Cluster-based</td>
<td>Proactive</td>
<td>No</td>
<td>Sink</td>
</tr>
<tr>
<td>[3]</td>
<td>Flat</td>
<td>Reactive</td>
<td>No</td>
<td>Fully</td>
</tr>
<tr>
<td>[10, 22]</td>
<td>Flat</td>
<td>Reactive</td>
<td>Yes</td>
<td>Sensor devices</td>
</tr>
</tbody>
</table>

In most application fields, some sensor devices can be frequently in motion, and sometimes with a relatively high speed. In the routing process, this type of sensor devices should be avoided in the path selection, because they can disturb the stability of routes by involving frequent control data exchange, and hence more consumption in terms of energy. This issue is not addressed by the existing protocols in the literature. Moreover, due to the limited local view of the sensor devices, the existing solutions lack precision about the individual load of each sensor device in the routing process. This involves an imbalance in the routing load, which in the long term jeopardizes the network lifetime. The problem of load-balancing in MWSN is a challenging issue, which remains open even with the huge effort devoted in the literature. The communication overhead is also an open issue, where the existing solutions spend a considerable part of energy when exchanging the control data packets. The proposed protocol faces all of
these issues. We introduce the notion of mobility history in order to select the most stable routing path. The proposed protocol takes into account the signal strength and the number of times the sensor devices are in charge of routing. In order to deal with the communication overhead, the proposed protocol exploits the unused coding space in the packet fields, where it embeds without communication overhead the control data. The proposed protocol operates into two scenarios, namely request-oriented with a reactive routing and event-oriented with proactive routing.

3. The proposed protocol

In this section, we give the detailed description of the proposed protocol. We present first the proposed dissimulation technique, which allows the sensor devices to communicate the mobility information to the sink without overhead. Then, we present the different steps of the proposed routing solution.

3.1. Dissimulation

The IEEE 802.15.4 standard defines two functioning modes in MWSNs: beacon mode and non-beacon mode. In the beacon mode, the network operates by a periodically sending beacon frames to synchronize and exchange control information among the sensor devices. The non-beacon mode is generally used for sensor devices that sleep most of the time, and when an event happens, they wake up instantly and send an alert frame. In the context of our work, the proposed protocol operates in beacon mode.

The idea of the dissimulation consists exploiting the beacon frames, which are part of the network functioning, in order to embed important control information. Instead of overloading the network with additional control messages, we dissimulate the control data in the unused coding space of the messages that are compulsorily transmitted. This part of the proposed protocol allows to reduce considerably the communication overhead, and hence saving the energy consumption. The dissimulation is not an independent service provided by the network. This process is an important part of our contribution, which is implemented through the proposed protocol itself. Instead of inserting the control data as a separated bloc of information, the proposed protocol embeds it without any communication overhead, which sets the proposed protocol apart from the literature. In this context, we distinguish one main difference, which is about the stack layer, where the proposed protocol can be directly implemented whatever the used standard. In contrary to the existing solutions, most of them calculate the necessary size of data packets or tags without considering the existing packet format. In the following, we give an overall analysis to show the applicability of this concept with respect to two concrete communication technologies.
The most important transmission protocols in sensor networks are surveyed in [11]. Compared to the other network technologies, MWSNs are often targeted for data with lightweight sizes (e.g., humidity, soil moisture, and temperature). We notice that ZigBee [13] and WiFi [14] are often used in MWSNs. That’s why we limit the scope of this analysis to the latter cited standards. Furthermore, the proposed protocol does not depend on any specific communication standard or standardized MAC/routing approach. It complies with any format of communication standard packets. Wi-Fi and ZigBee are presented just as illustrative examples in order to explain the ideas behind the proposed solution.

WiFi and ZigBee include four types of frames, namely the command, beacon, data and acknowledgment frames. In the context of our work, we focus on the dissimulation in the data link layer, which is common to the considered standard. The general form of these types of frames in the data link layer contains several fields, namely the frame control, checking errors, addresses, sequence control and range. Figure 2 and 3 illustrate how the fields are exploited following, respectively, the WiFi and ZigBee standard.

<table>
<thead>
<tr>
<th>2 byte</th>
<th>2 byte</th>
<th>6 byte</th>
<th>6 byte</th>
<th>6 byte</th>
<th>2 byte</th>
<th>6 byte</th>
<th>4 byte</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ctrl frame</td>
<td>Duration</td>
<td>Adr1</td>
<td>Adr2</td>
<td>Adr3</td>
<td>Ctrl sequence</td>
<td>Adr4</td>
<td>CRC</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2 byte</th>
<th>2 byte</th>
<th>log₂(n) byte</th>
<th>log₂(n) byte</th>
<th>6 byte</th>
<th>log₂(ilm/2312) byte</th>
<th>6 byte</th>
<th>4 byte</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ctrl frame</td>
<td>Duration</td>
<td>Adr1</td>
<td>Adr2</td>
<td>Adr3</td>
<td>Ctrl seq</td>
<td>Adr4</td>
<td>CRC</td>
</tr>
</tbody>
</table>

Figure 2: Exploitable fields in WiFi

The frame control field is non-exploitable because it contains necessary information, such as the frame type, the protocol version and other important control flags. Also, the frame check and the frame check sequence fields are non-exploitable because they check the presence of transmission errors. The dynamism of data space allocation does not allow to exploit these fields. However, the addresses, the sequence number and the radius/range fields depend on the network size, the observed phenomena data size and the maximal size of the data that can be transmitted.

In the context of our work, each sensor device is assigned a logical address linked to its physical address, where the sink holds the global table of correspondence. The ZigBee radius field and the WiFi range field denote the maximum hop number that a packet can travel. In
the worst case, the packet crosses all the network sensor devices. We notice that the network size is proportional to the possible hop number. The exploitable coding space is decreased when increasing the sensor device number.

The control sequence field in WiFi contains two sub-fields, namely the fragment control and the sequence number. The latter is exploitable, because it is used to reorder the frames of the same packet at the reception. The frame number depends on two parameters: the maximal frame data size and the sensed data size. In most of the MWSN applications, the data size is lightweight, and hence, the sequence number field can be efficiently exploited.

Figures 4 and 5 summarize the total exploitable coding space for dissimulation regarding, respectively, ZigBee and WiFi as a function of the sensed data size and the network size. This analysis denotes the applicability of the proposed dissimulation approach in the case of MWSNs. Whatever the used standard, a considerable coding space could be exploited in order to exchange control messages without overhead. As illustrated in Figure 6, the control message is sent end-to-end through dissimulation over the beacon frames until reaching the sink. The message contains the identities of the neighbors having either join or leave the sensor device communication range. This information is necessary for the sink in order to compute the best routing path. In what follows, we present the details of the routing approach.

### 3.2. Routing process

We consider a MWSN including a set of sensor devices deployed on a monitored area, administered by a single sink having no restraints on storage, computation and energy. The sensor devices are not supposed homogeneous in terms of hardware characteristics (storage, battery, processing, transmission, etc.). The sink is stationary, however the sensor devices are completely mobile. With the proposed protocol, the sensor devices are not involved in the routing path.
Figure 4: Exploitable coding space in ZigBee

Figure 5: Exploitable coding space in WiFi
selection process, where the sink is in charge to determine the best routing path. To do this, the sink operates first to recover the complete view of the network topology with the different signals strength among the sensor devices. The sink computes the optimal routing path depending on its network topology view and the load of each sensor device. This way, it equalizes the routing path usage to balance the sensor devices energy consumption. The proposed protocol operates under three components, namely (1) the network discovery, (2) the routing paths selection and mobility management, and (3) the data routing. In what follows, we describe each component with respect to both request and event oriented MWSN applications.

3.2.1. Network discovery

This step is common to both request and event oriented MWSN applications. The main purpose of this step is the construction of the initial overall network topology view by the sink. The initialization process is carried out only once in the network bootstrapping step. In highly dynamic scenarios where the sensor devices having to stop moving, the initialization process will not be executed again. The sensor device mobility presents no constraints against this process execution. The required time of initialization messages exchanging is negligible compared to the physical mobility of sensor devices. The message propagation is performed through electromagnetic waves, which follows the light speed. Hence, at the instant of execution of this step, the sensor devices have no enough time to physically move. After the network deployment, each sensor device sweeps around through a hello packet using its maximal power range. Upon receiving the packet from its neighbors, each one estimates and saves its neighbor devices signal strength. Then, it creates a neighboring list containing each neighbor, its identity and signal strength. Finally, it broadcasts by dissimulation the neighboring list using its own maximal power range to the sink in order to constitute the overall view of the network topology. The maximal power range information gives to the sink more precision in the view construction since the communication is not supposed symmetric between the neighboring devices. If a sensor
device $\vartheta_i$ is in the communication range of $\vartheta_j$, this does not imply systematically that $\vartheta_j$ is in the communication range of $\vartheta_i$. The network discovery step is associated to a threshold $T$. $T$ is the required time for a sensor device to decide waiting for any more possible replies from its neighbors or not. This time is the same for all the sensor devices and its value depends on the application area requirements (network density, transmission rate, etc.). Each sensor device compares its timer $t$ to the threshold $T$, and the network discovery step is considered achieved when $t$ exceeds $T$. Finally, the sink maps the overall view of network topology. Figure 7 illustrates the flowchart of the network discovery step.

![Network discovery flowchart](image)

Figure 7: Network discovery flowchart
3.3. Routing paths selection and mobility management

This step is also common for both request and event oriented MWSN applications. The optimal routing path is computed by the sink when it requires a specific data (respectively, for a future event) from a given sensor device. Then, the routing path is sent to its corresponding sensor device. The determination of the optimal routing path is an important phase to optimize the network lifetime. The path computation is performed by the sink, which takes into account three important parameters, namely the neighbor signal strength, the mobility history and the number of times a sensor device has participated in the routing process. This information is obtained from the network topology view that is updated by the sink through the dissimulated mobility control messages. The sink explores the network topology view and then determines the best routing path leading to the destination based on the quality of the intermediate sensor devices. In order to increase the network lifetime, the sink balances the routing load among all the sensor devices. The load balancing is ensured through the routing path selection process, which makes it possible to diversify the routes that lead to the different destinations in the network. The sink performs this process, where the sensor devices are discharged with the aim to preserve the energy consumption. To achieve that, the sink maintains for each sensor device \( \vartheta_i \) its corresponding load factor, denoted by \( L_i \). When a sensor device \( \vartheta_i \) participates in routing, the sink increments \( L_i \).

Figure 12 illustrates the flowchart of the routing process with mobility support for both event and request oriented scenarios. The mobility has a significant impact on the topology change and implicitly on the selected routing path stability. For this purpose, we incorporate a module of mobility monitoring. This module allows the logging of the movement made by the different sensor devices. In this context, we distinguish two types of mobility that could be considered in MWSNs, namely the controlled and uncontrolled mobility patterns. The controlled mobility assumes that each sensor device is equipped with a mobilizer, which is controlled by the sensor itself. The uncontrolled mobility assumes that the sensor devices are unable to move independently. In some applications, the sensor devices are deployed on mobile agents (e.g., human body, vehicles, and animals) assisting them in the movement. This type of movement is uncontrollable and generates random trajectories and placements.

The presented mobility types do not present constraints regarding the proposed protocol. In the case of controlled mobility, the sink can automatically prevent the movement of sensor devices, because the speed and trajectory information are known by the sensor device and the sink, which allows the latter to update the network topology view dynamically and efficiently. In the case of uncontrolled mobility, the proposed protocol operates as follows. The quality of the link and the received signal strength from a neighbor device are mobility-sensitive parameters. The mobility of a sensor device is modeled through the quality of the radio signal strength generated by its neighbors. When a sensor device moves, its movement weakens the signal...
reception for some neighbors and strengthens it for others. The movement may also break or create other communication links. The sink requires this important information in order to update its overall view of network topology, and also to select the most stable sensor devices in the routing paths.

The optimal routing paths are selected by the sink through the network topology view, using the neighboring information sent by the sensor devices. The event that affects the network topology view is the link breaking and creation. When one of these events are perceived, the sink is alerted in order to update the network topology view, as well as the underlying optimal routing paths. The topology change history represents the past mobility of each sensor device. We represent the mobility history by a table containing the mobility index of each sensor device, that indicates the number of times has created or broken a communication link. If a sensor device moves and loses contact to another one, both of them alert the sink about the movement of each other. In this case, the sink updates the mobility index of both sensor devices. For instance, let’s consider the scenario illustrated in Figure 8. We have a network of size 4, where the sensor device 1 moves and loses contact to all the others. In this case, the mobility history will evolve from \((0, 0, 0, 0)\) to \((3, 1, 1, 1)\). Finally, the sensor device 1 has the greatest mobility index, representing the less stable sensor device in the network.

It is essential to emphasize that is not necessary getting with precision which sensor device has been moved. The sensor devices with least stable links will have a high mobility index, and they will be disadvantaged in the optimal routing path selection. This is typical in the case of sensor device group movement. For instance, let’s consider the scenario illustrated in Figure 9. We have a network of size 4, where the sensor device 1 moves and loses contact to all the others. In this case, the mobility history will evolve from \((0, 0, 0, 0)\) to \((3, 1, 1, 1)\). Finally, the sensor device 1 has the greatest mobility index, representing the less stable sensor device in the network.
devices 2, 3 and 4 have more stable links between each other compared to the sensor device 1.

The movement detection is performed through the exchanged beacon messages sent at each unit of time. A sensor device considers that a link is broken with its neighbor, if it no longer receives its beacon messages. A sensor device is considered in movement if at least one link is created or broken. In the case of motion detection by a sensor device, the latter communicates this information to the sink through the dissimulation process. The latter maintains for each sensor devices \( \vartheta_i \) its proper mobility history, denoted by \( M_i \). At each link creation or breaking by \( \vartheta_i \), the sink increments \( M_i \). The mobility history does not change according to the signal strength. Therefore, if the sensor device moves without creating and/or breaking links, the mobility history will not be affected. However, the signal strength could be used for movement prediction. The mobility history parameter is involved in the routing path selection in order to disadvantage the selection of routing paths including intermediate sensor devices in continuous mobility. From the overall view of network topology, the sink explores the neighbors gradually until to spread a given sensor device. Finally, the sink identifies the best routing path including a set of intermediate sensor devices \( \vartheta_i \), which optimize the signal strength \( S_i \), the load factor \( L_i \) and the mobility degree \( M_i \). The trade-off between the latter parameters is maintained by an objective function \( \mathcal{F} \), where the best routing path \( r^* \) is selected such that
\[ F(r^*) = \max_{k=1}^{l} \left( S_{\min}(r_k) \cdot L_{\min}(r_k) \cdot M_{\min}(r_k) \right), \]  

(1)

where \( l \) is the number of available routing paths, \( S_{\min}(x) = \min(S_1, S_2, \cdots, S_{|x|}) \), \( L_{\min}(x) = \min(L_1, L_2, \cdots, L_{|x|}) \), and \( M_{\min}(x) = \min(M_1, M_2, \cdots, M_{|x|}) \).

Once the best routing path is selected, the sink constitutes and transmits an announcement packet, denoted by \( \mathcal{A} \), which contains for each sensor device \( \vartheta_i \) its best routing path \( r_i^* \). This operation is illustrated on Figure 10. The best routing path is used by the sensor device in order to communicate its forthcoming data packet. The packet \( \mathcal{A} \) is structured as

\[ \mathcal{A} = (\vartheta_1, r_1^*) \parallel (\vartheta_2, r_2^*) \parallel \cdots \parallel (\vartheta_n, r_n^*). \]  

(2)

At packet reception from a sensor device \( \vartheta_i \), the sink recomputes the routing paths for all the network sensor devices. It re-explores the network topology, computes the new best routing paths and updates the precedent ones.

The routing path is sent to its corresponding sensor device by the sink. Hence, before holding such a routing path, there is no sink-to-node routing mechanism, and all the sensor devices can communicate directly with the sink.
devices do not know how to reach each other. The sink in one-hop communication performs the dissemination of the routing paths to the sensor devices. We believe this is not a hard assumption, due to the today advanced wireless technology (e.g., WiMax can reach about ten kilometers of range communication). Furthermore, the proposed protocol is a generic solution and does not rely on a particular addressing scheme. Moreover, multiplying the number of radio communication interfaces is not required for the proposed protocol. However, depending on the application domain, if is required more than a radio communication interface on each sensor device, this has no impact on the proposed protocol operations. Besides, the proposed protocol is quite adapted for several types of application. For instance, wireless body area networks can be considered as an illustrative field of application. The sensor devices are deployed in the human body, such as the sink (smart-phone, smart-watch, etc.) can reach each one of them in one-hop without needing to deploy several radio communication interfaces on the devices. It is important to notice that during the transmission, the signal amplification involves a considerable part of energy consumption. Therefore, it is primordial that the data passes through a routing path, by adjusting in hop by hop the communication range of the intermediate sensor devices. This way, the latter devices save their energy resources and distribute the data transmission load among the other sensors.

We notice that the routing path transmission happens just when the sink receives a data packet from a given sensor device. Each sensor device checks the field corresponding to its identity. If it is concerned by the change, the new routing path replaces the old one. A given sensor device \( \vartheta_i \) could be aware that it is not concerned if \( r^*_i = \emptyset \). For example, considering the announcement \( \mathcal{A} = (\vartheta_1, \emptyset) \parallel (\vartheta_2, r^*_2) \parallel (\vartheta_3, \emptyset) \parallel \cdots \parallel (\vartheta_n, \emptyset) \). The only sensor device concerned by the change is the sensor device \( \vartheta_2 \). Figure 11 illustrates the mobility management process.

3.3.1. Data routing

This step consists of request and data communication between the sink and the sensor devices. Depending on the type of the application orientation, the routing process is designed differently. We distinguish two application orientations, namely request-oriented and event-oriented. In the event-oriented scenario, as soon as a sensor device detects an event, it should alert instantly the sink. In this context, each sensor device is beforehand configured with the optimal routing path leading to the sink. Later, when an event is detected, the sensor device transmits the sensed data to the sink over the held routing path. In the case of request-oriented applications, the sink is in charge to communicate the reply routing path to the sensor device when it transmits the request packet.

In the case of request-oriented MWSN applications, the process consists of the request packet forwarding from the sink directly to the sensor device in one-hop, and inversely the data packet forwarding from the sensor device to the sink in multihop. When the sink requires a specific data

17
from a specific sensor device, it selects and embeds the data routing path to the request packet. The propagation of the data packet is performed through the source routing process. Each sensor device holds a list containing the different signal strengths of its neighbors. From the signal strength, the sensor device can estimate the distance that separates it from its neighbor and thus can adjust its signal when transmitting. For this purpose, RSSI (Received Signal Strength Indication) or LQI (Link Quality Indication) can be used [26].

At the reception of the data packet, each intermediate sensor device removes its identity from
the path, and forwards the packet to its successor. This process is reiterated till the packet meets the sink. In the case of event-oriented MWSN applications, the sink pre-configures each sensor device in the beginning with its optimal routing path. Later, when an event is detected, the sensor device transmits the sensed data to the sink over the help path. For both types of MWSN applications, upon receiving the packet by the sink, the latter accumulates the load factor of the participating sensor devices. This way, the sink equalizes the load among all the network sensor devices. Figures 13 and 14 illustrate, respectively, the routing process in the request-oriented and event-oriented contexts.

4. Performance evaluation

The performance evaluation is performed by simulations, that we have developed using the Matlab programming language. In this section, we present first the environment and simulation parameters, followed by the discussion of the obtained results.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network size</td>
<td>20</td>
</tr>
<tr>
<td>Monitored area</td>
<td>100m × 100m</td>
</tr>
<tr>
<td>Communication range</td>
<td>20m</td>
</tr>
<tr>
<td>Interval of requests</td>
<td>5 min</td>
</tr>
<tr>
<td>Data size</td>
<td>4 bytes</td>
</tr>
<tr>
<td>$(\alpha, \beta)$</td>
<td>$(1 , \mu\text{Joule}, 2 , \mu\text{Joules})$</td>
</tr>
<tr>
<td>Initial residual energy</td>
<td>3 Joules</td>
</tr>
<tr>
<td>GPS data reception rate</td>
<td>50 bps</td>
</tr>
<tr>
<td>$\theta$</td>
<td>10%, 20% and 50%</td>
</tr>
<tr>
<td>$(\delta, \gamma)$</td>
<td>(5 min, 100%), (50 min, 50%) and (100 min, 25%)</td>
</tr>
</tbody>
</table>

4.1. Simulation parameters

In Table 2 we summarize the main simulation parameters. We have considered an initial arbitrarily deployed topology of a network composed of a collection of 20 sensor devices in a monitored area of 100m × 100m. The network is supervised by a single sink with a randomly chosen position. At each period of 5 min, a randomly chosen sensor device communicates the sensed data to the sink. The sensor devices have the same wireless communication medium of 20m. The simulation scenario is designed to be close to the specificities of the WSN environments. The used simulation parameters allow getting less dense topologies with the aim leading to mobility-sensitive network connectivity by favoring scenarios of constraining topologies with frequent partitioning. The data size is 4 bytes. We have considered the collision probability over the communication channels. During a transmission, the data frame can be interfered by
Figure 12: Routing and mobility management flowchart
another communication with a probability $P_C = 0.2$. In this case, the sensor device should resend the data frame until the neighbor receives it. Later, this probability is varied randomly for the lifetime evaluation (cf. Table 3).

The developed simulator estimates if a link exists between the sensor devices regarding the Cartesian distance separating them. It estimates the energy consumption using the model proposed by Heinzelman et al. [19]. This model is considered as one of the most used energy models for wireless communication in the literature. It is important to emphasize that the proposed protocol does not depend on a specific energy model. This aspect has been introduced only in the simulations in order to quantify the individual energy consumption of each sensor device as a function of the packet transmission and reception. Furthermore, the same energy consumption model is used in the simulations for all the compared protocols. Following this
model, if a sensor device sends a $k$-bits packet over a distance $d$, it spends in Joules

$$E_T = k \cdot (\alpha + \beta \cdot d^2),$$

where $\alpha$ is the electrical energy and $\beta$ is the empirical energy. If a sensor device receives a $k$-bits packet, it spends in Joules

$$E_R = k \cdot \alpha.$$ (4)

In the simulations, the parameters $\alpha$ and $\beta$ are set, respectively, to $1 \mu$Joule and $2 \mu$Joules.

The initial residual energy of each sensor device is set to 3 Joules. The performances of the proposed protocol are compared to those of LASeR [10] and Directed-Diffusion [18], which are described in Section 2. Directed-Diffusion is one of the reference protocols in the field of routing in sensor networks. That’s why, we have judged interesting to include it in the comparison. The protocol LASeR addresses explicitly the problem of control data overhead and response time. The simulations are performed over an unpredictable mobility scenario, which is supported by both protocols.

Each protocol is executed until the energy depletion of the first sensor device in the network. We have performed the evaluation regarding the two important aspects in the context of sensor networks, namely the energy consumption and the load-balancing. The energy consumption represents the spent energy, in Joules, by all the network sensor devices, considering the packets transmission and reception, the beacon messages exchange and the GPS communication overhead. The load-balancing aspect is represented by the residual energy standard deviation of the network sensor devices, calculated at a given instant by

$$\sqrt{\frac{\sum_{i=1}^{n} (E_i - \bar{E})^2}{n}},$$

where $E_i$ is the sensor device $\vartheta_i$ residual energy, $\bar{E}$ is the average of residual energies, and $n$ is the network size. The GPS communication energy is calculated regarding the number of visible satellites and their corresponding GPS data reception rate. We have considered for the protocol LASeR, the best case with a strict minimum number of visible satellites, which is 3 and a rate of 50 bps of GPS data reception. We have also considered the best scenario case for LASeR in the data transmission, where the network is supposed reliable and only one path is followed when routing the data toward the sink. However, we have considered the worst case scenario for the proposed protocol in the routing paths updating, where at each topology change, each sensor device receives a new routing path of length $n^2$.

\footnote{In the worst case, a routing path could include all the network sensor devices.} Following LASeR, a proportion $\theta$ of sensor device
devices are equipped with GPS. We have evaluated, three variants of LASeR with respectively, $\theta = 10\%$, $\theta = 20\%$, and $\theta = 50\%$.

The metric varied is the mobility intensity, which is represented by two important parameters, namely the topology change frequency and the percentage of mobile sensor devices. At each period of time $\delta$, a threshold rate $\gamma$ of sensor devices are randomly selected to change their positions. We have performed the simulations regarding three scenarios: (1) high dynamic environment with $\delta = 5$ min and $\gamma = 100\%$, (2) moderate dynamic environment with $\delta = 50$ min and $\gamma = 50\%$, and (3) low dynamic environment with $\delta = 100$ min and $\gamma = 25\%$. The mobility degree is an important parameter, where the topology change frequency influences the message overhead that could be generated to update the network topology view in the sink side, and hence, influences implicitly the energy consumption. We note that the sensor devices mobility do not follow a predefined path or a particular mobility model. The sensor devices move randomly and unpredictably, which is represented by a random topology change. The sensor devices can move with any speed and take any trajectory. Future sensor device locations cannot be predicted. The mobility event of a sensor device creates or breaks one or more links between the mobile sensor device and its neighbors. The compared protocols are tested for 100 different scenarios, with which we have computed the confidence intervals with a threshold of 99\%.

4.2. Obtained results

Figure 15 represents the energy consumption as a function of time in the case of high dynamic environment (refer to Figure 16 for the corresponding confidence intervals). We note that the network lifetime regarding LASeR is around 320 min, which is independent from the rate $\theta$. The increase of $\theta$ influences highly the total energy consumed in the network due to the expensive energy consumption by the GPS. This overhead becomes more expensive when a high number of sensor devices are equipped with GPS. We note that $\theta$ does not affect the network lifetime. Directed-Diffusion consumes more energy because it operates with an uncontrolled broadcast. However, we notice that the network lifetime is longer than LASeR due to the load-balancing of energy consumption, where Directed-Diffusion selects the optimal reverse routing path toward the sink. The proposed protocol consumes less energy in a dynamic environment. This is due to the network topology view maintenance, which is updated periodically by the mobility information dissimulated by the sensor devices to the sink through the beacon frames. Even the mobility control messages are dissimulated, this could be not enough to cover all the required messages. Indeed, the concurrent protocols abstract the network topology in order to overcome the mobility management issue. For this reason, they consume a lot of energy in the distributed request broadcasting for routes recovery. In parallel, the proposed protocol consumes also a part of energy on each sensor device when receiving the routing configurations. Moreover, another
part of energy is consumed when collecting information about the network topology change. However, the energy gain is not mainly due to the dissemination of routing configurations, but also through the mobility information dissimulation, which is an important part of our contribution.

Figure 15 represents the energy consumption as a function of time in the case of moderate dynamic environment (refer to Figure 18 for the corresponding confidence intervals). The network lifetime following LASeR does not change, however, those of Directed-Diffusion decrease slightly. This is due to the fact that the most solicited sensor devices during the routing are those close to the sink. In this case, there is a fairly high probability that there be sensor devices that have not moved from the vicinity of the sink, which accelerates their energy depletion. The performance of the proposed protocol is even better, not only with respect to energy consumption, but also with respect to network lifetime, which is nearly 7200 min.

Figure 19 represents the energy consumption as a function of time in the case of low dynamic environment (refer to Figure 20 for the corresponding confidence intervals). Again, the network lifetime following LASeR does not change. The lifetime following Directed-Diffusion decreases and is almost equivalent to the LASeR results. This is due to the relative position stability of the sensor devices, which makes the closer sensor devices to the sink more busy. That’s why they
tend to run out more quickly. The best performances of the proposed protocol are emphasized in this case, because there are even fewer messages. The network lifetime is still ten times better than those of the other protocols.

Figure 16 represents the load-balancing as a function of time in the case of high dynamic environment (refer to Figure 22 for the corresponding confidence intervals). The results summarize the network lifetime of each protocol, taking into account the mobility frequency of the sensor devices. We note that the load-balancing following LASeR is not good, which is shown by the residual energy standard deviation that increases continuously. This value begins approximately at 0.2 Joule and reaches later around 1.5 Joule at the end of the protocol execution. This implies that the difference between the residual energies of the different sensor devices is very important and that the protocol does not take into account the load-balancing in routing. Moreover, some of the sensor devices are equipped with GPS, which unbalances the energy consumption. The proposed protocol and Directed-Diffusion show good load-balancing throughout the simulation, which remains approximately stable at $10^{-2}$ Joule. This means that the sensor devices have consumed all theirs total energies at approximately the same time. Directed-Diffusion uses flooding to reach the destination sensor device. Therefore, all the sensor devices participate in the routing task and consume approximately the same energy. However, this causes more important
energy consumption. The proposed protocol is better because it allows at the same time higher network lifetime. The routing paths are selected by taking into consideration the number of times the sensor devices have been requested for routing. Moreover, the selected routing paths are more stable due to the mobility factor. The proposed protocol and Directed-Diffusion are very close, which means that the sensor devices consume approximately their energy in the same manner. However, following Directed-Diffusion, the network dies earlier, because of the data packet flooding, where all the sensor devices participate in the routing process.

Figure 23 represents the load-balancing as a function of time in the case of moderate dynamic environment (refer to Figure 24 for the corresponding confidence intervals). LASeR and Directed-Diffusion show approximately the same results in contrast to the proposed protocol. The latter results follow higher network lifetime, which is about 7200 min compared to 500 min for Directed-Diffusion.

Figure 25 represents the load-balancing as a function of time in the case of low dynamic environment (refer to Figure 26 for the corresponding confidence intervals). It demonstrates the best results for the proposed protocol, allowing a network lifetime of 7200 min and very significant load-balancing.

In Table 3, we show the efficiency of each protocol by measuring the network lifetime. The
Figure 18: Confidence intervals for network energy consumption under a moderate dynamic environment

Table 3: Comparison of the protocols in terms of network lifetime

<table>
<thead>
<tr>
<th>Protocol</th>
<th>High mobility</th>
<th>Moderate mobility</th>
<th>Low mobility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directed-Diffusion</td>
<td>12 hours 24 min</td>
<td>11 hours 41 min</td>
<td>11 hours 32 min</td>
</tr>
<tr>
<td>LASEr ($\theta = 10%$)</td>
<td>5 hours 25 min</td>
<td>5 hours 24 min</td>
<td>5 hours 24 min</td>
</tr>
<tr>
<td>LASEr ($\theta = 20%$)</td>
<td>5 hours 24 min</td>
<td>5 hours 21 min</td>
<td>5 hours 20 min</td>
</tr>
<tr>
<td>LASEr ($\theta = 30%$)</td>
<td>5 hours 21 min</td>
<td>5 hours 12 min</td>
<td>5 hours 9 min</td>
</tr>
<tr>
<td>Proposed protocol</td>
<td>2 days 19 hours 4 min</td>
<td>4 days 11 hours 56 min</td>
<td>3 days 15 hours 41 min</td>
</tr>
</tbody>
</table>

latter represents the interval of time that separates the network deployment from the time of the energy depletion of the first sensor device. We have performed the simulations with different loss probabilities between each pair of sensor devices. We have used a matrix of loss probabilities, which each cell contains a randomly generated value of loss probability. This part of simulation summarizes the overall performance, in which the proposed protocol achieves the best results. It remains to emphasize that the proposed protocol is slightly less efficient in terms of latency with comparison to the other protocols. Figure 27 illustrates the obtained results in terms of response time (refer to Figure 28 for the corresponding confidence intervals). The chosen routing paths following the proposed protocol are not, necessarily, the shortest ones, which interprets its latency regarding the other protocols. The gap is approximately in the order of 0.1 ms, which is largely offset by the obtained results in terms network lifetime.
5. Conclusion

Routing in MWSNs is a challenging issue due to both limited resources of sensor devices and mobility management. In this paper, we have proposed a new routing protocol for sensor networks that supports mobility. Two variants of the proposed protocol are developed for request and event oriented MWSN applications. The route discovery is performed by the sink, and the sensor device mobility history is introduced to compute the most optimal routing path that groups the most stable and unloaded sensor devices. To reduce the network load, a new technique of dissimulation has been proposed, which consists in concealment of some important communication information in the exchanged beacon frames. The load-balancing is ensured by the sink with the distribution of the routing task depending on the number of times a sensor device is requested to forward data. The simulation results show that the proposed protocol is efficient in terms of energy consumption and load-balancing, where it generates very less overhead when exchanging routing control messages.
Figure 20: Confidence intervals for network energy consumption under a low dynamic environment.
Figure 21: Load-balancing energy consumption under a high dynamic environment

References


Figure 22: Confidence intervals for load-balancing energy consumption under a high dynamic environment
<table>
<thead>
<tr>
<th>Time (min)</th>
<th>Proposed protocol</th>
<th>LASeR with $\theta = 10%$</th>
<th>LASeR with $\theta = 20%$</th>
<th>LASeR with $\theta = 50%$</th>
<th>Directed-Diffusion</th>
</tr>
</thead>
<tbody>
<tr>
<td>1,000</td>
<td>0.2</td>
<td>0.4</td>
<td>0.6</td>
<td>0.8</td>
<td>1.0</td>
</tr>
<tr>
<td>2,000</td>
<td>0.4</td>
<td>0.8</td>
<td>1.0</td>
<td>1.2</td>
<td>1.4</td>
</tr>
<tr>
<td>3,000</td>
<td>0.6</td>
<td>1.0</td>
<td>1.2</td>
<td>1.4</td>
<td>1.6</td>
</tr>
<tr>
<td>4,000</td>
<td>0.8</td>
<td>1.2</td>
<td>1.4</td>
<td>1.6</td>
<td>1.8</td>
</tr>
<tr>
<td>5,000</td>
<td>1.0</td>
<td>1.4</td>
<td>1.6</td>
<td>1.8</td>
<td>2.0</td>
</tr>
<tr>
<td>6,000</td>
<td>1.2</td>
<td>1.6</td>
<td>1.8</td>
<td>2.0</td>
<td>2.2</td>
</tr>
<tr>
<td>7,000</td>
<td>1.4</td>
<td>1.8</td>
<td>2.0</td>
<td>2.2</td>
<td>2.4</td>
</tr>
</tbody>
</table>

Figure 23: Load-balancing energy consumption under a moderate dynamic environment


Figure 24: Confidence intervals for load-balancing energy consumption under a moderate dynamic environment
Figure 25: Load-balancing energy consumption under a low dynamic environment


Figure 26: Confidence intervals for load-balancing energy consumption under a low dynamic environment
Figure 27: Comparison of response time

Figure 28: Confidence intervals for response time


