Check for updates

Research Article

International Journal of Distributed Sensor Networks

International Journal of Distributed Sensor Networks
2016, Vol. 12(7) 1–18
© The Author(s) 2016
DOI: 10.1177/1550147716659427
ijdsn.sagepub.com
SAGE

Enhanced group-based wireless ad-hoc sensor network protocol

Marwa Khedher[1], Jaime Lloret[2] and Ali Douik[3]

Abstract

Communication is the major energy consumption source in wireless ad-hoc sensor networks. Thus, an efficient trade-off between the energy cost of the communication and network's performance is a key challenge in conceiving a wireless ad-hoc sensor network. In this article, we propose an improved group-based architecture for wireless ad-hoc sensor networks. An optimized group forming procedure and an efficient communication operation are introduced. In order to validate the proposed approach, we suggest a group-based strategy to monitor pharmaceutical drugs during transportation. Real measurements of temperature and vibration were performed to validate the effectiveness of our approach.

Keywords

Wireless ad-hoc sensor network, overhead, communication, connectivity, election, monitoring pharmaceutical drugs transportation conditions

Date received: 27 March 2016; accepted: 20 June 2016

Academic Editor: Suat Ozdemir

Introduction

Wireless ad-hoc sensor network (WAHSN) is a network which allows to keep an eye on a physical environment. Distributed nodes are deployed in a sensing area in order to gather useful information for a specific application. Ad-hoc networks do not require any predetermined locations for nodes, because it is generally used for remote or inaccessible areas.[1] Since WAHSNs are typically conceived to operate in remote areas, it requires a self-management protocol which is able to operate without possibility of maintenance. For example, in WAHSN dedicated for monitoring active volcano,[1] nodes could be thrown from airplanes over the desired sensing area. Thus, deployed nodes should be able to set up a network, operate their sensing tasks, establish interactions with other nodes, and certainly overtake network failures.

Many issues could affect the network's performance namely energy efficiency, scalability, and resource management. For this purpose, WAHSNs were a focus of interest of many research works. Many distributed network architectures were proposed in the literature going from clustering,[2,3] zone-based,[4] grid-based[5] to group-based protocols.[6] All of these algorithms come over hierarchical networks. They were commonly used because of their effectiveness to solve the cited issues. These techniques divide the network into groups through specific grouping criteria in order to enhance the network performances.

In cluster-based protocols,[2] nodes are divided into small groups called clusters. Each cluster is formed by a cluster head and cluster members. The cluster head has a leader role. It manages the cluster in addition to the forwarding task. It collects, aggregates, and re-sends

[1]National Engineering School of Monastir, University of Monastir, Monastir, Tunisia
[2]Instituto de Investigación para la Gestión Integrada de Zonas Costeras, Universidad Politecnica de Valencia, Valencia, Spain
[3]National Engineering School of Sousse, University of Sousse, Sousse, Tunisia

Corresponding author:
Marwa Khedher, National Engineering School of Monastir, University of Monastir, Monastir 5121, Tunisia.
Email: khedher.marwa@gmail.com

Creative Commons CC-BY: This article is distributed under the terms of the Creative Commons Attribution 3.0 License (http://www.creativecommons.org/licenses/by/3.0/) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (http://www.uk.sagepub.com/aboutus/openaccess.htm).

data to the base station. Consequently, elected clusters will be greedy in dispersing energy. To solve this problem, a rotation of cluster heads was suggested; however, the election process remains an expensive operation in terms of energy consumption. At each election phase, nodes exchange a large number of packets in order to form the clusters which lead to increase the overhead and cause an expensive communication cost.

In zone-based protocol,[4] the network is divided into geographical zones. Each node will belong automatically to a zone through its position. In this kind of architecture, the sensing area should be known in advance in order to make the network partition into zones. However, a WAHSN does not commonly provide any predefined infrastructure measurements for the deployed area. Moreover, since each node will join a zone due to its geographical location, the number of nodes in different zones could cause unbalanced groups.

Although all these architectures present many advantages, group-based architectures were elected as the more powerful in comparison with other architectures in terms of energy efficiency. As we mentioned above, the energy consumption depends highly on the number of exchanged packets. We focus our interest on group-based architecture owed to many benefits of this kind of topology. First, group-based division ensures the flexibility, scalability, and fault tolerance of the network. In fact, new nodes could easily join the network and depleted nodes could disconnect without causing any dis-functionality. Moreover, any failed operation could be carried by other nodes. On one hand, this architecture ensures a distribution management between groups, because it spreads tasks between groups which consequently allow to minimize delays. On the other hand, data and measurements could be accessed from any group while all information are saved on local database. This architecture ensures also an efficient and energy aware transmission.

Energy consumption is a major issue in designing an ad-hoc sensor network. The management of configuration, maintenance, and transmission in the network may generate an expensive overhead. The more communication messages are exchanged, the more energy is consumed. The start point of this article is considering that reducing the amount of transmitted messages reduces the whole energy consumption in the network. We had focused our interest on the design of a low cost group-based architecture by reducing the amount of transmission packets used during the organization of the network. This allows to reduce the whole network overhead and decreases eventually the dispersed amount of energy.

In this article, we present an improved group-based architecture over WAHSNs. It is based on maintaining a trade-off between minimizing the network overhead and ensuring good performances. It is a self-organized architecture which uses a reduced amount of communication packets over the network operation.

The remainder of this article is organized as follows: section "Related work" reports the research work relative to group-based architectures. Proposed architecture is detailed in section "Architecture description." Section "Architecture protocol and algorithms" presents the protocol flow messages. The topology maintenance is described in section "Topology maintenance." An analytical model for a new neighborhood selection between groups is illustrated in section "Problem formulation." Section "Real deployment and validation" shows a real-world application which would be efficient using our proposed protocol. Finally, section "Conclusion" resumes the achieved work and presents the possible future work.

Related work

There are many research works in the literature where group-based architecture was presented. In fact, Lloret et al.[7] demonstrate the efficiency of the group-based mobile ad-hoc network (MANET) routing protocols. A comparison between three routing protocols in the group-based network was performed to validate the effectiveness of such architecture in MANET networks. Lloret et al.[8] compared three MANET routing protocols with group-based architecture in order to prove the effectiveness of group-based topologies.

Moreover, Lloret et al.[9] outline the related work and existing systems in relation with group-based topologies showing the benefits and drawbacks of each work. Authors classified this kind of topology into planar and layered ones.

Furthermore, Garcia et al.[10] propose an energy efficient topology which consists of a cooperative organization of groups. Once a node detects an event, all nodes of the group share the alert and it is sent to the most adequate neighbor group. This ensures that the alert is forwarded efficiently to the right destination, and that the appropriate actions are taken. Authors demonstrate also that decreasing the number of transmissions, which is provided by the cooperative groups topology, improves the wireless sensor networks (WSNs) and decreases the total energy consumption.

An environmental monitoring is presented in Garcia and Lloret[11] using a cooperative group-based topology. When an event is detected, an alert is launched and the information is shared with neighboring groups in order to change the propagation route and the level of the alert. This cooperation ensures more efficiency in energy consumption in the whole network.

After group formation, Beydoun and Felea,[12] introduced a hierarchical tree to create a routing table in each node of the network in a distributed manner. Two

metrics are used for the routing. The first one is the minimum energy consumption per bit of transmitted information. The second metric ensures that the transmission is always done along the path that has the maximum capacity measured in terms of bits.

Grouping methods were also used in security issues in wireless networks. In fact, Kifayat et al.[13] proposed a group-based key management scheme for mobile and static sensor networks. The proposed scheme consists of using distinct keys at different levels in the network. Therefore, data confidentiality and high resilience against node capture attack are ensured.

Moreover, a new lightweight group-based trust management scheme (GTMS) for WSNs was proposed by Shaikh et al.[14] The proposed scheme is dedicated for clustered networks. It consists of three main features. First, this scheme evaluates the group trust of sensor nodes contrary to traditional trust management schemes which target trust values of individual nodes. Second, GTMS uses a distributed trust management approach for intra-group topology and a centralized trust management approach for inter-group topology. Third and last, GTMS maintains a mechanism to detect malicious nodes in addition to some degree of prevention mechanism.

Kifayat et al.[15] proposed a novel group-based key management protocol in order to solve security issues in WSNs. The communication and data confidentiality of the entire group are compromised because the leader node in the group is able to decrypt data from all member nodes. Authors suggest that encrypted data from member nodes could be prevented for the aggregation. Instead, it is performed with encrypted values and the result decryption is only achieved by the sink.

Mantri et al.[16] proposed a group-based data aggregation method. In this method, node grouping is based on available data and correlation in the intra-cluster. Cluster heads grouping is also performed to reduce the energy. Moreover, the proposed method provides an additive and divisible data aggregation function at cluster head which leads to minimize the energy consumption. In fact, aggregated information are transmitted to remote sink by cluster heads.

Chen et al.[17] considered a group-based network roaming in proxy mobile IPv6 (PMIPv6) domain in 6LoWPAN-based wireless body area networks. An enhanced group mobility scheme is introduced which aims to reduce the hand-off delay, signaling cost, and the number of control messages.

M Haneef et al.[18] have proposed energy efficient routing algorithm based upon the framework of low energy adaptive clustering hierarchy (LEACH) protocol. They considered the deployed redundant nodes to cover major fraction of energy depletion in the network. This redundancy was considered as an advantage for increasing the lifetime of network.

Lloret et al.[6] have developed a group-based protocol which consists of partitioning the network into groups where none of group member has an extra-managing task. A group in this protocol is a set of nodes that are sharing same resources and are associated through predefined criteria. Nodes from close groups interact with each other to create connections between them. In this article, we noted a large number of exchanged messages while processing which increases the overhead of the network. In fact, in group creation, authors consider each node separately at the beginning of network; however, in real application, a network starts typically with a set of nodes and new nodes could join the network later. Furthermore, authors consider some specific parameters which take into account node's capacities to establish intra-group and inter-groups links. Using these parameters can prevent nodes with low level of capacities to join the network. Therefore, a border node with low potential will not be able to establish any inter-links. In this case, the inter-group connectivity could be neglected. Moreover, the central node selection procedure does not ensure that nodes with high potential are chosen as central nodes. Backup central nodes were defined in order to replace the original ones once these latter are depleted. This raises the amount of exchanged messages. Finally, disconnecting nodes from the network do not need any message exchanges, because it will be already noticed by the absence of "keepalive" messages.

None of the cited related work has focused on an optimized central node selection neither on border node connectivity. However, many issues could be caused if the sensing area is not totally covered and connected.

The main objective of this work is to overcome the weakness of previous work by improving the way nodes are configured over the network, their communications as well as the groups connectivity. We aim to develop an efficient group-based architecture that is able to minimize the overhead of the network and definitely to manage the network effectively.

Architecture description

We suggest a new architecture based on the division of the network into groups of nodes. It aims to minimize the network overhead by reducing the control messages. In fact, overhead is the major issue of this architecture. The main objective is to organize the nodes and allow them to transmit and receive data in more efficiently way through a consistent management. We should take into account that an ad-hoc network must be automatically organized and instantaneously deployed and able to assume traffic changes.

The starting point of our architecture is a set of wireless sensor nodes randomly deployed in a sensing area

which form an ad-hoc network. They are able to detect and collect data under their radio coverage area. Every node should have specific parameters to be a part of the proposed architecture:

- Identifier: each node has a unique identifier;
- Type: identifies the type of node: border or normal. Initially, all nodes are normal;
- Max_distance: it represents the maximum distance to be a group member. It is always shorter than or equal to a predefined value. It can be changed by the received signal strength indication (RSSI) value. It is used to establish connections between group members;
- Position (node.x, node.y);
- Energy level (node.E).

We can split our architecture protocol into an organization phase and a transmission phase:

- Organization phase: here, nodes will be deployed randomly in the sensing area. Central nodes are chosen by election and a division into groups is performed. At the end of this phase, each node will belong to a group.
- Transmission phase: in this phase, each node will provide information in order to route data between groups.

The organization phase occurs while deploying nodes into the sensing area. Let us suppose that we dispose of a WSN composed of N nodes. Central nodes are the most important actors because they will limit the boundaries of the group. The central node will be the first node in each group.

In the central nodes selection, we should take into account that they are not too close to each other so some nodes could not join any group. Central nodes should also be provided with high capabilities. Moreover, the number of elected central nodes depends on the whole number of nodes in the network and the desired size of each group. Accordingly, we aim to split nodes into balanced groups in terms of size. Therefore, we suggest that 20% of the total network node will be elected as central nodes. This choice refers to the 20/80 rule suggested by Chang et al.[19] where they show that this is the best average of election. Thus, we choose to keep the same percentage. The number of groups is equal to the number of central nodes in the network.

To sum up, the election of the central nodes is made as a function of the network features, the number of nodes, and the node's capacity. To cover all these needs, we develop an election method which is efficient, inexpensive, and does not require lot of resources which will be described in the next section.

Our metric is that each group member is only one hop to the central node in order to delimit the group size. The number of hops is counted as the number of hops between two nodes of the group. Central nodes initialize the organization with the group members. Each elected central node will invite nodes in its neighborhood to join its group. A node can join the group only if the distance between them is shorter than or equal to a predefined value. When a new node joins a group, it acquires the group identifier from the central node. Therefore, each node will join the group whose central node is the closest.

If a node receives more than a join invitation, it will choose the invitation with the strongest RSSI value, change its type to border, and define the group from which it has received an invitation as a border group. Every node of the network has a unique identifier, as well as nodes of the same group share a unique group identifier. In the same group, node members have connections with some other group members only if the distance between them is shorter than or equal to a predefined value.

There are two types of nodes in the network: border and normal nodes. At the beginning, all nodes are normal. Border nodes are nodes situated on the edge of each group. A node changes its type to border when it receives more than an invitation to join a group. This means that border nodes are the nodes in common coverage area.

Let us suppose that we dispose of six nodes as shown in Figure 1. Node 1 and node 4 were elected as central nodes. They send invitation messages to others nodes. Nodes 2 and 3 have received more than one invitation message. Therefore, each of them will choose the central node which has the lower distance to join its group. Thus, node 2 will join the group of the central node 1 and node 3 will join the group of the central node 4 as shown in Figure 2.

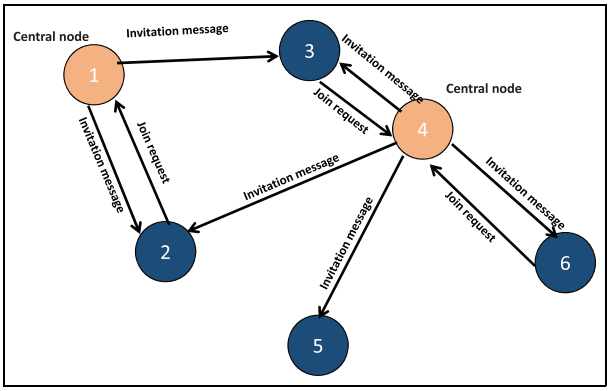

Figure 1. Messages exchanged when a node receives join requests from many central nodes.

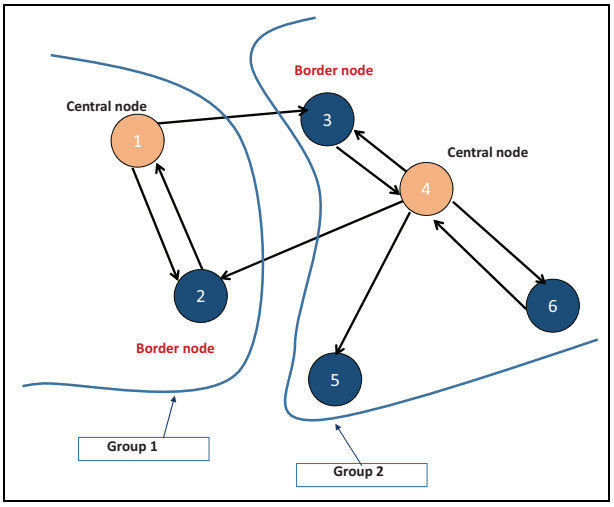

Figure 2. Group division when a node receives join requests from many central nodes.

All nodes in the group share same group information. In fact, each node has an intra-group table where it saves this information.

On the other hand, each border node has to establish links with border nodes of neighbor groups. These nodes will play an interfacing role between groups. In fact, in addition to its intra-group table, border nodes have an extra table so-called inter-group table. In this table, border nodes collect and save information about border nodes of their group, border nodes of neighbor groups, and neighbor group identifiers. Moreover, updates of theses tables are shared between linked border nodes in order to maintain all border node informed once any modification occurs.

At the end of organization phase, nodes will split into groups as shown in Figure 3 where we consider four groups of nodes. Border nodes have connections with other border nodes of close groups and all nodes inside each group have local connections.

Each node in a group knows where each node of its group is and how to reach it. Every border knows where border nodes of close groups are and how to reach them. The flow chart presented in Figure 4 resumes the group formation in the network.

In the transmission level, many alternatives can occur. If the source and destination nodes belong to the same group, a local routing protocol will be used to make the intra-routing task. However, if the source and destination nodes belong to different groups, border table will allow border nodes to route data using an appropriate routing protocol. Therefore, we define as well two kinds of routing protocol to be implemented for the forwarding process: inter-group protocol and intra-group protocol. The intra-group protocol should be used if the information must be routed in the same group. On the other hand, once the neighboring links were defined, an inter-group protocol is defined in order to find the best path to send data from nodes of different groups through border nodes.

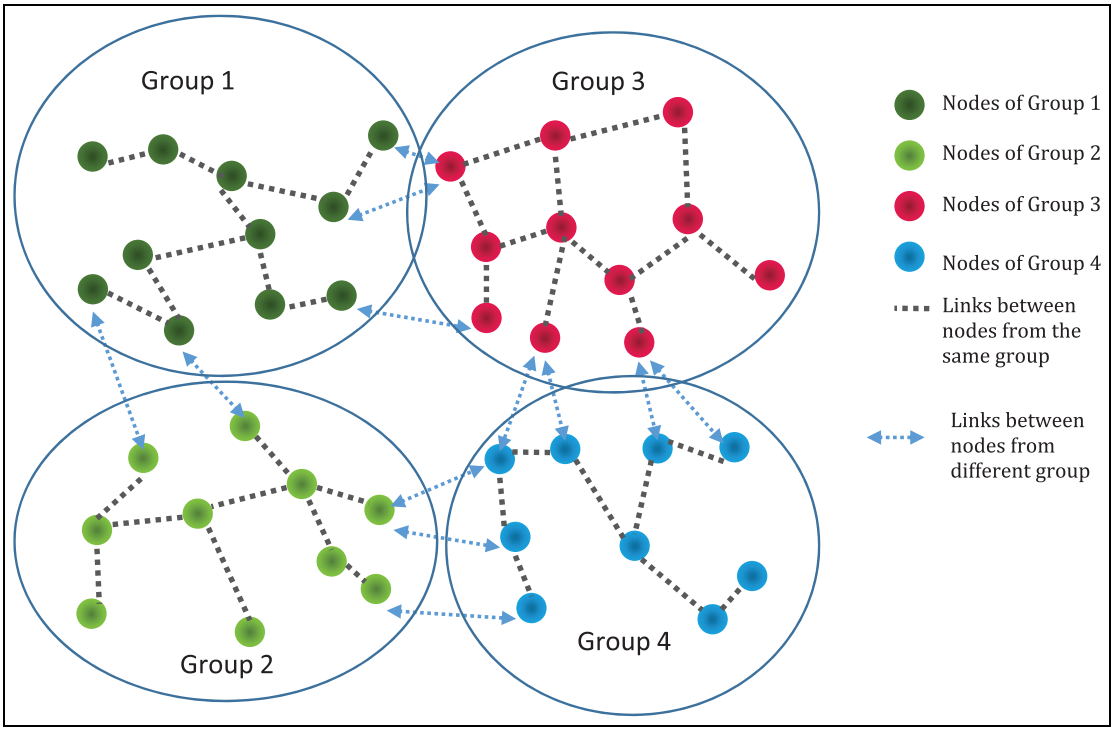

Figure 3. Groups in ad-hoc sensor network.

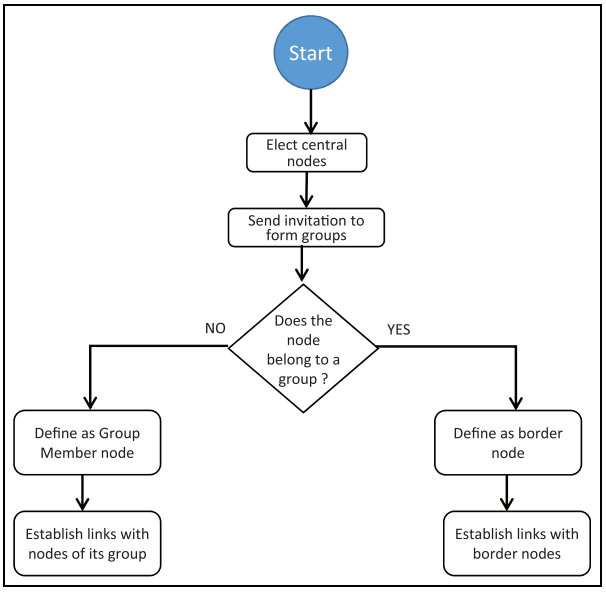

Figure 4. Flow chart of the group formation.

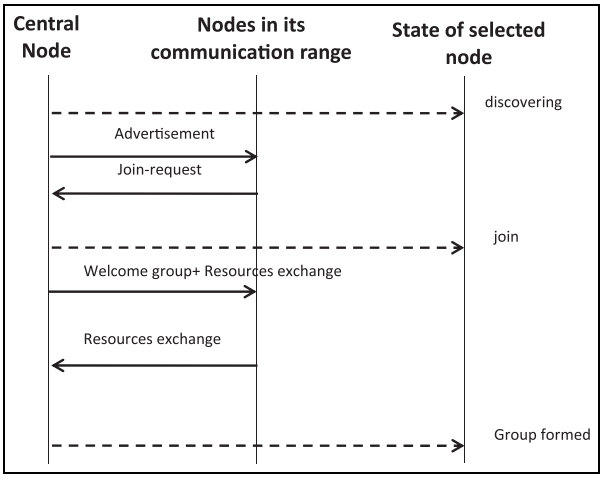

Figure 5. Discovery phase.

The first step to send data from one group to another is sending the data to the border node of the source group. Border nodes are responsible to send data to the destination group via border nodes. Once data arrive to the destination group, a local routing protocol ensures the transmission to the destination node.

Architecture protocol and algorithms

In this section, we present the exchanged messages to establish the grouping operation. We can describe the implementation of the protocol through four main steps: central node election, discovery, adjacency, and transmission.

Central node election

Let us suppose that we have N randomly deployed nodes in the sensing area. While we aim to divide the network into groups and that each group starts with a central node, we will elect 20% of nodes as central nodes. This election takes into account few parameters such as node's energy, number of available connections and the size of the sensing area.

We propose a distance-based election algorithm to ensure choosing the best set of nodes. First, we choose only nodes that provide more than 50% of their energy level E. Then, we made a random selection of the desired number of central nodes and we calculate the total distance between them. Next, we save these selected nodes as best elected central nodes. Second, a new random election is performed and total distance is calculated. If the new total distance is higher than the last distance, then we replace the best elected central nodes by the new set; otherwise, we keep the last selection. This operation is made for 50 iterations until finding the largest total distance between elected central nodes. Finally, the central nodes which ensure the largest total distance will be elected as the central nodes of the network.

Once a node has been defined as a central node, it is provided with group identifier. The main role of the central node is to delimit each group and ensure that each one of them does not exceed certain radius. The central node election algorithm is described in the pseudo-code algorithm 1.

Discovery

A central node starts its discovery phase when the election has been finished. It broadcasts an "invitation" message to nodes in its communication range in order to invite them to join its group. When a node receives an ''invitation'''' packet, it will send back a ''join request'' to the central node. A "group welcome" message will be forwarded to ensure that the node has successfully joined the group. Figure 5 illustrates the messages exchanged in this phase.

When a non-central node receives more than one invitation, it chooses the central node with highest RSSI value. Central nodes will keep sending broadcast for a reasonable scan time and it stops when it reaches the maximum number of connections.

Once each central node defines its members of its group, it shares information with them. If a node receives and invitation, but it belongs to another group, then it becomes a border node. Figure 6 illustrates the choice of border nodes.

Algorithm 1: Central node election algorithm

```
Return: Set of Elected Central nodes
  Best_Distance = 0;
  Total_Distance = 0;
  Deploy N nodes randomly;
  while (iter ⩽ Max_iterations) do
      Select M = a random set equal to 20% of N such as node[i].Energy⩾50% of total energy;
      for i = 1:M do
          for j = 1:M do
              Distance(i, j) = √((node[i].x − node[j].x)^2 + (node[i].y − node[j].y)^2);
              Total_Distance = Total_Distance + Distance(i, j);
          end
      end
      if Best_Distance ⩽ Total_Distance then
          Best_Distance = Total_Distance;
          Set_of _Central_nodes = M;
      end
  end
```

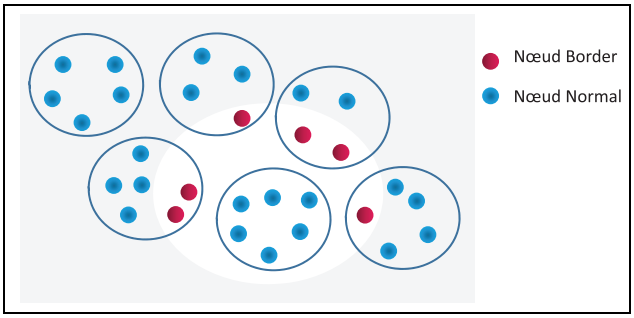

Figure 6. Border node selection.

Establishing links

We can find two kinds of links: links intra-groups and links inter-groups.

Intra-group. As shown in Figure 7, nodes in the same group establish local connections between them. Each node sends a "link request" message. Once a node receives a "link request" message, it replies with a "link acknowledgment" only if the distance between them is lower than a predefined value.

Linked nodes from the same group exchange periodically "keepalive" messages. In case of non-reception of "keepalive" messages from one node, it will be deleted from the intra-group table. Each node provides an intra-group table where it saves all information about the group.

At the end of this phase, all nodes in the same group share the same intra-group table. Each member node has an entry in this table which includes information about each node: node identifier, node type, available resources, number of connections and local linked nodes.

Inter-group. Each border node should establish links with border nodes from the same group as well as from other groups. Border nodes play the role of a relay between groups. Therefore, it sends a "border advertisement" message in order to detect other border nodes. Once a border node receives an "advertisement," it replies with a "border join" message in order to establish links. Only border nodes that are far from other border nodes at a distance lower than a predefined value will be connected. A "border acknowledgement" message is send back to ensure that links were established.

Linked border nodes exchange periodically "keepalive" messages. Once it has no reply from one border node, then it will delete its information from the inter-group table. The exchanged message flow for intra-group linking is shown in Figure 8.

Each border node has, in addition to its local table, an inter-group table where it saves all linked border nodes. The scanning time dedicated to discover border nodes should be properly chosen. An optimized neighborhood method will be introduced to reduce the redundant links between border nodes. It will be described in section "Problem formulation." This procedure looks at smoothing the routing process later. When a packet data should be transmitted from one group to another, it should be made through these border nodes.

Border nodes of the same group share their inter-group tables at the end of the operation. Each border node has an entry in this table which includes information about other border node: node identifier, available resources, number of connections, linked border nodes, and border groups.

Transmission

Once all these operations were accomplished, the transmission process takes place through routing protocols.

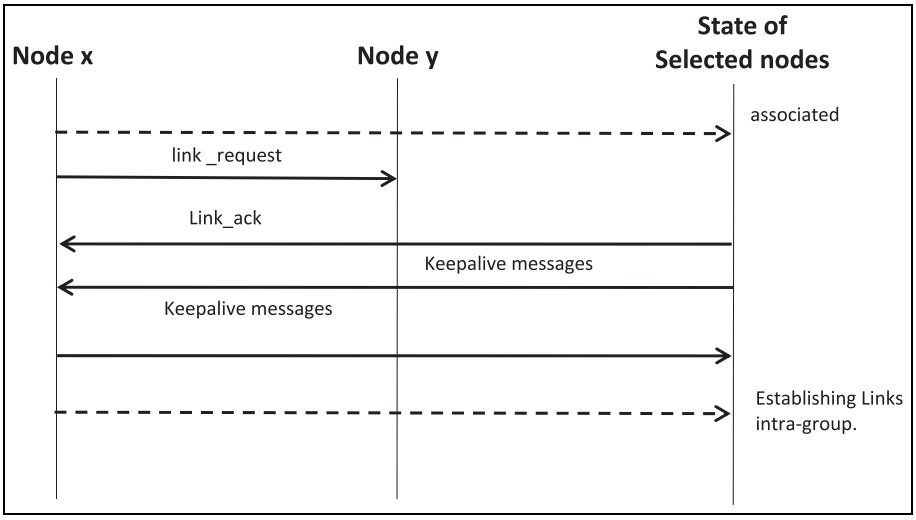

Figure 7. Establishing links intra-groups.

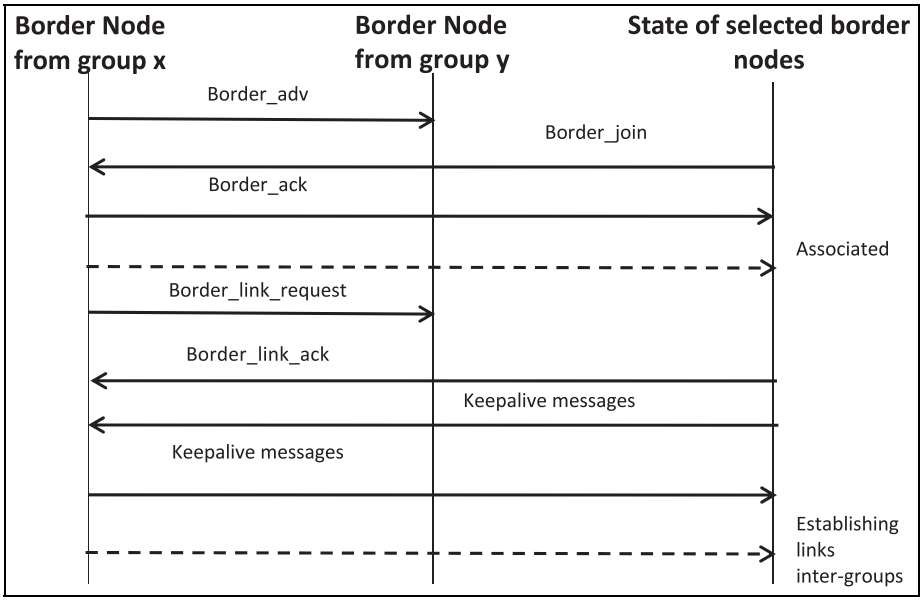

Figure 8. Establishing links inter-groups.

A route discovery process takes place once the organization into groups of nodes is finished. Let us consider that a source node will send information to a destination node. Two cases are considered:

1. If the source and the destination have the same group identifier which means that the information will be routed locally inside the group.
2. If the group identifier of the source and destination are different, then the packet is sent to the nearest border node which will use its inter-group table to find the best path to the destination group. This route uses only border nodes to transmit information. If the destination group is neighbor to source group, the packet should be transmitted to a border node of the destination group. This node will in its turn perform the routing task inside the group. In the case where the destination group is not one of the proximity groups, then the packet will be routed through border nodes of one or more groups until reaching the destination group. Border nodes will also route the packet to the destination node.

An example of routing between border nodes is illustrated in Figure 9 where we consider a source node

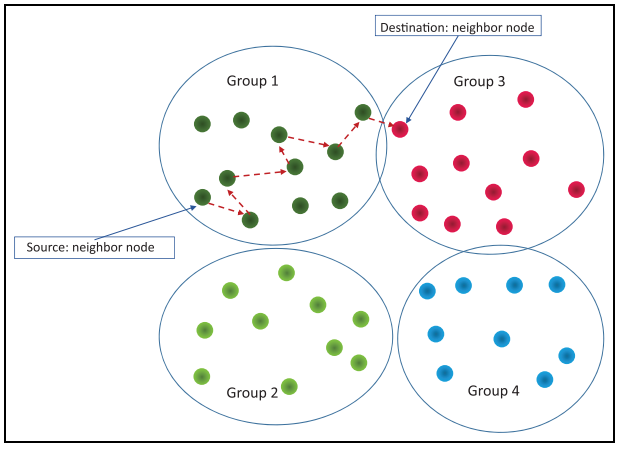

Figure 9. Example of routing between border nodes.

and destination node from different groups. A discovery route process will be launched. Data are routed through border nodes until reaching the destination group.

Each transmitted packet should have at least the source identifier, the source group identifier, the destination identifier, the destination group identifier, next hop or the whole path, and the data to transmit.

In the literature, we can find two types of routing protocols in ad-hoc networks: table-driven routing protocols which preserve a routing table even if no transmission is needed and on-demand routing protocols where routes are discovered only when it is required. When an inter-group transmission is needed, a route discovery is instantly launched. This allows to reduce energy consumption.[19] Therefore, we suggest to use a table-driven routing protocol inside each group and on-demand routing protocol to manage the inter-group routing operation.

Topology maintenance

When a network topology is being created, it is obvious to consider that many changes could occur in the network such as failure, mobility, or join of a new node. Some changes lead to update a part or even the whole architecture. Therefore, some backup strategies should be introduced. If the node that causes the changes is a normal node, only the intra-group table of the concerned group will be updated. However, if it is about border node, then both inter and intra-group tables will be actualized.

When a new node joins the network, it broadcasts a "new_node_adv" message to advert its presence. When a central node receives this message, it sends back a "join request" to invite him to join its group. The new node becomes a group member by sending an "acknowledgment" message. Then, an update of tables will occur and the network will be ready to work with the new node. The exchange of messages is shown in Figure 10.

In case where a node leaves the network because of failure, it will be noted by the absence of "keepalive" messages exchanged regularly between nodes. Once other nodes find it out, updating tables is mandatory to delete its entry.

Regarding a node mobility, we can consider it as disconnected node from a group and will join as a new node in another group in a different position. The messages flow is similar to the flow of new node join explained above.

This architecture is self-organized and able to adapt the network configuration according to the environmental parameters. Nodes are able to deal with changes and failures without any human intervention.

Problem formulation

According to the proposed architecture, neighborhood between border nodes plays a key role in reducing the communication cost. Our network is composed of a large number of sensor nodes deployed in the sensing area. Two node types are defined: border and normal. We will focus our interest only on reducing communication cost between border nodes. In this section, we introduce an optimized neighboring mechanism which reduces the flow of exchanged messages.

Inter-group communication model

The network could be modeled by a graph $G = (V, E)$, where V is the set of vertices which represent border nodes in the network and $E \subseteq V^2$ is the set of communication links among them. If distance d between node border node i and border node j is lower than the communication range R, then $e(i,j) \in E$

$$E = \left\{ e(i,j) \in V^2 / d(i,j) \leq R \right\} \tag{1}$$

Let us consider also g_i, $i = 1, \ldots, m$ as the number of groups among the network. The resulting graph is not static while new connections appear and disappear at any moment and nodes could be disconnected over time.

Let G be an example of graph that represents a possible network configuration (Figure 11). g_i and g_j are two adjacent groups. We count the number of edges that connect a border node from g_i to a border node from g_j and note it as the $N(g_i, g_j)$. Note also $N(g_i)$ and $N(g_j)$ the number of border nodes of g_i and g_j, respectively. The probability of connection between a border

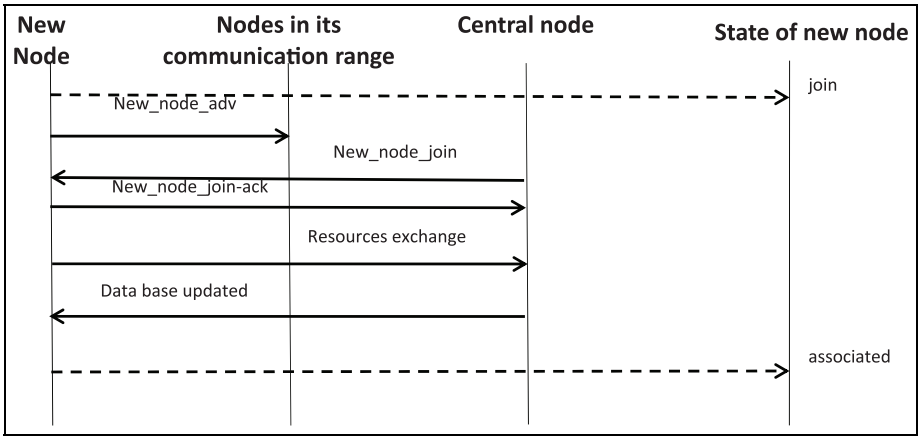

Figure 10. Messages when a new node joins the network.

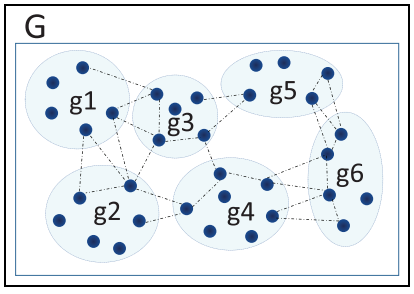

Figure 11. Initial graph *G*.

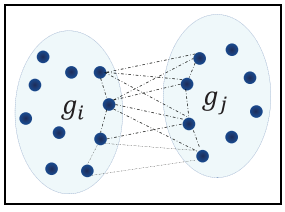

Figure 12. Links between two adjacent groups g_i and g_j.

node from g_i and a border node from g_j could be calculated as follows

$$p_c = \frac{N(g_i, g_j)}{N(g_i) \cdot N(g_j)} \tag{2}$$

If we consider that each border node will establish a link with all border nodes in its communication range, then we will find a large number of links between border nodes as illustrated in Figure 12. As we can note, the number of links is very important. Therefore, we aim to reduce the number of links using an optimized mechanism which eliminates the unnecessary links and which also ensure the intra-group connectivity.

Graph reducing algorithm for an optimal inter-group connectivity

Rather than having multiple links between border nodes which makes the communication more expensive, an optimized way is to reduce the number of links by a graph reduction algorithm.

The border selection algorithm takes as input the graph G and gives a sub-graph of G_c as output such as $G_c = (V_c, E_c)$ where $V_c \subseteq V$ and $E_c \subseteq E$. G_c should maintain the connectivity as the original graph G.

We suggest to apply the minimum spanning tree (MST) problem[20,21] to define inter-group links between border nodes. It allows to find a low-cost spanning tree from a graph using weighted edges. A weight function is defined for each edge.

Let us consider $V = \{v_1, v_2, \ldots, v_n\}$ is a set of vertices which represents the border nodes of each group and $E = \{e_{1,2}, e_{1,3}, \ldots, e_{i,j}, \ldots, e_{n,m}\}$ such as $e_{i,j} = 1$ if v_i and v_j have an edge and $e_{i,j} = 0$ otherwise.

Each edge has a weight value $w_{i,j}$ that represents the cost: it depends on the Euclidean distance between the energy level of the two concerned nodes. The weight of each edge could be calculated as follows

$$\omega_{i,j} = \frac{d(i,j) \cdot Available_{con}}{Max_{con}} \times \left(\frac{E(i,j)}{k_1} - 1 \right) \tag{3}$$

where $E(i,j)$ is the sum of the energy level of nodes i and j. $d(i,j)$ defines the Euclidean distance. K_1 is the minimum energy level of a node to operate. $Available_{con}$ defines the available number of links and Max_{con} is the maximum number of links.

Note $X = \{x_{1,2}, x_{1,3}, \ldots, x_{i,j}, \ldots\}/i \neq j$ such as

$$x_{i,j} = \begin{cases} 1 \text{ if } e_{i,j} = 1 \text{ and is selected} \\ 0 \text{ otherwise} \end{cases} \tag{4}$$

The result graph is a spanning tree formed by the x vectors. The MST-based border problem can be formulated as follows

$$\min f(x) = \sum w_{i,j} \cdot x_{i,j} \quad (5)$$

where the product between $w_{i,j}$ and $x_{i,j}$ is a Hadamard product. If $w_{i,j} \leq 0$, no link could be established.

The MST-based border selection algorithm consists of three main phases:

Step 1: Each border node collects information about its neighbor border nodes by performing a discovery process as explained in section "Architecture protocol and algorithms." It forms the border graph G. This graph contains all reachable border nodes.
Step 2: Using the collected information, MST algorithm is performed between them in order to find the new G_c border graph. The Prim's algorithm is applied locally at each border node. It starts by choosing a random vertex and marks it.
Step 3: Check all the vertices that are adjacent to the marked vertex and select the vertex that has the minimal weight and that does not create a cycle and mark it.
Step 4: Repeat step 2 until all the vertices are marked.

The flow chart in Figure 13 illustrates the algorithm of the suggested MST.

Real deployment and validation

Our proposed architecture might be applied in several real-world application going from agriculture to health care and from home appliances and indoor

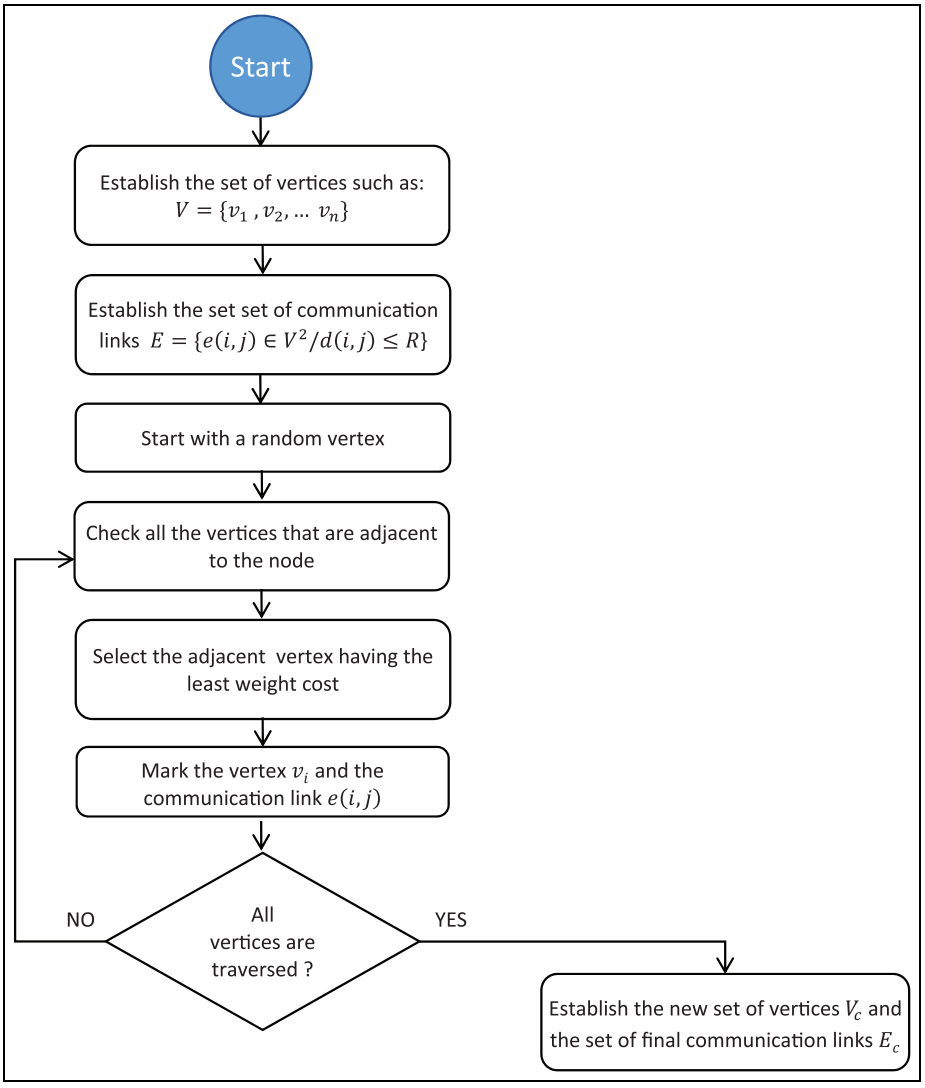

Figure 13. Flow chart of MST algorithm.

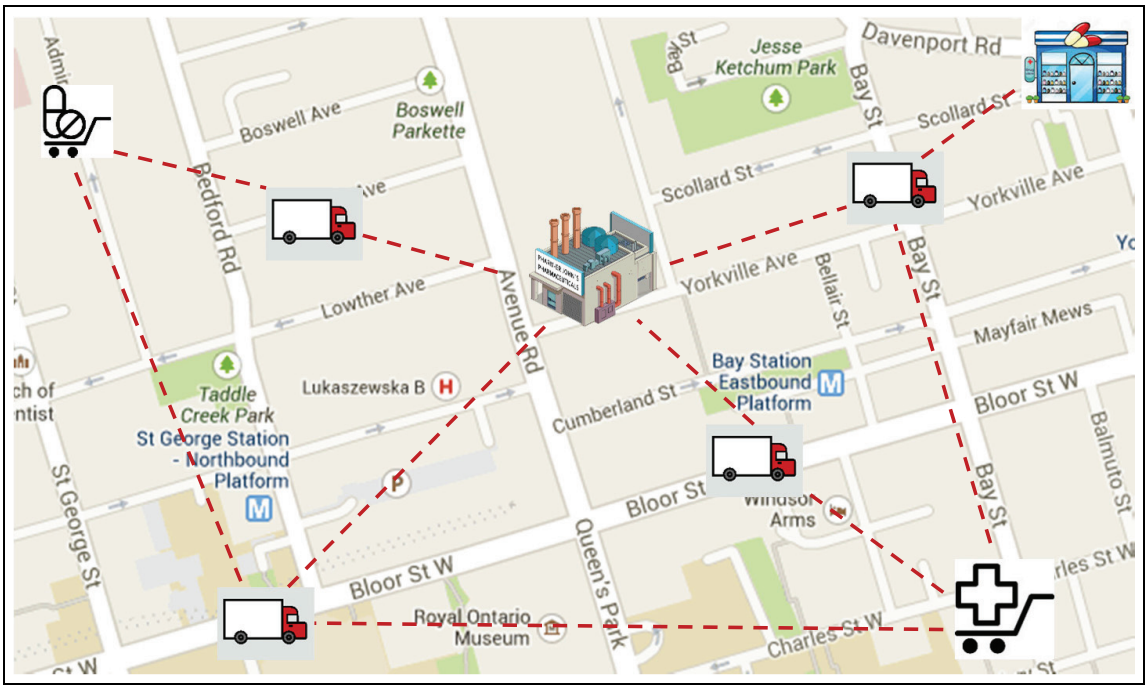

Figure 14. Architecture description in a real application.

applications to transportation and vehicular networks.[1,20] Nowadays, suitable methods to transport sensitive products without breaking or damage remain a challenge issue. In fact, medication and almost all pharmaceutical products could easily be damaged if it was imperfectly displaced. Moreover, some pharmaceutical drugs should be delivered in a cold or even frozen environment; others are glass packaged. Therefore, a convenient transport condition is necessary. We suggest to use group-based WSNs to monitor and track pharmaceutical products from manufacturer until reaching buyers. The objective of this network is to ensure the safety of medicines and track the problem in case where any product has undergone a hit or any mismanagement. Information about place and time should be saved.

In this section, we present an illustrative application of group-based architecture. First, we will describe a cooperative monitoring algorithm for pharmaceutical products. Then, a brief description of the used hardware will be presented. Finally, few measurements were performed in order to validate our proposed algorithm.

Application description

We propose a network which allows a cooperative monitoring of pharmaceutical products. Pharmaceutical drugs must be attentively carried. As shown in Figure 14, a communication network is implemented between manufacturer, transportation actors, which are responsible for the delivering task, and end buyers.

Figure 15. Example of sensor deployment into boxes.

The network gathers data from sensor nodes in boxes and processes sensor data. All collected data are saved in a local database. Pharmaceutical drugs are enclosed into boxes to which we attach nodes as shown in Figure 15.

The node will keep gathering and sending information about vibration and temperature periodically during the transportation operation. Therefore, an accelerometer is integrated in the node in order to control the vibration. This sensor is very useful especially for glass packaged products to avoid their damage. Likewise, the node is equipped with a temperature

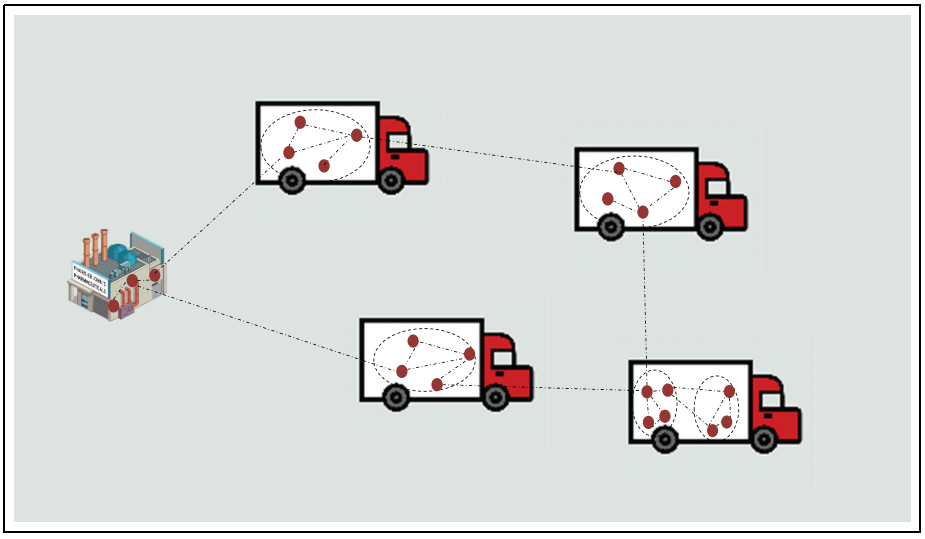

Figure 16. Group-based network for pharmaceutical drugs monitoring.

sensor. The use of this sensor could be perceived when we dispose of pharmaceutical drugs that need to be kept cold or frozen while transportation. All these collected information could be checked at any time by the pharmaceutical industry as well as by the end buyers. We suggest even to include nodes into containers.

The sensor node is activated when pharmaceutical products are enclosed into boxes that will be transported. The network allows tracking the trace of pharmaceutical drugs via sensor nodes.

We set few thresholds of temperature and accelerometer depending on the transported pharmaceutical drugs. If the gathered data exceed these thresholds, an alert will be launched to warn the person in charge. This allows to supervise, analyze, and even stop any occurred problem in a short time.

This network permits also to monitor the time of transportation. Analysis allows to improve transport conditions and avoid deterioration of products. Any undergone anomaly such as temperature variation or a hit will be noticed.

The benefits of group-based network in monitoring pharmaceutical products are the fact that we can consider one or many groups in many positions at the same time: in the warehouse, in containers, and so on. Moreover, in one container, we can consider few nodes packaged with pharmaceutical drugs as source nodes and one node as a destination. Therefore, nodes could operate at the same time in different locations through groups as shown in Figure 16. The container driver could provide the destination node to be alerted in case of damage as shown in Figure 17.

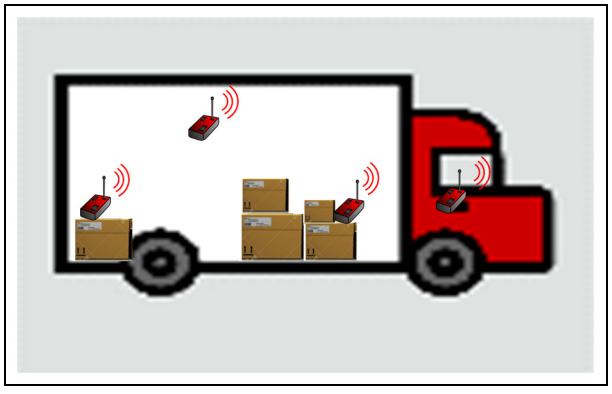

Figure 17. Example of deployment into a container.

Hardware description

We choose to work with Waspmote[22] nodes developed by Libelium. It is an extensible board dedicated for real deployment. Waspmote is provided with an Atmega 1281 running at 8 MHz, 4 KB of memory RAM, and an SD card of 2 GB. Waspmote is equipped with three-axis accelerometer and sensor temperature which are integrated on its board. The node is powered by a rechargeable battery. According to the datasheet, Waspmote could work until 7000 m with XBee-802.15.4-Pro radio. Therefore, we will use the IEEE 802.15.4 radio module operating at 2.45 GHz called "pro XBee" manufactured by Digi with a transmit power of 63 mW.

Sensor measurements

In this subsection, we present few test measurements gathered by the Waspmote in different environmental conditions in order to examine the performance of the proposed prototype. We place a network prototype of few nodes in many sets of pharmaceutical drugs. The prototype consists of few nodes that are able to gather

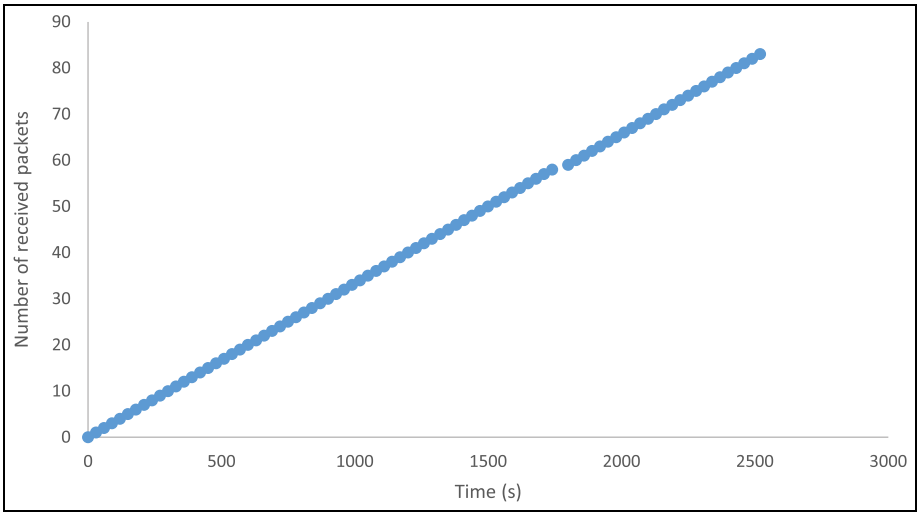

Figure 18. Number of received packets per seconds.

information about temperature and three-axis accelerometer.

The first test was was performed in order to observe the number of received packets compared to send ones. We consider a group of four nodes and one central node. The six nodes represent the group members. These nodes gather information about vibration and temperature each 100 s and send the gathered data to the central node.

The number of total received packets is equal to 83 packets; however, the number of total send is equal to 100. We observed many packets lost. Next, we had considered five nodes integrated in boxes and one gateway with the driver as shown in Figure 19.

Two nodes were elected as central nodes to form two groups. Each of the remained nodes has joined a group after exchanging discovery messages. At the end, we disposed of two groups; one group has two group members and the other one is formed by three nodes. We used carrier sense multiple access with collision avoidance (CSMA/CA) as a media access control (MAC) protocol, the gateway as the destination node, and remaining nodes as source ones. Each source node looks for the best route to send data to the gateway. Measurements were taken for 3000 s. The number of total received data in the gateway is represented in Figure 20.

The second objective was observing indoor and outdoor temperature values. Figure 21 illustrates values recorded during 1 h in outdoor. Temperature values were measured each 30 s. As we can see, the temperature had slight variations during the measurements time. The relevant values are comprised between 23.25°C and 24°C.

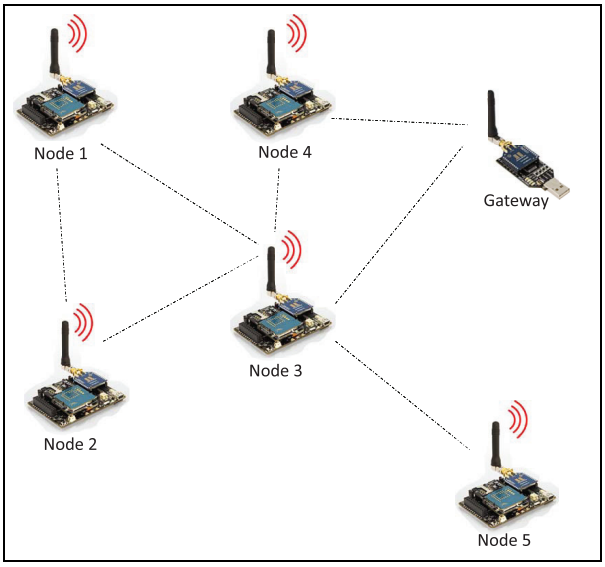

Figure 19. Network prototype.

Figure 22 illustrates the values recorded during 1 h inside a container. Temperature values were measured each 30 s.

The temperature value has suddenly decreased at the second 400 from 27°C to 25.75°C. Then, it increased gradually to reach again 27.5°C at the second 1200. The maximum noted value is equal to 27.75°C and the minimum one is 25°C.

The last measurement test was dedicated to detect vibration into a set of pharmaceutical drugs. For this purpose, we gather data from a three-axis accelerometer during 25 s. We purposely made a vibration to the box of pharmaceutical drugs for few seconds. Figures 23–25

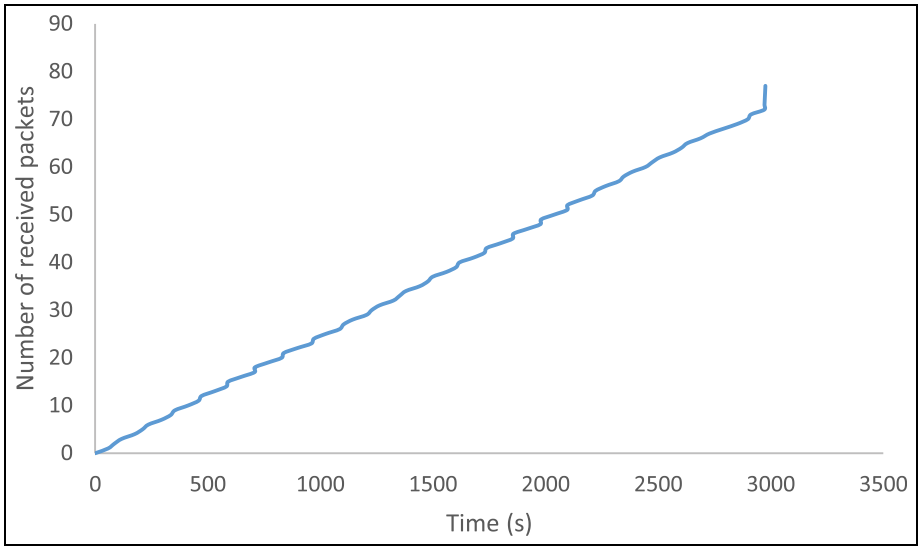

Figure 20. Number of received packets per seconds.

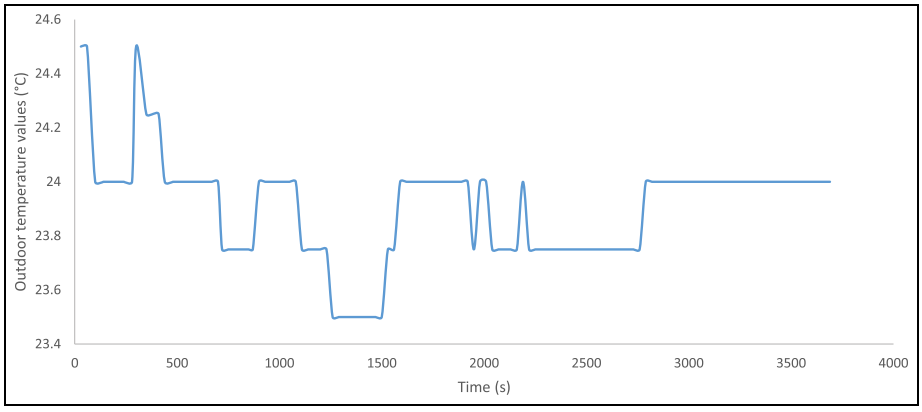

Figure 21. Outdoor temperature values.

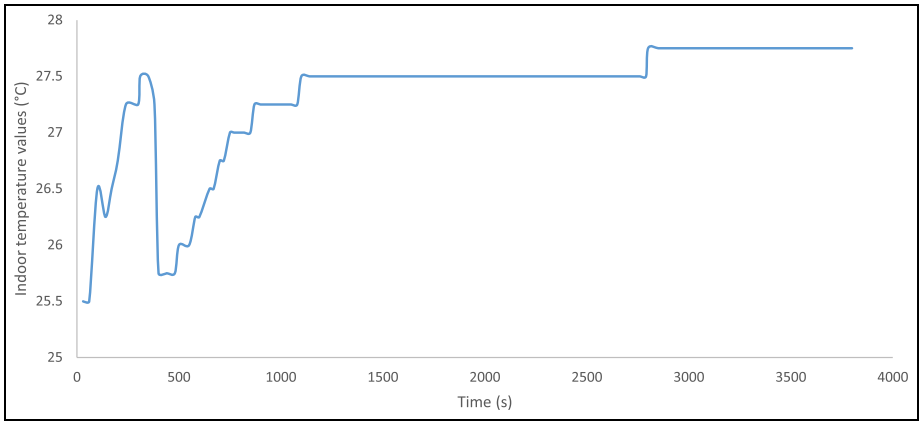

Figure 22. Indoor temperature values.

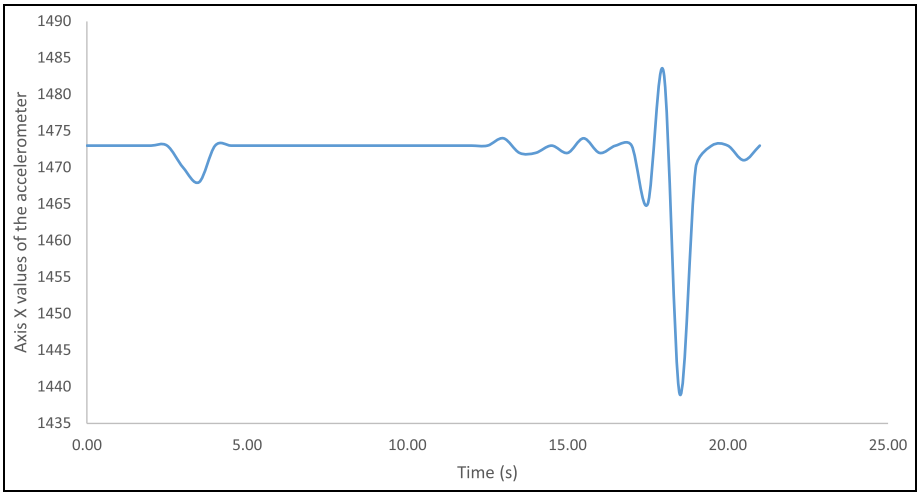

Figure 23. *X*-axis values of the accelerometer.

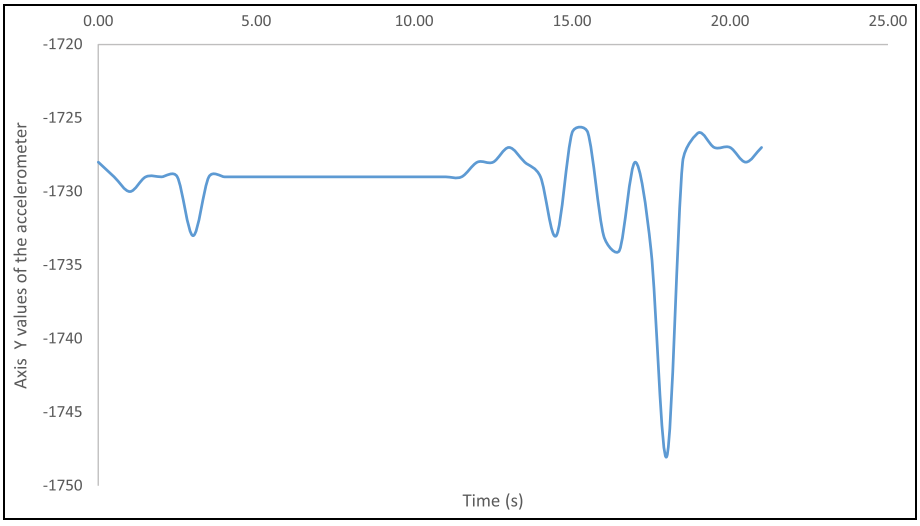

Figure 24. *Y*-axis values of the accelerometer.

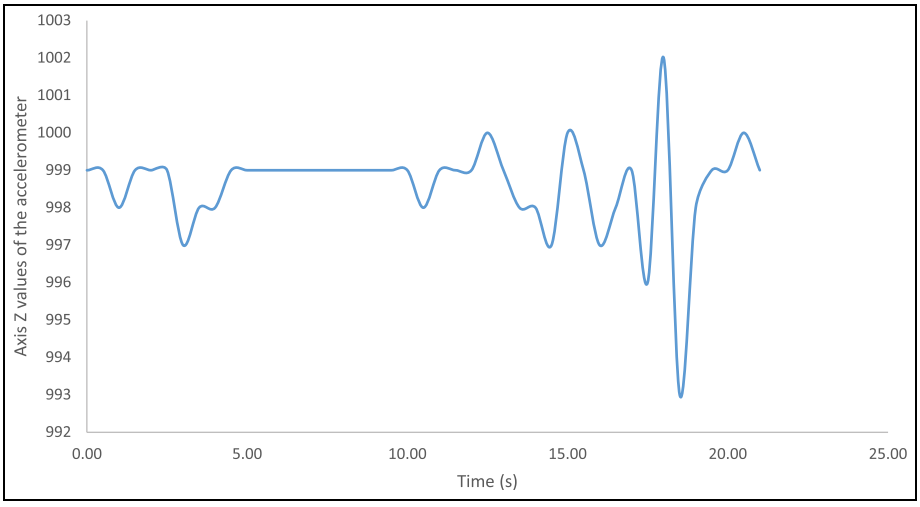

Figure 25. *Z*-axis values of the accelerometer.

present, respectively, the gathered data by the accelerometer on its *X*-axis, *Y*-axis, and *Z*-axis.

The most significant variations occurred between the 17th and 19th second. The impact is shown in the three axes. After the 20th second, the values remain stable.

Conclusion

In this article, we have introduced a new group-based architecture for ad-hoc networks. An optimized group division is performed in order to get balanced groups and a covered sensing area. An optimized communication protocol was thoroughly presented. Details about operation and fault tolerance were explained as well. We proposed to use table-driven routing inside each group and on-demand routing protocol to route data between groups. Furthermore, we suggested the use of the minimal tree spanning in the neighbors selection between groups. This method ensures the inter-group connectivity. Finally, we had illustrated our architecture by a real-life application. A cooperative monitoring for pharmaceutical products was presented using Waspmote nodes and ZigBee wireless technology. The proposed architecture improves the efficiency by ensuring extensibility, flexibility, and fault tolerance at the same time.

As future work, we intend to reinforce the infrastructure reliability and security by integrating security mechanisms. The objective is to add an adequate encryption method to protect the information gathered by the sensors. Moreover, we look at including actuators in addition to sensors in order to directly control physical world. We think that our proposed architecture is able to solve many issues and enhance the network to obtain higher performance and lower energy consumption in many real-life applications. Therefore, we aim to apply our proposal in many other real-life applications where we can add multimedia sensors or agriculture sensors.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

References

1. Dargie WW and Poellabauer C. *Fundamentals of wireless sensor networks: theory and practice*. Chichester: John Wiley & Sons, 2010.
2. Singh SP and Sharma SC. A survey on cluster based routing protocols in wireless sensor networks. *Proced Comput Sci* 2015; 45: 687–695.
3. Liao Y, Qi H and Li W. Load-balanced clustering algorithm with distributed self-organization for wireless sensor networks. *IEEE Sens J* 2013; 13: 1498–1506.
4. Beydoun K, Felea V and Guyennet H. Wireless sensor network infrastructure: construction and evaluation. In: *Proceedings of the 5th international conference on wireless and mobile communications, 2009 (ICWMC'09)*, Cannes, 23–29 August 2009, pp.279–284. New York: IEEE.
5. Peng IH and Chen YW. Energy consumption bounds analysis and its applications for grid based wireless sensor networks. *J Netw Comput Appl* 2013; 36: 444–451.
6. Lloret J, Garcia M, Tomás J, et al. GBP-WAHSN: a group-based protocol for large wireless ad hoc and sensor networks. *J Comput Sci Technol* 2008; 23: 461–480.
7. Lloret J, García M, Boronat F, et al. MANET protocols performance in group-based networks. In: Mammeri Z (ed.) *Wireless and mobile networking*. New York: Springer, 2008, pp.161–172.
8. Lloret J, Garcia M and Tomas J. Improving mobile and ad-hoc networks performance using group-based topologies. In: Miri A (ed.) *Wireless sensor and actor networks II*. New York: Springer, 2008, pp. 209–220.
9. Lloret J, Palau C, Boronat F, et al. Improving networks using group-based topologies. *Comput Commun* 2008; 31: 3438–3450.
10. Garcia M, Sendra S, Lloret J, et al. Saving energy and improving communications using cooperative group-based wireless sensor networks. *Telecommun Syst* 2013; 52: 2489–2502.
11. Garcia M and Lloret J. A cooperative group-based sensor network for environmental monitoring. In: Luo Y (ed.) *Cooperative design, visualization, and engineering*. Berlin; Heidelberg: Springer, 2009, pp.276–279.
12. Beydoun K and Felea V. WSN hierarchical routing protocol taxonomy. In: *Proceedings of the 2012 19th international conference on telecommunications (ICT)*, Jounieh, Lebanon, 23–25 April 2012, pp.1–6. New York: IEEE.
13. Kifayat K, Merabti M, Shi Q, et al. Group-based key management for mobile sensor networks. In: *Proceedings of the 2010 IEEE Sarnoff symposium*, Princeton, NJ, 12–14 April 2010, pp.1–5. New York: IEEE.
14. Shaikh RA, Jameel H, d'Auriol BJ, et al. Group-based trust management scheme for clustered wireless sensor networks. *IEEE T Parall Distr* 2009; 20: 1698–1712.
15. Kifayat K, Merabti M, Shi Q, et al. Group based secure communication for large-scale wireless sensor networks. *J Inf Assur Secur* 2007; 2: 139–147.
16. Mantri D, Prasad NR and Prasad R. Grouping of clusters for efficient data aggregation (GCEDA) in wireless sensor network. In: *Proceedings of the 2013 IEEE 3rd international advance computing conference (IACC)*, Ghaziabad, India, 22–23 February 2013, pp.132–137. New York: IEEE.
17. Chen YS, Hsu CS and Lee HK. An enhanced group mobility protocol for 6LoWPAN-based wireless body area networks. *IEEE Sens J* 2014; 14: 797–807.
18. Haneef M, Wenxun Z and Deng Z. MG-LEACH: multi group based LEACH an energy efficient routing algorithm for wireless sensor network. In: *Proceedings of the 2012 14th international conference on advanced*

communication technology (ICACT), Pyeongchang, Korea, 19–22 February 2012, pp.179–183. New York: IEEE.
19. Chang YC, Lin ZS and Chen JL. Cluster based self-organization management protocols for wireless sensor networks. *IEEE T Consum Electr* 2006; 52: 75–80.
20. Fazio P, De Rango F, Sottile C, et al. Routing optimization in vehicular networks: a new approach based on multiobjective metrics and minimum spanning tree. *Int J Distrib Sens N* 2013; 2013: 598675.
21. Saravanan M and Madheswaran M. A hybrid optimized weighted minimum spanning tree for the shortest intra-path selection in wireless sensor network. *Math Probl Eng* 2014; 2014: 713427.
22. Waspmote, http://www.libelium.com/products/waspmote/