Border Surveillance using sensor based thick-lines

Ramzi Bellazreg*, Nourredine Boudriga* and Sunshin An+
* University of Carthage Tunisia and + Korea University
Email : ramzi_bellazreg@yahoo.fr; noure.boudriga2@gmail.com; sunshin@dsys.korea.ac.kr

Abstract—Wireless Sensor Networks (WSNs) are being used in many applications ranging from target surveillance in battle fields to intelligent home networking. From the recent applications, in which the WSNs are used, we can find the border surveillance applications. The first aim of this class of applications is to monitor a country border and detect the presence of the intruders near this border line. In this paper, we propose a global framework based on WSNs to design such applications. Then, we investigate the architectural issues needed to ensure good detection and tracking of the targets. We also propose a deployment strategy of nodes and the routing technique used to transmit the data through the network nodes.

Index Terms—WSN, border surveillance, sensor deployment, target tracking.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are used in many applications covering both military and civilian domains. The first goal of the use of a WSN-based solution is to monitor a particular event in a sensed area. In particular, a surveillance application monitors either an area or a borderline. One of the most recent surveillance applications of WSNs, one can consider the border surveillance applications. This kind of applications is becoming critical due to the increase of the risks of intrusion on borders. Due to the global risks near their borders, governments are frightened of the appearance of intruders on their borders, either for unauthorized importation of goods or for terrorism actions. Then all governments have demonstrated a need a good and efficient surveillance system to control suspect activities on borders.

Typically, WSNs within these applications are based on small devises connected through radio links and are able to detect the presence of intruders in the monitored area. However, a good monitoring necessitates certain coverage requirement to avoid shadowing areas and missing measurements. Based on these facts, the sensors have to be efficiently deployed to provide a good quality of coverage. An efficient deployment of sensors has to satisfy many requirements including the degree of coverage, network connectivity, and network maintainability. For those reasons one of the most important tasks in implementing a WSN for Border Surveillance is the deployment phase.

Many recent works have addressed border surveillance applications based on WSNs. Many solutions using WSNs have organized the network nodes as a line-sensor [5-9], where every movement going over a barrier of sensors is detected, in this case, sensor nodes deployment should guarantee barrier coverage. Compared to full coverage, a barrier coverage based on a perfect linear deployment requires fewer sensor nodes and may experience radio disconnection due to sensor failure and depletion. In addition, this kind of linear architecture does not permit the tracking of intruders, since the intruders are detected only when crossing the line-sensor and their future movements cannot be tracked. Furthermore, in the barrier coverage model, the sensor nodes are not able to locally determine whether the barrier coverage is ensured [1]. This limitation impedes the development of localized algorithms. Barrier and k-barrier coverage require, for instance, that all crossing paths in a monitored region are covered by at least one sensor node or k distinct sensor nodes, respectively.

In [2], Sun et al. proposed a 3-layered hybrid network architecture for border patrol. In Bordersense [2], advanced sensor networks technologies have been deployed, including multimedia sensor nodes, mobile sensor nodes, and scalar sensors, which could be deployed underground or above the ground. The authors analyzed the k-barrier coverage requirements in terms of sensor density when the sensor nodes are deployed randomly in a belt in front of the border according to the Poisson point process with spatial density. The high cost of the deployment of multimedia sensors (cameras) makes the deployment of Bordersense for larger borders difficult. Furthermore, a uniform distribution of sensor nodes cannot be achieved in such environment.

Liu et al. [3] investigated the construction of sensor barrier on long strip area of irregular shape when sensors are distributed according to Poisson point process. To ensure that trespassers cannot cross the border undetect, multiple disjoint sensor barriers will be created in distributed manner covering large scale boundaries [3]. Then, a segmentation technique has been proposed to achieve continuous barrier coverage of the whole area.

In [4], Dudek et al. proposed a demonstrator, consisting of 10 sensor nodes, for WSNs in the frame of border surveillance application and with which the basic functionality of the network along with trespasser detection have been tested. The case of border surveillance when sensor are randomly but non-uniformly deployed has been investigated in [5,6]. Uniform sensor deployment is useful in theoretical analysis but remains unrealistic in the real deployment where a non-uniform placement is obtained do to several environmental factors. Saipulla et al. [6] assessed that barrier coverage could be obtained under line based deployment and outperforms that of Poisson model. K-barrier coverage has been the focus of [1]. S. Kumar et al. proposed an algorithm to determine whether a belt region is k-barrier coverage or not and
introduced the notions of weak and strong barrier coverage. Weak barrier coverage detects intrusion attempts when trespassers go over a barrier of stealthy sensors, however, strong barrier coverage detects intrusion when even sensors are not stealthy. Most of the proposed frameworks for border surveillance assumed a line-based network where barrier or k-barrier coverage is ensured. Under this assumption, we drastically reduce the number of needed sensors to monitor a given border, this amelioration is obtained at the expense of the performance of the network. In other words, line-based deployment at best ensures the detection of all intrusion attempts, but will not allow to take an internal decision about tracking the intruders. Furthermore, the sensor nodes deployment which follows a uniform distribution [2,3] is not realistic due to environmental factors and sensor nodes deployment process (air-dropping, throwing from aircraft). Another limitation of the proposed models is the silence about the connectivity issue which is closely related to coverage issue. To enhance the performances of border surveillance WSN, it is recommended to deal with connected-coverage. In this paper, we will deal with connected coverage in border surveillance WSN under the full coverage model and we will also treat the routing process which has not been addressed in the presented works.

In this paper, we present an implementation framework of Border surveillance solutions using Wireless Sensor Networks. In particular, we provide the following contributions:
- a global network architecture for border surveillance based on three types of components deployed on a thick line architecture set up along the border;
- a deployment strategy to comply with many constraints on the network operation, including coverage maintenance, connectivity preservation, and routing quality of service;
- a mechanism of routing management to ensure an optimal and efficient process of data relaying and reporting between the different nodes. We also present the mechanism of elaboration of the routing tables at the different levels of the network.

The rest of the paper is organized as follows. The architecture of the network and the different node features are introduced in Section II. Section III describes the detailed steps of the deployment strategy proposed for the different nodes in the network. In Section IV, we present a routing scheme to be used in our framework. Section V assesses the efficiency of the proposed deployment protocol through some conducted simulations. Finally, Section VI concludes the paper.

II. ARCHITECTURAL ISSUES

In this section, we will present the global architectural issues of the network that will be used by our border surveillance system. We will first, present the hierarchy of the nodes used and the functionalities assured by each type of node. Then we will present the global network architecture and the disposition of the nodes in the monitored area.

A. Node Hierarchy

Sensor networks can be classified into two categories: flat sensor networks and heterogeneous sensor networks. In a flat WSN, all the sensor nodes have the same sensing, communication and processing characteristics. A heterogeneous WSN integrates various sensor types with different capabilities. For instance, some sensors may have larger battery lifetimes and more powerful processing resources. The presence of heterogeneous nodes (i.e., nodes with an enhanced energy capacity or communication capability) in a WSN has the advantage of increasing network reliability and lifetime. Typically, a large number of inexpensive nodes perform simple sensing tasks, while a few expensive nodes (that may be embedded on mobile platforms) provide network control, data filtering, fusion and transport. This segregation of roles promotes a cost-effective design of the network as well as a more efficient implementation of the overall sensing application. In this paper, we consider the particular case of a heterogeneous wireless sensor network for border surveillance. To ensure efficient border surveillance, we will use three kinds of nodes. Each one of those types is responsible of a specific goal.

- The Basic Sensing Nodes (BSN): Those nodes compose the first hierarchical level. They are the most elementary nodes in the considered architecture. The first rule of a BSN is to detect the presence of an event or an intruder. After detecting events, a BSN will report the gathered data to the nearest DRN (Data Relay Node). In addition, to this major mission, a BSN can be charged of relaying other sensor’s reported data. That will be the case, when a BSN has not directly a DRN in its transmission range.

- The Data Relay Nodes (DRN): those nodes are in the second hierarchical layer of the network. The first responsibility of those nodes is to collect the data received from the different BSN nodes. The second function of the DRN is to route those reports to the nearest Data Dissemination Node (DDN). This can be done in a one hop manner (directly to the DDN) or in a multi-hop (through intermediate DRN nodes) manner. Thus, each DRN has hierarchically a set of BSN under its control and is responsible of routing their reports to a DDN. The exchange of data between the BSNs and the DRN to which they are attached will be in duplex mode. This is useful, because in addition to the routing task, the DRN will be charged of the BSN management. The DRN will be responsible of communicating some operating orders to the BSNs such as scheduling management, energy consumption control, or routing information.

- The Data Dissemination Nodes (DDN): Those nodes compose the third layer of our network. Hierarchically, under each DDN node we have many DRNs. The DDN node receives the reports from the DRNs. Its rule is to send the collected data to Network Control Center (NCC) for analysis. The global nodes hierarchy is represented in Figure 1.
B. The Network topology

In this subsection, we will present the topology of the network or, in other terms, the physical repartition of the nodes. We consider a thick line network because it enlarges the area covered by the network and permits a tracking of the intruders. In fact, if we consider a linear network, the target will be detected only one time when it crosses the line covered. But, if we consider a thick line network, a whole strip is covered and then many BSN nodes will detect the target along this strip and the sensing task is more realistic, more efficient, and reflects the behavior and displacements of the targets. Thus, in addition to the detection process, intrusion tracking and location estimation can be performed. The topology of the network is represented by Figure 2.

III. THE DEPLOYMENT STRATEGY

The aim of the deployment is to ensure an optimal and efficient quality of coverage and reporting.

A. The deployment of the DRN nodes

As presented in the previous section, we will consider a thick line topology for the network. For the DRN, we will deploy them in a linear manner and this line will be the main artery of the network. When deploying the DRNs on this virtual line, we have to ensure that all the nodes are mutually connected. Such linear repartition is connected when any DRN node have at least two other DRNs in its communication range and is placed between those nodes. We denote by \( RC_{DRN} \) the communication range of the DRNs. Thus, a good deployment have to ensure the probability of presence of at least one DRN in each segment of width \( RC_{DRN}/2 \).

As represented in Figure 3, when considering the segments s1, s2 and s3 and deploy a BSN in each segment we will have a full covered network. In fact, the maximum distance between any couple of points P1 in s1 and P2 in s2 will be less than \( RC_{DRN} \) (and respectively the distance between any couple of points P2 in s2 and P3 in s3 will be less than \( RC_{DRN} \)). Then, having a DRN in each segment of width \( RC_{DRN}/2 \) will ensure a full connectivity of the network, because each DRN will be connected to a left and right neighbor. Having two neighbors in the two directions, each DRN will have a patch to all the other DRNs of the network.

\[
N_{DRN} = D / (RC_{DRN}/2)
\]  

The deployment of the \( RC_{DRN} \) node will not be done in a deterministic manner (or known positions) but as shown previously, each segment of larger \( RC_{DRN}/2 \) will contain one DRN.

B. The deployment of the BSN nodes

The first constraint of the deployment of BSNs that should be ensured is that the DRNs must have the capability to communicate to each one of the BSNs in a one hop connection. Based on this constraint, the larger of the strip should be \( 2 * RC_{DRN} \) and the DRN line is in the center of the strip. In fact, if the large of the strip is superior to \( 2 * RC_{DRN} \), we can have a BSN node far from the DRN line of a distance superior to \( RC_{DRN} \) and then it is not in the connectivity range of its hierarchical relative DRN.

At this step, we estimate the width of the strip and determine the number of the required BSNs. A good quality of the BSNs deployment has to ensure an efficient coverage of the monitored area (which is the first goal of the conceived network). For the deployment strategy, we will use the deployment solution proposed in [12]. This method is an extension of the solution presented by the authors in [11] and takes into account the effects of natural environments. In this deployment method, we rely on the log-normal shadowing model proposed in [10] to represent radio propagation in natural environments. Due to the effect of radio environment factors in real contexts, every sensor does not have a uniform range distribution according to the propagation direction. Therefore, we propose
a new deployment strategy that takes into account the impact of radio effects. For this, we denote by \( R_i \) the sensor range in direction \( i \) (the value of \( i \) varies between 0 and 359). We considered a disc of radius \( R_t \) that represents the target and expanded this area with the respective \( R_i \) in each direction. We will denote by \( S \) the surface of the area.

An example is depicted in Figure 4, where it is clear that the sensors \( S_1 \) and \( S_2 \) detect the target of radius \( R_t \) because their coverage surfaces intersect with the disc of radius \( R_t \). However, sensor \( S_3 \) does not cover the target. Based on this reasoning, it can be said that for the target to be \( k \)-covered, the area \( S \) must contain at least \( k \) sensors. Therefore, the required density of the BSN nodes is given by Equation 2.

\[
\rho_s = \frac{k}{S} \tag{2}
\]

Thus, we have shown that the next step for coverage control consists in calculating the area of the surface \( S \). Analyzing the statistical properties of the variation of \( R_i \). The corresponding probability density function is given by Equation 3.

\[
p(R) = \frac{1}{\sigma \sqrt{2\pi}} \exp\left(-\frac{(R - \mu)^2}{2\sigma^2}\right). \tag{3}
\]

Consequently, the area of the surface \( S \) is then given by Equation 4.

\[
S = \int_{R=0}^{R=R_{max}} \int_{\theta=0}^{\theta=2\pi} (R_\theta + R)dRd\theta \tag{4}
\]

where \( p_\theta(R) \) gives the probability that the range is equal to \( R \). Then, we will calculate the integral of \( (R_\theta + R) \) when varying \( \theta \) between 0 and \( 2\pi \). This gives the area of the sector of radius \( R_\theta + R \) and angle \( \theta \).

\[C. \text{ The deployment of the DDNs} \]

Let us first notice that the DDNs deployment has not many requirements to comply with. In fact, we do not have neither coverage density needed nor required connectivity between the deployed DDNs. A DDN needs only to receive data from the DRNs, either by one-hop connectivity or multi hop DRNs connectivity.

\[\text{Thus, we need only to define the number of the DRNs using the same superior hierarchical DDN. Having, the total number of the DRNs, we can then determine the number of needed DDNs in the whole network. This number is given by equation 5.} \]

\[
N_{DDN} = \frac{(N_{totalDRN})}{(N_{DRNperDDN})} \tag{5}
\]

To be sure the DDN nodes are in the communication range of the DRNs, they will be deployed in a strip centered around the DRN line of \( 2 \ast R_{CDRN} \) width. The DDNs will be deployed in the strip with regular intervals. We do not need really rigorous positions of the DDNs because in all the cases, those nodes will receive data routed through many DRNs.

\[\text{IV. THE ROUTING TECHNIQUE} \]

In this section, we present the routing procedure used in the proposed architecture. The process of detection begins at the BSNs which detect and prepare the data related to the occurring events in their area of coverage. Then, the BSN has to send this data to the nearest DRN using a routing tables. Each BSN is assumed to have a routing table that indicates the route to the corresponding DRN. Each line of the routing table contains the following information:

- The Deive Identiﬁer (the Mac address) of the next hop;
- The Deive Identiﬁer of the DRN; and
- The number of hops to reach the DRN through this route;

The routing tables of the BSNs are constructed dynamically after exchanges between the nodes through a 2-step process:

\[\text{First Step: Periodically, each DRN sends a beacon message that indicates its presence. This message is a multicast message because it can be used by any BSN. At the end of this step, the BSNs that can send directly data (in one hop) to a DRN will detect that fact. The transmission range used when sending this type of message has to be } R_{CDRN} \text{ and not } R_{CBSN}. \]

In fact, if we send the beacon message using \( R_{CDRN} \) communication range it will reach BSNs that are distant from the DRN of more than \( R_{CBSN} \). Thus, they will suppose having a DRN directly reachable but, in fact, it is not in their communication range and the routing information will be false. At the end of the first step, some BSNs will add a direct route to a DRN in their routing table. The devise identifier of the DRN is sent in the beacon.
message. The beacon message has the format.

\{DRN\_Presence, DRN\_Devise\_Identifier\}

Second step: Each BSN will send its routing table to its neighbors. When receiving the routes declarations from a neighbor, each BSN will update its routing table, if necessary. The update is done if the received route indicates fewer hops to reach the DRN than the available route. Each BSN sends its routing table periodically to ensure that all the routes in the whole network are up to date. The BSN also sends its routes immediately when its local routing table is changed. This message has the following format.

\{Route\_Update, Source\_Devise\_Identifier, DRN\_Devise\_Identifier, number\_of\_hops\}

After some exchange rounds between the BSNs, all the routing tables will be filled in and every BSN will have an indication of a route in direction of its hierarchically attached DRN. The number of the rounds needed to have a converged network is relative to \(RC_{BSN}\) and to the width of the strip \(2 \times RC_{DRN}\).

B. The routing from DRN to DDN

Once an optimal route is built, the data is relayed through the BSNs and reaches the corresponding DRN. This data is sent (through intermediate DRNs) until it reaches a DDN. As presented in the deployment strategy section, each DRN will have two adjacent DRN neighbors and then at least two possible paths to a DDN. The routing table of each DRN contains two entries and each one describes one of the routes. Each entry has these attributes.

- The devise identifier of the neighbor (the next hop);
- The devise identifier of the DDN;
- The number of intermediate DRNs on this route.

The DRN nodes then select the best route (that presents the minimal intermediate hops, for instance) to reach the DDN. The establishment of the routes at the DRNs is done through routing updates between the DRN neighbors.

V. Simulations

In this section, we first present the simulation model used to evaluate the performances of the proposed network architecture. Then, we discuss the results of some conducted simulations. The aim of those simulations is to analyze the routing process proposed in this paper.

A. The simulation model

The characteristics of the simulation model are listed in the followings:

- The communication range of the DRNs is equal to 80 meters;
- The monitored area considered in the simulation is 1000m

\* 160 meters (2 \(RC_{DRN}\));
- We will consider in the simulations many values for the k-coverage quality varying form k=1 to k=9;
- We also considered many sensing and communication ranges for the BSNs to study their impact on the quality of the deployment.

Considering this model, we conducted two simulations. The aim of the first simulation is to study the impact of the k-coverage parameter on the routing technique and the number of the hops needed to reach the DRN line. In the second simulation, we varied the communication range of the BSNs and studied the impact of this parameter on the number of non-connected BSNs. By non-connected BSNs we meant a node which does not have a path to the DRN line.

B. The variation of the number of hops

In this simulation, we varied the coverage factor k and measured for each value the mean number of hops needed for a BSN to reach the DRN line. We also measured the maximum number of hops for each value of k. We fixed the communication range of the BSNs to \(RC_{BSN} = 20m\). The results of this simulation are represented by Figure 5.

![Figure 5: The number of hops](image)

We can observe in this simulation, that the worst mean value for the number of hops is equal to 4 intermediate nodes, which is an acceptable value. Also, when considering the worst case of all the conducted simulations, the maximum number of hops detected for all the BSNs is equal to 12 intermediate sensors. Then, we can deduce that our routing proposed deployment and routing techniques, gives good performances regardless to the number of hops needed to reach the DRN line.

C. The number of non-connected BSNs

In the second simulation, we have observed the number of the non-connected BSNs. This metric gives an indication on the quality of the deployment and the relative connectivity percentage. In the first part of this simulation, we fixed the parameter k to 1-coverage and varied the BSNs communication range from \(RC_{BSN} = 6m\) to \(RC_{BSN} = 24m\). The table I represents for different values of the Communication range, the total number of the deployed nodes and the number of the nodes that have not a route to a
DRN node.

Figure 6 represents the percentage of non-connected sensors.

![Percentage of non-connected BSNs for 1-coverage](image)

Figure 6: Percentage of non-connected BSNs for 1-coverage

We can remark from the results, that we have a small number of sensors non-connected. We remark that as well as the communication range increases the percentage of not-covered nodes becomes less.

In the second part of the second simulation, we conducted the same simulation as the previous case but for 2-coverage deployment. We varied the BSNs communication range from $RC_{BSN} = 6m$ to $RC_{BSN} = 24m$.

The table II represents for different values of the Communication range, the total number of deployed nodes and the number of the nodes that have not a route to a DRN node. We notice from the previous table that the number of the non-covered sensors is less than those for the case of $k=1$ for 1-coverage. In fact, for $k=2$, we have more sensors deployed than in the case of $k=1$; and thus we have more possibilities of finding routes. Therefore, when we have a larger value for $k$ (which is general the case in most deployments), we may have a very little percentage of non-covered nodes. For example, for this simulation, the percentage is varying between 0.16% and 0.64%.

Table I: The non-connected nodes for 1-coverage

<table>
<thead>
<tr>
<th>$RC_{BSN}$</th>
<th>6 m</th>
<th>8 m</th>
<th>10 m</th>
<th>12 m</th>
<th>14 m</th>
<th>16 m</th>
<th>18 m</th>
<th>20 m</th>
<th>22 m</th>
<th>24 m</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number total deployed nodes</td>
<td>7534</td>
<td>4296</td>
<td>2094</td>
<td>1884</td>
<td>1376</td>
<td>1054</td>
<td>832</td>
<td>674</td>
<td>558</td>
<td>468</td>
</tr>
<tr>
<td>Non-connected nodes</td>
<td>34</td>
<td>17</td>
<td>10</td>
<td>7</td>
<td>5</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Table II: The non-connected nodes for 2-coverage

<table>
<thead>
<tr>
<th>$RC_{BSN}$</th>
<th>6 m</th>
<th>8 m</th>
<th>10 m</th>
<th>12 m</th>
<th>14 m</th>
<th>16 m</th>
<th>18 m</th>
<th>20 m</th>
<th>22 m</th>
<th>24 m</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number total deployed nodes</td>
<td>15068</td>
<td>8412</td>
<td>5388</td>
<td>3768</td>
<td>2752</td>
<td>2108</td>
<td>1664</td>
<td>1348</td>
<td>1116</td>
<td>936</td>
</tr>
<tr>
<td>Non-connected nodes</td>
<td>24</td>
<td>16</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>8</td>
<td>8</td>
<td>6</td>
<td>6</td>
<td>6</td>
</tr>
</tbody>
</table>

VI. CONCLUSION

In this paper we developed a solution for the border surveillance problem using Wireless Sensor Networks. The main contributions in this paper aim at presenting a framework to ensure border surveillance. We presented the general architectural aspects of the network used. We also proposed deployment and routing techniques to be used in this network. The deployment has to ensure several constraints in particular the coverage of the sensed area and the connectivity of the nodes to ensure a good quality of coverage and an efficient exchange of the sensed data. An extension of this paper includes the use of different parallel string to build along the border so that an efficient tracking and interception of intruders can be provided. A second extension will address the detection of failing sensor and builds mechanisms for their replacement.

REFERENCES