A Wireless Sensor Network Border Monitoring System: Deployment Issues and Routing Protocols

Mohammad Hammoudeh, Fayez Al-Fayez, Huw Lloyd, Robert Newman, Bamidele Adebisi, Ahcène Bounceur and Abdelrahman Abuarqoub

***Abstract*—External border surveillance is critical to the security of every state and the challenges it poses are changing and likely to intensify. Wireless Sensor Networks (WSN) are a low cost technology that provide an intelligence-led solution to effective continuous monitoring of large, busy and complex landscapes. The linear network topology resulting from the structure of the monitored area raises challenges that have not been adequately addressed in the literature to date. In this paper, we identify an appropriate metric to measure the quality of WSN border crossing detection. Furthermore, we propose a method to calculate the required number of sensor nodes to deploy in order to achieve a specified level of coverage according to the chosen metric in a given belt region, while maintaining radio connectivity within the network. Then, we contribute a novel cross layer routing protocol, called Levels Division Graph (LDG), designed specifically to address the communication needs and link reliability for topologically linear WSN applications. The performance of the proposed protocol is extensively evaluated in simulations using realistic conditions and parameters. LDG simulation results show significant performance gains when compared to its best rival in the literature, Dynamic Source Routing (DSR). Compared to DSR, LDG improves the average end-to-end delays by up to 95%, packet delivery ratio by up to 20%, and throughput by up to 60%, while maintaining comparable performance in terms of normalized routing load and energy consumption.**

***Index Terms*—Chain-type wireless sensor networks, WSN routing protocols, media access control, border security and surveillance, linear networks, network coverage and connectivity, strong barrier, weak barrier.**

I. Introduction

Securing international borders is a complex task that involves international collaboration, deployment of advanced technological solutions and professional skill-sets. However, there are many factors hindering the development of an effective system for international border security and surveillance. In the current tight financial climate, governments strive to secure their borders, but also ensure that costs are kept low. This is particularly challenging to achieve given very long land and maritime borders. For instance, the external land border of the EU from 1 January 2007 is 7.958 km and the maritime borders are nearly 80.000 km long [1]. With borders of this length, a very large number of trained border guards and resources are essential. Training and equipping border guards is very expensive. Moreover, it is not always feasible to deploy border guards along the borders due to the hostile topography, severe weather conditions, and political or military conflicts.

Wireless Sensor Network (WSN) technology offers an intelligence-led, cost effective solution for monitoring vulnerable points on the international borders. A WSN is a set of resource-constrained devices that monitor the environmental conditions. A network of unattended self-organizing sensors can significantly cut the number of personnel in a border agency. Additionally, the continuous monitoring reduces the chances of missing any potential criminal activity. The ability of a WSN to operate without human involvement and in situations where other surveillance technologies are impractical has made it favorite for deployment in hostile hazardous environments. Yet WSNs can be easily integrated with existing systems to provide a common data set at every point of intervention. Data integration from multiple systems is a key feature of modern day border control and surveillance systems.

Some WSN applications impose a linear network topology, e.g., international border security, gas/petrol pipeline monitoring and rail track monitoring. The linear topology has nodes daisy chained using radio communication. Linear WSN (LWSN) topologies are characterized by sparse node deployment, long transmission distances, and alignment of nodes along a virtual line. This range of characteristics introduces new challenges that make solutions proposed for traditional WSNs inapplicable to LWSNs.

The current research in LWSNs addresses problems as they arise from a narrow application perspective. For instance, many routing protocols were proposed for pipeline monitoring applications [2], [3], [4]. In such protocols, data collection is typically accomplished through specialized mobile or power-rich nodes. In border security, this is not always possible. For example, in wild forests, it is unfeasible for an unmanned vehicle to bypass large natural obstacles. Therefore, there is a need to tackle the problem fundamentally at the topological level. This paper contributes a cross layer communication protocol that is tailored to address the requirements of LWSNs. We apply this protocol to border security and surveillance as it presents a complex set of challenges that are generic enough to cover most LWSN applications. Routing deals with issues such as data reliability, timeliness, error rate, network lifetime, and system scalability; these determine the success of any WSN system.

The rest of this paper is organized as follows. Section II

M. Hammoudeh, F. Al-Fayez, H. Lloyd and B. Adebisi are with the Manchester Metropolitan University, UK. E-mail: {m.hammoudeh, f.al-fayez, huw.lloyd, b.adebisi@mmu.ac.uk
R. Newman is with the University of Wolverhampton, UK. E-mail: r.newman@wlv.ac.uk
Ahcène Bounceur is with the University of Brest, France. E-mail: ahcene.bounceur@univ-brest.fr
A. Abuarqoub is with the Middle East University, Jordan. E-mail: aabuarqoub@meu.edu.jo
Manuscript received June 30, 2016; revised August 26, 2016.

surveys routing protocols designed for LWSN applications. Section III presents an architecture for LWSN-based border surveillance system. Section IV identifies and evaluates the quality of intruder detection metrics and their suitability for a border monitoring applications. Section V presents the details of network segmentation and inter-cluster routing protocol. In Section VI, the path simulation and routing evaluation results are presented and discussed. Finally, conclusions are drawn and future work is suggested.

II. Related Work

In [5] a hybrid WSN architecture for border patrol systems is described. The main contribution of this paper is to outline techniques from the literature to calculate node density and determine the number as well as the location of monitoring towers. However, the cost of such a system is extremely high and its multi-phase sensing could introduce significant reporting delays. The collaboration between sensors in different layers requires complex coordination techniques. Furthermore, the integration of the multimodal data is not a trivial task.

More recently, a border intrusion detection system that aims to enhance the coverage quality and detection accuracy has been proposed in [6]. A model to calculate the amount of redundancy required to guarantee the quality of sensing coverage is presented. The authors do not give the full details of the model and ignore the practical difficulties of node deployment. Moreover, the claims made by the authors on reduced false alarms, determining the direction of crossing, detection accuracy were not verified experimentally.

A maritime border surveillance system was proposed in [7]. It focuses on distinguishing between ship-generated waves and ocean waves.The main limitation of [7] is that it requires a dense network to achieve low miss-rate, especially with small vessels, because of the high noise in the sea. Additionally, it is based on a grid network topology, which is difficult to realize in real-world deployments such as dropping nodes from a plane.

The work in [8] presents an energy-aware routing protocol for WSN-based border surveillance. The authors propose a routing algorithm that splits sensor nodes to several scheduling sets and keeps track of the energy level of each sensor node. This algorithm is based on the routing algorithm published in [9], which addresses the m-coverage and n-connectivity problem. This routing algorithm considers the scenario where the heterogeneous sensor nodes are randomly distributed in a circular region, which renders it unsuitable for border surveillance applications.

In [10], a set of well-known routing protocols, Ad hoc On-Demand Distance Vector (AODV), Optimized Link State Routing Protocol (OLSR) and DSR, were simulated using OPNET. It was found that DSR performs better than other protocols in border surveillance applications. The authors propose a minor modification to DSR to achieve better energy management in border surveillance applications. The proposed modification does not achieve significant energy gains and is hardware platform specific. The study focuses on energy consumption without giving any attention to any quality-of-data or Quality-of-Services (QoS) aspects.

FleGSens [11] is basic system for area surveillance using only simple passive infrared sensors for trespass detection. It focuses on ensuring integrity and authenticity of reported events in the presence of an attacker who may compromise a limited number of nodes. The network itself follows a grid topology. The hop-based routing ignores load balancing and link reliability, which are critical in hostile environments and could have considerable impact on the packet delivery ratio and timeliness. Moreover, the grid topology does not match the requirements of international border applications, which typically favor linear topologies. Relying on such assumptions limits the scalability and usability of [11].

It is evident from the literature survey that there is no systematic approach to the application of WSNs to border security and surveillance. Most reviewed systems are built with narrow application objectives in mind. There is no serious attempt to address the fundamental challenges imposed by large-scale border security and surveillance at the topological level. The linear structure of the network topology necessitates new solutions not only at the application level, but also at the data link and application levels. As the network infrastructure becomes more complex, it needs to accommodate several applications. These applications have many, potentially conflicting, requirements such as timeliness, reliability, data accuracy and energy efficiency. It is important to accommodate these requirements before a generic architecture for linear-based WSN that covers a wide spectrum of application is realized.

III. System Architecture

Most of the current WSN systems for area monitoring are multi-layered systems. To overcome the drawbacks of multi-layered systems, explained in Section II, we propose a flat, modular system architecture to offer timely, mission-centric event detection. The proposed architecture is open to any hardware platform and does not assume any sensing modality. Flat systems comprise a set of Basic Sensor Nodes (BSN), which collaborate to detect and report events.

Conventional border surveillance systems rely on of fixed checkpoints, Monitoring Towers (MT), mobile vehicles, and border guards. Border guards could be equipped with man-pack antennas. The proposed network architecture builds on top of the existing border surveillance infrastructure. BSNs are deployed in unattended ground to provide higher granularity for monitoring.

Surveillance towers, which may be stationary or mobile, e.g., armored vehicle dispatched to incident, collect and route data to the wired network. Surveillance towers can host powerful and reliable multimedia sensors, i.e., radars and cameras. Information from BSNs and the multimedia sensors can be fused at the MT to reduce the false alarm rate. After the MT confirms an intrusion reported by a BSN(s), they report the intrusion location to the remote control and command center.

Due to coverage considerations and to reduce the miss-rate, the number of deployed BSN(s) is expected to be very large. Hence, the network is divided into several segments. A segment comprises a MT and the BSNs to its left and

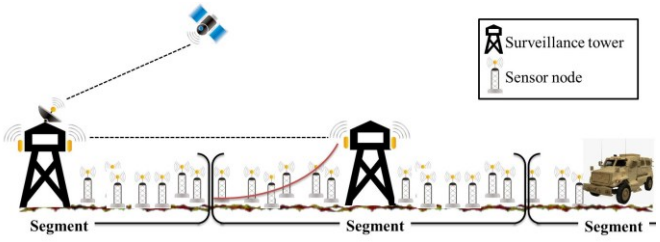


Figure 1. A sketch of the system architecture adopted in this work.

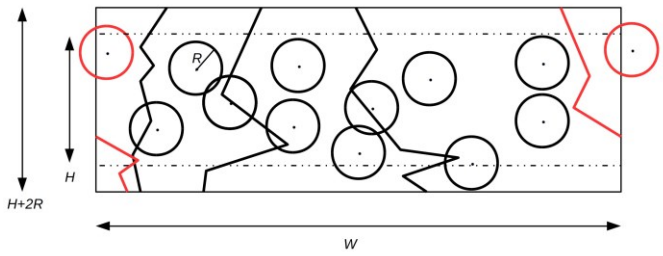


Figure 2. Schematic representation of the sensor deployment simulation. The red sensor disc and path illustrate the implementation of the cyclic boundary condition.

right, which transmit their data to it. Similarly, MTs coordinate with each other to improve the detection rate. The details of the segmentation process are given in Section V. Figure 1, sketches the described network architecture.

IV. Detection Quality and Sensor Density

In this section we consider how to determine the required network width and node density for a border surveillance network. Coverage is a crucial metric to determine the capacity of monitoring. Connectivity ensures that the data can be delivered to the base-station with the specified QoS guarantee. In the context of border security, the problem is often formulated as a *k*-barrier of a belt region [8], [12], [13], [14]. For border surveillance applications, it is assumed that the intruders attempt to cross the width of the belt. A belt is a region bounded by two approximately parallel curves. A given belt region is said to be *k*-barrier covered if all crossing paths through the region are *k*-covered, i.e., they overlap at least *k* sensors.

Barrier coverage can be further subdivided into *strong* and *weak*. [12] introduce the notion of strong *k*-barrier formation, in which there are *k* disjoint strong barriers crossing the region. [13] derive a condition on the sensor density required to form a *k*-barrier with high probability. Several subsequent authors have developed algorithms for finding strong barriers in an already-deployed network in some optimal way [15].

A weak barrier is one in which all *orthogonal* crossing paths overlap the sensing area of at least one network node. Exact and approximate expressions for the probability of formation of a weak barrier with a given node density are given by [16]. Similarly to strong barriers, we can define a weak *k*-barrier as one in which all orthogonal crossing paths overlap at least *k* nodes. A condition for the formation of weak *k*-barriers was derived by [12]. [17] derive bounds on the probability of formation of weak *k*-barriers, and present an efficient algorithm for determining whether a given deployment of sensors satisfies the weak *k*-coverage condition, and if not, what fraction of the region is covered.

[18] introduced the *DetQM* metric. This is the probability that an intruder is detected by at least one node, integrated over all possible straight line paths through the sensing region, with a certain probability that an intruder travels through a narrow corridor called the *Trespasser's Favorite Path* (TFP) region. They conclude that *DetQM* is significantly reduced when the probability of following TFPs is high. In fact, the probability of detection is minimum when intruders follow straight line paths orthogonal to the border region, and this corresponds to *DetQM* in the limiting case when the probability of following TFP is 1, and the TFP region has zero width.

In the remainder of this section, we attempt to answer two important questions: (1) What is the appropriate metric in order to measure the detection quality of the network? (2) What is the required number of sensor nodes to deploy to achieve a specified level of coverage according to the chosen metric in a given belt region, while maintaining radio connectivity within the network? To answer these questions, we compare four metrics of detection quality as functions of the BSN density for parameters appropriate for a border intrusion detection network: P_S, the probability of strong barrier formation, P_W, the probability of weak barrier formation, $P_\perp$, the probability of detection of orthogonal paths and quantities *DetQM*. These are calculated either by applying the appropriate analytical formulae or are derived from using monte-carlo methods, where no closed form exists.

We consider a rectangular border region of width w along the border direction, and depth h normal to the border, in which sensors are randomly deployed with a mean line density ρ. The mean surface density of sensors in the region is therefore $\sigma = \rho/h$. The sensors deployed in the region have a sensing radius r, with the probability p of sensing an intruder given by the binary model, that is for a sensor at $\underline{\mathbf{r}}_\mathbf{s}$ and intruder at $\underline{\mathbf{r}}_\mathbf{i}$, $p = 1$ for $|\underline{\mathbf{r}}_\mathbf{s} - \underline{\mathbf{r}}_\mathbf{i}| < r$, 0 otherwise. The simulation domain used for the calculations in this section (and the path simulations of section VI-A) is shown schematically in Figure 2.

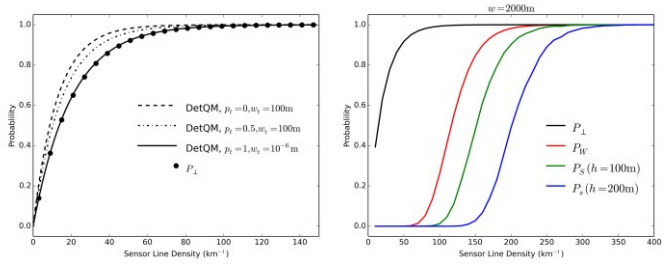
A. Detection probability and DetQM

[19] show that in the limit where the sensing region is large compared to the individual sensors, the probability of detection of a path is distributed according to a Poisson distribution. An intruder is detected by any sensors which are within a distance r of the path: the expectation value of the number of sensors within r of an orthogonal path is simply $2\rho r$, so the probability of there being no such sensor is

$$P_0 = e^{-2\rho r}$$

(from the Poisson distribution) and hence the probability of detection of orthogonal paths is

$$P_\perp = 1 - P_0 = 1 - e^{-2\rho r}.$$



a b

Figure 3. a. Comparison of *DetQM* and $P_\perp$ b. $P_\perp$, P_W (approximate formula), and P_S (Monte-Carlo)

It is straightforward to show that *DetQM* tends to $P_\perp$ as the width of the TFP region tends to zero, and the TFP probability tends to one. Figure 3a shows values of *DetQM* plotted against sensor density for $w = 2000$m, $h = 100$m and various values of the TFP parameters (two cases with $w_t = 100$m, and the limiting case $p_t = 1$, $w_t \to 0$. Note that since the expression for *DetQM* contains a singularity at $w_t = 0$, we set this parameter to a small value (10^{-6}m) in order to approach the limit. The figure confirms that *DetQM* tends to $P_\perp$ in the limit, and that even with $p_t = 0.5$, *DetQM* overestimates the detection probability considerably compared to $P_\perp$.

B. Radio Communication

The probability that a node can communicate with at least one other node can also be derived from the Poisson distribution. The expectation value of the number of node centers within the radio communication distance R_{radio} of a given node is $\pi\rho R^2_{\text{radio}}/h$, and hence the probability that a node can communicate is

$$P_{\text{radio}} = 1 - e^{-\rho\pi R^2_{\text{radio}}/h}$$

Since R_{radio} is typically $\approx 2r$, we find that

$$P_{\text{radio}} > P_\perp \quad \text{if} \quad h \;;\mathrm{S}\; 2\pi r$$

For typical deployments (say, $r = 25$m and $h = 100$m) this condition is easily satisfied so nodes connect with high probability, when $P_\perp$ is also high.

C. Barrier Coverage

We calculate the probability of strong barrier coverage using a Monte-Carlo approach. For strong barrier coverage, we require that there are no possible paths crossing the domain, which do not intersect at least one sensor's detection region. This is equivalent to finding a continuous chain of overlapping sensing regions, which also overlaps both edges of the domain in the x direction. The calculation proceeds by deploying random sensor fields, and searching for strong barriers by constructing a graph in which each vertex represents a sensor, and the edges are the lines joining the sites of pairs of sensors with overlapping sensing regions. We then perform a depth-first search of the graph, seeking a path from one edge of the domain to the other. If the traversal is successful and a path is found, then the sensor field has strong barrier coverage. Note that if either boundary has no overlapping sensors, there can not be a strong barrier.

Figure 3b shows $P_\perp$, P_W (from [16]'s formulation) and P_s for two barrier heights as functions of sensor line density. Note that strong barrier coverage is dependent on the height of the barrier region, and is less likely for the larger value of h, since strong barrier formation depends on the surface density of sensors.We see that forming a strong barrier with high probability requires a much higher density of sensors than are needed to form a weak barrier with the same probability.

D. Discussion

DetQM is seen to overestimate the probability of detection of intruders, and hence to systematically under-specify the sensor density. This is acknowledged by [18] who note that trespasser's favorite paths should be taken into account. However, we argue that in the absence of knowledge of the details of intruders' movements (and any TFP regions) we should make the assumption that intruders are acting in order to minimize their probability of detection. We must further assume that intruders have no knowledge of the locations or sensing ranges of the sensors, in which case they will achieve this goal by taking the shortest possible path through the border region. This argument has also been used by [17] as a justification for using weak barrier coverage, in which all such paths are detected. We therefore argue that $P_\perp$, the probability of detection of intruders who minimize their risk of detection, is a better measure of the detection quality of the network than *DetQM*. In any case, $P_\perp$ is the most conservative measure based on detection probability since it is formally the lower limit; furthermore, *DetQM* tends to this limit if the most conservative assumptions are made.

We show that metrics based on barrier formation will potentially over-specify the network. For the same probability, barrier formation requires much higher sensor density than path detection. Using barrier formation as a metric also leaves open the question of how many intruders are likely to penetrate the network. For example, with strong barrier formation we know the probability that *no* intruders will penetrate, but in the cases where no barrier is formed we have no measure of the likely rate of intrusion. A detection probability-based metric can easily be included in any analysis which seeks to compare the cost of deployment with some measure of the cost of intrusions.

Finally, we note that in a real deployment, the algorithm due to [17] can be run centrally and concurrently within each barrier segment to provide an estimate of $P_\perp$, by calculating the weak barrier fraction.

V. Network Segmentation and Inter-cluster Communication

In this section we present a new LWSN segmentation and communication protocol with the aim of reducing energy usage and transmission delays whilst maintaining or improving the system's quality of service. Reduction of energy usage requires careful attention to the network topology during its

initialization phase. During this, a network connectivity graph is built by the MTs. Each local MT is assigned level 0. BSNs are assigned to various logical network levels in a breadth-first order. In effect, the level of a BSN is directly proportional to the number of hops to reach the MT. Occasional connectivity updates are used to deal with temporal changes in the wireless channel.

The allocation of BSNs to network levels is critical since the amount of energy consumed by each BSN varies relative to its location from its MT. BSNs in the lowest network levels suffer greater power consumption, because data from higher levels travel through them to reach the MT. Simultaneously, border surveillance applications require immediate notification of time sensitive information. BSNs in the highest network levels, i.e., nodes located farthest from the MT, experience the longest delays. Therefore we focus our analysis on the transmission delays of these BSNs. The communication protocol described is general-purpose and cross-layer. It is designed to address with the aforementioned requirements of a LWSN.

A. Energy Balancing by Limiting the Transmission Distance

We propose applying transmission power control techniques to achieve energy savings in lower network levels. We aim to balance energy consumption across a network segment by dynamically adjusting BSNs transmission power based on their network level. When increasing the distance traveled at each hop, the end-to-end delay decreases at the cost of higher power consumption [20]. For a shorter per-hop transmission distance, less energy is consumed due to lower transmission power, while end-to-end delay increases linearly proportional to the number of hops on the path to the sink. Therefore, limiting the transmission distance/power of BSNs in lower network levels is expected to reduce their energy expenditure enough to compensate for the high-workload they incur. Similarly, BSNs in higher network levels transfer data over longer distance to the reduce-end-to end delay.

A BSN transmission power model needs to consider the hardware design of a node and the requirements of the communication standards. The power of a certain signal is calculated as

$$p = \rho S_0 d^{-\alpha} E$$

where ρ is the fixed transmitter power, S_0 is the channel gain between typical Tx-Rx, d is the distance between Tx-Rx, and α is the path-loss exponent ($\alpha > 2$). The distance is estimated from the Received Signal Strength (RSS) as

$$D(km) = 10^{(L - 32.44 - 20log(f))/20}$$

where L is the maximum path loss and f is the signal frequency in MHz.

The proposed power control technique can also be used by MAC protocols to improve the probability of successful data transmissions. Moreover, the number of collisions is expected to decrease as only nodes with overlapping coverage will contend to access the medium. This improves network bandwidth utilization, reduces the hidden and exposed terminal problems, and reduces end-to-end delays. At the physical layer, using a higher transmission power allows coding and modulation methods with a higher bit/baud ratio. This is particularly beneficial, because adjusting the bandwidth based on the current workload increases energy savings.

B. LDG: A Routing Protocol for LWSNs

The main objectives of the Levels Division Graph (LDG) protocol are: (1) To organize BSNs into network segments; (2) To allocate BSNs according to a communication cost and reliability into smaller manageable levels; and (3) To establish the shortest/most cost-efficient/most reliable link to the MT.

We assume that each MT is equipped with a bi-directional antenna. Messages are labeled *left* or *right* depending on which transceiver they are sent over. The LDG algorithm is initialized by each MT broadcasting beacon messages (called level_msg) containing its ID, direction (left or right), $level_k$, and synchronization information. In the initial level_msg, $level_k$ is set to 0 and the broadcast transmission power is limited to r_s (the maximum radio range of a BSN). All BSNs that receive the initial level_msg set their level to L_1 or R_1 depending on the direction of that message. BSNs in levels L_1 or R_1 can communicate with the MT directly. Having several direct links with the MT provides fault tolerance and load balancing. BSNs in higher levels use a backoff mechanism to delay any actions on the received level_msg. During the backoff time, BSNs wait to receive all potential level_msg. At the end of the backoff time, every BSN chooses the 'best' level_msg it received. The source of the best level_msg is recorded as the next hop to the MT. The 'best' message is defined in Subsection V-C. Each BSN down the communication tree increments the received level value by 1 and adds the cost of its link to the received cumulative path cost. Using the received level and path cost information, BSNs determine which MT to join.

The level_msg broadcast process continues until the left direction of the MT at one end of the segment meets the right direction of the MT at the other end of the segment. Nodes located at the level where the two directions meet choose to join the nearest MT over the most reliable link and do not re-broadcast any level_msg.

C. Link Selection in LDG Algorithm

BSNs use a cost metric to choose the 'best' MT and the 'best' parent to reach that MT. The cost metric defines the effective path as the shortest, most reliable, and energy efficient path. It accommodates the effects of communication interference resulting from simultaneous transmissions. Information about link quality is provided by the MAC layer. The data routing tree is built based on the quality of the link and the residual energy of all nodes up the tree. The paths offering high energy level, but poor link quality, or vice versa, are given high cost to avoid coverage/communication holes Similarly, paths having high residual energy and poor link quality suffer from high bit error rate, which leads to increased retransmissions causing energy depletion and high end-to-end delay.

The proposed cost metric incorporates the residual energy of the potential parent, distance to reach it and the quality of the link connecting the two nodes. The cost of the link

used for sending 1 bit from BSNs i in $level_i$ to node j in adjacent $level_j$ can be calculated as follows

$$Cost(i, j) = \frac{d(i, j)}{L_q(i, j)} \times \frac{E_i}{E_j}$$

where $d(i, j)$ is the distance between i and j, L_q is the i-j link quality indicator, and E_i and E_j are the residual energy of i and j, respectively. The E_i/E_j is introduced to increase the communication cost with BSNs with low residual energy.

The link quality approximations depend on the Channel State Information (CSI). In this work, we adopt the RSS as the link quality indicator. RSS is widely adopted in the literature for this purpose. It was proven that the RSS, if higher than about $-87dBm$, correlates closely with the PDR [21]. The overall cost of the link, including the end-to-end delay, is calculated as

$$Cost_l(i, j) = w(i, j)^{\alpha} \times (L_d)^{\beta}$$

where α and β are non-negative integers and L_d is the delay incurred on the link. α and β are constants of proportionality for the weight adjustment. The link end-to-end delay can be calculated using the method described in [22]. If no received level_msg advertisements satisfy both requirements of energy efficiency and low end-to-end delay, then the BSN with maximum energy and CSI value below the β threshold will be selected as the next hop or the minimum CSI with energy above the α threshold will be selected as the next hop candidate.

The algorithm for the parent selection considers the full path to the MT to ensure that the algorithm equalizes the length of the segment and balances its membership. The cumulative path is the summation of the weights of individual links forming the path from the node to the MT. The cumulative path cost is given as

$$Cost(i, MT) = \sum w_t(i, i_p) \ldots w_t(j, bs)$$

where i is to be associated with MT, i_p is the parent of i, and j is the vertex of edges connecting the last BSN in the path to the MT forming the path, P, from i to bs.

D. Communication Phase

In this phase, BSNs send notifications to their MT. Each BSN on the route to the MT updates the path residual energy level in the transmitted message. When energy levels of any BSN node drop below a critical threshold, a local path reconfiguration process is started. The low-power BSN sends a path_update message asking all neighboring nodes to advertise their cost value. This message contains the ID of the previous node on the path (n_p). Upon receiving the path_update, n_p enters into a maintenance state and starts its backoff timer. All nodes hearing the path_update message except n_p respond by sending a level_update message, which is the same as the level_msg. Only nodes in the maintenance state read the level_update messages. At the end of the backoff time, n_p selects a new parent offering the best path. Path updates are not expected to occur frequently, because load-balancing is one of the main design factors of the cost metric used to establish routes to the MT.

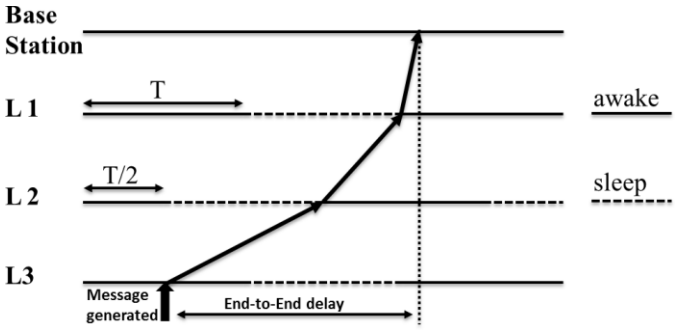


Figure 4. Shifted sleep/wake scheme.

E. LWSN Duty Cycle

In this subsection, we present the design of a synchronous wake-up-scheduling scheme for LWSNs that adheres to the unidirectional end-to-end delay constraints posed by large-scale border surveillance applications. Each node at level l_{i-1} has parents P_n at level l. We denote one period of the wake-up cycle as an interval and we examine P_n consecutive intervals BSNs in every level apply the same wake-up pattern in their corresponding interval and sleep in the other $P_n - 1$ intervals. For instance, in a basic periodic wake-up pattern where $P_n = 2$, every node is assigned two parents p_1 and p_2. If p_1 is awake, p_2 can go to sleep and vice versa. In this setup, the child node views the same pattern as in the always-up single parent case and enjoy the same chances to send a message. Therefore, the end-to-end delay stays unchanged while BSNs wake up P_n times less frequently as the single-parent case. Consequently, the formula for delay distribution is the same as in the single-parent case, but the effective wake up time is scaled down by a factor of P_n. During any interval, a BSN may wake up several times. The effective wake up period is calculated as

$$T = \lim_{\{t \to \infty\}} \frac{t}{N_t}$$

where N_t is the number of wake-ups in period t. This means that BSNs wake up once every T sec. In the multi-parent case, the effective wake up period is t/P_n.

At the network layer level, the receive-send-sleep cycle is implemented by shifting the wake-up pattern of the BSNs in even levels by $T/2$. T is the length of the wake up period. In this scheduling scheme, the worst-case delay is when a message is generated by a child immediately after the wake-up of the parent of the node. In this scenario, the first hop needs T seconds and the following $(h-1)$ hops each needs $T/2$ seconds. The worst-case end-to-end delay is $(h+1)T/2$ and the distribution of delay is $D = h/2T$.

This wake up shifting scheme reduces the end-to-end delay by half when compared to fully synchronized schemes, where all BSNs in the network wake up at the same time based on a fixed T. The overall distribution delay in the multi-parent case is $D = h/2P_nT$. Finally, we note that for a given sleep schedule, we simply adjust the BSN density required for a given sensor coverage by a constant factor corresponding to the mean duty cycle of the BSN. This is because at any one

time, the randomly deployed nodes will still be distributed according to a Poisson distribution.

VI. Evaluation

A. Monte-Carlo Simulations

In this section we describe experiments using a Monte-Carlo simulation code which computes the probabilities of intruder detection and of strong and weak barrier coverage. Let x be the coordinate along the border region, and y the coordinate normal to x. The simulation domain is bounded by $x \in [0, w]$, $y \in [-h/2-r, h/2+r]$. Sensors are deployed in the region $x \in [0, w]$, $y \in [-h/2, h/2]$. The boundaries at $x = 0$ and $x = w$ are cyclic, so that intruder paths, which cross one of these boundaries are continued from the opposite boundary. The cyclic boundary condition for sensors is implemented by simply replicating any sensor in $x \in [w - r, w]$ at $x^t = w - x$, and any sensor in $x \in [0, r]$ at $x^t = w + x$.

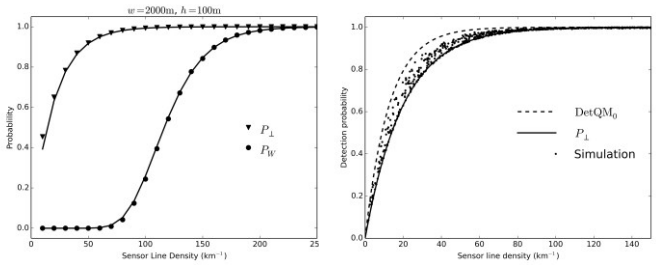
In order to investigate the effects of the movement pattern of intruders on the detection probability, and validate the choice of $P_\perp$ as a metric for detection quality, we carried out a series of monte carlo simulations of intruder movement. We model the movement of intruders as piecewise linear paths, which start at $y = h/2 + r$ and end at $y = -h/2 - r$. The path segments are chosen randomly from a distribution in which the length of the segment is uniformly distributed between limits L_0 and L_1, and the angle which the segment makes with the y axis is uniformly distributed in the interval $[-\Delta\theta/2, \Delta\theta/2]$, with $\Delta\theta < \pi$ (i. e. the intruders never move back towards the their starting point).

The simulation proceeds by generating a number (N_{trials}) of random sensor fields. For each sensor field, a set of random intruder paths is generated which are tested for overlap with the sensors. We specify the total number of random sensors and paths (N_s and N_p), and N_{trials}, the number of trials, is derived as follows. The expectation value of the number of sensors in a trial is given by $\langle n_s \rangle = \rho w$. We then calculate the expected number of trials, $N_{\text{trials}} = N_s / \langle n_s \rangle$. The number of paths per trial is then $n_p = N_p / N_{\text{trials}}$.

For each trial, the number of sensors is selected randomly from a Poisson distribution of mean $\langle n_s \rangle$, and these are randomly distributed over the sensing region. For each trial field, n_p paths are created with random starting points at the top edge of the field. Each path is tested for overlap with the sensors. Trials are continued until the total number of sensors deployed is $\geq N_s$. The mean detection probability is then given by the fraction of paths which intersected a sensor.

The simulation also computes the weak barrier formation probability, and the mean weak barrier coverage fraction (which is equivalent to $P_\perp$, since it represents the fraction of the barrier that is covered to orthogonal paths). Both of these quantities can be derived from a given sensor field using the algorithm due to [17]. Figure 5-a shows results for $w = 2000$m and $h = 100$m. Markers show the simulation results for weak coverage fraction and weak barrier probability, the lines show the analytical formulae for $P_\perp$ and P_W. The simulation and analytical results are in very good agreement.

To investigate the effects of intruder paths on the detection probability, we performed an ensemble of simulations. Each simulation chose random values for the parameters controlling the intruder path distribution (ρ, L_0, L_1, subject to the constraint $L_1 > L_0$, and $\Delta\theta$). We use $w = 2000$m, $h = 100$m, $r = 25$m, $1\text{m} < L_0 < 100\text{m}$, $L_0 < L_1 < 100\text{m}$, $1\text{m}^{-1} \rho < 200\text{m}^{-1}$. For each run in the ensemble, $N_s = N_p = 10^4$.



a b

Figure 5. a. Comparison of analytical formulae for coverage with simulation results. b. An ensemble of simulations with random path parameters. Each marker represents a complete run of the simulation with a randomly chosen distribution of path parameters and BSN density.

Parameter	Min	Max
L_0	1 m	100 m
L_1	L_0	100 m
ρ	10 m^{-1}	200m^{-1}
$\Delta\theta$	0	π

The results of the runs are shown in Figure 5b. Each marker represents one simulation run (a full set of trials with a randomly chosen set of path distribution parameters). The solid lines represent the analytical values for $P_\perp$ and DetQM$_0$, the value of *DetQM* with $p_t = 0$ (no trespasser's favorite paths). All the simulation points are bounded between these two curves. As expected, $P_\perp$ represents a lower limit on the detection probability. The simulation shows that even with quite extreme values for the path selection parameters, *DetQM* overestimates the detection probability if trespassers' favorite paths are ignored.

B. Network Segmentation and Communication

In this section LDG's performance is compared against the well-known DSR protocol [23]. Both DSR and LDG use on-demand route discovery and maintenance mechanisms. DSR is recognized as one of the most suitable routing protocols for LWSNs [10]. It is widely cited in the literature and several trusted and well-tested DSR implementations are available on various network simulators. DSR and LDG were implemented in the NS2 network simulator [24].

1) Performance Metrics: In this subsection, we define the metrics used to measure the performance of the LDG protocol.

1) **Average End-to-End Delay**: Let $Delay_i$ be the time separating the transmission of a packet i from the source node and its reception at destination. Let P_T be the total number of packets that are correctly received. The average end-to-end delay is given as

$$D = \frac{i \ldots N_s \; Delay_i}{P_T} second$$

2) **Packet Delivery Ratio (PDR)**: PDR is expressed as the ratio between the number of packets successfully delivered to a destination and the number of packets sent by source node. PDR can be presented as

$$PDR = \frac{\text{no. of delivered packets}}{\text{no. of sent packets}}$$

3) **Network Lifetime**: This metric shows the ability of the routing protocol to load balance energy consumption. We define this metric as the average lifetime of all BSNs. This metric is calculated as

$$NL = \frac{1...N_s\ TE_i - TS}{N_s}$$

where TS is the starting time of the network simulation, and TE_i is the time when i dies. If i remains alive during the entire simulation experiment, TE_i will be set to the simulation end time.

4) **Total Throughput**: Measures the number of packets successfully transmitted to the final destination per unit of time. This metric is calculated by dividing the cumulative size of all received data by the duration of the simulation experiment. It is presented as

$$T = \frac{\text{no. of received packets} \times \text{packet size}}{\text{simulation time}}_{bit/second}$$

5) **Normalized Routing Load (NRL)**: The NRL is defined as the average number of control packets transmitted per data packet delivered to the sink node. It is presented as

$$NRL = \frac{\text{no. of control packets}}{\text{no. of data packets}}$$

6) **Average Energy Consumption (AvEC)**: The AvEC measures the amount of power consumed at each BSN during the network operation. In NS-2, the calculation of energy expenditure at each node takes into account the power consumed for packet transmission and reception, the one consumed during the time where the radio is in sleep mode, and the energy consumed by the environment sensing operations (sensor boards). AvEC on each node is calculated as

$$AvEC = \frac{Energy\ (I - R)}{N_s}$$

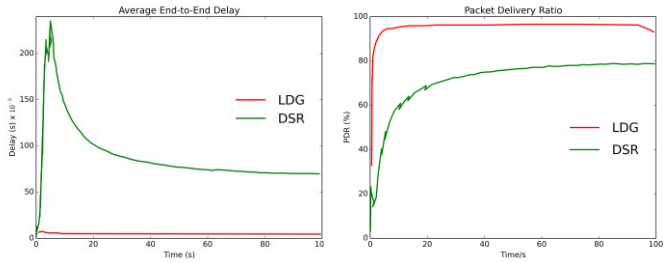
where I is the initial energy level of a node, and R is its remaining energy at the end of the simulation.

C. Simulation Model

The simulated LWSN contains 200 stationary BSNs, which are randomly scattered within an area of $2000m \times 100m$. BSNs have a wireless transmission range of $50m$ and sensing range of $25m$. Each simulated network contains three MTs. Two of them are located on both extremities of the network chain, and one in the middle. These nodes are assumed more powerful in terms of energy capacity and wireless communication range. During the simulation time of $100s$, a subset of BSNs is periodically and randomly chosen to generate the data traffic load and send it to the MTs. The sender's traffic load as well as the data packet size are maintained constantly throughout the simulation time. Table I summarizes the parameter settings used in our simulation experiments.

Table I
SIMULATION PARAMETERS

No. of nodes	200
Simulation area	(200m×200m) Square
BSN radio range	$50m$
Source BSN data rate	$1pkt/s$
No. of MTs	3
Radio Bandwidth	250 Kbps
Data packet size	32 byte



a b

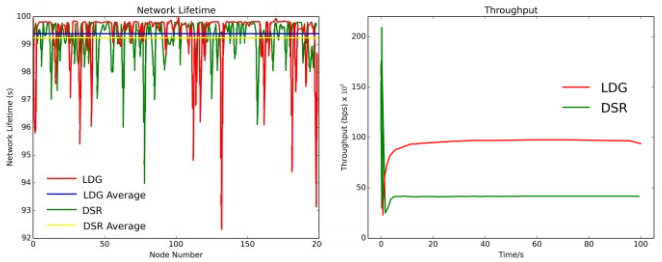
Figure 6. a. Average End-to-End delays of LDG and DSR. b. PDR of LDG and DSR.

D. Results and Discussion

1) Average End-to-End Delay: Figure 6a shows the variation of average end-to-end delays for both LDG and DSR, as a function of simulation time. LDG generates shorter packet delivery delays compared to DSR during the entire simulation time. The performance gap between the two protocols attains its maximum during the first $40s$ of the simulation time. When $t = 5s$, one packet transmission with DSR took $220ms$, while it was reduced by 95% and took $5ms$ in LDG. This is explained by the differences in the route discovery mechanisms of each protocol. During the network initialization phase, almost every operation of data packet transmission requires a route discovery step, due to the absence of previously discovered paths. In LDG, this step takes into account the chain topology nature of the LWSN by dividing the network into small logical levels. The route discovery process is executed in a localized manner within each level only, requiring shorter time to converge compared to DSR. In the latter, route request packets are flooded throughout the entire network, adding extra delays to the route discovery phase, and hence to the whole process of packet transmission.

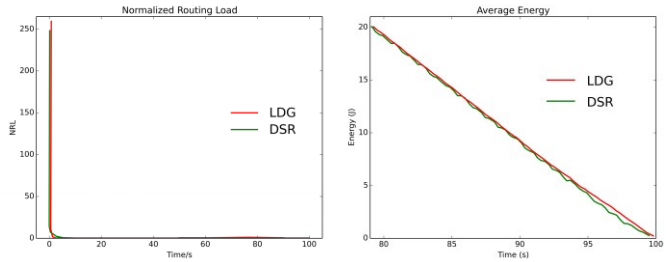
After second 40 of the simulation time, the performance gap between LDG and DSR becomes smaller, but remains considerable. This is due to the difference in discovered routes quality between LDG and DSR. Adopting multi-level network partitioning in LDG allows sending nodes to discover shorter and more reliable paths to the MTs. Shorter paths result in shorter end-to-end delays due the small number of forwarding nodes in each route. In addition, considering link reliability when selecting routes in LDG helps to reduce the delivery delay and the number of retransmissions.

2) PDR: As shown in Figure 6b, LDG achieves higher PDR when compared to DSR. The average PDR performance gain averages around 20% all along the simulation period.



a b

Figure 7. a. Network lifetime results of LDG and DSR. b. Throughput simulation results of LDG and DSR.



a b

Figure 8. a. Simulation results of NLR for LDG and DSR. b. Average Energy consumption in LDG and DSR.

It can be observed also that LDG offers higher PDR from the early network initialization phase, it reaches 90% in less than 3 seconds. While DSR spends 21 seconds for the PDR to reach 70%. The high PDR in LDG is a direct consequence of the reduced route setup overhead. LDG relies on localized communication between nodes belonging to the same level to establish a route between the data originator and the MT. Moreover, LDG uses links reliability to determine the best path. In contrast, DSR is heavily based on flooding the network with a high number of control messages. This causes increased contention, congestion, and collisions, preventing this protocol from being able to successfully deliver more than 30% of the transmitted data packets. DSR does not have an effective mechanism to remove route caches, which contain broken or non-minimum hop routes. Using stale routes leads to loss of data packets and wastes network bandwidth. This problem is further exacerbated by route replies from intermediate nodes and snooping data packets.

3) Network Life: The results in Figure 7a highlights the lifetime of each BSN in both LDG and DSR networks. BSNs showing shorter lifetime are seen when LDG is used. The plots demonstrate that the number of BSNs with a lifetime under 96*s* is higher in the case of LDG, compared to DSR. This is mainly caused by the multi-level communication adopted in LDG. Although this technique considerably minimizes the routing overhead, it may sometimes cause the overuse of some nodes that are responsible for routing messages between consecutive levels. It is important to note that load balancing is one of DSR's main design factors; it supports the use of multiple routes to any destination for load balancing. However, for the global network lifetime, LDG outperforms DSR, with a higher number of BSNs that remain alive until the end of the simulation. This can be confirmed when comparing the average node's lifetime for each routing protocol. It is shown that this value is a higher in LDG than in DSR.

4) Throughput: During the initialization phase, LDG and DSR showed opposite behaviors in their throughput performance (Figure 7b). Drastic degradation in throughput occurred with DSR during the first 5 seconds of simulation time, and a minimum value of 20*kb/s* has been measured. This poor performance is due to the high number of route request/route reply messages generated in DSR during this particular phase, which results in congestion, and reduces the available bandwidth for data packet transmission. Unlike DSR, LDG showed better performance during this phase, where the throughput increased with a higher load of data traffic, reaching a maximum value of 100*Kb/s*. When the network attained a steady state, both LDG and DSR showed a stable throughput, with higher values for LDG that outperforms DSR by 60%. This proves the ability of LDG to carry out routing operations in a transparent and lightweight manner without affecting the rate of successful data packet delivery. In DSR, when an intermediate BSN receives a bad route reply,it retries to send the waiting packets along that route. When a link along that route fails, an error packet is sent back to the sources, which then issue a new route request packet, starting the discovery all over again. Attempting to salvage a packet using another bad route results in a waste of bandwidth and increased delivery delay.

5) NRL: Figure 8a provides the measurements of the NRL for LDG and DSR. Higher values of routing overhead are generated for both protocols at the beginning of the simulation experiments. This is logical since any packet transmission during this phase necessitates a route discovery process, due to the lack of previously discovered routes. However, we note that DSR requires more routing traffic load than LDG for this particular phase. In fact, LDG recorded an NRL value below 240, while this metric was above 260 for DSR. The reduced routing overhead in LDG is achieved due to multi-level network partitioning based on link reliability and BSN residual energy. In contrast to DSR, all routing packet transmissions are localized in LDG and no network-wide flooding is required. It can also be observed from Figure 8a that LDG reached the NRL steady state earlier than DSR. By the NRL steady state, we mean the ability BSNs to send data packets using cached routes with a minimum or null NRL. LDG needed less than 2 seconds to be able to send data packets without the need for routing messages ($NRL = 0$), while DSR needed more than 5 seconds. The data salvaging and gratuitous replies of DSR degrades its performance when routes are fresh.

6) Energy Consumption: The plots in Figure 8b reveal comparable performance of DSR and LDG in terms of average energy consumption with slight improvement in LDG. Both protocols consume less energy as the data traffic load decreases towards the end of simulation. Furthermore, the maximum value of average energy consumption (20 Joules) recorded by

LDG during a high data traffic load can be considered good performance for a LWSN. The total energy consumption is mainly due to overhearing. Since this is highly dependent on the sender's radio range, LDG is based on dynamically varying the radio range to reduce total amount of consumed energy. This also saves energy at the sender by not transmitting at full power at all times.

VII. Conclusion

WSNs possess many key features that contribute to their effectiveness as a border surveillance technology. This paper studied the complex and sometimes conflicting requirements for such a WSN system. After determining that detection probability or orthogonal paths is an appropriate metric for measuring the crossing detection quality of the LWSN, we presented a method that calculates the required network density to achieve the specified level of coverage, while maintaining radio connectivity within the network. Then, given the required number of sensor nodes to deploy to achieve a specified level of coverage according to the chosen metric, we addressed the problem of determining the quality of coverage in the deployed network. The second major contribution presented in this paper is to the development of a cross-layer routing protocol that is energy efficient and maintains critical QoS measures, such as timeliness and accuracy. Despite using international border monitoring and surveillance as an application scenario, the proposed methods and protocols are generic and can be applied to any topologically linear WSN application, such as railway or gas pipeline monitoring.

Future avenues of work include implementing the system on a hardware platform and testing it with real life scenarios, such as various intrusion models, complex terrains and different sensing modalities. Currently, the authors are building 50 WiFi-based BSNs, which are equipped with accelerometer vibration sensors. This hardware platform is designed to accept a broad range of sensor types, which will allow testing the proposed system in other applications such as gas pipeline monitoring.

References

[1] E. U. C. House of Lords, "Frontex: the eu external borders agency," *Authority of the House of Lords*, March 2008. [Online]. Available: http://www.publications.parliament.uk/pa/ld200708/ldselect/ldeucom/60/60.pdf

[2] L. Boaz, S. Kaijage, and R. Sinde, "Wireless sensor node for gas pipeline leak detection and location," *International Journal of Computer Applications*, vol. 100, no. 18, pp. 29–33, August 2014.

[3] A. O. Adejo, A. J. Onumanyi, J. M. Anyanya, and S. O. Oyewobi, "Oil and gas process monitoring through wireless sensor networks: A survey," *Ozean Journal of Applied Science*, vol. 6, no. 2, 2013.

[4] M. Hammoudeh, R. Newman, C. Dennett, S. Mount, and O. Aldabbas, "Map as a service: A framework for visualising and maximising information return from multi-modalwireless sensor networks," *Sensors*, vol. 15, no. 9, p. 22970, 2015. [Online]. Available: http://www.mdpi.com/1424-8220/15/9/22970

[5] Z. Sun, P. Wang, M. C. Vuran, M. A. Al-Rodhaan, A. M. Al-Dhelaan, and I. F. Akyildiz, "Bordersense: Border patrol through advanced wireless sensor networks," *Ad Hoc Netw.*, vol. 9, no. 3, pp. 468–477, May 2011. [Online]. Available: http://dx.doi.org/10.1016/j.adhoc.2010.09.008

[6] T. Yang, D. Mu, W. Hu, and H. Zhang, "Energy-efficient border intrusion detection using wireless sensors network," *EURASIP Journal on Wireless Communications and Networking*, vol. 2014, no. 1, pp. 1–12, 2014. [Online]. Available: http://dx.doi.org/10.1186/1687-1499-2014-46

[7] H. Luo, K. Wu, Z. Guo, L. Gu, and L. M. Ni, "Ship detection with wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 7, pp. 1336–1343, July 2012.

[8] Y. Dong, H. Chang, Z. Zou, and S. Tang, "Energy aware routing algorithm for wsn applications in border surveillance," in *Technologies for Homeland Security (HST), 2010 IEEE International Conference on*, Nov 2010, pp. 530–535.

[9] Y. Jin, L. Wang, J. Y. Jo, Y. Kim, M. Yang, and Y. Jiang, "Eeccr: An energy-efficient m -coverage and n -connectivity routing algorithm under border effects in heterogeneous sensor networks," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 3, pp. 1429–1442, March 2009.

[10] H. Sharei-Amarghan, A. Keshavarz-Haddad, and G. Garraux, *Routing Protocols for Border Surveillance Using ZigBee-Based Wireless Sensor Networks*. Springer Science, 2013, pp. 114–123.

[11] P. Rothenpieler, D. Kruger, D. Pfisterer, S. Fischer, D. Dudek, C. Haas, A. Kuntz, and M. Zitterbart, "Flegsens - secure area monitoring using wireless sensor networks," in *International Conference on Sensor Networks, Information, and Ubiquitous Computing*, 2009.

[12] S. Kumar, T. H. Lai, and A. Arora, "Barrier coverage with wireless sensors," in *Proceedings of the 11th Annual International Conference on Mobile Computing and Networking*, ser. MobiCom '05. New York, NY, USA: ACM, 2005, pp. 284–298. [Online]. Available: http://doi.acm.org/10.1145/1080829.1080859

[13] B. Liu, O. Dousse, J. Wang, and A. Saipulla, "Strong barrier coverage of wireless sensor networks," in *Proceedings of the 9th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, ser. MobiHoc '08. New York, NY, USA: ACM, 2008, pp. 411–420. [Online]. Available: http://doi.acm.org/10.1145/1374618.1374673

[14] Y.-T. Hou, T.-C. Lee, B.-C. Jeng, and C.-M. Chen, "Optimal coverage deployment for wireless sensor networks," in *2006 8th International Conference Advanced Communication Technology*, vol. 1, Feb 2006, pp. 5 pp.–527.

[15] H. Luo, H. Du, H. Huang, Q. Ye, and J. Zhang, *Barrier Coverage with Discrete Levels of Sensing and Transmission Power in Wireless Sensor Networks*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015, pp. 14–23.

[16] P. Hall, *Introduction to the theory of coverage processes*, ser. Wiley series in probability and mathematical statistics: Probability and mathematical statistics. John Wiley & Sons Australia, Limited, 1988. [Online]. Available: https://books.google.co.uk/books?id=zcGmAAAAIAAJ

[17] L. Li, B. Zhang, X. Shen, J. Zheng, and Z. Yao, "A study on the weak barrier coverage problem in wireless sensor networks," *Computer Networks*, vol. 55, no. 3, pp. 711 – 721, 2011.

[18] C. Komar, M. Y. Donmez, and C. Ersoy, "Detection quality of border surveillance wireless sensor networks in the existence of trespassers' favorite paths," *Computer Communications*, vol. 35, no. 10, pp. 1185 – 1199, 2012.

[19] L. Lazos, R. Poovendran, and J. A. Ritcey, "Analytic evaluation of target detection in heterogeneous wireless sensor networks," *ACM Trans. Sen. Netw.*, vol. 5, no. 2, pp. 18:1–18:38, Apr. 2009.

[20] Z. Fan and X. Liu, "Energy synchronized transmission control for energy-harvesting sensor networks," *International Journal of Computers Communications & Control*, vol. 11, no. 2, pp. 194–208, 2016.

[21] D. S. J. De Couto, D. Aguayo, J. Bicket, and R. Morris, "A high-throughput path metric for multi-hop wireless routing," in *Proceedings of the 9th Annual International Conference on Mobile Computing and Networking*, ser. MobiCom '03. New York, NY, USA: ACM, 2003, pp. 134–146. [Online]. Available: http://doi.acm.org/10.1145/938985.939000

[22] R. S. Oliver and G. Fohler, "Probabilistic estimation of end-to-end path latency in wireless sensor networks," in *2009 IEEE 6th International Conference on Mobile Adhoc and Sensor Systems*, Oct 2009, pp. 423–431.

[23] D. A. Maltz and D. C. Johnson, "The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4," RFC 4728, Mar. 2013. [Online]. Available: https://rfc-editor.org/rfc/rfc4728.txt

[24] NS-2, "The network simulator," Online, June 2016. [Online]. Available: www.isi.edu/nsnam/ns/