A Novel Economic Barrier Coverage Using Wireless Networks

AbdelRahman A. Eldosouky*, Ahmed Abdul-Monem Ahmed, Ibrahim E. Ziedan*****

* (Computer and Systems Engineering Department, Faculty of Engineering, Zagazig University, Egypt.)
** (Computer and Systems Engineering Department, Faculty of Engineering, Zagazig University, Egypt. Networks and Communication Systems Department, Taibah University, Saudi Arabia.)
***(Computer and Systems Engineering Department, Faculty of Engineering, Zagazig University, Egypt.)

ABSTRACT

Barrier coverage in wireless sensor networks has important applications in various battlefield and homeland security. Its goal is to effectively detect intruders that attempt to cross a region of interest by forming a chain of sensors with overlapping sensing areas. However, the usage of sensor networks in barrier coverage is limited because of its high cost. In this paper, we introduce a low cost technique to achieve barrier coverage. As the value of RSSI is affected when an intruder passes through the barrier, this technique depends on using Received Signal Strength Indicator (RSSI) to detect intruders in place of actual sensors. A proposed protocol to construct the system in this way is presented. Moreover, it is shown that no extra nodes are required to use this technique, and less power is required than using actual intrusion sensors. Practical experiments to measure change in RSSI due to intruders in an outdoor field are recorded.

Keywords **- Barrier coverage, intrusion detection, power consumption, RSSI, wireless sensor network.**

1. INTRODUCTION

Wireless sensor networks (WSNs) are a particular type of ad-hoc networks comprising hundreds or thousands of battery operated sensor nodes with basic signal processing and computational capabilities. Each node is equipped with a small processor, a memory, and a wireless communication module. A variety of mechanical, thermal, biological, chemical, optical, and magnetic sensors may be attached to the sensor node to measure environmental phenomena.

These nodes collect data of interest within a sensing field and transmit them to a sink for further processing. WSNs are generally deployed in large-scale, unstructured environments, which are difficult to be monitored manually. Applications of WSNs include battlefield surveillance, environmental monitoring, biological detection, smart spaces, industrial diagnostics, and others. [1].

A common application of WSNs is barrier coverage. In this application, sensor nodes are deployed with in a long, narrow region along a boundary of interest with the aim of detecting unauthorized intrusions. Barrier coverage is used on boundaries such as country borders, coastal lines, and boundaries of battlefields. The union of the covered areas of sensors forms a barrier that detects intruders when they enter the covered area [2].

The high cost of WSNs limits its practical use in barrier coverage. In order to decrease the cost, network can be deployed without sensors, saving both money required to buy them and effort used to attach sensors to the nodes and program them. In order to detect intruders, we depend on the phenomenon of radio irregularity rather than usual sensing. When a signal propagates within a medium, it may be reflected, diffracted and scattered. Each effect occurs to a different extent in various media. The human body comprises liquid, bone and flesh, which selectively absorbs, reflects or scatters RF signals [3]. Consequently, in the presence of human activity in the network, different signal components are absorbed at different time instances, resulting in signal strength fluctuations at the receiver. Thus, in RF propagation, radio irregularity arises to a higher level in the presence of human activity.

Channel characteristics, such as Received Signal Strength Indicator (RSSI) and Link Quality Indication (LQI), are affected by radio irregularity. Therefore, when an intruder passes through the network there will be a change in the values of RSSI and LQI. This idea has been used in network security to detect human interference in the network [4] where some experiments had been done to prove that human interference in the network causes a significant change in RSSI. The authors made their experiments in a laboratory not in a real site where the medium has a different effect on the signal.

In this paper, we propose a protocol for constructing the barrier coverage without sensors. Experimental results show that RSSI could be used to detect intruders in several situations in an outdoor field. We conducted experiments in an open field similar to real sites where barrier coverage is needed. We compare our proposed method to the barrier that uses sensors in terms of power consumption and number of required nodes.

The rest of the paper is organized as follows. In section 2, the network model and terminology are presented. Proposed protocol of building the system is then described in section 3. Experimental setup and results are given in section 4. A comparison with actual intrusion sensors is then discussed in section 5. Finally, concluding remarks are given in section 6.

2. NETWORK MODEL AND TERMINOLOGY

The network model used in this paper is similar to that assumed in a previous work [5]. A sensor network N is a collection of sensors deployed over a belt region. All sensors are static. They do not move after deployment. The location of each node in the network is assumed to be known to the node itself and the base station (BS) using either on-board GPS unit or other localization mechanisms. Therefore, the BS is assumed to know the map of the entire network. The belt region is a two-dimensional rectangular area of length l and width w. The belt has two parallel boundaries that may be referred to as the top and bottom boundaries; where the other two boundaries are the left and right.

Sensors are distributed within the rectangle area uniformly at random. The sensing model of each sensor follows the widely adopted binary disk model. Each sensor has a sensing range RS and can detect any intruders within its sensing range. Two nodes are said to be connected in terms of sensing if their sensing areas overlap. In other words, node Si is connected to node S_j if and only if $|S_i-S_j| \leq 2R_S$, where $|S_i-S_j|$ represents the Euclidian distance between the two sensor nodes [6]. A sensor barrier is formed by a set of connected sensors, with overlapped sensing areas, that intersect both the left and right boundaries of the belt.

Intrusion movement is assumed to occur from one side to the other. Thus, an intruder's path is said to be a crossing path if it crosses from one parallel boundary to the other. A crossing path is orthogonal if its length is equal to the belt's width w. However, the crossing pass may take any shape between the two parallel boundaries. Fig (1) shows a network with two barriers. Note that not all nodes contribute in forming the barrier.

The strength of the barrier coverage in a sensor network can be measured by the number of disjoint barriers in the network. A sensor network is said to provide k-barrier coverage over a deployment region if all paths through the region intercept at least k distinct sensors [5].

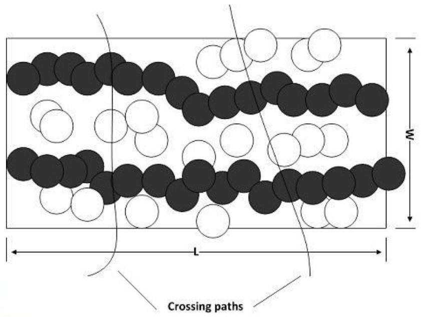

Fig (1): Network with two barriers (shaded nodes).

Each node has a communication module, and the communication region of each node is represented by a disk with radius R_C. In order for the network to be connected in terms of communication, location of any active node should be within the communication range of one or more active nodes such that all active nodes can form a connected communication backbone. The relationship between radio connectivity and sensing coverage intuitively depends on the ratio of the communication range to the sensing range. It has been proved that if R_C>= 2*R_S and the region is sensor covered then the sensors covering that region are connected [7].

RSSI indicates the strength of the received radio signal, taking into account that RSSI does not imply quality of the signal. RSSI is usually a 5-to 10-bit number obtained from the physical layer where the number of bits is hardware-dependent. LQI is an8-bit value obtained from the MAC layer; its value is based on the received signal strength as well as the number of errors received, and it varies from 0 to 255.Values of RSSI and LQI are sensitive to climatic changes [8].

3. PROPOSED PROTOCOL

In order to use RSSI between two nodes in place of the actual sensors, the two nodes should be connected, that they are in the radio range of each other. In the proposed protocol, a data packet is periodically sent from one node to the other in order to measure the received signal strength. If an intruder passes between two connected nodes, the signal transmitted between them will be affected, and there will be a change in the value of RSSI at the two nodes. This change will be an indication to the presence of an intruder. The same happens when actual sensors are used. We simply use RSSI to sense the presence of an intruder. The following steps describe the proposed protocol. In this protocol we assume that BS knows each node's location and radio range, and there must be at least one path of radio connectivity between the two sides of the field so that coverage can be achieved.

1. Based on nodes locations and radio ranges, BS constructs a graph for the network and finds the disjoint barriers in the network. An algorithm to determine these disjoint

barriers based on a maximum flow algorithm can be found in [9].

2. BS informs each node contributed in a barrier with its neighbors in the barrier.
3. BS sends a command to nodes contributing in barriers to begin the exploration period which stays for 60 seconds.
4. During the exploration period, each node (including BS) records and calculates the range of accepted values (min-max) of RSSI and LQI for each one of its neighbors.
5. After the exploration period, each node begins to send periodic data packets to its neighbors and records RSSI and LQI values.
6. If a packet sent from one of its neighbors does not match the range of accepted RSSI values, the node sends an alarm message to the BS contains its ID and the ID of the detected node that sent this packet.
7. When BS receives two alarm messages from two nodes that detected each other, BS considers this an intruder.
8. The exploration period is repeated once every 12 hours to calculate new accepted values for RSSI and LQI to decrease the effect of climatic change. This process is done alternately between disjoint barriers to keep some barriers working while the others are in their exploration periods.

4. EXPERIMENTS

In this section, we describe the experimental setup and present the detailed results when the proposed protocol is used in intrusion detection instead of actual sensors.

4.1 Setup

A test bed was built from five nodes and a base station. These nodes were considered to form a barrier. The nodes were all of IRIS type from Crossbow Technologies. IRIS was used for two reasons. First, it used AT86RF230, a low-power 2.4 GHz transceiver, which included an Omni-directional antenna, which was the closest to the sensing disk model assumed. Second, it used an XM2111CA processor based on the Atmel ATmega1281microcontroller, a low-power microcontroller. BS was connected to a laptop during experiments to store collected data.

Tiny OS was used to program nodes. Experiments began by sending a command from the base station to all nodes to start the exploration phase for 60 seconds, in which each node calculates the range of accepted values (min-max) of RSSI for each of its neighbors. After the exploration period, each node began to monitor its neighbors. If a packet sent from one of its neighbors did not match the range of accepted RSSI values, the node sent an alarm message to BS indicating that there was an intruder between these two nodes.

Nodes were programmed to send a small 25-byte data packet to its neighbors every 1 second. This time is chosen such that no intruder would be able to pass the whole area covered by the node in a much lesser time.

IRIS used the moduleAT86RF230 as a transceiver, which offered many output power levels used for communication, ranging from -17.2 dBm to 3 dBm. By increasing the power level, the radio range of the node can be increased. In our experiments, the output power of 0 dBm was used.

4.2 Results

Experiments were conducted in an open area, which was a desert land with trees planted on one of its edges. Trees were about 3 meters in height. This place was chosen in order to represent a real environment for applying barrier coverage. Two types of experiments have been conducted. In the first type, nodes were placed on the land and away from trees. In the second one, nodes were placed between trees where a node could be on the land or on the tree stem. Both of these types could be examples of country borders, where barrier coverage is mostly needed. Moreover, as in barrier coverage where nodes are scattered randomly in the area, we placed nodes at different distances, randomly selected, from each other. The following subsections summarize the test results for these two types of experiments.

4.2.1Placing nodes in a desert land

Nodes and BS were placed according to the layout shown in Fig. (2); distances (in meters) are also shown. All nodes were nearly at the same height.

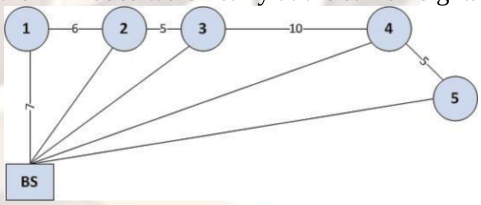

Fig (2): Network layout, desert land

During the 60-second exploration period, each node determined maximum and minimum RSSI and LQI values for all of its neighbors, and also BS. After that, a person moved from the direction of BS and passed between nodes 1 and 2 but close to node 1. This is illustrated in Fig (3) below.

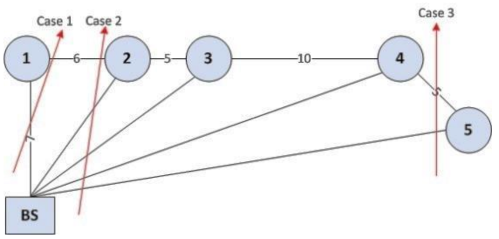

Fig (3): Original network layout showing crossing paths.

Both nodes 1 and 2 reported that there was a difference in RSSI values for each other. RSSI values for this case are shown in Table 1.

Table 1. RSSI values in dBm for case 1.

Node ID		1	2
RSSI for node 1	Min	-	-85
	Max	-	-84
	New	-	-88
RSSI for node 2	Min	-85	-
	Max	-84	-
	New	-88	-
RSSI for BS	Min	-77	-79
	Max	-61	-61
	New	-69	-77

It is clear from the table that RSSI had changed and become out of the accepted range (max-min) due to this intruder's movement. It was also noticed that the range of RSSI values for BS is large that is the change due to intruder's movement has been accepted and not reported. Table 2 shows values of LQI for this case. It is noticed that LQI for links between nodes was the maximum (255) in the exploration period and did not change when an intruder moved. For links between BS and nodes, LQI was also the maximum in the exploration period but showed a noticeable decrease due to intruder's movement.

Table 2. LQI values for case 1.

Node ID		1	2
RSSI for node 1	Min	-	255
	Max	-	255
	New	-	255
RSSI for node 2	Min	255	-
	Max	255	-
	New	255	-
RSSI for BS	Min	255	255
	Max	255	255
	New	240	249

In rest of results we will show who reported the intruder no matter this report was generated by a change in RSSI or LQI.

Now a person moved from the direction of BS and passed between nodes 1 and 2 but close to node 2 that is indicated in Fig (3) as case 2. Results for this case are shown in Table 3. It is noted that BS reported that there is a change in the values related to node 3. This could be due to the closeness of the intruder to node 2 which affected node 3.

Table 3. Intrusion detectors for case 2

Node ID	Detector 1	Detector 2
1	2	BS
2	1	BS
3	BS	

Now a person from the direction of BS and passed between nodes 4 and 5 that is indicated in fig (3) as case 3. Results for this case are shown in Table 4. Nodes 4 and 5 reported the difference between each other which means that there is an intruder; BS also reported the change in the link to both nodes.

Table 4. Intrusion detectors for case 3

Node ID	Detector 1	Detector 2
4	5	BS
5	4	BS

4.2.2 Placing nodes between trees

Nodes and BS were placed according to the layout shown in Fig (4); distances in meters are also shown in the figure. Nodes 1, 3 and 5 are placed on the land between trees, while nodes 2 and 4 were placed on the tree with heights 1.5 and 1.2 meters respectively.

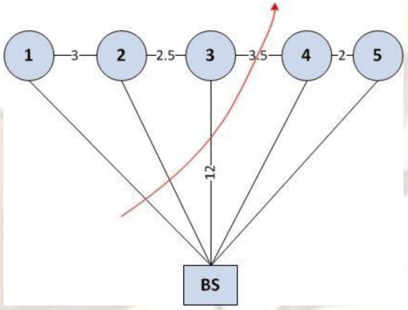

Fig (4): Layout of nodes placed between trees, showing the crossing path.

The exploration period is also set for 60 seconds, after that a person moved in the direction shown in fig (4).Values that suffer a change in this case are shown in table 5,where empty fields in the table refer to new values that are within the range and not reported.

The intruder was also detected by both nodes 3 and 4.Also nodes 2 and 3 reported a change in RSSI values for each other, which could be an indication to another non-existent intruder between them. This happened due to signals reflection between trees and intruder which affected other links in the network. This false alarm is considered a problem if the system is used to track intruder's movement between nodes, but as barrier coverage is concerned with detection only this would not be a problem.

Table 5. RSSI values in dBm when nodes are placed between trees

Node ID		2	3	4
RSSI for node 2	Min	-	-84	
	Max	-	-83	
	New	-	-80	
RSSI for node 3	Min	-84	-	-88
	Max	-83	-	-87
	New	-80	-	-89
RSSI for node 4	Min		-88	-
	Max		-86	-
	New		-91	-
RSSI for BS	Min	-81	-89	
	Max	-61	-69	
	New	-85	-65	

4.2.3 Analysis

In an open field with no interferences, RSSI values for links between nodes have a small range of accepted values. When an intruder moves between nodes, RSSI values change and become out of this range. On the contrary, links between BS and nodes have a large range of accepted RSSI values that could not be used for intruder's detection.

LQI values for links between nodes in an open filed don't change due to intruder's movement. These values remain always at the maximum value so they could not be used in detection. The contrary with BS, where LQI values gives indication for intruders crossing links between BS and other nodes.

From these results, the system of barrier coverage should be built depending on RSSI values not LQI values. As in barrier coverage, links between nodes only are considered in the constructing barriers. But if the link between a node and BS is to be used LQI can be considered in this case.

For the case of placing nodes between trees, RSSI values also showed a small range in links between nodes and a large range for links between BS and nodes. But in this case, intruder's movement caused RSSI values to be out of the accepted range. This means RSSI values are sufficient to detect changes for both links concerned to nodes BS, and no need to use LQI. Also in this case, intruder's movement could cause false alarms in other nodes due to signal reflections. This false alarm will not be a problem as the intruder is already detected.

5. Comparison of the Proposed System to a System with Actual Intrusion Sensors

In order to compare the proposed system with an actual intrusion detection sensor, we used the information provided by SmartDetect project [10] as a real implementation of intrusion detection sensors. The work [10] also included a valuable survey about actual types of sensors that can be used in intrusion detection. The survey made a qualitative comparison of many possible types of intrusion detection sensors indicating their pros and cons. Based on this survey, project's team used the analog Panasonic motion sensor AMN24111 as the best choice for aspects of performance, pricing and availability. Therefore, in the present work we compare the usage of AMN24111 sensor to the usage of RSSI. The comparison is in terms of both number of nodes required to build the network and power consumption.

5.1 Number of required nodes

Using RSSI to detect intruders will depend on existence of two nodes at the same time as they should be in the communication range of each other in order to receive the sent data packets. This is different from using actual sensors as the detection depends on the sensing range of one node only.

However the system will not need any modifications in number of nodes or their distribution because the used communication range R_C is at least double the sensing range R_S which guarantees that the network is connected. So if the communication ranges of two nodes are overlapped, that there is no gap between them, this implies that they are connected and can exchange data packets. Fig (5) illustrates this situation. Moreover if R_C is greater than $2*R_S$, the system will need fewer nodes to achieve the same barrier coverage.

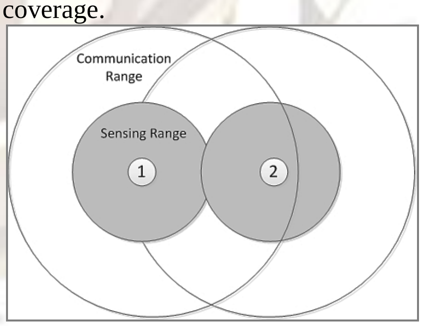

Fig (5): Sensing and communication ranges of two nodes.

For IRIS working at 0 dBm power level, it was shown in [11] to give a radio communication range of 55 meters, while AMN24111 has a sensing range of 10 meters maximum. But since it is sufficient to have a communication range of 20 meters, we can save energy by using a lower power level by nodes which guarantees 20 meters coverage. Another benefit of using this large communication range is that the system can be built from fewer nodes saving more money.

5.2 Power Consumption

In this part we discuss the difference in power consumption between using RSSI andAMN24111. AMN24111 covers a horizontal angle of approximately 110 degrees and thus usually three sensors are used and are oriented at 120 degrees relative to each other to obtain an omnidirectional sensing range. Energy consumed byAMN24111 sensor can be calculated using its datasheet. As the sensor is supposed to work continuously we can calculate the energy consumed as the product of Voltage, Current, and Time. Typical values for consumed current and voltage are mentioned in the datasheet. It was found that three sensors will consume 150 mj in a minute of continuous sensing.

Now usage of the proposed technique will save the power used by the sensors but will add extra power consumption due to messages being sent and received by nodes in the network. But calculating the power consumed by a node for sending and receiving data is not so easy, as even if you know the working Current and Voltages of the node you still miss the amount of time spent in sending or receiving. Calculating this power is usually done by practical measurements.

For IRIS module and our experimental parameters we used the practical measurements in [12] for calculating the energy consumed for sending and receiving the same amount of data at 0dBm power level. It was found that for the node to send and receive data from its two neighbors in the barrier every 1second, it will consume about 114 mj in a minute which is less than the energy consumed by the actual sensorAMN24111.More energy can also be saved by using a lower power level in communications than 0 dBm.

6. CONCLUSION

Experiments performed in an open field verified that RSSI can be effectively used in barrier coverage. This, according to the proposed technique, is supposed to replace actual intrusion sensors. Building a system in such a way will significantly decrease the cost of the network as it cancels the cost of actual sensors. Experiments showed that when an intruder passes between two nodes, he is detected by the change in RSSI in these two nodes. The proposed technique also proved that no more nodes are required to get the same barrier coverage as in the case of actual sensors. Another important issue of power consumption was considered, and it was shown that the system will use less power than the original system.

REFERENCES

[1] J. Yick, B. Mukherjee and D. Ghosal. Wireless Sensor Network Survey. *Computer Networks, Vol. 52, Issue 12,* Aug. 2008, 2292-2330

[2] K. Ssu, et. al., K-Barrier Coverage with a Directional Sensing Model, *International Journal On Smart Sensing And Intelligent Systems, Vol. 2, No. 1*, March 2009, 75-93.

[3] G. Zhou, et. al., Impact of radio irregularity on wireless sensor networks, *Proc. MobiSys,* 2004, 125-138.

[4] M. Kamel, A. Ahmed and H. Ragai, Addressing spatial signature for security in wireless sensor networks, *Proc. EICI,* 2012, 15-18.

[5] S. Kumar, T. Lai and A. Arora, Barrier Coverage With Wireless Sensors, *Wireless Networks, Vol. 13, Issue 6,* Dec. 2007, 817-834.

[6] A. Saipulla, B. Lui and j. Wang, Barrier coverage with airdropped wireless sensors, *Proc. MILCOM,* 2008, 1-7.

[7] G. Xing, et. al, Integrated Coverage and Connectivity Configuration For Energy Conservation in Sensor Networks, *ACM Transactions on Sensor Networks, Vol. 1, Issue 1,* Aug. 2005, 36-72.

[8] N. Baccour, et. al, Radio Link Quality Estimation in Wireless Sensor Networks: A Survey, *ACM Transactions on Sensor Networks, Vol. 8, Issue 4, Article 34,* Sept. 2012.

[9] A. Eldosouky, *Barrier Covergae in Wireless Sensor Networks*, M. A. Thesis, University of Zagazig, Egypt, 2013.

[10] SmartDetect Project Team, Wireless Sensor Networks for Human Intruder Detection, *Journal of The Indian Institute of Science, Vol. 90, No. 3,* Sep. 2010, 347-380.

[11] E. Garcia, A. Bermudez and R. Casado, Range-Free Localization for Air-Dropped WSNs by Filtering Neighbourhood Estimation Improvements, *Communications in Computer and Information Science, Vol. 133*, 2011, 325-337.

[12] T. Prabhakar, et. al, Energy Consumption Profile for Energy Harvested WSNs, in H. Venkataraman and G. Miro, Ed. Florida, *Green Mobile – Energy Optimization and Scavenging Techniques for Mobile Devices and Networks.* 1 (CRC press, 2012), chap. 12.