BORDER SURVEILLANCE AND INTRUSION DETECTION USING WIRELESS SENSOR NETWORKS

Mosad Alkhathami, Lubna Alazzawi and Ali Elkateeb
[1,2]Department of Electrical and Computer Engineering,
Wayne State University, Detroit, USA
[3]Department of Electrical and Computer Engineering,
University of Michigan-Dearborn, USA

ABSTRACT
In the last decade, the usage of wireless sensor network (WSN) has become a powerful tool that connects the physical and digital world. Currently, WSNs are applied in numerous applications such as the monitoring of buildings, wildlife and habitats, smart electrical grid control, and border control which this paper will cover it. Among countries, border protection is a sensitive issue and measures are being taken to improve security at the borders. In addition to physical fencing, smart methods using technology are being employed to increase the alertness of security officials at the borders. Border control using wireless sensor network is one way to do. The conventional border patrol systems are highly labour intensive, requiring constant human involvement. However, in recent years, unmanned aerial vehicle, grouped sensors and camera equipped surveillance towers have been added as border patrol measures. Moreover, such systems suffer from problems ranging from false alarms to line of sight limitations. In addition, there is the lack of a coordination unit to provide accuracy to the system. Therefore, this study presents the simulation of border surveillance using WSN arrays as a method of surveillance and intrusion detection system to measure and solve the above critical issues.

KEYWORDS: *Wireless Sensor Network, ZigBee, border control, surveillance &Area monitoring.*

I. INTRODUCTION

The Wireless Sensor Network (WSN) is an emerging technology that uses distributed sensors with communications infrastructure to monitor or record environmental conditions. WSN provides distributed network and Internet access to sensors, controls, and processors that are deeply embedded in equipment, facilities, and the environment. WSN has enormous applications in every field include disaster relief, agriculture, environment monitoring, medical applications, security, etc. One of the most recent monitoring applications of WSNs is the border control application. This kind of application is becoming critical due to the increase of the risks of intrusion on borders. Border protection is a sensitive issue and measures are being taken to improve security at the borders. Border control using wireless sensor network is one way to do it. It is a well-known fact that the border control is vital to the security of the nation and its citizens all over the world.

All countries' borders and ports are busy places, with tens of millions of cargo containers and hundreds of millions of legal travellers entering the country each year. Border control means measures adopted by a country to regulate and monitor their borders [1]. Border control regulates the entry and exit of people and goods across a country's border. Border security is a primary concern of the national security agenda in this period of terrorism and threats of terrorism. The problem with protecting these boundaries is the distance to be covered and the intensity of labor to employ. Conventional systems of border patrol consist of troops and checkpoints on international roads.

At these checkpoints, the patrol stops traffic, inspects the vehicles and passengers, and curtails any illegal activity. On the expansive border zones, patrols occur along predetermined routes and set intervals, requiring extensive human resources to patrol even a small area [2]. Therefore, monitoring

the border in real-time with accurate results and minimum human involvement requires several complementary technologies. A WSN can provide accurate detection and tracking of intrusion with minimal human participation. Because of the border surveillance's significance, several research challenges need to be addressed before a practical realization is implemented. Thus, in this paper, we first provide the role of WSN and an explanation of border patrol techniques. Existing border patrol techniques are presented in Section 3. Then, in Section 4, the sensor node deployment methodology is discussed. Also in section 5 we cover the intrusion detection system design and the simulation and analysis of proposed system will be in section 6. Finally, the paper is concluded in section 7, and future work in section 8.

II. THE ROLE OF WSN IN BORDER SURVEILLANCE

For any country to maintain peaceful relations with its neighbours there is a need to establish a fire free zone in the borders, here the wireless sensor network system is at use. Soldier presence in the borders may lead to unexpected conflicts and ultimately result in a war. Wireless networking systems are required in less population dense areas where there is chance for illegal human operations, where as it is not necessary in places which have high density of population and security. Another difficulty present in the highly populated area is that the sensors will detect the disturbances caused by people living in that area [3]. The impact of sensor networks for habitat and environmental monitoring will be measured by their ability to enable new applications and produce new, otherwise unattainable, results.

The WSN's role within the range of its application in border surveillance, similar to the other types of the WSN system applications, boils down to the data gathered from a variety of the sensor types such as seismic, motion detectors, and thermal cameras. Some types of the advanced WSN devices process the gathered raw data, and then send an alert command or the aggregated raw data to border guard service command centre, which is supposed to take appropriate actions on the defence of the frontier. Copious amounts of research from various credible organizations have defined WSN usage as one of the appropriate strategies for mitigating border surveillance issues [4].

III. EXISTING BORDER PATROL TECHNIQUES

Border patrol systems have recently become interested in tackling concerns regarding national security. The border patrol systems and techniques have recently begun to address the concerns about national security. One of the major challenges concerning the protection of long stretches of borders is the necessity for intensive human involvement in patrolling locations. With the invention of different electronic patrol techniques, this involvement helps to decrease the need for such measures. Several works have been done recently in the field of security surveillance of the country's borders with WSN. The author found that many works have addressed border surveillance applications based on WSNs. Many solutions using WSNs have organized the network nodes as a line-sensor, where every movement going over a barrier of sensors is detected. In this case, the deployment of sensor nodes 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 [2].

Researchers from Germany investigated the construction of sensor barriers on long strip areas of irregular shapes when sensors are distributed. To ensure that trespassers cannot cross the border undetected, multiple disjoint sensor barriers will be created in distributed manner covering large-scale boundaries. Then, a segmentation technique was proposed to achieve continuous barrier coverage of the whole area [5]. Researchers at the University of Virginia and Carnegie-Mellon University have developed an energy efficient WSN system for detecting moving vehicles through a passage line in a stealthy manner. They deployed 70 MICA2 sensor nodes running Tiny OS along a 280-feet-long perimeter. The sensor nodes were equipped with a magnetometer, as well as acoustic and photo sensors [6]. Ohio State University researchers have deployed 90 sensor motes with metal object detection capabilities. The main objective of the project was to detect and classify moving metallic objects, such as tanks and armed vehicles. They considered a surveillance scenario of breaching a perimeter or within a region. The system provide target detection, classification, and

tracking for moving metallic and nonmetallic objects. They used an algorithm called Logical Grid Routing Protocol for the routing and the localization. They also used 90 MICA motes equipped with magnetic sensor nodes for the simulation [7].

Amongst these studies, Unmanned Aerial Vehicles (UAVs) for mid-air surveillance have been used lately to track routinely and detect track unlawful border crossing. Due to the outsized coverage as well as high mobility of the UAVs, the concentrated human participation in low-level surveillance practices can be minimized. UAV significantly contributes to the redirection of human resources decision management activities and processing the collected data by UAV [1].

IV. SENSOR NODE DEPLOYMENT METHODOLOGY

Since the border requires to be monitored at every location, thereby making it significantly difficult to carry out an intrusion, multiple sensors can be deployed to simultaneously monitor given points within the border, guaranteeing that the failure of one node would not necessarily compromise the network's integrity. A WSN deployment can usually be categorized either as a dense deployment or a sparse deployment depending on the number of nodes that are required to suitably cover the network. Examples of dense deployment and the sparse deployment models are shown in Figures 1 and 2.

In order to suitably cover the border, the dense deployment model is used, making it possible for the security coverage of the entire border to be achieved [8]. The dense deployment model is achieved by ensuring that the radius of coverage of each of the sensors is contained within the next neighbouring sensor, thereby guaranteeing that each point within the border is optimally covered. Newer wireless sensor networks have the ability of relocating after deployment, thereby making it possible for the remote to control their placement and distribution within the border.

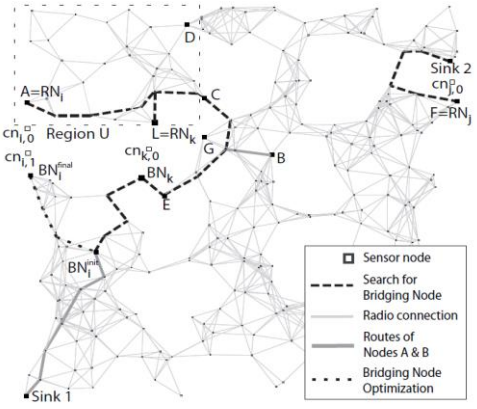


Figure 1: Sparse deployment model.

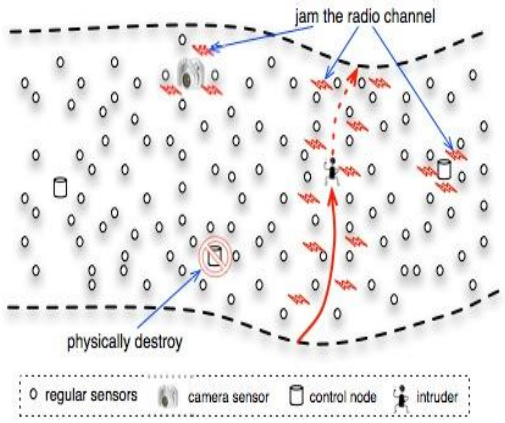


Figure 2: Dense deployment model.

4.1 Analysis of Factors Affecting Node Deployment

There are many factors to consider in order for the node deployment planner to build a wireless sensor network in the border environment. The factors affecting node deployment are mission area, target type, mission task, sensor type, terrain, vegetation, available number of nodes, and communication and intrusion probability among others [9]. In addition, composite factors, which are some combinations of environmental factors, should be considered such as the relationship between sensing ranges, RF communication range and node deployment type, in order to calculate the node placement [10]. In Figure 3 the relation of environmental factors and composite factors are shown.

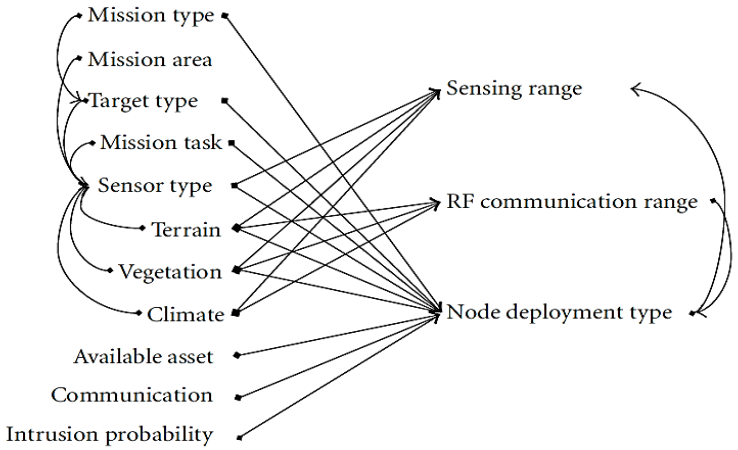


Figure 3: Relational diagram for environmental and composite factors.

4.2 Deployment of Sensor Node Based on Sensing Range

The area of coverage is one of the most considerable parameters in the node deployment. The assessment of the WSN coverage area is based on a particular sensor model that uses a metric schedule to measure the total volume of coverage provided by the WSN deployment. Furthermore, the placement of the optimized sensor is also not an easy problem. The complexity is often introduced by the need of employing the smallest quantity of sensors in order to meet the WSN requirements of application and decrease the uncertainty in the sensor's ability of detecting the objects, the distortions to which are chiefly caused by the terrain or unfavourable physical environment of the sensor [11]. In addition to the coverage of the sensor nodes, another vital consideration is the connectivity of the signals that are sent, necessitating that all the nodes be placed in a position to reach the data sink [12]. If the node has no direct route through which it can be able to reach the data, then it has been placed beyond the coverage area and there exists no possible means through which its data can be collected.

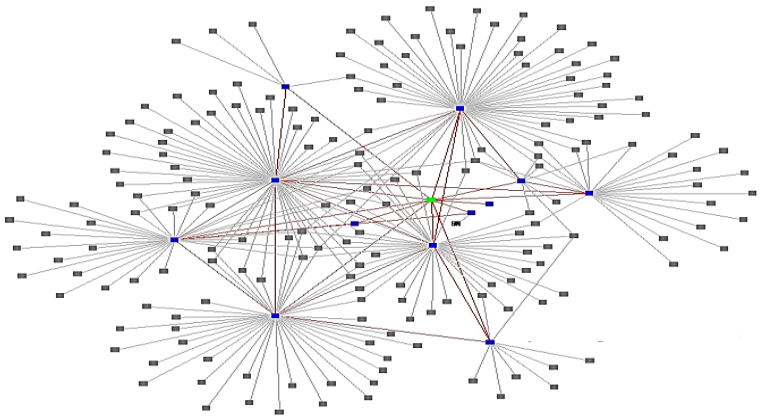


Figure 4: Area Coverage in WSN

4.3 Deployment of Intruder Detection Sensors

Sensor nodes are used to relay signals to the server upon the detection of an intruder. But even so, these sensor nodes are faced with the challenge of energy depletion which results in a decreased network lifetime. Sensor nodes are normally deployed in the fields to detect any intrusion or incorrect movements. They use wireless systems to send the signals to the base/server hence making them easily deployed without the intruder noticing. The intrusion detection systems come in two types; the single sensing detection and multi-sensing detection. Just as their name suggests, the single sensing detection only uses the sensor to detect an intrusion whereas the multi-sensing uses more than one sensor node to detect an intrusion. Intruders' detection in a two dimensional homogeneous wireless sensor networks majorly relies on two models; the system model and the mathematical model. In the system model, the sensors are randomly and uniformly deployed resulting in a 2-D network. WSNs are homogenous in nature and have to be equal in all their characteristics. For instance, they have equal sensing range, node density, and transmission range. The single sensor only detects an intruder who is within the sensing range which covers a diameter range. On the other hand, the mathematical model uses multiple sensors distributed in a field, and they can only detect an intruder who is walking within their sensing diameter. In [13] the intruder's movement was followed by the movement of the intruder past the sensors, this was either in a straight line or randomly. For random movements, the area covered by an intruder can be calculated by:

$$A_{IS}= 2*D*r_s+ \pi(r_s^2/2)$$

In a scenario that an intruder is dropped from an aircraft at a random position, such as shown in Figure 5, then the movement is computed by determining the probability of an intruder being detected under different scenarios, in which we use the following equations:

$$A_{IR}= 2*D*r_s+ \pi r_s$$

Theorem 1: Suppose an intruder is detected by a single cluster head. Immediately it comes close to the boundary in a 2D homogenous WSN. The probability of detection is given by:

$$P\ (D=0) = 1\text{-}e^{-n}$$

Where P (D) is the probability n_d is the node density and r the radius.

Theorem 2: Instances where an intruder can move a maximum distance D_M from the boundary without detection in a 2D-homogenous Wireless Sensor Networks. The probability of detection is given by:

$$P\ (D\leq D_M) = 1\text{-}e^{-in}$$

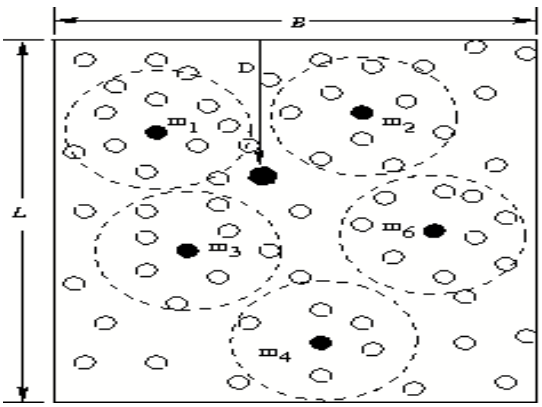


Figure 5: Intrusion Detection in 2D-Homogeneous WSNs

WSN can also detect intruders though a 3-D homogenous network. The 3-D homogenous intruder detection shown in figure 6 also relies on the two models; the system model and the mathematical model. Just like the 2-D homogeneous wireless sensor networks, the system model uses wireless sensors that have the same capacity in terms of transmission range, sensing range, and node density. While the mathematical model uses the detection probability of both the multiple and the single sensing detection for a 3-D, a sensor immediately detects an intruder, and the information is passed to the base station by the cluster head. In a field with a cluster of sensors in an area (A), an intruder may move without being detected for a given distance (D), then area will be given by:

$$Avb = \pi r_s^2 * D + (2/3)\ \pi r_s^3$$

In the case that an intruder is dropped from an aircraft and the movement originates from a random point then the area moved is given by:

$$Avr = \pi r_s^2 * D + (4/3)\, \pi r_s^3$$

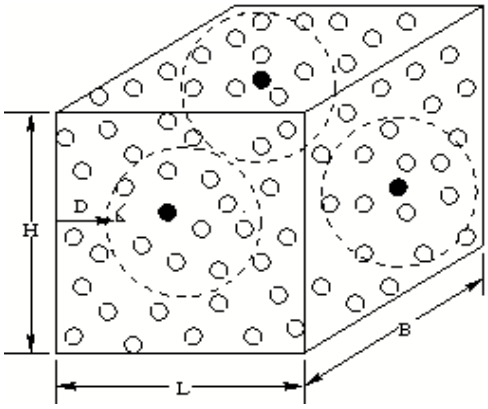


Figure 6: Intrusion Detection in 2D-Homogeneous WSNs

V. INTRUSION DETECTION SYSTEM DESIGN

The design of an intrusion detection system is a very application-specific task, especially because of the peculiarity of the considered deployment environment. Therefore, in this section we first present the architecture of the distributed intrusion detection system, and then discuss the system topology in detail.

5.1 The Architecture of the Intrusion Detection System

The placement of the WSNs in an extended geographical area requires the deployment of a low-power sensor-based architecture that is fitted with components that are characterized by low-power consumption and reduced monitoring requirements. While the conventional handheld, mobile technologies are supported by the implementation of protocols that are directed towards reducing the amount of power consumed through the implementation of a narrow-set of application requirements, WSNs have to support a large-scale number of sensors within a wide geographical area that is characterized by a comparatively low average bit-rate transmission [14].

In this regard, the design of the WSN architecture should make considerations of power consumption requirements together with the density of the population of the sensors within a given geographical area. Multi-hop routing architecture presents a suitable design topology for the sensor distribution, allowing significant power saving options as well as scalability in order to cover a larger area within the border. Also, depending on the conditions detected, the protocols that have been embedded within the node determine whether the remote user or the next-neighbouring WSN node should be alerted. In either case, the detecting node supplies the attributes of the event to the remote user and/or next WSN, thereby making it possible for environmental disturbances to be detected.

5.2 The System Topologies

The topology is crucial element, which plays an important role in minimizing various constraints like limited energy, latency, computational resource crisis and quality of communication. We can distinguish many possible topologies. The most used topologies are presented in the followings: mesh topology and tree cluster topology. The topologies and the internal architecture are two important aspects of the communication in wireless sensor networks especially to connect the nodes with each other. The selection of best topology in accordance with the internal architecture of the wireless sensor node is very critical job so that proper communication can be there in between all the nodes according to the application [15]. Here is an explanation of the most used topologies. First, Mesh topologies are nodes regularly distributed to allow transmission only to a node's nearest neighbours. An advantage of mesh topologies is that, while all nodes are possibly identical and have the same computing and transmission capabilities, certain nodes can be designated as coordinators

that take on additional functions. If a coordinator fails, another node can then take over these duties. Figure 7 below shows an example of the mesh topology. The second topology is tree cluster topology. The tree cluster topology is a special case of tree topology in which a parent with its children is called a cluster. In each cluster they identified by a cluster ID. Also when they connect to each other, they have to connect direct with the head cluster and the head cluster could connect with the coordinator, Figure 8 below shows an example of the tree cluster topology [16, 17].

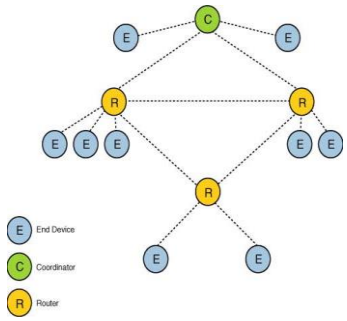


Figure 7: Mesh Topology

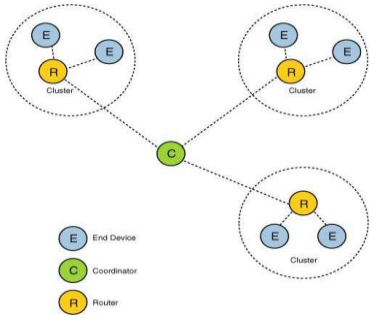


Figure 8: Tree Cluster Topology

VI. SIMULATION AND ANALYSIS OF PROPOSED SYSTEM

Simulation and modelling are important approaches in the development and evaluation of the systems in terms of time and costs. In our simulation shows the expected behaviour of the system based on its simulation model under different conditions. Hence, the purpose of the simulation model is to determine the exact model and predict the behaviour of the real system. WSN applications must be tested on a large scale, and under complex and varying conditions in order to capture enough wide range of interactions, both among nodes, and with the environment.

Also the WSNs simulators allow users to isolate different factors by tuning configurable parameters. There are many different possible platforms for simulation and testing for WSNs. Different aspects like energy efficiency, resources, decentralized collaboration, fault tolerance, simulation scenarios, global behaviour etc. Each of them work with different simulation program, the most popularly used simulators for WSNs are: OPNET, Ns-2, JavaSim, GloMoSim, and SensorSim.

For the purpose of simulation, we have used OPNET Modeller 17.5, which is a leading environment for modelling and simulations. The OPNET or "Optimized Network Engineering Tools" is powerful computational software used to model and simulate data networks. This simulation tool provides a comprehensive development environment to support modelling of communication networks and distributed systems. The OPNET simulator shows a clear result instead of doing it in the border area. Our overall simulation process begins by choosing the area that we want to do the test on, then we decide how many nodes needed for this test, as showing in table 1.

Table 1: Simulation Parameters

Parameter	Value
Simulation time	Until the end of network lifetime
Number of nodes	50
Simulation area	5000m X 1000m
Number of runs per data point	10 times
Number of cluster heads	5% of number of nodes

All of this work is done by using wireless sensor ZigBee node. The ZigBee is applicable for low data rate monitoring and control applications in virtually every industry worldwide [18]. ZigBee's primary advantage is the ability to fit into cheap and widely available 8-bit microcontrollers. ZigBee protocol is the most popular among all the wireless sensor network communication protocols. Also The ZigBee protocol is based on the IEEE 802.15.4 standard. Table 2 shows the specifications of ZigBee technology.

Table 2: ZigBee Specifications

Parameters	ZigBee Value
Transmission range(meters)	1 - 100
Battery life (days)	100 – 1.000
Throughput (kb/s)	20 – 250
Transmit Band	2.4GHz
Transmitted Power	0.05
ACK mechanism	Enabled

We used an example: area of 5000 m x 1000 m as part of the USA/Canada border as shown in Figures 9 and 10. Then we set the attributes, and choose the statistic that should be collected as shown in simulation attributes in table 3. In this work also the network model primarily is used to specify the topology of the network, i.e. the relative placement of the nodes. The distributed mesh and tree cluster topologies that are implemented in the OPNET environment are shown in Figures 11 and 12 respectively.

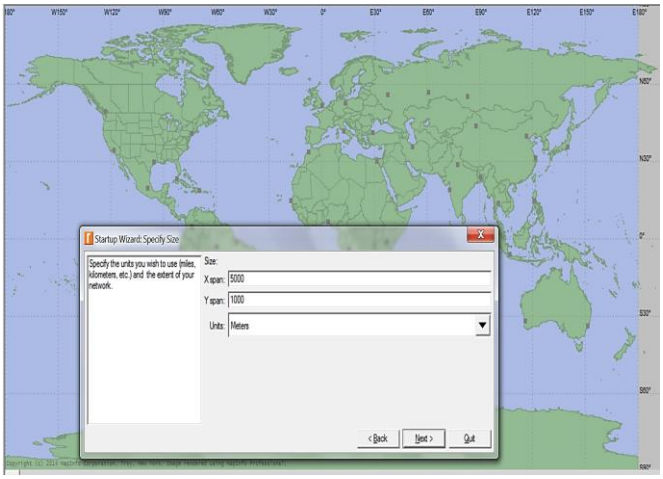


Figure 9: Distance of 5000m X 1000m

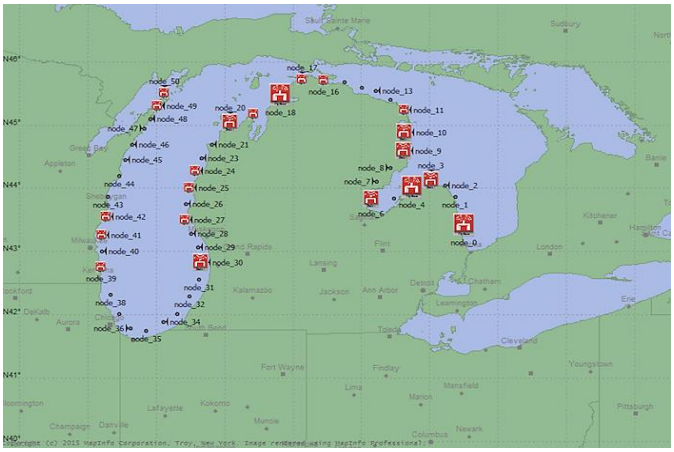
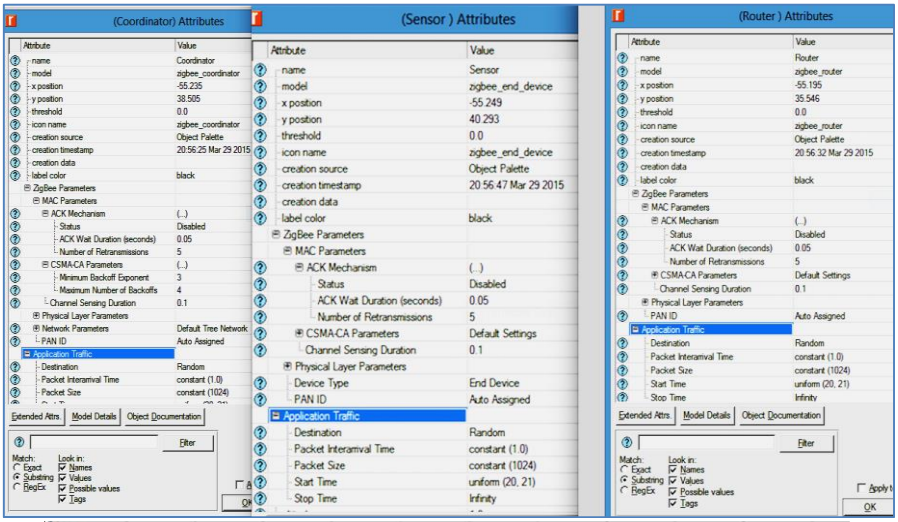


Figure 10: Distributed Nodes

Table 3: Simulation Attributes



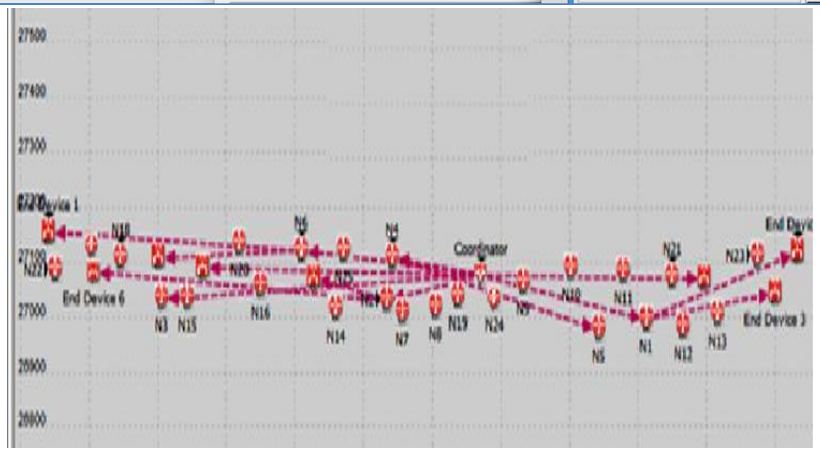


Figure 11: Distributed Mesh Topology

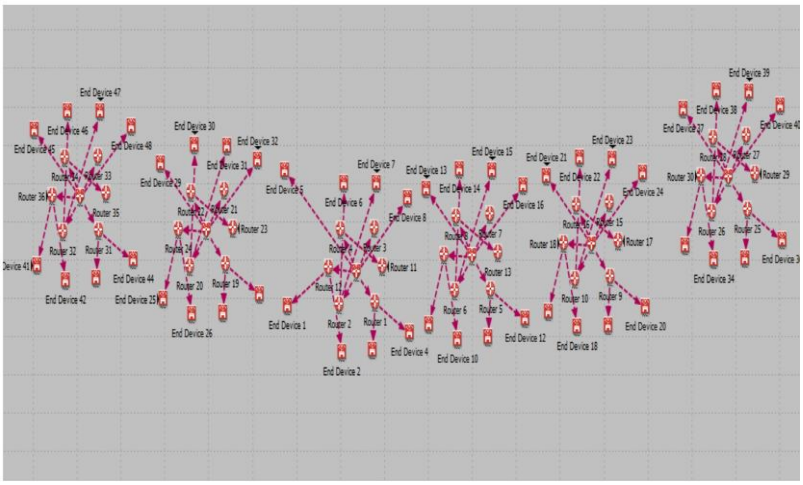


Figure 12: Distributed Tree Cluster Topology

6.1 The Quantitative Metrics Used for Comparison

In order to compare how the two types of topologies; distributed mesh topology and tree cluster topology will perform, the quantitative metrics are used:

A. Data Dropped

The Data dropped is the data quantity transmitted correctly starting from the source to the destination within a specified time (seconds). Higher layer data traffic (in bits/sec) dropped by the 802.15.4 MAC due to consistently failing retransmissions.

B. Throughput

The throughput is the difference between the number of data packets sent and the number of data packets received. Also known as network throughput of successful message delivery over a communication channel over a physical or logical link, and it is usually measured in bit/s.

C. End-to-End Delay

The End to end delay is a measurement of the network delay on a packet and is measured by the time interval between a message is queued for transmission at the physical layer, till the last bit received on the node. Also the end to end delay refers to the time taken for a packet to reach from source to destination in a network.

D. Reliability

Wireless sensor networks used in border surveillance comprise a large number of sensor nodes, characterized by limited storage, processing, and battery capabilities. Since the lifetime of any sensor node depends on the lifetime of the battery, we could say there are elements in the sensor nodes which are perfect reliability. So the reliability of a sensor node could be equal to the reliability of its battery used [19, 20].

6.1 Simulation Results

The simulation results concern the total events, average, and speed traffic in sending and receiving data in 50 numbers of nodes. The Data Drop, Throughput, and End-to-End Delay are analyzed across the full ZigBee stack, under different topology deployment strategies with 50 numbers of nodes. The ZigBee simulation modules which we use in this paper are operated at 2.4GHz with a maximum throughput of 250kbps. In our simulation, we considered two topologies, (Mesh and Tree) topology. After we ran the simulation with only 50 nodes, the data drop, in mesh topology was up to 200 (bits/sec) but in the cluster topology was up to 10,000 (bits/sec), which means mesh topology is much better than the cluster as shown in Figure 13 and 14. The result of throughput when approaching a steady state is 33,000 (bits/sec) in the mesh topology and 100,000 (bits/sec) in cluster topologies as shown in Figures 13 and 14. The maximum throughput is achieved in cluster topology while the mesh topology has lowest throughput. Finally the End-to-End found in mesh topology is 0,012 Delay per second and in cluster topology found 0.024 Delay per second. From results obtained using distributed mesh topology and tree cluster topology that, we found that the Mesh Topology is better to use than the tree cluster of using 50 nodes.

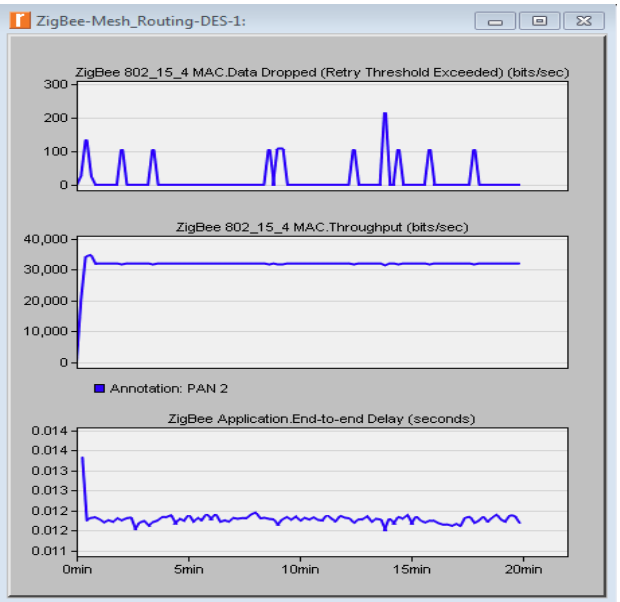


Figure 13: Mesh: Data Dropped, Throughput, and End to End Delay

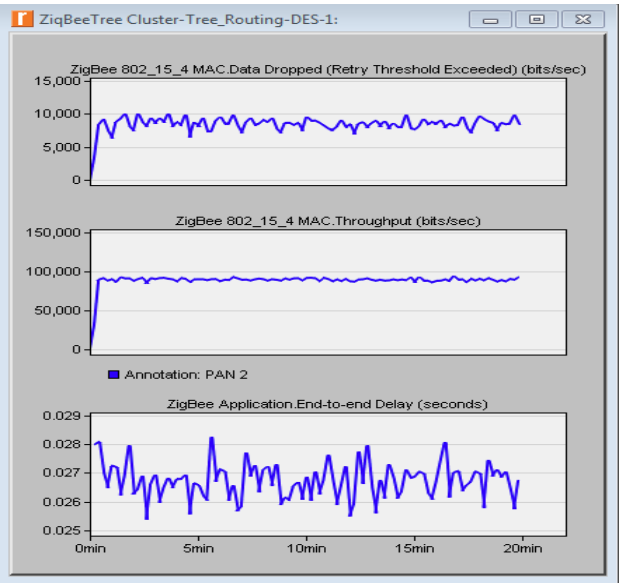


Figure 14: Tree cluster: Data Dropped, Throughput, and End to End Delay

VII. CONCLUSION

Wireless sensor nodes represent an emerging technology used in intrusion detection and border surveillance applications. The UAVs represent an emerging technology that is chiefly applied by the border guard services in order to provide surveillance at the border line. WSN combines the use of existing border control techniques with electronic detection systems. These technologies combined only offer line of sight detection, but also non line of sight detection. Moreover, the flexibility, high sensing, and simple use of wireless sensor networks make it an important part of our lives. Also the new technology hardware and software helps to protect the border control, for example, OPNET software. This paper was to investigate the performance capabilities of OPNET Modeler in simulating ZigBee WSNs. It concluded that the OPNET has good potential in simulating ZigBee since it can provide a vast variety of reports and statistics at different network topologies (mesh and Cluster). By analyzing the results obtained after running the two types of topologies, it was shown that the mesh is much better than tree cluster. Also during the our simulation, we found the maximum distance nodes can connect from 50 to 125 m and it is possible to increase this distance sometimes with the OPNET software.

VIII. FUTURE WORK

The wireless sensor networks have become indispensable to the realization of smart technology. The border control implementation using WSN will construct smart technology systems. In this paper the simulation have been done with 50 nodes for tow different type of topologies, which show the result of throughput, end-to-end delay and data dropped. This simulation gives us a good explanation of which topology should we use. In the future work, we would like to test our topologies for 100 nodes with two different topologies mesh and cluster. Furthermore, we will do the same with 300 nodes and 500 nodes to check the evaluations of the proposed deployment and operation of border sense system. Also more tests will be done on larger testbeds with different number of nodes and system complexity. Finally we will develop a system for tracking and detection any movement, and check the performance of this system.

REFERENCES

[1]. Sun, Zhi, et al, (2011) "BorderSense: Border patrol through advanced wireless sensor networks." Ad Hoc Networks 9.3, 468-477.

[2]. Bellazreg, Ramzi, Noureddine Boudriga, and Sunshin An (2013) "Border Surveillance using sensor based thick-lines." Information Networking (ICOIN), International Conference.

[3]. Felemban, Emad, (2013) "Advanced border intrusion detection and surveillance using wireless sensor network technology".
[4]. Karl, Holger, and Andreas Willig. Protocols and architectures for wireless sensor networks. John Wiley & Sons, 2007.
[5]. Maharrey, Brandon, Lim, Alvin, & Gao, Song, (2012) "Interconnection between IP Networks and Wireless Sensor Networks", International Journal of Distributed Sensor Networks.
[6]. J. Li,(2011) 'Compressing Information of Target Tracking in Wireless Sensor Networks', Wireless Sensor Network, vol. 03, no. 02, pp. 73-81.
[7]. J. B. McKitterick, April (2004) "Sensor deployment planning for unattended ground sensor networks," in Unattended/Unmanned Ground, Ocean, and Air Sensor Technologies and Applications VI, Proceedings of the SPIE, pp. 382–392.
[8]. Y. Kim, (2011) "A study on operational procedures and deployment method of surveillance reconnaissance sensor network system," Agency for Defense Development ADDR-425-111039.
[9]. Sharma S., Kumar D. (2013) "Wireless Sensor Networks- A Review on Topologies and Node Architecture". International Journal of Computer Sciences and Engineering. Vol.-1(2), pp 19-25.
[10]. A. Ibrahim Abdu,(2013) 'An Adaptive Energy-Aware Transmission Scheme for Wireless Sensor Networks', WCMC, vol. 1, no. 1, p. 14.
[11]. Shaila, K., et al, (Feb. 2014) "Probabilistic Model for Single and Multi-Sensing Intrusion Detection in Wireless Sensor Networks." 8727Volume 16, Issue 1, Ver. IX , PP 51-66.
[12]. Z. Sun, P. Wang, M. Vuran, M. Al-Rodhaan, and I, (2011) Akyildiz, 'BorderSense: Border patrol through advanced wireless sensor networks', Ad Hoc Networks, vol. 9, no. 3, pp. 468-477.
[13]. Sharma, Shamneesh, Dinesh Kumar, and Keshav Kishore, (2013) "Wireless Sensor Networks-A Review on Topologies and Node Architecture." International Journal of Computer Sciences and Engineering: 19-25.
[14]. Busse, Marcel, Thomas Haenselmann, and Wolfgang Effelsberg (2006) "TECA: A topology and energy control algorithm for wireless sensor networks." Proceedings of the 9th ACM international symposium on Modeling analysis and simulation of wireless and mobile systems. ACM.
[15]. Jung, Sewook, Alexander Chang, and Mario Gerla,(2007) "Comparisons of ZigBee personal area network (PAN) interconnection methods." Wireless Communication Systems,. ISWCS. 4th International Symposium on. IEEE.
[16]. Prasad P. Netalkar, Yasha Kaushal, N. Shekar V. Shet. (2014) " Zigbee Based Wireless Sensor Networks for Smart Campus " IJMER ISSN: 2249–6645, Vol. 4, Iss.7, July.
[17]. Singh, Santar Pal, and S. C. Sharma (2015): "A Survey on Cluster Based Routing Protocols in Wireless Sensor Networks." *Procedia Computer Science* 45, pp: 687-695.
[18]. Li, Wei and Zhang Wei,(2013) "Coverage Hole and Boundary Nodes Detection in Wireless Sensor Networks." Journal of Network and Computer Applications 48.2, pp: 35-43.
[19]. Halder, Subir and Das Bit Sipra,(2014) "Enhancement of Wireless Sensor Network Lifetime by Deploying Heterogeneous Nodes." Journal of Network and Computer Applications 38.1,106-124.
[20]. Hammoudeh, Mohammad, and Robert Newman (2015) "Adaptive routing in wireless sensor networks: QoS optimisation for enhanced application performance." Information Fusion 22 pp: 3-15.

AUTHORS

Mosad Alkhathami is a full-time Ph.D. candidate of Electrical and computer Engineer at Wayne State University. He received his M.S. in Telecommunication system from DePaul University for Graduate Studies/ Chicago in 2011, the B.S in Electrical and Computer Science from Purdue Calumet University/ Hammond, IN 2009. Mosad Alkhathami, is now doing his Ph.D. thesis in the field of embedded systems and wireless sensor networks.

Lubna Alazzawi received her PhD from University of Technology and University of Michigan-Dearborn, USA joint program. Dr. Alazzawi is currently working in the Department of Electrical and Computer Engineering at Wayne State University, USA. Prior to joining Wayne State University, She was teaching in the Department of Electrical and Computer Engineering at University of Michigan, Dearborn, USA. She also worked there as a postdoctoral research fellow. Her research interests include embedded systems, high-speed networks reliability and security, wireless sensor networks, smart sensors and FPGA chip design.

El Kateeb received his PhD from Concordia University (Montreal), MSc from Kent University (UK), Post Graduate Diploma from Imperial college (UK) and University of Technology (Iraq), and his BSc from University of Technology (Iraq). He is currently an Associate Professor in the Department of Electrical and Computer Engineering at University of Michigan, Dearborn, USA. Prior to joining the University, he was working with Acadia University (Canada) as an associate/assistant professor. He also worked in different Canadian companies and he received the ATI Technologies Inc. award. His research interests include high-speed networks, computer architecture, reconfigurable computing, and computer applications. He has over 60 papers published in international journals and conferences.