Border Security Control via Distributed WSN Technology

Mosad H Alkhathami, and Dr Lubna Alazzawi

Department of Electrical and Computer Engineering, Wayne State University, Detroit, MI

fc0233@wayne.edu, drlubna@wayne.edu

Abstract— Wireless Sensors Network (WSN) combine sensing, signal processing, decision capability, and wireless networking capability in a compact, low power system. 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.

Keywords— Wireless Sensor Network, border control, surveillance &Area monitoring

1- Introduction

Over the past two decades, wireless sensor networks (WSNs) together with the various applications that they have been assigned have undergone a rapid evolution, becoming a vital technology in today's evolving world as well as a central research area in academia. Sun et al. define wireless sensor networks as the spatially distributed self-directed sensors that are used to monitor the physical and environmental changes within their area of implementation –such as changes in motion, temperature, pressure or noise [1]. Over the years, the application of these sensor networks has met tremendous evolution and customization, with users deploying the solutions in security, agriculture, ecological monitoring, healthcare sciences and the even in the military. Meanwhile, the need for the implementation of real-time border intrusion detection and control has become an increasingly tough factor for most countries, often necessitating a large outlay of manpower and financial resources, which are inextricably faced with a high level of false alarms, together with sightline constraints. In this regards, the implementation of the WSNs in border control, surveillance and monitoring presents a suitable and intelligence means through which these problems can be solved. The WSNs combine the properties of signal sensing, transmission, decision-making as well as wireless network capabilities within low-power consumption, low-cost, compact device, presenting suitable solution that can be implemented across a large-scale geographical area [2].

2- Detection of Intuder Using WSN

WSN detect the intruders in a previously unknown territories. The intruders are detected and investigated. WSN applied hierarchical learning/communication structure. Each model of the network can monitor the local region and then communicate through the wireless channels with the other nodes for the collaborative production of a high-level representing on the state of the environment. Such networks can be used to monitor the large areas for a low cost. The system can uses the mobile robots to make the process of detection more autonomous and flexible. The senor nodes of WSN learn the model of the environment applying the ART neural network and then, the changes are compared to the normal model and are reflected as anomalies, caused by the possible intruders.

3- Wireless Sensor System Architecture

A primary consideration in the implementation of the WSNs is the associated power consumption requirements and sources for battery energy. 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 (smaller than 1Kbps) [1].

In this regards, the design of the WSN architecture should make considerations of this 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.

4- Wireless Sensor Node Architecture

The node architecture is comprised of the sensor which is connected to a low-power analog-to-digital converter so as to transform the detected analog signal from the environment into an digital signal for transmission. A spectrum analyzer is connected to this output so as to examine the current conditions and possibly invoke reactive actions depending on the current conditions. These components are in continuous operation, thereby necessitating the implementation of low-power cycles [3]. A control unit and wireless distribution interface is also attached to the node, which makes it possible for the node to transfer current environmental and physical settings to the next-neighboring node in a multi-hop architecture. Depending on the conditions detected, the protocols that have been embedded within the node determine whether the remote user or the next-neighboring 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.

a. Node Hierarchy

The wireless sensor network is comprised of a large distribution of small sensor nodes, spatially distributed across the expanse of the border. In order to save on power consumption, the node architecture is configured in a hierarchical manner such that the nodes within the architecture are either in an election phase of data transfer state. During the election phase, the nodes scan the physical characteristics of the environment in order to determine the occurrence of any changes. At the beginning of this phase, a set of hierarchical nodes is selected from the available node hierarchy on a random basis, allowing the clustered nodes to send a short range of broadcast messages to the neighboring nodes in order to alert them of their presence. During this phase, each of the neighboring nodes, on receiving the broadcast message, sends an acknowledgement message to the cluster head, allowing the cluster head to determine a set of associate cluster heads based on the amount of elapsed time after sending of the request as well as the signal strength of the acknowledgement. According to the node hierarchy structure, the head-set architecture of the node consists of the cluster head together with the associated nodes that are located within the enterprise.

Different states of the wireless sensors are contained within the hierarchy, with new sensors joining the hierarchy as candidate nodes. During the beginning of the iteration phase, a given set of cluster heads are selected from the available set of clusters, with the selection made depending on whether they are active or not-cluster heads are chosen as all those sensor nodes that have an active status. This defines the election phase which determines the cluster heads and a set of associate nodes in accordance with the signal strength. During the data transfer phase, the active nodes transfer data to the next nearest associate node, which is followed by the active node changing its state to passive associate status. At this time, the node that receives the transmission is transformed to become the active node, remaining in this state until it passes the message to the next available node. At the end of the iteration, the members are assigned a non-candidate role, until the next iteration is started where the next head-set is selected.

b. Area Coverage and Connectivity

WSN area coverage is a measure of the quality of service provided by the sensor networks, interpreted as the measurable level of signal availability of the devices which effectively determines how well the sensors are able to monitor their environment. 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 [2]. 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.

The first step in the deployment of the WSN as suitable solutions for border security is determining the level of traffic and environmental conditions that is to be monitored. The coverage problem for wireless sensor networks relates to the need for the arrangement to significantly decrease the number of nodes that are placed within the area, while at the same time guaranteeing that each point within the border is suitably and optimally covered so as to detect the presence of intrusion. It is also worthwhile to note that the degree of coverage defines the total number of wireless sensors within the network whose sensory range have influence over a given location within the field of interest [3]. In this case, since the border requires to be monitored at every location thereby making 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.

Typically, border security requires the monitoring of a large geographical area, primarily working towards the identification of the presence of an environmental breach within a set barrier. The sensor networks in this case would need to carry out a full or blanket coverage, implying that the entire border is within the sensing range of the sensors that have been deployed. In order to achieve this type of coverage within a border setup, the nodes are placed in an r-strip construct such that each node within the configuration is placed at an r distance away from the next neighboring node, thereby creating a region where each location has a sensor associated with it [5]. At the intersection of the sensor coverage regions are areas that are covered by two sensors at the same time.

Connectivity within the WSN scenario defines the ability of one node to reach the other node either through one hop or a series of multiple hops. Similar to the degree of coverage, the degree of connectivity of a given wireless sensor network is said to be k (read as k-node-connectivity) in a situation where the removal of one node from the network disconnects the existent communication routes.

5- Deployment Methodology

The WSN deployment technique is either categorized as being dense or sparse depending on the number of nodes that are required to suitably cover the network. 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 [6]. The dense deployment model is achieved by ensuring that the radius of coverage of each of the sensors is contained within the next neighboring 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 use to control their placement and distribution within the border.

6. Routing Between Nodes

Routing of the sensed environmental and physical conditions within the border is achieved through the transmission of the results in a multi-hop manner, based on the shortest distance to the remote user. This means that in order to adequately route the signals within the network, the considerations of the level of traffic between the nodes is carried out in lieu of the physical distance between them. While a particular node might be physically close to the transmitting node, the level of traffic directed towards this node by other communicating nodes in the network may prevent the first node from using this route as it would incur too much delay in navigating through the traffic [2].

7. Shortest Distance Algorithm

The shortest distance algorithm seeks to determine the mean packet delay of a communicating node, given that the current network capacity together with the average network flow can be calculated. After determining the mean delay from all the communication routes, we can be able to determine a flow-weighted average communication speed for the network, making it possible to calculate the mean packet delay for the entire wireless network [4]. These weights determine the differentiated route capabilities for each direction, expressed in terms of the number of packets per second. The average delay for each routing direction can be calculated using the formula [5]:

$$T_i = 1/(\mu c - \lambda)$$

Where, T_i represents the amount of packet delay in seconds, C represents the network capacity for the given route in bits per second, λ represents the average packet flow in number of packets per second, and μ represents average packet size expressed in bits.

The average delay time for the wireless network can thence be derived from the weighted sum of the delay from all the routes. Accordingly, this makes it possible to find the path that has the smallest value for the average delay time. To calculate the shortest distance, we also need to calculate the waiting factor for each route. That route that has the least value calculated for the waiting factor represents the shortest route. This done using the formula [5]:

$$W = \lambda_i / \lambda$$

Where, λi represents the average packet flow in a given route, and λ represents the average packet flow within the wireless network

8. Application

The application of the Wireless Sensor Networks will require the deployment of small, limited sensing devices throughout the entire geographical expanse of the border, having the capability of interacting with the WINs node architecture within a heterogeneous network [6]. This implementation will also require integration with Linux-based sensing devices that can be integrated with the existent network infrastructure [7]. Additionally, scalable application of the WSN encompasses the use of small, low power devices with the ability to scavenge for energy from the operating environment, through the use of attached photocells and other piezoelectric materials that have the ability of generating electrical energy, thereby increasing the relative lifespan of the transmission [8].

9. Conclusion

The design successfully details the implementation of multi-hop, low-power Wireless Sensor Networks for border patrol. While the design implications present significant complexities with regards to the management of power, it is a far better solution as compared to other alternatives such as manual patrols and radar surveillance. Through the calculation of the shortest distance, the technique makes it possible for the determination of the least amount of time and shortest route for transmission, leading to significant reductions in delay. On a national scale, the WSN solution will make it possible for countries to carry out border monitoring over land, air and even water.

Reference

[1]Z. Sun, P. Wang, M. Vuran, M. Al-Rodhaan, A. Al-Dhelaan and I. Akyildiz, 'BorderSense: Border patrol through advanced wireless sensor networks', *Ad Hoc Networks*, vol. 9, no. 3, pp. 468-477, 2011.

[2]A. Ibrahim Abdu, 'An Adaptive Energy-Aware Transmission Scheme for Wireless Sensor Networks', *WCMC*, vol. 1, no. 1, p. 14, 2013.

[3]D. Lee, 'Energy Harvesting Chip and the Chip Based Power Supply Development for a Wireless Sensor Network', *Sensors*, vol. 8, no. 12, pp. 7690-7714, 2008.

[4]C. Kao and W. Yang, 'Energy Efficient System-on-chip Design for Wireless Body Area Sensor Network', *Electric Power Components and Systems*, vol. 42, no. 7, pp. 737-745, 2014.

[5] GUPTA, 'Model of Real Time Architecture for Data Placement in Wireless Sensor Networks', *Wireless Sensor Network*, vol. 2, no. 1, 2010.

[6]J. Li, 'Compressing Information of Target Tracking in Wireless Sensor Networks', *Wireless Sensor Network*, vol. 03, no. 02, pp. 73-81, 2011.

[7]B. Sabarish, 'Improved Data Discrimination in Wireless Sensor Networks', *Wireless Sensor Network*, vol. 04, no. 04, pp. 117-119, 2012.

[8]N. Bulusu and S. Jha, *Wireless sensor networks*. Boston, MA: Artech House, 2005.

[9]R. Faludi, *Building wireless sensor networks*. Beijing: O'Reilly, 2011. Authors

Authers

1-Mosad Alkhathami is a full-time Ph.D. candidate ofElectrical 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, now doing his Ph.D. thesis in the field of embedded systems and wireless sensor networks. My email addresses: Fc0233@wayne.edu

2-Dr. Lubna Alazzawi has received her Ph.D. from University of Technology and University of Michigan, Dearborn-joint program. She taught at the Department of Electrical and Computer Engineering at University of Michigan, Dearborn. She also worked there as postdoctoral researcher fellow. She is currently teaching at the Department of Electrical and Computer Engineering at Wayne State University. Dr. Alazzawi has worked in diversified areas of communication networks reliability and security, wireless sensor networks, smart sensors, embedded systems and FPGA chip design.