Framework for a Fault Tolerant National Wireless Border Security System (NWBSS)

Yaknan J. Gambo[1*], John A. Odey[1], and Charles I. Saidu[2]

[1]*Department of Computer Science, Federal University Wukari, Wukari, Taraba State, Nigeria.*
[2]*Department of Computer Science, Baze University Abuja, Nigeria.*

Abstract— Issues of security have always been the primary focus of every society and the demand for a good and efficient security system can never be overemphasized in our contemporary times. Developing countries like Nigeria are faced with security issues like never before in their existence due to many issues bordering around negligence and lack of technological sophistication that gave rise to the status quo. One of these issues of great concern is border management and control. In this research we exploit the potentials of LoRa and mesh network topology to design a framework for a wireless sensor border security system. Our objective is to provide a robust framework for an efficient and computerized National Wireless Border Security System that will aid in securing our national borders effectively.

Index Terms—Security, LoRa, Wireless Sensor Network, Sensor, Fault Tolerant Network, Border Security

1 Introduction

The healthy and effective growth of any society cannot be actualized with an ineffective security. Maslow stated that in a society, people are motivated to achieve certain needs. When one need is fulfilled a person seeks to fulfill the next one[1]. The question is how can one pursue higher goals when the basic primary needs are not met? A key primary need in our discourse is the need for peace and security. No human can maximize and utilize their full potential in an insecure environment.

Security business is a serious business, a cliché void without the effective use of modern trends of information technology in the realization of an effective security system as we are in an information age. Human activities border around the use of our senses in relation to our environment. There are highly sensitive devices designed to trigger certain actions when activated by human activities. These devices can be used to supply data that can be used to elucidate meaningful information.

In this research, we are interested in designing and implementing an efficient fault tolerant wireless sensor network for border security. This will enhance the effective management and control of national borders. The modifications we propose are specific to the geographical and prevalent situations within the Nigerian city states which have in recent times suffered from the menace of terrorism and smuggling problems.

2 Significance of the Study

Recent advances and innovation in the Internet of Things (IoT) through research has projected that by the year 202, 50 billion smart things will be connected to the Internet [2]. This is a pointer that the benefits of connectedness can be exploited to physically secure the sovereign borders of a nation. This study shows that border security can be made digitized, effective, and efficient to seamlessly militate against terrorist activities. It is noteworthy that most African countries are now saddled with the challenge of terrorist attacks, and the technological know-how capable of monitoring and safeguarding borders are not employed. This study seeks to address these issues in the framework provided.

.

3 Literature Review

3.1 Sensors

Simply put a sensor is a device capable of detecting and responding to physical stimuli such as movement, light, or heat etc. [3][4]. These sensors span several orders of magnitude in physical size. Some sensors like biological sensors, smart dust, lab-on-a-chip span from a nanoscopic scale (1 – 100nm in diameter) to mesoscopic scale (100-10,000nm in diameter) while other sensors like ID tags, bioterrorism sensors, radars, sonars span from microscopic scale (10 - 1000µm in diameter) to macroscopic scale (millimeter – meter range in diameter) [4].

3.2 Sensor Network

A collection of several sensors connected via some form of computer network to share information and act as a team constitutes what is known as a sensor network.

Corresponding author: Email: yaknanjohn@gmail.com

Kazem, (2007), defined a sensor network as an infrastructure comprised of sensing (measuring), computing, and communication elements that gives an administrator the ability to instrument, observe and react to events and phenomena in a specified environment [5]. They further went on to say that networked sensor systems are seen by observes as an important technology that will experience major deployment in the next few years for a plethora of applications not the least being national security.

3.3 Types of Wireless Sensor Network

There are five types of wireless sensor networks (WSN)[6]:

i. Terrestial WSN
ii. Under water WSN
iii. Underground WSN
iv. Multi-Media WSN
v. Mobile WSN

These sensor network operate based on their location[7]. There are countries whose border cuts across several types of terrain and as such various wireless sensor network types must be considered in securing such situations.

3.4 Challenges of Wireless Sensor Network

Sensors are usually equipped with multiple components among which include computation engine, communication and storage subsystem, and battery supply, sensing or actuating devices. Of all the components in a sensor, power supply consumption poses a big challenge since frequent replacement of the batteries is often not practical due to the large number of nodes in the network [8]. Also, Liu (2009) opined that nodes in wireless sensor networks are prone to failure due to energy depletion, hardware failure, communication link errors, malicious attack, and so on. Unlike the cellular networks and ad hoc networks where energy has no limits in base stations or batteries can be replaced as needed, nodes in sensor networks have very limited energy and their batteries cannot usually be recharged or replaced due to hostile or hazardous environments [9]. So, one important characteristic of sensor networks is the stringent power budget of wireless sensor nodes. Two components of a sensor node, sensing unit and wireless transceiver, usually directly interact with the environment, which is subject to variety of physical, chemical, and biological factors [9].This brings about the need for fault tolerance in the wireless sensor network which is the ability of a system to deliver a desired level of functionality in the presence of faults [10]. Also, the sensing unit and the transceiver unit of the sensor node tend to have an adverse effect of power consumption. We intend to exploit the recent advances a company called Libelium has made in the area of transmission modules that offer a wider range of coverage and higher interference immunity whilst minimizing power consumption [11]. The device developed by Libelium is called LoRa which is a new, private and spread-spectrum modulation technique which allows sending data at extremely low data-rates to extremely long ranges. The low data-rate (down to few bytes per second) and LoRa modulation lead to very low receiver sensitivity (down to -134 dBm), which combined to an output power of +14 dBm means extremely large link budgets: up to 148 dB, that means more than 22 km (13.6 miles) in line of sight (LOS) links and up to 2 km (1.2 miles) in non-line of sight (NLOS) links in urban environment. This makes LoRa outperform other traditional modulation schems, such as Frequency-Shift keying(FSK) and also makes it well suited for low-power and long-range transmissions[12].

3.5 Security Wireless Sensor Network

Security monitoring networks are composed of nodes that are placed at fixed locations throughout an environment that continually monitor one or more sensors to detect an anomaly. A key difference between security monitoring and environmental monitoring is that security networks are not actually collecting any data. This has a significant impact on the optimal network architecture. Each node has to frequently check the status of its sensors, but it only has to transmit a data report when there is a security violation [13]. This shows that in the case of a wireless sensor network used for security, there is minimal transmission of data which in turn conserves energy. In this research we are concerned about detection and recovery of faults within the wireless network to ensure an effective security system and how to cover a wide border area that covers different kinds of environmental terrain saddled with a lot of physical obstacles that can cause interference within a wireless network.

4 PROCEDURE

In this research, we present an efficient architecture for a fault tolerant National Wireless Border Security System (NWBSS). The proposed system uses LoRa modulation devices that cover a wide range area of about 22km radius with minimal interference. LoRa transceiver modules have low data rates and since the data expected from security sensors are only sent when an intrusion occurs, LoRa is an idle device for our border security in energy conservation. LoRa transceivers will be mounted on Waspmote expansion devices that can be equipped with different kinds of sensors, 3G and GPS modules. For our architecture we use an event or motion sensor, video camera, thermal, and temperature sensors. These sensors communicate with one another at certain intervals to cater for fault tolerance and also communicate wirelessly over a longer range with a Meshlium outdoor Linux mesh gateway device that routes sensor data to a datalogger or a web interface for processing.The system is designed in such a way that video cameras only come on when motion sensors detect sizeable motion and thermal sensors determine the degree of heat emanating from an intruder. We believe that this will conserve energy and reduce redundant data. Also, the sensor nodes in this

IJSER

architecture are equipped with small 7.2v – 100mA flexible solar panels [14]to recharge battery cells which increases battery life span for longer periods. We see this as a valid advantage for countries in the tropic regions of the world that enjoy huge amounts of sunshine.

TABLE 1:
HARDWARE SPECIFICATION

SN	DEVICE	SPECIFICATION
1.	Waspmote 3G + GPS module	Equipped with a both a 3G and GPS module
2.	Flexible Solar panel 7.2V – 100mA	For charging of sensor batteries especially the multi-sensor PTZ camera
3.	Presence Sensors	Sensitive to valid movements by sizeable things.
4.	Temperature Sensors	Compliments the presense sensor
5.	SX1272 915MHz RF LoRa capable module with special 4.5dBi Antenna	Provide upto 22km radius of network coverage
6.	Meshlium Xtreme IoT Gateway	IoT gate way to connect any sensor to any cloud Platform. Ethernet or 4G/3G/GPRS protocols[15]
7.	Viper multi-sensor PTZ camera by Infiniti Electronics	Meets and exceeds MIL-STD-810F military ratings for shock, vibration, temperature and dust/water ingression[16]

5 NWBSS SECURITY ARCHITECTURE

5.1 Hardware Specification

The hardware specification proposed for this architetureis based on current best hardware standards and are presented in Table 1.

5.2 Framework Design

The framework presented in Figure 1 provides a fault tolerant wireless sensor network that is capable of optimizing energy resource and secure terrestrial borders against intrusion. It is important to note that this framework is expected to be complimented by a rapid response security team situated at certain distances for effective arrest and mitigation of possible intrusion.

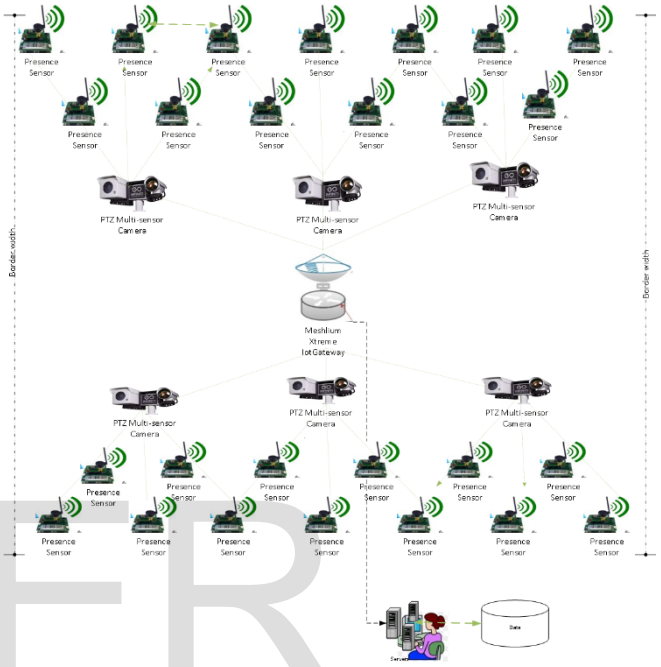
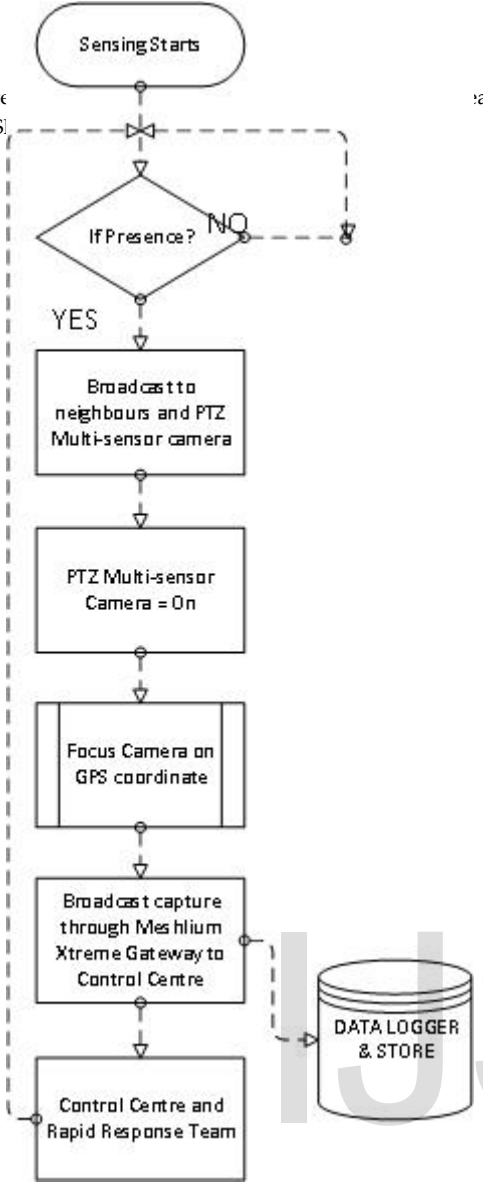


Fig. 1. Frame work of WSN for Border Security

In Fig. 1, the presence sensors which have a coverage radius of about 200m each are placed 100m apart to ensure that each presence sensor has atleast 5 to 6 others within its coverage area. If one of the sensors is tampered with or fails the others can still detect presence and broadcast. Also, each presence sensor is equipped with a GPS and a LoRa module for pinpointing the exact location of a presence and for broadcasting the message for about a distance of 22km respectively. The boardcast in addition to sending to other sensors within its reach also sends to the Meshlium Xtreme gateway to the control centre for accurate mapping.

In the framework, the PTZ multi-sensor cameras which have a coverage radius of 10 to 20km are placed are placed at equal distances of about 4km apart and each can respond to signals coming from sensors within its coverage area. It is only when a presence is detected that the PTZ multi-sensor Camera with military precision standard is triggered after it has received a message from the presence sensor with the GPS coordinate of the intruder. The camera then focuses on the location with a thermal sensor to capture the situation and broadcast it through a Meshlium Xtreme Gateway to the nearest control centre and storage for necessary action from a rapid response team.

IJSER



5.3 Sensing Data Flow

Fig. 2 presents the sensing data flow in the security framework.

Fig. 2. Sensing Data Flow

6 Conclusion

The architecture presented provides a fault tolerant wireless security system that can be implemented in securing national borders and other perimeters from intruders and illegal entries especially for countries that are saddled with immigration problems, smuggling issues and terrorist activities. Further work can be done to design an interface for the control and management of this architecture.

References

[1] C. D. Green, "Classics in the History of Psychology," *Classics in the History of Psychology*, 2002. [Online]. Available: https://psychclassics.yorku.ca/Maslow/motivation.htm. [Accessed: 27-Jul-2018].

[2] FTC, "IoT Privacy & Security in a Connected World," *FTC Staff Rep.*, no. January, p. 71, 2015.

[3] [www.wikipedia.com], "Sensor - Wikipedia," *Wikipedia*. .

[4] C. Descriptions, "Sensor / Actuator Class Descriptions," pp. 1–2, 2014.

[5] K. Sohraby, D. Minoli, and T. Znati, *WIRELESS SENSOR NETWORKS Technology, Protocols, and Applications*. New Jersey, USA: John Wiley & Sons, Inc., 2007.

[6] N. Srivastava, "Challenges of Next-Generation Wireless Sensor Networks and its impact on Society," *J. Telecommun.*, vol. 1, no. 1, pp. 128–133, 2010.

[7] D. Puccinelli and M. Haenggi, "Wireless Sensor Networks : Applications and Challenges of Ubiquitous Sensing," pp. 19–29.

[8] F. Koushanfar, M. Potkonjak, A. Sangiovanni-, and Vincentelli, "Handbook of Sensor Networks : Fault Tolerance in Wireless Sensor Networks," in *New York*, M. ILYAS and I. MAHGOUB, Eds. CRC Press LLC, 2005, p. 4.

[9] H. Liu, A. Nayak, and I. Stojmenovi, *Guide to Wireless Sensor Networks: Fault –Tolerant Algorithms/Protocols in Wireless Sensor Networks*. Springer London, 2009.

[10] M. Demirbas, "Scalable design of fault-tolerance for wireless sensor networks," The Ohio State University, 2004.

[11] Libelium, "Waspmote LoRa 868MHz 915MHz SX1272 Networking Guide." Libelium, 2014.

[12] Aloÿs Augustin, J. Yi, T. Clausen, and W. M. Townsley, "A Study of LoRa : Long Range & Low Power Networks for the Internet of Things," *Sensors MDPI*, pp. 1–18, 2016.

[13] J. L. Hill, "System Architecture for Wireless Sensor Networks by," UNIVERISY OF CALIFORNIA, BERKELEY, 2003.

[14] FlexSolarCells, "PowerFilm Solar Cell: MP7.2-75 Flexible Solar Panel 7.2V @ 100mA," *FlexSolarCells*. [Online]. Available: http://www.flexsolarcells.com/index_files/OEM_Components/Flex_Cells/pages/PowerFilm-Solar-OEM-11-Solar-Cell-Module-MP72-75.php. [Accessed: 27-Jul-2018].

[15] Libelium, "Meshlium Xtreme - The Internet of Things IoT Gateway - Smartphone Detection _ Libelium." Libelium.

[16] Infiniti, "Viper, A Military-Grade PTZ Camera System _ Infiniti Electro-Optics," *Infiniti Electro-Optics*. [Online]. Available: https://www.infinitioptics.com/cameras/viper. [Accessed: 27-Jul-2018].

Yaknan J. Gambo has a B. Sc Computer Science (ABU, Zaria); M. Sc Computer Science (ABU, Zaria) and has been lecturing in the Federal University Wukari, Nigeria since 2012. He is a member of the ACM both locally (Ibadan Chapter) and Internationally.

John A. Odey has a B. Sc Computer Science, M. Sc Computer Science, Ph. D Computer Science (China) and lectures at the de-

IJSER

partment of Computer Science Federal University Wukari, Nigeria

Charles I. Saidu has a B. Tech Information Tech (FUT Yola), M.Sc. Computer Science (ABU, Zaria) and Ph. D in view (AUST, Abuja). He currently lectures at the Department of Computer Science Baze University, Abuja, Nigeria.

IJSER