The 11th International Multi-Conference on Complexity, Informatics and Cybernetics

March 10 - 13, 2020 – Orlando, Florida, USA

PROCEEDINGS

Volume I

Edited by:

Renata Baracho
Nagib Callaos
Suzanne Lunsford
Belkis Sánchez
Michael Savoie

Organized by

International Institute of Informatics and Systemics

Member of the International Federation for Systems Research (IFSR)

COPYRIGHT

ISBN: 978-1-950492-24-4 (Colección) ISBN: 978-1-950492-25-1 (Volumen I)

Monitoring Network for Nuclear Research Laboratory Using WSN and IoT Devices

Kaio ROCHA
University Center Tocantinense Presidente Antonio Carlos - UNITPAC
Araguaína, Tocantins, Brazil

Matheus COSTA
University Center Tocantinense Presidente Antonio Carlos - UNITPAC
Araguaína, Tocantins, Brazil

Marcia SAVOINE
Nuclear and Energy Research Institute - IPEN/USP
Araguaína, Tocantins, Brazil

ABSTRACT

This work presents a proposal of implementation of an automatic monitoring system for environments who does experimentation and manipulation of ionizing radioactive particles, having as a base scenario the structures off nuclear energy research laboratories through sensors coupled to integrated microprocessor circuit boards, to carry out the communication between the sensors a Wireless Sensor Network with star topology was raised by resorting in the Internet of Things paradigm. For the network security, the concept of layered access level was applied, specifically, access level according to the criticality off the process and environment whose the sensors are exposed to.

Keywords: WSN. IoT. Layered access. Nuclear scenarios. defense-in-depth.

1. INTRODUCTION

The study of ionizing particles is one of the great vanguards among various areas of science, especially in oncology for tumor treatment and in power generation through thermonuclear power plants. In Brazil, the safety and monitoring of ionizing radiation nuclear research laboratories is performed almost entirely manually, which leaves safety gaps and delays in emergency response.

Applying a sensing network using WSN - Wireless Sensor Network with IoT devices enables a feature to mitigate these security breaches, as well as substantially streamlines decision making in the event of a critical situation, showing one of the many applications that aggregating these technologies makes possible.

This paper is organized as follows: in addition to this introductory section, there is the Section 2 that establishes the theoretical framework, the Section 3 that presents the methodology. In Section 4, the results and discussions about the work, and finishes in Section 5 with the final considerations.

2. THEORETICAL FRAMEWORK

WSNs are made up of several Sensor Nodes for the purpose of gathering information about the physical and environmental conditions of their application site. IoT builds a premise that all electronic objects within the same location must be within the same network, which allow decision-making on gathered data, a concept that when applied within a WSN acts as an amplifier of possibilities and enhancer of the existing ones.

WSN – Wireless Sensor Network

[1] state that WSNs consist of sensors that aim to probe a particular environment, process environmental data and transmit this data to an end user, having applications in crop management, industrial production, urban traffic and so on.

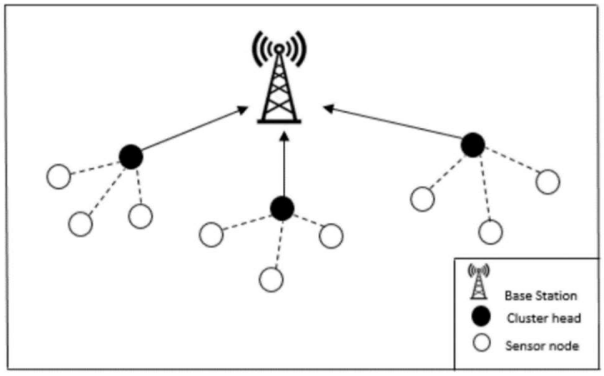

Figure 1: Example of WNS in cluster topology. Source: [2].

In this sense, wireless sensor networks consist of a large number of Sensor Nodes, from tens to thousands, aggregated within an application-specific topology, which, when inserted into an environment, allows obtaining any environmental data depending on the available resources and network characteristics, described by [3], such as addressing type, which is unique when there is a need to know the location from which the data was taken; the type of data aggregation, whether it is still centralized on the network before being sent to the base station or if all data is sent individually to the base; the type of mobility of the sensors, i.e. whether they are mobile or fixed; the need to restrict data access as to who has access or when someone may have

access; the number of sensors, which depends completely on the application; limitation of available power, because systems installed in remote locations have their uptime limited to the amount of power available; ability to self-organize the network in case of physical loss or malfunction of any of the devices.

These characteristics show that building a WSN has great potential for mitigating emergency events in any application, as the data obtained through sensors can be used in human engineering or in activating emergency devices such as sprinklers in the instance of a fire event.

IoT – Internet of Things

According to [4], IoT can be defined as a network infrastructure that can be used with automatic configurations by using standards and protocols that support network interoperability.

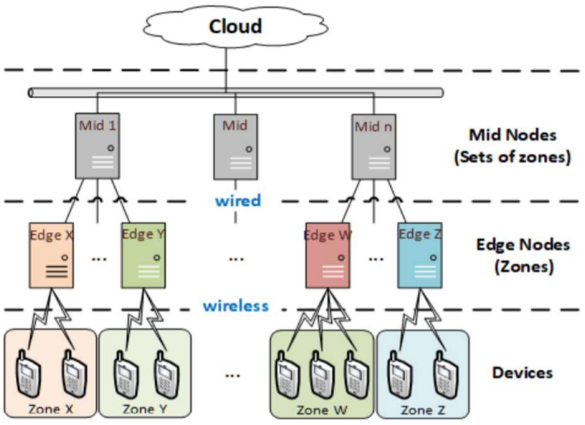

Figure 2: Example off IoT for telephony services. Source: [5].

The infrastructure of an IoT network is made up of its digital devices or "things", the data aggregation device, which is usually a network card, and a place for data storage, such as its own server or a cloud server, on this server not only is performed data capture but also refinement, statistical processing and the possibility of programming triggers and response to the data. This concept has the ability to create a data gathering and abstraction interface when used in conjunction with a WSN, and consequently creates an autonomous sensing system.

Layered access level

The layered access level comes from the concept of defense-in-depth that was born in the military, this strategy proposes the division of a locality into parts and the creation of a barrier in the front of each part to delay or even stop an enemy during a siege.

Thus, when this concept is applied to a WSN, it consists of a proposal to distribute privileges and restrictions within the network to specific users or user groups in order to show the same effects of the military strategies, that is to delay or stop an attack.

According to [6], defense-in-depth is a layered defense framework consisting of a robust communications network tailored to intrusions, as well as applications that tolerate power outages and function properly even in the event of a cyber-attack.

For [7], partitioning the level of access between users comes from the need to ensure the integrity and privacy of data flowing within a network, from which can derive various types of access control, such as independent users or cascading hierarchy, the latter is ideal in contexts where multiple users must have access to different data and processes.

The defense-in-depth concept applied to Information Technology can be fully adapted for wireless sensor networking with IoT devices in the critical environments of nuclear laboratories. This concept coupled with other elements can provide risk mitigation and increase the security of these hostile environments.

3. METHODOLGY

The test scenario consists of a nuclear research laboratory for handling radioactive material and was selected because it has a low level of access control and security in the integrated devices, allowing invasions by physical and digital means, it is also considered a critical and hostile environment as it is a place for handling radioactive material. Currently the laboratory has a single network and the physical access has no access delimitations, the manipulation laboratory is the only point with more rigorous control because it contains high radiation levels, having a dosimeter as monitoring system (individual component to monitor the radiation amount in which the user is exposed). The environment description can be viewed in Figure3.

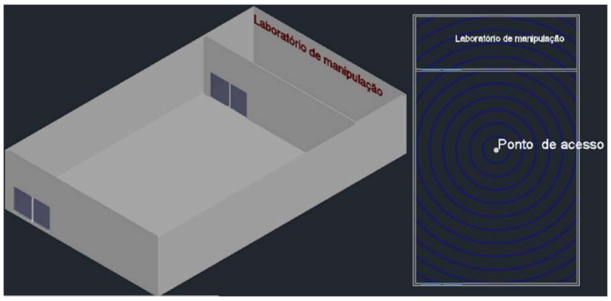

Figure 3: Representation of network propagation in the manipulation laboratory in isometric and superior views.

The setting of the scenario was based on the interaction of a group of Nodes forming a topology that can be applied later in the places to be monitored.

In the laboratory facilities, access zones are delimited according to its criticality where the presence of Nodes (WeMos D1 R2 Wifi ESP8266 Card) will be linked to a specific monitoring Sensor (Figure 4), that being: presence (PIR), temperature / humidity (DHT11) and ambient radiation level (DIY Geiger Counter); Each zone will be bounded by a physical access key using RFID technology (RC 522).

Data collection should rely on real-time analysis techniques, in this context Blynk was used as a hardware-independent IoT platform with device management, data analysis and machine learning.

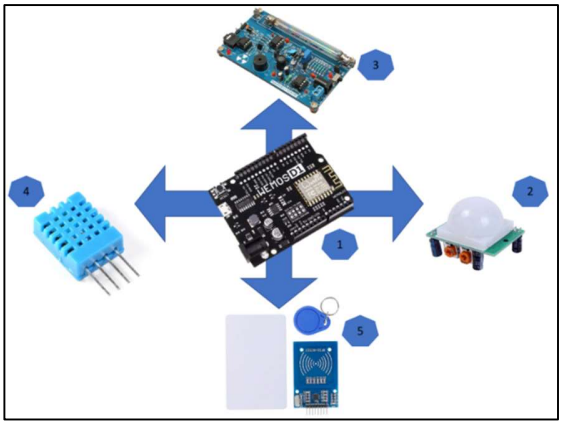

Figure 4: Node and sensor modules used on the tests, 1. WeMos D1 R2 Wifi ESP8266, 2. PIR, 3. DIY Geiger Counter, 4. DHT11 e 5. RC 522.

4. RESULTS AND DISCUSSIONS

The survey of the proposed scenario led to a restructuring of the nuclear research laboratory for manipulation of radioactive material, with the application of cascade access level techniques the environment now has new permission levels. Featuring five Zones (from A to E) each with their own unique network and aspects (Figure 5).

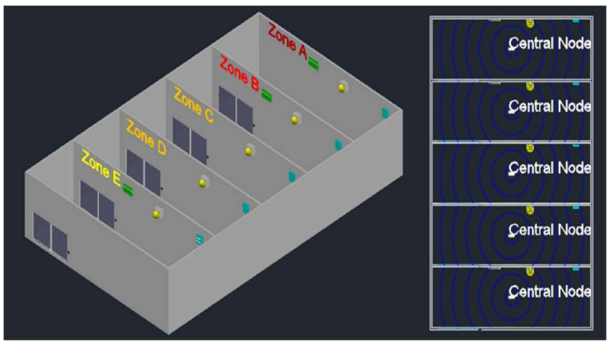

Figure 5: Representation of network propagation in the proposed scenario, isometric and superior view.

Zone E, considered a high-flow region because it contains the lab access door, has the rearguard role for radiation perception if Zone A and B sensors fail. Zones D and C are intended for information processing where most peripherals are stored, cyber security should be further enhanced by the need to avoid data leaks and cyber-attack.

Lastly, Zone B and A are the most physically critical areas, as there is manipulation of radioactive material in them, the monitoring system must be active and stable over any invasion attempt. The availability of sensors for each zone is presented in the Figure 6.

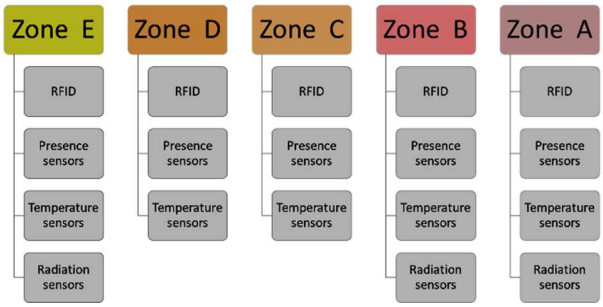

Figure 6: Availability of sensors for each zone.

The experiment carried out had 5 nodes (WeMos D1 R2 Wifi ESP8266 Card) assigned to Zone A, so they used the temperature, radiation and presence sensors. The purpose of the test was to aggregate all Nodes by collecting environmental information and relaying it in information format and alerting to possible events, as well as physical access by confirming the reading of the RFID module (Figure 7). The proposal to place each sensor to a different node is directly linked to security, because if a Node is lost the zone will be maintained with other sensors, however if there is a problem with the central node the whole zone is affected.

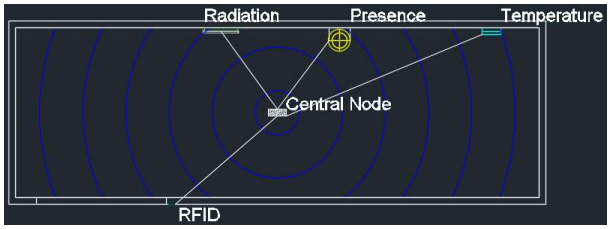

Figure 7: Availability of sensors for each zone.

Star topology was used for node aggregation, which was made easier thanks to the Blynk platform by saving large lines of code and reducing the amount of processing done by the Node. The information and data collected goes to the Blynk server and then displayed on the smartphone, it was possible to use alerts, being necessary to place each parameter in the nodes through algorithms. For the central node a wireless router was used. Data on temperature status and radiation level is easily expressed in the Blynk dashboard which is modular and adaptable to different monitoring profiles (Figure 8). It was observed that the sensor nodes were able to communicate with the central node providing the data in real time, the only caveat found was for the radiation sensor, because it was not possible to perform measurement tests because we did not have access to materials that emit ionizing radiation.

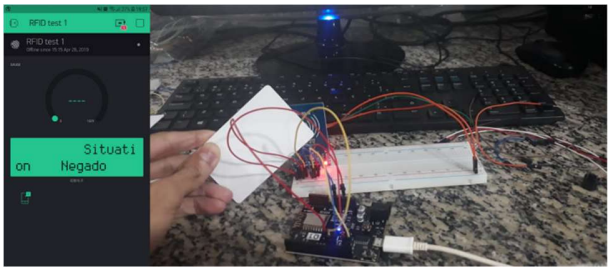

Figure 8: Blynk dashboard and RFID card test respectively, a card without access privilege was used in the test.

5. CONCLUSIONS

The distribution and choice of sensors proved to be effective in detecting intruders by physical pathways due to the use of presence sensors and RFID access tags, for detecting increased saturation of radioactive particles in the laboratory air, only the humidity sensor data could be evaluated, because until the end of this work, access to the ionizing radiation emitting materials was not obtained to test the functionality of the sensor, and for the safety of the network itself, the layered access fulfilled its function of limiting accessing critical zones to as few users as possible, only the essential ones, which would be ideal for highly critical environments, while external zones remained more accessible environments.

For future work we plan to perform tests for the other zones together, test attack simulations, gain access to radioactive materials to test the sensor and develop our own interface so that the WSN becomes independent of an external application such as Blynk.

6. REFERENCES

[1] Chun, Z.; Lejun, G. **An Improved Force-Based Deployment Algorithm for Wireless Sensor Network.** 17 th IEEE International Conference on Communication Technology. Chengdu, China. 2017.

[2] Osanaiye, O.; Alfa, A.; Hancke, G. **A Statistical Approach to Detect Jamming Attacks in Wireless Sensor Networks.** MDPI: Sensors, vol. 18. 2018.

[3] KAHN, Imran et al. **Wireless Sensor Network Virtualization: A Survey.** IEEE Communications Surveys & Tutorials, vol. 18, Issue: 1. 2016.

[4] AHMED, Ali et al. **Modern IoT Architectures Review: A Security Perspective.** 8th Annual International Conference on ICT, 2017.

[5] López, M.; Muñoz, I. **SAT-IoT: An Architectural Model for a High-Performance Fog/Edge/Cloud IoT Platform.** IEEE 5th World Forum on Internet of Things. 2019.

[6] Li, Z; Shahidehpour, M. **Defense-in-depht Framework for Microgrid Secure Operations against Cyberattacks.** IEEE Power & Energy Society General Meeting, 2017.

[7] HE, Daojing et al. **Accountable and Privacy-Enhanced Access Control in Wireless Sensor Networks.** IEEE Transactions on Wireless Communications, 2015.