ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 12, December 2014

# Intelligent fire sensing using wireless sensor network

**Pradeep Kumar[1], M.S.Anuradha[2]**

M.Tech [Scholar], Department of ECE, AUCE, Andhra University, Visakhapatnam, AP, India [1]

HOD, Department of ECE, AUCE for Women, Andhra University, Visakhapatnam, AP, India [2]

**Abstract***:* Forest and rural fires are one of the main causes of environmental degradation in Mediterranean countries. Existing fire detection systems only focus on detection, but not on the verification of the fire. However, almost all of them are just simulations, and very few implementations can be found. Besides, the systems in the literature lack scalability. In this paper we show all the steps followed to perform the design, research and development of a wireless multisensor network which mixes sensors with IP cameras in a wireless network in order to detect and verify fire in rural and forest areas of Spain. We have studied how many cameras, sensors and access points are needed to cover a rural or forest area, and the scalability of the system. We have developed a multisensor and when it detects a fire, it sends a sensor alarm through the wireless network to a central server. The central server selects the closest wireless cameras to the multisensor, based on a software application, which are rotated to the sensor that raised the alarm, and sends them a message in order to receive real-time images from the zone. The camera lets the fire fighters corroborate the existence of a fire and avoid false alarms. In this paper, we show the test performance given by a test bench formed by four wireless IP cameras in several situations and the energy consumed when they are transmitting. Moreover, we study the energy consumed by each device when the system is set up. The wireless sensor network could be connected to Internet through a gateway and the images of the cameras could be seen from any part of the world.

**Keywords**: multisensory, wireless sensor network.

## I. INTRODUCTION

Heat and smoke detectors are the most commonly used fire detection devices [1-4]. Heat detectors are designed to detect a fixed amount of heat present at the detector or a rapid increase of heat in the area of the detector. Smoke detectors can detect the presence of smoke in an area (when it reached the ceiling where the detector is normally located.) There are two common types of smoke detectors, ionization and photoelectric. Care should be taken in selecting the type of detector to be used. Ion detectors will detect a flaming fire faster, but a photo electric detector will detect a smoldering fire quicker in most situations. Manual fire alarm boxes are usually placed (as a minimum) at all exits on each floor in a building. If an automatic sprinkler system is present in a building, water flow devices are used to indicate that system's operation.

More detailed information on all of these devices is covered in later sections of the project. In order for the automatic detection devices, such as heat and smoke detectors, to provide the intended protection, care must be taken in selecting the level of coverage to be used. The fact is that a detector of any type cannot detect a fire (in a reasonable amount of time) unless it is intimate with the fire. So in order to effectively detect the presence of a fire, total coverage using smoke and heat detectors should be provided.

In some cases where property protection or mission protection is the goal, the owner may choose to install a complete automatic sprinkler system. This system would then be monitored by the fire alarm system to ensure its operational integrity.

This papers deals with some of the major issues of wireless network system of fire alarm system like basic architecture, protocols, platforms, .etc. Wireless network system is an infrastructure comprised of sensing [5,6] (measuring), computing, and communication elements that gives an administrator the ability to instrument, observe, and react to events and phenomena in a specified environment.

The administrator typically is a civil, governmental, commercial, or industrial entity. The environment can be the physical world, a biological system, or an information technology (IT) framework. Network(ed) sensor systems are seen by observers 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 [7,8].

Typical applications include, but are not limited to, data collection, monitoring, surveillance, and medical telemetry. In addition to sensing, one is often also interested in control and activation.

## II. WIRELESS SENSOR NETWORKS

From a generic perspective the sensor networks deal with space and time: location, coverage, and data synchronization. Data are the intrinsic ‘‘currency’’ of a sensor network. Typically, there will be a large amount of time-stamped time-dependent data. Therefore, sensor networks often support in-network computation.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 12, December 2014

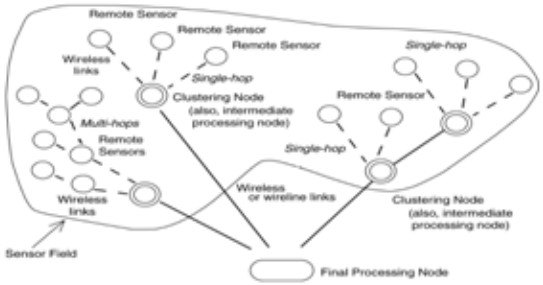


Fig.1: Wireless Sensor Network

A Wireless sensor network is composed of a large number of sensor nodes that are densely deployed. To list just a few venues, sensor nodes may be deployed in an open space for fire sensing; on a battlefield in front of, or beyond, enemy lines; in the interior of industrial machinery; at the bottom of a body of water; in a biologically and/or chemically contaminated field; in a commercial building; in a home; or in or on a human body. A sensor node typically has embedded processing capabilities and onboard storage; the node can have one or more sensors operating in the acoustic, seismic, radio (radar), infrared, optical, magnetic, and chemical or biological domains. The node has communication interfaces, typically wireless links, to neighboring domains as shown in the figure 1. Wireless Sensor nodes are scattered in a special domain called a sensor field. Each of the distributed sensor nodes typically has the capability to collect data, analyze them, and route them to a (designated) sink point. Figure 1 depicts a typical WSN arrangement. Although in many environments all WNs are assumed to have similar functionality, there are cases where one finds a heterogeneous environment in regard to the sensor functionality.

The important issues pertaining to WSNs are

a. Sensor type,
b. Sensor placement,
c. Sensor power consumption,
d. Operating environment,
e. Computational/sensing capabilities and signal processing,
f. Connectivity, and telemetry or control of remote devices.

It is critical to note in this context that node location and fine-grained time (stamping) are essential for proper operation of a sensor network; this is almost the opposite of the prevalent Internet architecture, where server location is immaterial to a large degree and where latency is often not a key consideration or explicit design objective. In sensor networks, fine-grained time synchronization and localization are needed to detect events of interest in the environment under observation. Location needs to be tracked both in local three-dimensional space (e.g., On what floor and in which quadrant is the smoke detected? What is the temperature of the atmosphere at height h) and over a broader topography, to assess detection levels across a related set (array) of sensors (e.g., What is the wind direction for wind containing contaminated particles at milepost i, i + 1, i + 2, etc., along a busy highway?). Localization is used for functionality such as beam forming for localization of target and events, geographical forwarding, and geographical addressing. Embedded sensor networks are predicated on three supporting components: embedding, networking, and sensing. Embedding implies the incorporation of numerous distributed devices to monitor the physical world and interact with it; the devices are nodes of small form factors that are equipped with a control and communication subsystem. Spatially and temporally-dense arrangements are common. Networking implies the concept of physical and logical connectivity. Sensor networks require sensing systems that are long-lived and environmentally resilient. Unattended, untethered, self-powered low-duty-cycle systems are typical.

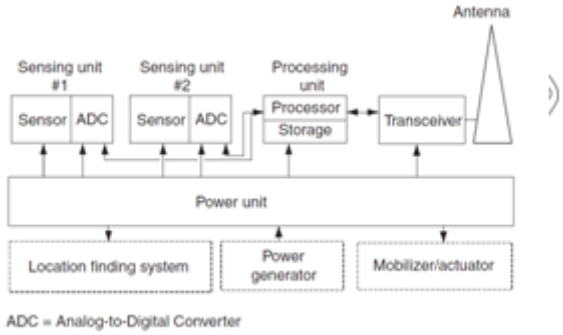


Fig.2: Sensing Node Structure

## III. SOFTWARE IMPLEMENTATION

To support the node operation, it is important to have open-source operating systems designed specifically for WSNs. Such operating systems typically utilize a component-based architecture that enables rapid implementation and innovation while minimizing code size as required by the memory constraints endemic in sensor networks.

TinyOS is one such example of a de facto standard, but not the only one. TinyOS's component library includes network protocols, distributed services, sensor drivers, and data acquisition tools; these can be used as-is or be further refined for a specific application. TinyOS's event-driven execution model enables fine-grained power management, yet allows the scheduling flexibility made necessary by the unpredictable nature of wireless communication and physical world interfaces. TinyOS has already been ported to over a dozen platforms and numerous sensor boards. A wide community uses TinyOS in simulation to develop and test various algorithms and protocols, and numerous groups are actively contributing code to establish standard interoperable network services.

**Standards for Transport Protocols**

The goal of WSN engineers is to develop a cost-effective standards-based wireless networking solution that supports low-to -medium data rates, has low power consumption, and guarantees security and reliability. The position of

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 12, December 2014

sensor nodes does not have be predetermined, allowing random deployment in inaccessible terrains or dynamic situations; however, this also means that sensor network protocols and algorithms must possess self-organizing capabilities.

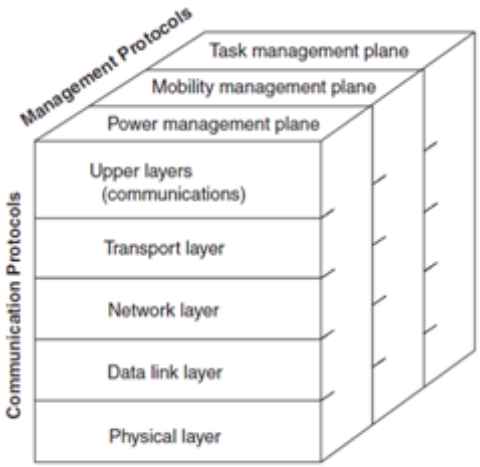


Fig.3: Protocol stack for WSN

## IV. SIMULATION RESULTS

At first, we have tested proposed intrusion detection system without any deployed intruders. The aim of this simulation was to measure the natural error ratio of watchdogs in different enviroments.

Packet Error Rate was fluctuating up to about 24 m and rapidly raised at the distance over 24 m. The maximum distance where all packets were lost was about 30 m.

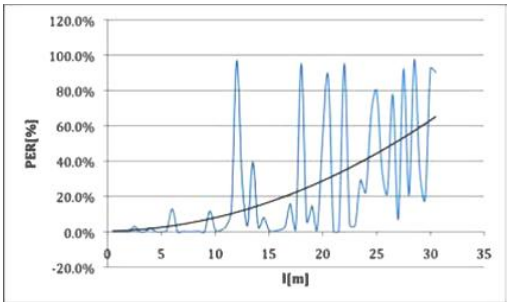


Fig.4: SimpliciTI Packet Error Rate Increase due to Distance Increase between Transmitter and Receiver

Packet Error Rate was fluctuating up to about 24 m and rapidly raised at the distance over 24 m. The maximum distance where all packets were lost was about 30 m.
The error ratios for selective forwarding attacks were defined as

$$\frac{bad\_counter}{good\_counter + bad\_counter} * 255$$

where bad_counter is a number of packets that weren't forwarded and good_counter is a number of packet that were forwarded. The error ratio will help us to estimate an ALERT_THRESHOLD for selective forwarding engines, that will lead to the acceptable number of false positives while maintaining the ability of WAS to detect selective forwarding attack (see Section 2.5) with a low ratio of dropped packets.

On following charts, the values on X-axis express the error ratios that are equal to or greater than the given value. For example the value of 100 includes all alarms with error ratio from 100 to 255.

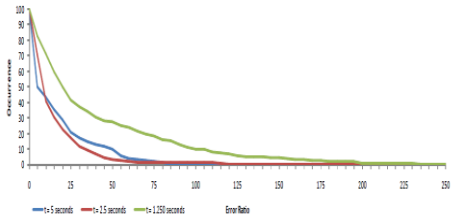

Fig.5: Sensing rate vs Occurrence

**Various sensing rate**

At first, we measured an error ratio in relation to a number of messages that were generated and transmitted through the network. Each detector was set to randomly choose 10 neighbors, whose average was under -86dB.We deployed 100 nodes in a topology. The testing is carried on three cases with different sensing period

1) t = 5 seconds, 2) t = 2.5 seconds, 3) t = 1.250seconds.

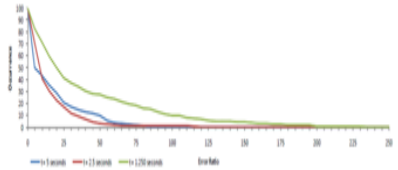

Fig.6: Dependence of Error Rate on Sensing Period

The results of this test are shown in Figure 6. We can see that increasing traffic in network makes
the detector monitoring technique less reliable. For sensing periods 5s and 2:5s there are almost no occurrences of errors with greater value than 90 (0% for t = 5s, 1.03% for t = 2.5s) so if we set the ALERT_THRESHOLD to 90 it would no false positives for t = 5s and four false positives for
t = 2.5s. In contrast, for t = 1.250s it would cause over 10% false positives.

We have also measured a number of packets that were lost because the receiver was in mid-reception of another packet. We can consider this value as a number of ambiguous collisions that occurred on the network. We can see that linear increase in the number of transmitted messages in network caused exponential increase of ambiguous collisions

**Various monitoring thresholds**

At the second test, we tested the dependency of error ratio on the value of MONITORING_THRESHOLD (A detector never monitors neighbors with lesser average RSSI than is MONITORING_THRESHOLD). For this simulation we have used the custom network topology

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 12, December 2014

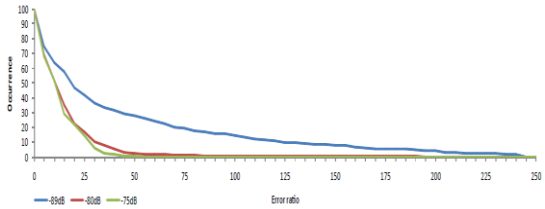


Figure 7: Dependence of error ratio on monitoring thresholds

Each node in the network worked with sensing rate t = 2.5s and we tried to set various monitoring thresholds : -90dB, -80dB and -75dB. WAS agents were activated in the same way as in the previous test (each node performed a single selective forwarding test), but each WAS monitored all its neighbors that was below the monitoring threshold.

The results of this test are shown on figure 7. It is obvious that when we limit monitoring only to nodes with stronger signal, an average error ratio is lower. On the other hand this reduces WAS performance, because each WAS agent can monitor only a limited subset of neighbors.

Table 1: Evaluation results Dempster-Shafer theory

| Window Size | Number of Experiments | Fires Detected | False Positives | False Negatives |
|---|---|---|---|---|
| 5 | 6 | 5 | 4 | 1 |
| 10 | 6 | 5 | 5 | 1 |
| 15 | 6 | 5 | 5 | 1 |
| 20 | 6 | 5 | 6 | 1 |
| 25 | 6 | 5 | 6 | 1 |
| 30 | 6 | 5 | 6 | 1 |
| 35 | 6 | 6 | 6 | 0 |

## V. CONCLUSIONS

We have shown the design, development and the performance test of a Wireless Sensor Network for rural and forest environments fire detection and verification. We have shown the deployment of a multisensor based on a Linksys WRT54GL router that is able to sense fire by infrared radiation and smoke. It is able to send an alarm if the combination of both physical sensors gives as a result that there is a fire. We have studied how many cameras, multisensors and access points are needed to cover a rural or forest area and the scalability of the system. The technology used has been IEEE 802.11g standard. It is flexible and it could be adapted to any type of environment. We have designed it trying to minimize the material cost of its implementation but without diminishing the quality of the video and taking into account the 802.11g WLAN performance. Our design is scalable because we can add access points easily and increment the number of wireless IP cameras attached to these access points. Moreover, it is easy to add emergent Technologies. When a fire is detected by a wireless IP multisensor, the sensor alarm is sent through the wireless network to a central server. The central server runs a software application that selects the closest wireless IP cameras to the sensor and sends them a message in order to receive real-time images from the affected zone. It lets the fire fighter corroborate the fire by means of a real time visualization of the place where the fire has taken place. The bandwidth consumption measurements given by our test bench show that the system supports up to 34 wireless IP cameras in each Access Point. We have demonstrated that the control messages developed imply little bandwidth consumption. So, our design is scalable because we can add access points easily and increment the number of cameras and sensors.

## REFERENCES

1. Vidal, A.; Devaux-Ros, C. Evaluating forest fire hazard with a landsat TM derived water stress index. *Agr. Forest Meteorol*. **1995**, *77*, 207-224.
2. *Decreto 3769/1972, de 23 de diciembre, por el que se aprueba el Reglamento de la Ley 81/1968 (BOE nº294, 7-12-1968), de 5 de diciembre, sobre Incendios Forestales, (BOE 13-2-1973)*. Available at http://www.boe.es/boe/dias/1973/02/13/pdfs/A02711-02724.pdf (accessed October 29, 2009)
3. Yick J.; Mukherjee, B.; Ghosal, D. Wireless sensor network survey. *Comput. Netw*. **2008**, *52*, 2292-2330.
4. Lloret, J.; Garcia, M.; Tomás, J.; Boronat, F. GBP-WAHSN: a group-based protocol for large wireless ad hoc and sensor networks. *J. Comput. Sci. Technol*. **2008**, *23*, 461-480.
5. Garcia, M.; Bri, D.; Boronat, F.; Lloret, J. A new neighbor selection strategy for group-based wireless sensor networks, In *The Fourth International Conference on Networking and Services (ICNS 2008)*, Gosier, Guadalupe, March 16-21, 2008.
6. *MODIS Web Page*. http://modis.gsfc.nasa.gov (accessed October 29, 2009).
7. Li, Z.; Nadon, S.; Cihlar, J. Satellite-based detection of Canadian boreal forest fires: development and application of the algorithm. *Int. J. Remote Sens.* **2000**, *21*, 3057–3069.
8. Doolin, D.M.; Sitar, N. Wireless sensors for wildfire monitoring. In *Smart Structures and Materials 2005: Sensors and Smart Structures Technologies for Civil, Mechanical, and Aerospace Systems*, San Diego, CA, USA, May 7, 2005.