ISSN 2348 – 7968

Wireless Intrusion Detection Using FPGA

T. Suresh kumar[#1], R. Sudhakar[#2]

[#1]Asst. Professor/IT, [#2]Asst. Professor/CSE, Nandha College of Technology, India

Abstract: **Wireless sensor networks are expected to become a major tool for various security and/or surveillance applications. The paper reports development of a wireless sensor network with a two-level structure of intrusion detection and classification. At the first level, relatively simple nodes with basic sensing devices, a microcontroller of low computational power and wireless transmission capabilities are used. The first level nodes are used as preliminary detectors of intrusions. The second-level sensor node is built around a high performance FPGA controlling an array of cameras. The FPGA based second-level nodes can be dynamically reconfigured to perform various types of visual data processing and analysis to confirm the presence of any intruders in the scene and to provide more details about the intruder, if any. The presented results are an example of a distributed network combining reasonable energy requirements with a relatively high level of intelligence. In particular, the network can assist a human operator so that he/she is engaged only to confirm the system's decision weather a detected intruder is a potential danger.**

Keywords: **Wireless Sensor Network, Intrusion and Detection, Field Programmable Gate Array**

I. INTRODUCTION

Wireless sensor networks are being used for various condition-based monitoring tasks such as habitat monitoring, environmental monitoring, machineries and aerospace monitoring and for security and surveillance. Such applications need tens to several hundreds of nodes. Each node can be equipped with various sensors (e. g. proximity, temperature, acoustic, vibration) to monitor conditions of the environment and possibly to fulfill other requirements of the task. Additionally, image sensors are usually present in security and surveillance applications where more detailed analysis of the environment is expected.

We have implemented the concept of a heterogeneous sensor network in an experimental platform eventually intended for various military and civilian applications where a visual surveillance of large areas is required. Visual surveillance in considered the most effective method of monitoring complex environments, but systems that could perform such a task fully autonomously and reliably are still very difficult to build. Visual assessment of a situation by a human is still considered the ultimate factor in taking important decisions. In complex scenarios, however, the amount of data transmitted across the network would make the human inspection and/or assessment of the situation very difficult. Thus, we have proposed a realistic approach, where a human operator can be supported by vision capabilities of the network that can automatically handle typical situations. The human intervention is needed only in special situation (or situations involving decisions which are reserved for humans).

The local computational intelligence of the selected nodes has been achieved by incorporating FPGA (field programmable gate array) devices into selected nodes. These FPGA based nodes can process the data received from other nodes and process the images in order to analyze the situation. The results are wirelessly transmitted to the higher level in the decision chain only if there is any intrusion or another unusual event so that the human operator can confirm (or reject) the system's decision that a potential danger has been detected.

II. DESIGN METHODOLOGY

In typical wireless sensor applications, the network nodes have to process all the data from a variety of sensors and at the same time have to efficiently manage the power to achieve a reasonably long operational lifetime. In the developed platform [1], two different types of nodes are used. The first level nodes are relatively simple with basic sensing devices (e. g. proximity, vibration, acoustic, magnetic sensors) and wireless transmission capabilities. They continuously monitor conditions in the protected zone and act as preliminary detectors of possible intrusions. The second level sensor nodes are built around a higher performance FPGA controlling an array of cameras. They perform more advanced data processing to confirm or reject the intrusion (before alerting a human operator). Each camera is activated after the corresponding first-level
nodes acquire data that may indicate a presence of an intruder, and transmit the warning message in wireless rk to the FPGA based second level nodes.

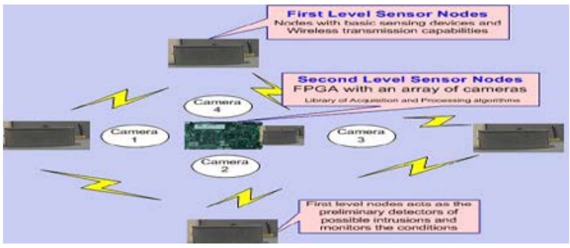

First Level Sensor Nodes
Nodes with basic sensing devices and Wireless transmission capabilities
Second Level Sensor Nodes
FPGA with an array of cameras
Library of Acquisition and Processing algorithms
Camera 4
Camera 1
Camera 3
Camera 2
First level nodes acts as the preliminary detectors of possible intrusions and monitors the conditions

Fig. 1. Basic structure of the developed sensor network.

A. First Level Nodes:

The first-level nodes (Fig. 2) incorporate a wireless communication chip, a low-cost microcontroller (performing sensor data acquisition, generating wirelessly-transmitted messages and interfacing the wireless chip) and basic non-vision sensors. Battery power supply is provided. The first level nodes [2] generally use very simple detection technique. Whenever a possible intrusion is sensed, the node wirelessly transmits a message containing the node identifier and (if several definitions of possible intrusions are simultaneously used) the type of sensed intrusion. To provide a higher level of reliability, the message may be repeated several times The first level nodes consume low power as they only transmit short messages (only if the sensors detect anything unusual) and perform very little computations

Fig. 2. The first-level node of the network.

B. Second Level Nodes

The second-level nodes area built around an FPGA module that can control up to four cameras. Additionally, the nodes are equipped with the same wireless communication components as the first-level nodes. Typically, one second-level node is associated with several first-level nodes, but the network structure is not permanent. We envisage that eventually ad hoc self-organization mechanisms will be used during the network deployment In the second-level nodes, the power consumption by both FPGA and cameras is relatively high. Therefore, only the kernel of a second-level node would be permanently active, while the other parts (e. g. the cameras) are activated only when a warning message from the first level is received. Two options are possible: (1) a second level node can be activated by any first-level node within the wireless range or a second-level level node can be activated by selected first-level nodes (i.e. the warning messages containing identifiers of other nodes are ignored). Upon activation, a second-level node camera captures a short sequence of images (typically two or three) that are subsequently processed using dedicated algorithms implemented in the node's FPGA[3] In general, the purpose of image processing is to extract the possible intruders from a captured image and to classify/identify them.

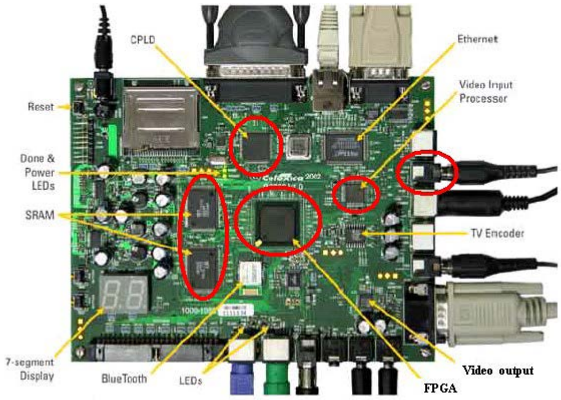


Fig.3. Components of the FPGA development board used in the second-level node.

After the task is completed, selected fragments of camera-captured images and/or other results produced by the algorithms may be wirelessly transmitted to the higher level in the decision chain (possibly including a human operator). Additionally, the second-level nodes can be periodically activated in order to update the background image.

III. INTRUSION DETECTION AND CLASSIFICATION

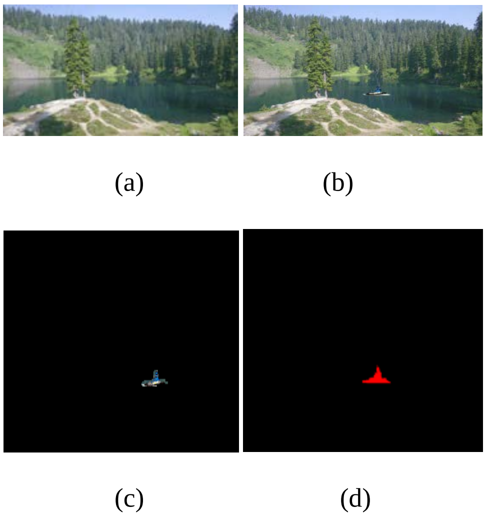
This section deals with the exemplary methodologies for FPGA-implemented [4] image processing, intrusion detection and classification. Visual analysis of the scene helps to make firm decisions and also gives more information about the event to the human operator immediately. Different systems used for surveillance, tracking and monitoring applications. But in this system, we use cameras with FPGAs to process the images acquired, analyze it in various ways and finally send back the results to a human operator(or some other system) for further actions, only if the system believes if there is an intrusion in that place. So that, the cameras need not work continuously, which otherwise might result in a higher power consumption. At the same time, the system will not miss any intruder in the environment. Various image processing algorithms have been implemented to perform different tasks. These algorithms share a library of image pre-processing operations which has been implemented in FPGA.

A. Background Update

Generally, there are three conventional approaches for the extraction of moving targets from a video stream. They are temporal differencing (two or three frame), background subtraction and optical flow. In this, temporal differencing is very adaptive to dynamic environments but does not perform well in extracting all relevant feature pixels. Back ground subtraction [5] is very sensitive to dynamic environment but provides complete feature data. And optical flow computation methods are said to be very complex and inapplicable to real-time applications unless there is a specialized hardware. In our method, we use background subtraction with additional image processing algorithms to compensate for the fluctuations of visibility conditions, minor motions of the environment components, vibrations of the sensor platform, etc. When we extract the targets by comparing the background images, it is necessary to update the background images often to get more perfect results. The FPGA-based second level nodes [6], updates the background images of the environment when they are idle and if they do not detect any new objects in its field of view. In the presence of new objects, it can send the information about the object to the human operator, and if it is not considered dangerous, it will be included in the next update. This might also vary according to the application, as each application requires different types of background updates.

B. Static Intrusion Detection:

In typical wireless sensor network applications, a huge amount of nodes will be deployed, and the amount of data for a human inspection and/or assessment can be very large. For example, when few hundreds of nodes are deployed in a forest, it is often difficult for a human operator to identify the intruders at all times as almost all images look very similar. In this method, when a warning message is received from the first level nodes indicating the presence of any intruder, the image of the intruder(s) and/or the silhouette of intruder are extracted by comparing the current images to the background image as shown in Fig. 4. and Fig. 5. respectively. The Fig.4 (a) shows a background image of the scene without any intruders; (b) shows the image of the same scene when a intruder enters, (c) and (d) shows the image of the intruder and the silhouette of the intruder respectively. We utilize the methods of mathematical morphology [7] and threshold values so that minor disturbances of the background are ignored.



(a) (b)

(c) (d)

Fig. 4. (a) Background of a scene. (b) New intruder entering the scene. (c) Image of the intruder. (d) Silhouette of the intruder.

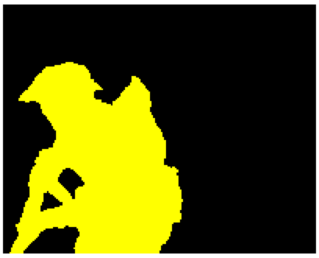


Fig. 5. Extraction of intruder's silhouette from the background.

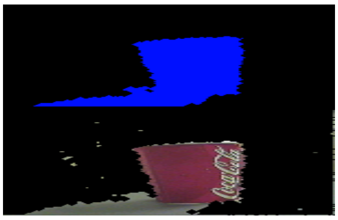


Fig. 6. Analysis of Intruder by its shape.

C. Dynamic Intrusion Detection

To analyze the dynamic ness of the intruder, the variations of the intruder's shape[8] are extracted from a sequence of images. This actually indicates how the intruder moves and the results can be subsequently used to classify the intruder by the type of its mobility.

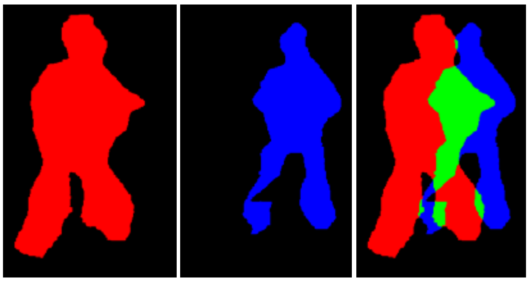


Fig.7. Silhouette variations in a sequence of images.

From the Fig. 7., we can determine that the intruder is apparently approaching the camera and turning to the left. The speed of the motion can be estimated from the relative size of both the silhouettes and their intersection.

D Advanced Analysis of Intruder Images:

In some of the applications, we might have an idea about the possible intruders, and in that case the system can identify whether the detected intruder is one of the intruders in the data base. This can be achieved by detecting various interest points in the intruder's image as shown in Fig.8(a). After detecting various interesting points of intruder, this information can be transmitted to the higher level nodes in the decision chain[9]. These interesting points can be received by the destination system with a database of images of known intruders. This method actually reduces the amount of data transmitted in the wireless network, thereby reducing the power consumption. These transmitted interesting points can be matched with the data base of known intruders to decide about the intruder as shown in Fig. 8.(b). This method makes the system fully autonomous but with the limitation that it cannot be applied to the applications that does not have any idea about the possible intruders. This method can also be applied if the second level nodes are attached to a mobile platform.

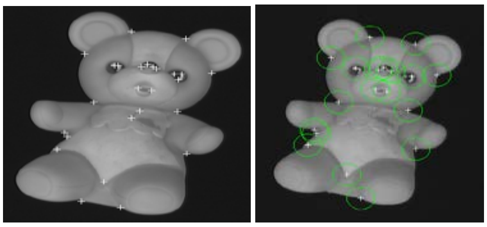


Fig. 8. (a) Detection of interest points. (b) Matching Interest points.

IV. COMMUNICATION ISSUES

In wireless networks, the efficiency and (sometimes) security of communication is an important issue. Although within our platform no special attempts have been made to develop new communication mechanisms, the existing standards have been thoroughly tested. Additionally, we have implemented (as a feasibility study) communication between FPGA devices directly connected to a wireless transceiver . It is believed that such a direct implementation of communication mechanisms within FPGA can lead to more compact and efficient nodes for the future sensor networks. The most bandwidth-consuming communication task is image transfer. Thus, the amount of transmitted visual data is reduced as described in Section 3. Additionally, we envisage various compression algorithms to be locally executed before transmission. Several papers have analyzed compression standards to be used in the wireless sensor network applications for efficient power management.

These algorithms can be designed to adopt certain parameters like compression ratio, image resolution based on the real-time situation. The image fragments and other results are encrypted using advanced encryption standard (AES128) before the transmission to provide more security which is an important requirement for many applications.

V. CONCLUSION

In this paper, we presented a two-level structure of nodes that can be used for intrusion detection and classification. Various visual assessment and processing algorithms implemented in FPGA have been discussed. The FPGA based second level nodes can be dynamically configured for different applications and tasks, even after the deployment of the nodes using online reconfiguration capabilities. The paper also describes about the transmission of analyzed results after encryption by

AES128 to add security to the wireless transmission. The results are transmitted back to the destination node for further decisions.

REFERENCES

[1] K. Obraczka, R. Manduchi, and J. J. Garcia-Luna-Aceves, *Managing the Information Flow in Visual Sensor Network.*

[2] D. Estrin, *Sensor network research: Emerging challenges for architecture, systems, and languages*.

[3] R. Collins, A. Lipton, and T. Kanade, *A System for Video Surveillance and Monitoring*.

[4] R. Collins, A. Lipton, H. Fujiyoshi, and T. Kanade, *Algorithms for cooperative multisensor surveillance*.

[5] J. Lach, D. Evans, J. McCune, J. Brandon, Power Efficient Adaptable Wireless Sensor Network, Military and Aerospace Programmable Logic Devices.

[6] B. Meffert, R. Blaschek, U. Knauer, R. Reulke, A. Schischmanow, F. Winkler *Monitoring traffic by optical sensors*.

[7] A.E. Gamal, *Collaborative visual sensor networks*,2004.http://mediax.stanford.edu/projects/cvsn.html

[8] M. S. Islam, A. Sluzek and L. Zhu, *Towards invariant interest point detection of an object.*

[9] M. S. Islam and L. Zhu, *Matching interest points of an object.*