Annales UMCS Informatica AI 4 (2006) 6-19

Annales UMCS
Informatica
Lublin-Polonia
Sectio AI

http://www.annales.umcs.lublin.pl/

Towards wireless sensor networks with enhanced vision capabilities

Andrzej Śluzek[1,2*], Palaniappan Annamalai[1], Md. Saiful Islam[1],
Paweł Czapski[1]

[1]Nanyang Technological University, Singapore
[2]Computer Science Institute, SWPS, Chodakowska 19/31, 03-815 Warszawa, Poland

Abstract

Wireless sensor networks are expected to become an important tool for various security, surveillance and/or monitoring applications. The paper discusses selected practical aspects of development of such networks. First, design and implementation of an exemplary wireless sensor network for intrusion detection and classification are briefly presented. The network consists of two levels of nodes. At the first level, relatively simple microcontroller-based nodes with basic sensing devices and wireless transmission capabilities are used. These nodes are used as preliminary detectors of prospective intrusions. The second-level sensor node is built around a high performance FPGA controlling an array of cameras. The second-level nodes can be dynamically reconfigured to perform various types of visual data processing and analysis algorithms used to confirm the presence of intruders in the scene and to classify approximately the intrusion, if any. The paper briefly presents algorithms and overviews hardware of the network. In the last part of the paper, prospective directions for wireless sensor networks are analyzed and certain recommendations are included.

1. Introduction

Adequate sensing capabilities are the key issue in a system working autonomously or semi-autonomously in unstructured, unfamiliar environments. Wireless sensor networks are one of the emerging technologies for providing such systems with the information about current conditions in a large fragment of the environment. In such networks, a huge amount of sensed data should be acquired and processed in real time. Thus, adequate hardware resources capable of real-time data processing and intelligent data selection mechanisms are needed in order to prevent informational and communicational saturation of the network [1].

Wireless sensor networks are being used for various condition-based monitoring tasks such as habitat monitoring, environmental monitoring [2],

[*] Corresponding author: *e-mail address*: assluzek@ntu.edu.sg

machineries and aerospace monitoring and for security and surveillance [3,4]. 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.

The most important challenge in such systems is to manage the huge information flow in the network nodes. The systems with various non-visual and visual sensors acquire and should process large amounts of data in real-time. Transmitting raw data from every node to other nodes and/or to the higher level occupies the bandwidth for a long period of time. This, in turn, reduces the reporting efficiency of the system by delaying or losing messages about an important event happening in the environment. Moreover, most of the raw data transmitted from the sensor nodes is unimportant, so that the energy (which is a precious commodity in autonomous systems) is wasted for communication and flooding the destination node with useless data.

The most straightforward solution is to provide the sensor nodes with a certain level of autonomous intelligence so that the captured data can be locally processed and analyzed, while only observation of significant importance or unknown situations would be reported to the higher level.

Initially, wireless sensor networks were defined (mostly because of the envisaged military applications) as large-scale, wireless, ad-hoc, multi-hop, unpartitioned networks of homogenous, tiny, and immobile sensor nodes. It has been shown in many non-military applications, however, that the above assumptions are inaccurate [5]. Wireless sensor networks can be heterogeneous, possibly mobile, and with different network topologies. Generally, their nodes have communicational, computational and sensing capabilities, though in diversified proportions [6].

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 situations (or those involving decisions 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 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.

This paper presents design methodology (for both hardware architecture and the embedded algorithms) for the current system and summarizes proposals for the future wireless sensor networks with enhanced vision capabilities. In Section 2, we overview the design of the network nodes. Section 3 presents image processing algorithms implemented in the FPGA nodes for intrusion detection and classification. Additional implementation issues are discussed in Section 4. The final Section 5 summarizes the results and highlights selected problems important for the future development of wireless sensor networks with enhanced vision capabilities. Unfortunately, some implementation details are not disclosed in this paper as the developed system is a feasibility study for a commercial product.

2. Architecture of the network

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 manage efficiently manage the power to achieve a reasonably long operational lifetime. Various architectures for different applications have been proposed by researchers in the recent years (e. g. [7-10]) but only a few papers discuss the power management in the wireless sensor networks in the context of the overall system design.

In the developed platform, 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. These sensor nodes are built around a simple micro-controller so that they consume very low power but their computational power is also very low. 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 presence of an intruder, and transmit the warning message in the wireless network to the FPGA based second level nodes. The overview of the network structure is shown in Fig. 1.

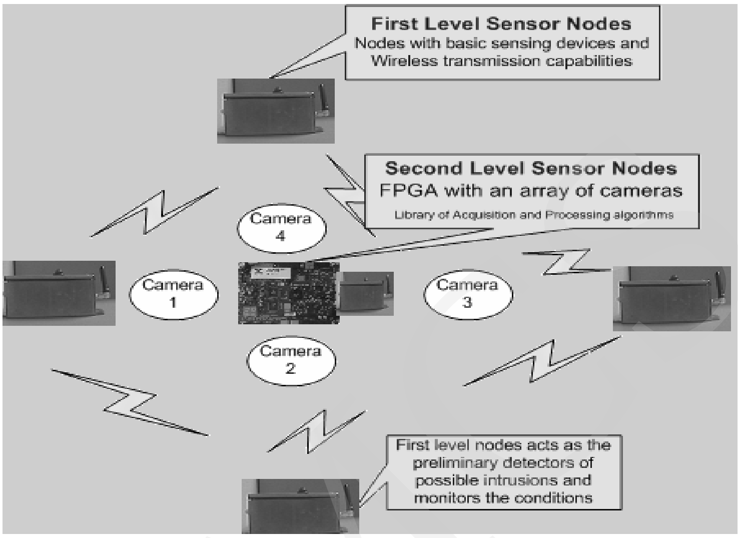
First Level Sensor Nodes
Nodes with basic sensing devices and Wireless transmission capabilities
Second Level Sensor Nodes
FPGA with an array of cameras
Library of Acquisition and Processing algorithms
Camera 4
Camera 1
Camera 3
Camera 2
First level nodes acts as the preliminary detectors of possible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

Fig. 1. Basic structure of the developed sensor network

2.1. 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. Currently, only infrared proximity sensors and vibration sensors are used, but additional options are planned (and the corresponding sensors are already available in the nodes).

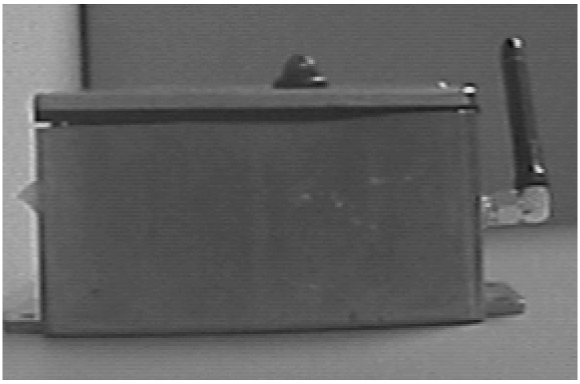

Fig. 2. The first-level node of the network

The first level nodes generally use very simple detection technique. For example, analog signals are just thresholded and only limited signal processing capabilities are available. They are assumed to be continuously active. For the first level nodes, a possible intrusion is defined as a particular coincidence of sensor readings. Different definitions of various intrusion types can be used, either for different applications or within the same application. 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. A standard communication protocol for low-power wireless networks is used. The intended message recipients are the second level nodes (those close enough to receive the message) which would perform more detailed analysis of the event.

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. Low energy consumption is a crucial issue since a very long operational lifetime is expected [6]. No online reprogrammability/ reconfigurability is envisaged and these first level nodes are assumed cheap expendables.

2.2. Second Level Nodes

The second-level nodes area is 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 (e.g. [11]).

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 option are possible: (1) a second-level node can be activated by any first-level node within the wireless range or (2) 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. In general, the purpose of image processing is to extract the possible intruders from a captured image and to classify/identify them. 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 (see Section 3).

In general, the peak energy consumption in a second-level node may be high, but the average power requirements could be low enough to provide long operational lifetime. In the prototype platform, power is supplied by a DC adaptor.

The prototype second-level nodes are built around a commercially available FPGA development board (see Fig. 3) with a powerful Virtex II chip (8,000,000 equivalent gates). However, only selected resources available in the board are used in the prototype (FPGA chip with external memory, CPLD module, CCD cameras and camera interfaces as shown in Fig. 3). Moreover, the overall usage of the FPGA capacity does not exceed 15% so that many other tasks can be simultaneously implemented within the same FPGA. Typically, these additional tasks are various visualization routines allowing testing and performance assessment of the node. In the final version, a much less powerful FPGA is envisaged. These nodes can be motionless or attached to a mobile platform.

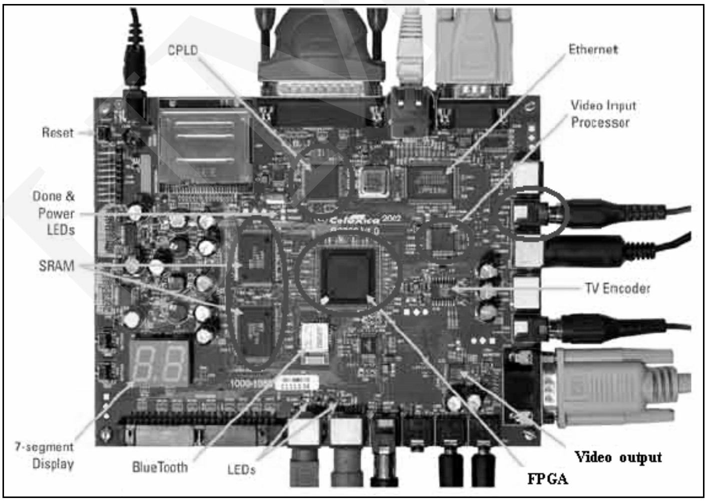

Fig. 3. Components of the FPGA development board used in the second-level node

3. Image processing in intrusion detection and classification

This section discusses the exemplary methodologies for FPGA-implemented image processing and intrusion detection and classification. Various systems used for surveillance, tracking and monitoring applications have been discussed in [3,4,9]. In our system, however, the camera-captured images are acquired, processed and analyzed by FPGA. The results are sent in a visual form to a human operator only if the system suspects something unusual is happening in the monitored area. Various image processing algorithms have been implemented in FPGA to perform different tasks. The library of developed algorithms can be used for adapting the network for changing conditions and/or requirements. Through online wireless reconfiguration of FPGA, the same hardware platform can be adapted to various tasks without redeploying the network.

The fundamental task of the developed network is to detect visible changes in the monitored area, i. e. to identify non-stationary (moving) components within camera-captured images. Generally, there are three typical approaches to the extraction of moving targets from a sequence of images (or a video stream) as discussed in [3]. These are: (1) temporal differentiation (two or three frame), (2) background subtraction and (3) optical flow. Temporal differentiation is very adaptive to dynamic environments but does not perform well in extracting all relevant feature pixels. Background subtraction is very sensitive to dynamic environment changes but provides complete feature data. Optical flow computation methods are considered too complex for real-time applications unless a specialized hardware is available. For our system, background subtraction has been selected. Although such an operation can be (hypothetically) implemented as a simple image comparison, a more sophisticated method is needed for more realistic applications. In general, the scene background may be affected by both illumination variations and minor configuration changes (e.g. swaying trees, grass, vibrations of the network nodes, etc.). The first problem can be solved by occasional background updates (see the later part of this section) but for the second one, a more sophisticated approach has been proposed. In the developed system, we apply a combination of subtractions in the RGB space (with a threshold defining the acceptable differences) followed by a sequence of selected morphological operations. The purpose of the morphological operations is to filter out differences caused by minor configuration changes.

3.1. Static intrusion detection

Silhouettes of intruders obtained by the background subtraction can be represented in three different forms: (1) a binary blob of the intruder's shape, (2) a full image within the extracted silhouette or (3) a rectangular outline of the intruder. Examples of the original scene, the scene with the intruder, and three variants of the intruder's silhouette are shown in Figs 4 and 5.

The binary silhouettes are useful for a classification of intruders using moment-based expressions of low order [17], from which several useful descriptors of the intruders can be derived. The full-image silhouettes can be further processed for detection of interest points and subsequently for the identification of known intruders (more details to be given in subsection 3.4). The rectangular outline is a convenient presentation of the intruder for a human inspection. The visual characteristics of the intruder's image remain unchanged while the amount of data to be wirelessly transmitted is dramatically reduced.

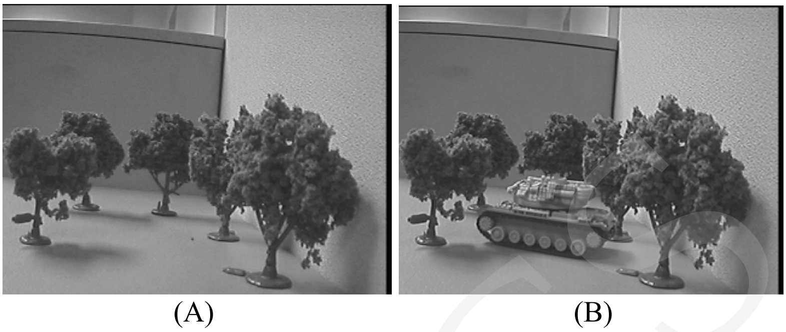

Fig. 4. An exemplary background image and the corresponding scene containing an intruder

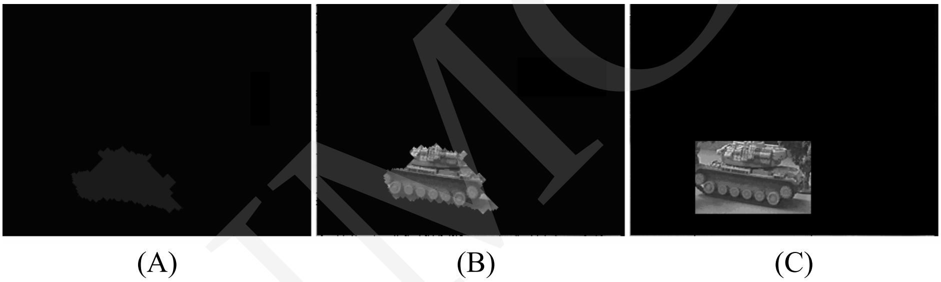

Fig. 5. Intruder's silhouettes extracted in three versions

If a human operator supervises a large number of nodes (with the attached cameras) the chances of visual intruder detection in a single image looking like Fig. 5C are much higher than in hundreds of images looking like Fig. 4B.

3.2. Dynamic intrusion detection

Detected intruders can be further characterized by using the variations of the intruder's shape 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. The example in Fig. 6 shows a pair of (overlapping) silhouettes of a human. A simple comparison of the low order moments calculated from both silhouettes, would indicate that a vertical intruder of irregular shape is moving toward the node and turning to the left. The speed of motion can be estimated based on the size changes and displacements of the gravity centre. Such a characteristics could be a sufficient evidence to recognize the intruder as a human.

In the case of some man-made objects, the silhouettes extracted from the images would have more consistent shapes so that a broad classification of such objects can be done within the second-level node by using moment invariants (e.g. [17,18]).

Generally, intrusions that can be satisfactorily identified at the second-level node are not sent for visual verification by a human operator. Unknown cases, however, have to be inspected. The images of such intruders would be wirelessly transmitted to the next level (which would usually incorporate a human operator). In order to save the bandwidth, actually only the rectangular outlines of silhouettes (e. g. Fig. 5C) are transmitted.

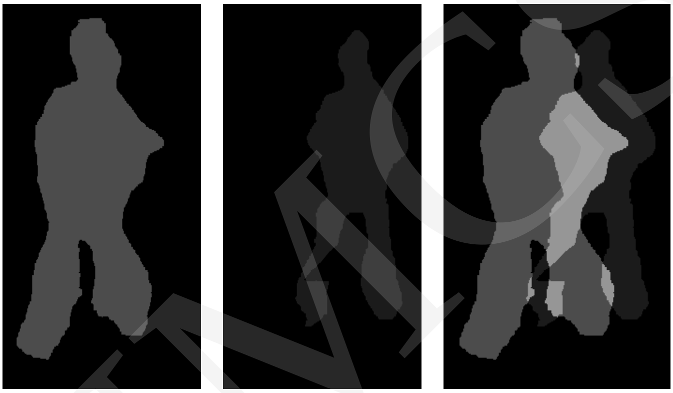

Fig. 6. Silhouette variations in a sequence of images

From Fig. 5 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 silhouettes and from their relative displacement in both images.

3.3. Background update

The presented system has been designed under the general assumption that the intruders can be associated with other physical phenomena, so that relatively simple sensors (proximity, vibration, magnetic, etc.) can be used as warning devices indicating potential presence of intruders. Thus, if there is a change in the camera-captured images without the presence of the corresponding sensor warnings, it should be considered a background change rather than intrusion.

Therefore, the algorithm used for intruder extraction can also be used for periodical background update. It is particularly useful if the background change is due to rapid illumination changes (additional shadows, etc.). For slow changes of the background a simple correlation method has been implemented. When the average value of correlation falls below a certain threshold (we have experimentally verified that for night conditions the threshold should be lower than for sunny days) the background is updated. The background updating procedure can be run periodically (excluding time intervals when the intrusion detection algorithm is active) with the frequency determined by both the expected dynamics of background changes and the power constraints of the second level nodes.

3.4. Advanced analysis of intruder images

In some of the prospective applications, selected intruders might be known to the system and such should not be considered a potential danger. Such detection, therefore, should not be reported to a human operator. Unfortunately, the moment-based classification methods mentioned in the previous sub-section are not robust enough for a positive verification of known intruders. Moreover, they generally fail when intruders are only partially visible. Therefore, selected methods originally developed for the vision-based robotic navigation are being adopted for the positive verification of known intruders.

The proposed approach is based on detection and matching interest points in a relative scale (e.g. [12,19]). Interest points (sometimes referred to as corner points) are easily perceivable small areas where the *corner response* (based on the matrix of 2D partial derivatives of the image intensities – see [12]) reaches its local maximum. In the database images of known intruders, the interest points can be automatically extracted and their characteristics memorized. The examples of interest points automatically found in two images of real objects are shown in Fig. 7.

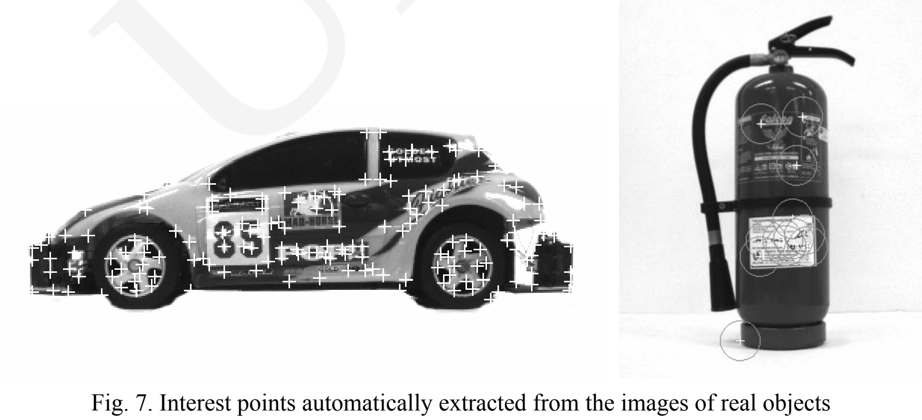

Fig. 7. Interest points automatically extracted from the images of real objects

If an intruder of interest is represented by a dataset of its interest points (including geometric relations between the points) an image of such an intruder can be hypothetically identified by matching image-extracted interest points to the dataset. The major practical difficulties, i.e. sensitivity to geometric and photometric transformations (i.e. illumination variation, scale of the objects, perspective distortions of 3D objects, etc.) have been successfully solved in the algorithm presented in [12] and [20]. The exemplary results of matching interest point of a model intruder and a camera-captured image of a partially visible intruder (under different illumination conditions and in a different scale) are presented in Fig. 8. It should be noted that the matching has been done for the intruding object only partially visible within a cluttered environment. The images to be analyzed within the developed systems contain only the intruder's silhouette so that the number of interest points to be extracted and matched is relatively small.

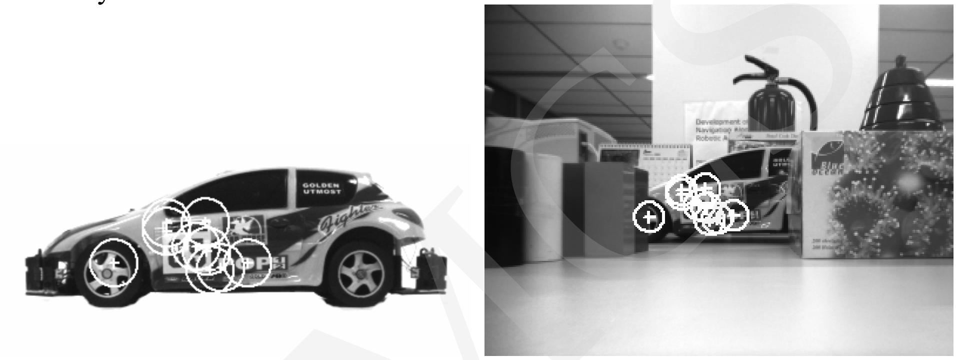

Fig. 8. Interest points automatically matched in a model image and a camera-captured view

Detection and description of interest points is a relatively simple operation that can be easily handled by the FPGA available in the developed nodes. Then, the characteristics of the points would be wirelessly transmitted to the higher level in the decision chain where the dataset of known intruders (and their interest points) is stored and the interest points can be matched, [13].

This method actually reduces the amount of data transmitted in the wireless network. Within the category of known intruders the system becomes fully autonomous, but the unidentified intrusions would still be reported to the human operator, i.e. their rectangular outlines (see Fig. 5c) would be transmitted wirelessly. This method can also be applied if the second level nodes are attached to a mobile platform as it can work even if the intruders silhouette has not been extracted from the background scene.

4. 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 (Fig. 9). 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. More details are presented in [21].

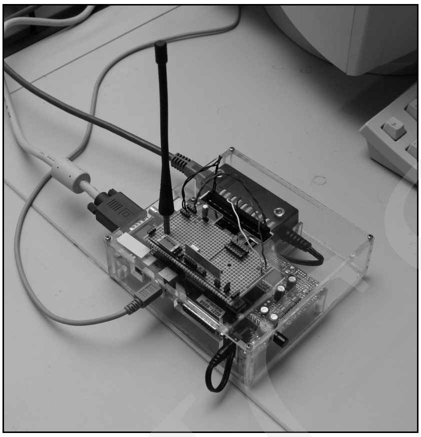

Fig. 9. Testbed for direct wireless communication between FPGA devices

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 [8,14]. These algorithms can be designed to adopt certain parameters like compression ratio, image resolution based on the real-time situation [8,15,16]. 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.

5. Future works and conclusions

The system reported in this paper has been implemented using commercially available development boards (RC200 FPGA development boards and Ember microcontroller boards). The final prototype model will have a dedicated architecture designed based on tests and further analysis as well as research. Similar concepts of an FPGA-based wireless sensor network are discussed in details in [5].

In a longer term perspective, several important issues have to be carefully analyzed and eventually optimized. Adaptability of the network is one of the most important requirements. In general, the low-level sensing mechanisms are less application dependent than the data processing and interpretation algorithms. Thus, a reconfigurable FPGA has been selected for the second-level nodes that perform the complex application-dependent tasks. Simultaneously, a library of FPGA configuration files is being gradually built so that the same hardware shell can be used for a variety of tasks. Since the FPGA chip can be reconfigured wirelessly, the application of the network can be changed/modified after it has been deployed. Additionally, we exploit the advantages of partial FPGA reconfigurability. By adapting this approach, we can keep permanent fragments of the tasks (e.g. standard image acquisition and preprocessing algorithms) in once-programmed structures of FPGA while the application-specific algorithms can be quickly deployed through fast partial reconfigurability.

Partial reconfigurability is a part of a more general problem of distributing the network functionalities between the programmable and fixed-logic (or once-programmable) components. While programmability (which in the sensor network is almost equivalent to reconfigurability) is generally a welcome feature, it also has significant disadvantages. Higher costs of reprogrammable components and significantly higher power requirements are the most important drawbacks of FPGA-based solutions.

Additionally, we are currently studying other aspects of the future development of wireless sensor networks with vision capabilities. For example, the problem of reliable network functioning in the case of a partial destruction or imperfect deployment is particularly important in certain applications. Again, it can be achieved by either increasing the number of nodes or by incorporating a higher level of reconfigurability into a node (or by a combination of both).

In this paper, we presented a two-level structure of nodes that can be used for visual intrusion detection and classification, with a preliminary support of various non-visual sensors. The FPGA based second level nodes can be dynamically configured for different applications and tasks even after the nodes are deployed using online (wirelessly) reconfiguration capabilities. Several algorithms of image processing and visual assessment implemented in FPGA have been discussed. This system can be an efficient intrusion detection one with a relatively high level of intelligence and reasonable power requirements, though still requiring a human assistance for the final decisions. Currently, a commercial product based on the developed platforms is being designed. We also believe the proposed concept of a wireless sensor network with enhanced vision capabilities could be a useful step in development of more advanced systems for man-machine collaboration.

Acknowledgment

The authors gratefully acknowledge the support and funding from IntelliSys Research Centre, a partnership between Nanyang Technological University (Singapore) and Singapore Technologies Engineering.

References

[1] Obraczka K., Manduchi R., Garcia-Luna-Aceves J.J., *Managing the Information Flow in Visual Sensor Networks*. Proc. WPMC 2002: 5th Int. Symp. on Wireless Personal Multimedia Communication, Honolulu, (2002).

[2] Estrin D., *Sensor network research: Emerging challenges for architecture, systems, and languages*. 10th Int. Conf. on Architectural Support for Programming Languages and Operating Systems (ASPLOS-X*)*, ACM SIGPLAN notices, (eds C. Norris and J.J.B. Fenwick), New York: ACM Press, 37(10) (2002) 1-4.

[3] Collins R., Lipton A., Kanade T., *A System for Video Surveillance and Monitoring*. Proc. of the American Nuclear Society (ANS), 8th Int. Topical Meeting on Robotics and Remote Systems, Pittsburgh, (1999).

[4] Collins R., Lipton A., Fujiyoshi H., Kanade T., *Algorithms for cooperative multisensor surveillance*. Proceedings of the IEEE, 89(10) (2001) 1456.

[5] Römer K., Mattern F., *The design space of wireless sensor networks*. IEEE Wireless Communications, 11(6) (2004) 54.

[6] Vieira M.A.M., da Silva Jr. D.C., Coelho Jr. C.N., da Mata J.M., *Survey on Wireless Sensor Network Devices*. Emerging Technologies and Factory Automation (ETFA03). IEEE 1 (2003).

[7] Bellis S.J., Delaney K., O'Flynn B., Barton J., Razeeb K.M., O'Mathuna C., *Development of Field Programmable Modular Wireless Sensor Network Nodes for Ambient Systems*. Computer Communications (accepted for special issue on Wireless Sensor Networks), to appear in 2005.

[8] Lach J., Evans D., McCune J., Brandon J., *Power Efficient Adaptable Wireless Sensor Network. Military and Aerospace Programmable Logic Devices*. Int. Conf. MAPLD 2003*,* Washington D. C., (2003).

[9] Meffert B., Blaschek R., Knauer U., Reulke R., Schischmanow A., Winkler F., *Monitoring traffic by optical sensors*. 2nd Int. Conf. on Intelligent Computing and Information Systems, Cairo, (2005).

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

[11] Islam M.S., Sluzek A., Zhu L., *Towards invariant interest point detection of an object*. 13th Int. Conf. in Central Europe on Computer Graphics, Visualization and Computer Vision, Plzen, (2005).

[12] Meguerdichian S., Koushanfar F., Potkonjak M., Srivastava M.B., *Coverage problems in wireless ad-hoc sensor networks*. IEEE Infocom, (2001) 1380.

[13] Islam M.S., Zhu L., *Matching interest points of an object.* IEEE Int. Conf. on Image Processing ICIP2005, Genova, (2005).

[14] Wu H., Abouzeid A., *Energy Efficient Distributed JPEG2000 Image Compression in Multihop Wireless Networks*. 4th Workshop on Applications and Services in Wireless Networks ASWN2004, Boston, (2004).

[15] Taylor C.N., Dey S., *Adaptive image compression for enabling mobile multimedia communication*. IEEE Int. Conf. on Communications 2001, Helsinki, (2001).

[16] Taylor C.N., Dey S., Panigrahi D., *Energy/latency/image quality trade-offs in enabling mobile multimedia communication*. in: Software Radio – Technologies and Services (ed. E.D. Re), Springer Verlag, (2001) 55.

[17] Hu M.K., *Visual pattern recognition by moment invariants*. IRE Trans.Inf.Theory, 8 (1962) 179.

[18] Maitra S., *Moment invariants*. Proc. of IEEE, 67 (1979) 697.

[19] Schmid C., Mohr R., Bauckhage C., *Evaluation of interest point detectors*. Int. Journal of Computer Vision., 37(2) (2000) 151.

[20] Islam M.S., Sluzek A., *Detecting and Matching Interest Point in Relative Scale*. Machine Graphics & Vision, accepted, (2005).

[21] Chen G.C.S., *Wireless communication between FPGA boards* SCE04-040 FYP report, NTU, Singapore, (2005).