HIGH-LEVEL ARCHITECTURE FOR A SINGLE LOCATION SURVEILLANCE POINT

Tomi Räty
Software Architectures and Platforms
VTT Technical Research Centre of Finland
Oulu, Finland
tomi.raty@vtt.fi

***Abstract*—The Single Location Surveillance Point (SLSP) is a distributed multi-sensor surveillance software system. It comprises of an arbitrary amount of sensors that collect readings from a single location, which is the surveillance point. Each sensor transmits its crude sensor data to a session server, which handles the connections between the components. The session server routes the crude sensor information to the logical decision making service. The logical decision making server automatically deducts the situation at the surveillance point based on the received sensor information. The logical decision making server informs the security manager server of the situation at the surveillance point. The security manager server's user interface displays essential information about the surveillance point to a human security administrator. The security manager server can transmit information to the nomadic security personnel's smart phones over wireless networks. The SLSP system decreases the amount of redundant information that otherwise would be handled by the human security administrator and the security personnel. This goal is achieved with a prominent architecture between the components and a server that conducts automatic decision making. The research is based on the constructive method of the related publications and technologies and the results are derived by the abstractive analysis of the available material. This paper illustrates the high-level architecture of the SLSP system.**

Keywords-component; Mobile & Wireless applications & services; Media and content distribution over wireless networks; Multi-sensor surveillance system

I. INTRODUCTION

Recent progress in computing, communication, and sensor technology are inciting the development of multiple new applications. This trend is apparent in pervasive computing, sensor networks, and embedded systems. During the past two decades, surveillance systems have been an area of vehement research. Recently, considerable research efforts have been concentrated on video-based surveillance systems, especially for public safety and transportation systems. [1]

The increasing demand for safety and security has resulted in more research in constructing more efficacious and intelligent automated surveillance systems. A future challenge is to develop a wide-area distributed multi-sensor surveillance system which has robust, real-time computer algorithms able to execute with minimal manual reconfiguration on variable applications. These systems should be adaptable enough to automatically accommodate and endure with the changes in the environment, such as lighting, scene geometry or scene activity. The system should be expandable; hence it should be based on standard hardware and exploit plug-and-play technology. [10]

To address the contemporary vicissitudes of surveillance systems, we have defined a Single Location Surveillance Point (SLSP) system and its architecture. The sensors survey and obtain information from a single mutual location. This area is the surveillance point. The SLSP architecture comprises of an arbitrary amount of miscellaneous sensors, a session server, a logical decision making server, a security manager server, and an arbitrary amount of end-devices, e.g., laptops, desktops, and smart phones.

The realized sensors consist of a biometrical sensor, an audio sensor, a video recorder, a network activity sensor, and an alternative video and motion sensor. The sensors monitor their immediate environment, which is called the surveillance point, and transmit knowledge about it to the session server. The session server routes the information to the logical decision making server. The logical decision making server collects all the information from the various sensors and performs logical deductions from the obtained information. These logical deductions indicate different situations of the surveillance point. The logical deductions are transmitted to the security manager server, at which a human security administrator resides via the session server. The human administrator can transmit information to the end-devices, e.g., laptops, desktops, and smart phones. The end-devices are registered to the SLSP system. The nomadic security personnel patrol in the premises, or they can be dispatched to the area, which is under surveillance. The nomadic security personnel can receive the information on their end-devices, e.g., smart phones, over wireless networks. The SLSP system decreases the amount of redundant information that otherwise would have to be handled by the human security administrator and the nomadic security personnel. Deductions based on the sensor

Proceedings of the Third International
Conference on Wireless and Mobile Communications (ICWMC'07)
0-7695-2796-5/07 $20.00 © 2007 IEEE

information are made automatically and they are informed to the security manager server. The human security administrator and the nomadic security personnel will not be inundated with superfluous information. Due to the disposition of the surveillance information, it is vital to transmit only the most important erudition as rapidly as possible. The security administrator server can be used to alert the patrolling nomadic security personnel of emergencies instantaneously. This can be conducted by the security manager administrator ordaining the distribution of critical information automatically and directly from the session server over a wireless network to the nomadic security personnel's end-devices, e.g., smart phones. This will make the reception of the crude sensor information and logical deductions quicker at the end-device, instead of having the information first being routed to the security manager server and the human security administrator deciding on what information to transmit to the end-devices. Another option is for the security manager administrator to select the received information, e.g., crude sensor information and/or logical deductions, which the security manager administrator wants to route to the nomadic security personnel's end-devices over a wireless network.

The conference paper is presented in the ensuing manner. First, the two most common and fundamental surveillance structures, video surveillance and audio surveillance, are presented. This is followed by a concise description of the current development of surveillance systems. Then Single Location Surveillance Point is presented in detail. This is followed by a comparison between the SLSP and theoretical paradigms presented. Finally, the conclusion recapitulates this conference paper.

II. VIDEO SURVEILLANCE STRUCTURES

According to Foresti et al., the importance of video surveillance techniques has augmented significantly since the latest terrorist incidents. Safety and security have become critical in numerous public areas, and there is a designated need to enable human operators to remotely monitor activity across large environments, e.g. shopping malls. Modern video-based surveillance systems utilize real-time image analysis techniques for efficacious image transmission, colour image analysis, event-based attention focusing, and model-based sequence comprehension. [3]

Trivedi et al. proclaim that the video surveillance activity has significantly augmented recently. Earlier work addressed mostly with single stationary cameras, but the current trend is to active multicamera systems. These systems provide multiple advantages over single camera systems. This includes multiple overlapping views for procuring 3D information and plying occlusions, multiple non-overlapping cameras for covering vast tracts, and active pan-tilt-zoom (PTZ) cameras for discerning object details. [8]

A. Generations of surveillance systems

Bramberger et al. state that cameras can be equipped with a high-performance onboard computing and communication infrastructure, coalescing video sensing, processing, and communications in an individual embedded device. By offering access to multiple views via the cooperation among individual cameras, networks of embedded cameras can possibly support more complex and demanding applications, containing smart rooms, surveillance, tracking, and motion analysis, than an individual camera. [1]

Video-based surveillance systems have developed in the three generations. First-generation surveillance systems utilized analogue paraphernalia throughout the plenary system. Analogue closed-circuit television cameras captured the observed scene and transmitted the video signals over analogue communication lines to the central back-end systems, which rendered and archived the video data. [1]

Second-generation surveillance systems employ digital back-end components, enabling real-time automated analysis of the incoming video data. Hence, an automated event detection and alarm raising substantially augmented the content of simultaneously monitored data and the plenary surveillance system's quality. [1]

Third-generation surveillance systems have finalized the digital transformation. In these systems, the video signal is converted into the digital domain at the cameras, which transmit the video data through a computer network, for instance a local area network. The digital cameras can also directly compress the video data to conserve bandwidth. The back-end and transmission systems of a third-generation surveillance system have also augmented their functionality. For instance, they employ intelligent hubs to gather the video data, accumulate the information from different cameras, and transmit it to the video archive and the operators. [1]

B. Smart cameras

Modern processor technology enables the implementation of smart cameras, which directly execute highly sophisticated video analysis. These smart cameras integrate video sensing, video processing, and communication into an individual embedded device. They are designed as reconfigurable and resilient processing nodes with self-configuration, self-monitoring, and self-diagnosis capabilities. Smart cameras maintain the prevailing paradigm shift from a central to a distributed control surveillance system. The main motivation for this shift is augmenting the surveillance system's functionality, availability and autonomy. Smart cameras are key components of these novel surveillance systems, because they offer adequate performance for onboard video processing and distributed control. These surveillance systems can respond autonomously to alterations in the system's environments and to detected events in the monitored scenes. [1]

III. AUDIO SENSOR STRUCTURES

Accurate and robust localization and tracking of acoustic sources is of interest to a variety of applications in surveillance, multimedia, and hearing enhancement. Miniaturization of microphone arrays incorporated with acoustic processing further augments the utility of these systems, but poses challenges to achieve precise localization performance due to abating aperture. For surveillance, acoustic emissions from ground vehicles offer a facilely detected signature, which can be employed for unobtrusive and passive tracking. [7]

An integrated miniature sensor array with localization and communication capability could be maintained as a low-cost, low-power small autonomous node in network configuration distributed over a vast region. This results to a higher localization performance in distributed sensing environments bypassing the requirement for excessive data transfer and fine-grain time synchronization among nodes, with low communication bandwidth and low complexity. Additional improvement can also be attained by fusion with other data modalities, such as video. [7]

IV. CURRENT DEVELOPMENT OF SURVEILLANCE SYSTEMS

As the personal computing era evolves into a ubiquitous computing one, there is a requisite for a world of completely connected devices with inexpensive wireless networks. Enhancements in wireless network technology interfacing with emanating microsensors predicated on MEM (Micro-Electro-Mechanical) technology is enabling sophisticated, yet inexpensive, sensing, storage, processing, and communication capabilities to be unobtrusively embedded into the everyday physical world. Embedded web servers can be utilized to connect the physical world of sensors and actuators to the virtual world of information, utilities, and services. Consequently, a rush of research activity has begun in the sensor networks domain, particularly in wireless ad hoc sensor networks. Even though many of the sensor technologies are not novel, some physical and technological barriers of performing wireless communications have confined the viability of such devices in the past. Some of the advantages of the newer, more capable sensor nodes are their abilities to establish large-scale networks, implement sophisticated protocols, decrement the amount of communication (wireless) required to execute tasks by distributed and local calculations, and implement intricate power saving modes of operation depending on the environment, the application, and the state of the network. [5]

Valera & Velastin presented the state of deployment of intelligent distributed surveillance systems, including a revision of contemporary image processing techniques, which are employed in different modules that constitute part of surveillance systems. Reviewing these image processing tasks, it has discriminated research areas that need to be scrutinized further, such as adaptation, data fusion, and tracking methods in a co-operative multi-sensor environment, extension of techniques to distinguish complex activities and interactions between detected objects. In terms of communication or integration between different modules, an examination of new communication protocols and the creation of metadata standards are required. It is vital to consider ameliorated means of task distribution that optimize the use of central, remote facilities, and data communication networks. One of the facets that will be inherent in the future for the development of distributed surveillance systems is the definition of a framework to design distributed architectures well established in the systems engineering best practice. [10]

Advances in information and communication technologies can potentially offer considerable improvements in the management of public places pertaining to safety and security. These include technologies, for instance, digital storage of video, transmission of video/audio streams over wired and wireless networks, etc. Discriminating features of the deployment of technology to maintain surveillance in modern urban environments includes large, geographically dispersed facilities and hierarchical multi-agency management structures. These are then construed into requirements of robust image processing, distribution, scalability, and usability. Video surveillance applications need to be real-time, because there is security requirement considering minimum time constraints. Video surveillance must low delay and timing constraints for processing. [2] & [11]

V. THE SINGLE LOCATION SURVEILLANCE POINT ARCHITECTURE AND COMPONENTS

The Single Location Surveillance Point comprises of three individual domains as in Figure 1. These three domains are 1) the Surveillance Domain, which comprises of an arbitrary amount and variety of sensors, and 2) the Security Administration and Surveying Domain, which comprises of the session server to which the sensors transmit their information and the logical decision making server, and the end-devices, e.g., the laptops, desktops and smart phones 3) the Security Personnel Management domain, which is intended for conducting security personnel from a remote and centralized location. This domain also provides an interface to the human security administrator.

Initially, sensors transmit their information to the session server. The session server transmits the crude sensor information to the logical decision making server. The logical decision making server is responsible of transmitting its logical deductions regarding the surveillance point to the security manager server through the session server. Then the security manager server can transmit orders, with the help of the human security administrator, to the security personnel, e.g., the laptop, desktop, and/or smart phones end-devices.

The data flow from the sensors of the Surveillance Domain is primarily the ensuing: 1) the crude sensor information is conveyed from the sensors to the session server, 2) the session server transmits all the crude sensor information it receives to the logical decision making server, 3) after performing the its automatic logical calculations, the logical decision making server transits its deductions to the security manager server and/or the nomadic security personnel via the session server. Then the human security administrator can issue orders to the end-devices, or even re-route the deduction information and/or crude sensor information, e.g., video footage, it receives to the end-devices.

The session server acts as an interface from which crude sensor information can be procured. The session server entails two fail-safe mechanisms: 1) if the crude sensor information cannot be distributed to the logical decision making server, then the session server will transmit the crude sensor information to the security manager server, and 2) if the crude sensor information cannot be distributed to the security manager server either, or if the session server is ordained by the security manager server to transmit the crude sensor information directly to the end-devices, then the session server will transmit the crude sensor information to the end-devices.

The Testing Environment is utilized during the Surveillance Domain's and the Security Administration and Survey Domain's development phases. The test server is primarily employed to test the session server on behalf of the network activity monitor. The test server may also be utilized to test the session server by providing artificial sensor information on behalf of the sensors.

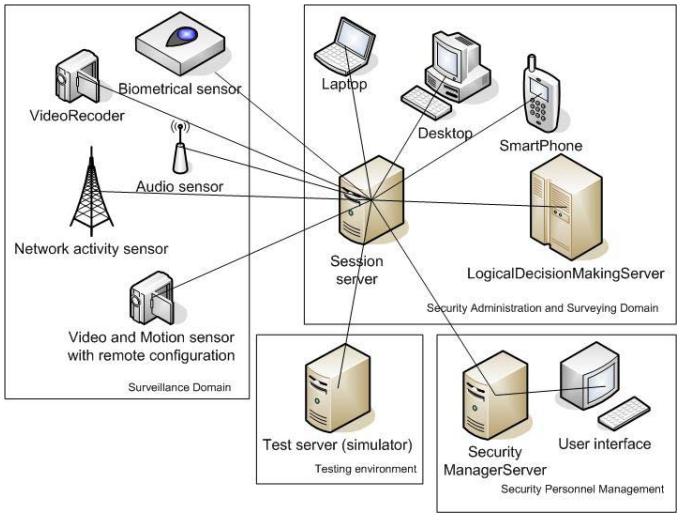

Figure 1. Single Location Surveillance Point.

A. *The Surveillance Domain*

The actual biometrical sensor will be a veritable fingerprint sensor hardware device accompanied with its software module stored on the session server. The network activity monitor surveys the current situation of the wireless network activity in its local environment. Its software module will also be stored on the session server.

The purpose of the video recorder is to deliver constant, pristine, and immaculate video stream to the receiving party. The video recorder utilized is the Axis 213 PTZ network camera. The audio sensor will provide real-time sound identification and localization with multiple microphones.

The video and motion sensor with remote configuration (VMSRC) comprises of a stationary video camera and a motion detector. The VMSRC can transmit the information obtained from its sensors to a remote receiver, the logical decision making server. The VMSRC provides an alternative and direct route from the VMSRC to the logical decision making server. The VMSRC entails the capability of creating a wireless and secure connection, e.g. GSM/GPRS, between the VMSRC and the logical decision making server.

The main functions of the Surveillance Domain's sensors are twofold: 1) Collect information from its ambit, and 2) Transmit the collected information to the session server of the Security Administration and Surveying Domain.

B. *The Security Administration and Surveying Domain*

The Security Administration and Surveying Domain comprises of the session server, the logical decision making server, and an arbitrary amount of end-devices., e.g., laptops, desktops, and smart phones. An end-device is reputed to be a device from which security personnel may view data related to security erudition. The session server handles information collection from the sensors of the Surveillance Domain. The gathered information may be either directly transmitted to end-devices and/or the security manager server, or transmitted to the logical decision making server for further information processing. If the information is transmitted to the logical decision making server, then the information from an individual sensor, or the consolidation of the sensor information, will processed further to deduct intricate information. The refined knowledge resulting from the logical decision making server is then transmitted to the session server. The session server conducts the ultimate decision of what end-devices and whether to transmit the security manager server the acquired refined knowledge. The session server handles/interacts with the sensors. The session server must store the information transmitted by the sensor accompanied with the date and timestamp. This information is stored to be reviewed later by security officials. The logical decision making server must have a modular structure to be expandable for new possible sensors. Additional sensors need to be attachable to the session server and the logical decision making server.

Out of the three end-devices illustrated in the SLSP system, i.e., the laptop, the desktop, and the smart phone, the smart phone will have the highest priority. Wireless technologies are deemed as interesting by contemporary research and science, for instance by Sagiraju et al. [6], Kaplan [4], and Tseng et al. [9] all of whom have conducted research pertaining wireless technology and surveillance/safety systems.

The main functions of the Security Administration and Surveying Domain's components, a.k.a. the session server, the logical decision making server, and the end-devices, are the ensuing:

For the session server: 1) Collection of information from the sensors of the Surveillance Domain, 2) Transmission of the collected information from the sensors to the logical decision making server, 3) Retrieval of the processed and refined information from the logical decision making server, 4.1) Transmission of the processed and refined information from the logical decision making server to the Security Personnel Management's security manager server, 4.2) If the logical decision making server is unavailable, then the session server will transmit the crude sensor information to the security manager server and 4.3) If the security manager server is unavailable or the human security administrator has ordained the session server to automatically distribute the crude sensor information and/or logical deductions to the end-devices, then the session server will transmit the crude sensor information and/or logical deductions to the end-devices, and 5) Perform as an interface to (and from) the assorted sensors.

For the logical decision making server: 1) Collection of information provided by the session server, 2) Refinement and processing of gathered information, either based on the particular sensor it originally resulted from and/or based on the consolidation of the sensors, and, 3) Transmission of the

refined and processed information to the Server for the distribution to the appropriate recipients.

For the end-devices: 1) Displaying/illustrating the plebeian or refined information to the security personnel, which has been received from 1.1) the Security Personnel Management's security manager server, but if unavailable 1.2) the logical decision making server, but if unavailable, or if ordained by the human security administrator of the security manager server then 1.3) the information received directly from session server.

C. *Testing environment*

The test server can induce different sensor information to the session server, and different test cases can be executed from the test server. This will conducted in a manner that the session server will postulate it is receiving input information from the sensors of the Surveillance Domain. Initially, the Test server will be used to test the pseudo-functionality on behalf of the network activity monitor, but can be elaborated to produce input regarding the other sensors of the Surveillance Domain.

The main functions of the Testing environment's component, a.k.a. the Test Server (simulator), are the following test functionalities: 1) Propagating artificial sensor information to the session server, and 2) Receiving responses from the session server.

D. *Security Personnel Management*

The Security Personnel Management comprises of the user interface and the security manager server. The Security Personnel Management is used to conduct and coordinate security personnel from a remote location. The end-devices of the security personnel are the end-devices of the Security Administration and Surveying Domain, e.g., the laptop, desktop and smart phones. The SLSP focuses chiefly on ambulating security personnel equipped with smart phones. The security personnel ambulate in their own patrol region. The information that the security management server receives from the Surveillance Domain, i.e., sensors, can be either crude or processed by the logical decision making server. The administrator can verbally ordain instructions to the security personnel through the user interface to the smart phones of the security personnel. The human security administrator at the user interface of the security manager server may also re-route the information it receives from the logical decision making server or even the crude sensor information, e.g., video footage, to the security personnel's smart phones. The human security administrator may also ordain the session server to automatically forward the crude sensor information and/or the logical deductions of the logical decision making server automatically.

The main functions of the Security Personnel Management's components are the ensuing:

For the security manager server: 1) Reception of processed information from the logical decision making server or if unavailable 2) The reception of the crude sensor information from the session server, 3) Routing of orders and communication data between the end-devices and the user interface, and 4) Transmitting crude sensor and/or logical deductions to the end-devices, either by ordaining the session server to transmit this information automatically or by allowing the human security administrator to selectively choose what crude sensor and/or logical deduction information to transmit to the end-devices.

For the user interface: 1) Displaying processed information received from the logical decision making server or crude sensor information from the session server, and 2) Receiving orders from the human security administrator and distributing them to the smart phones and/or the session server through the security manager server.

VI. A BRIEF SUMMARY OF SLSP SOLUTIONS COMPARED TO THE THEORETICAL PARADIGMS

The Single Location Surveillance Point system achieves the requirement of Foresti et al. by enabling human operators to remotely monitor activity across large environments. Trivedi et al. stated that multicamera systems are a current trend, the SLSP utilizes this approach, but in a different manner. The SLSP focuses on a single and remote point of surveillance, but with multiple sensors.

Bramberger et al. argued that in third-generation surveillance systems, the video signal is converted into the digital domain at the cameras, which transmit the video data through a computer network, for instance a local area network. The SLSP system is predicated on a similar functionality, the crude sensor information is distributed in a digital data format to a network. This network comprises of the session server, logical decision making server, security manager server, and the end-devices, e.g., the laptop, desktop and smart phone end-devices.

Bramberger et al. introduce systems to gather the video data, accumulate the information from different cameras, and transmit it to the video archive and the operators. Stanacevic & Cauwenbergh declare that additional improvement can also be attained by fusion with other data modalities, such as video. In addition, Megerian et al announce that some of the benefits of the newer, more capable sensor nodes are their abilities to establish large-scale networks, implement sophisticated protocols, decrement the amount of communication (wireless) required to execute tasks by distributed and local calculations, etc. Valera and Velastin declare that certain research areas need to be examined further, such as data fusion. The SLSP system handles all of the aforementioned issues. It entails resembling methods of operation, instead of only collecting video data, the SLSP system's session server culls multi-sensor information and transmits it to the logical decision making server. The logical decision making server performs automated deductions based on the crude sensor information and transmits its deductions to the security manager server at which the human security administrator resides. The obtained crude sensor information can be stored at the session server for any possible use required by authorities or administrators.

Bramberger et al. also proclaim that smart cameras maintain the prevailing paradigm shift from a central to a distributed control surveillance system. Additionally, Bramberger et al. promulgate that these surveillance systems can respond autonomously to alterations in the system's environments and to detected events in the monitored scenes.

The SLSP attains both requirements, the surveillance control in the SLSP is distributed over the logical decision making server and the security manager server. In addition, the fail-safe systems of the session server will coerce crude sensor information to secondary and tertiary recipients, if the currently primary recipient fails to receive the crude sensor information. The logical decision making server performs deductions automatically based on the inputs from the sensors.

Megerian et al. declare that wireless sensor networks provide a viable alternative to numerous existing technologies. Desurmount et al. and Velastin denote that wireless technologies provide advantages in surveillance systems. The SLSP system utilizes wireless connections. The crude sensor information may be transmitted over a wireless connection between the sensors and the session server. Also, the data connections between the session server and the logical decision making server, the logical decision making server and the security manager server, and between the security manager server and the end-devices may be wireless. Only the connection between the security manager server and the smart phone end-device is mandated to be wireless.

VII. CONCLUSION

This paper has illustrated the architecture of a high-level distributed multi-sensor surveillance system. The main advantage of the SLSP system is that it is a distributed surveillance system, which utilizes multiple sensors in automatically deducting the situation of the monitored point. The processed information is distributed to the security administration manager and the end-devices, e.g., smart phones, of the security personnel over a wireless network. In detail, the distribution of processed and refined critical information is transmitted to the session server from the sensors. Then the crude sensor information is transmitted to the logical decision making server. Both the logical deductions of the logical decision making server and the crude sensor information of the sensors can be transmitted to the security administration manager and the nomadic security personnel, which can only be reached over a wireless network. A fundamental advantage of the SLSP system is that it reduces the amount of redundant information which is delivered to the human security administrator and the nomadic security personnel. The SLSP system informs the human security administrator and the nomadic security personnel about situations that require intervention. The SLSP distributes the most vital information to the appropriate human users, i.e., the human security administrator and the nomadic security personnel, as quickly as possible. The current disadvantage of the SLSP is that it monitors only a single location. The SLSP can be applied to various locations at which automatic surveillance is desirable, e.g., entrances of buildings.

REFERENCES

[1] Bramberger, M., Doblander, A., Maier, A., Rinner, B., & Schwabach, H.: Distributed Embedded Smart Cameras for Surveillance Applications, Computer, Published by the IEEE Computer Society, February 2006, pp. 68-75.

[2] Desurmont, X., Bastide, A., Chaudy, C., Parisot, C., Delaigle, J.F., and Macq, B.: Image analysis architectures and techniques for intelligent surveillance systems, IEE Proc.-Vis. Image Signal Process., Vol. 152, No. 2, April 2005.

[3] Foresti, G.L., Micheloni, C., Snidaro, L., Remagnino, P., & Ellis, T.: Active Video-Based Surveillance System, IEEE Signal Processing Magazine, March 2005, pp. 25-37.

[4] Kaplan, L.M.: Local Node Selection for Localization in a Distributed Sensor Network, IEEE Transactions on Aerospace and Electronic Systems, Vol. 42, No. 1, January 2006, pp. 136-146.

[5] Megerian, S., Koushanfar, F., Potkonjak, M., & Srivastava, M.B.: Worst and Best-Case Coverage in Sensor Networks, IEEE Transactions on Mobile Computing, Vol. 4, No. 1, January/February 2005, pp. 84-92.

[6] Sagiraju, P.K., Agaian, S., & Akopian, D.: Reduced complexity acquisition of GPS signals for software embedded applications, IEE Proc.-Radar Sonar Navig., Vol. 153, No. 1, February 2006, pp. 69-78.

[7] Stanacevic, M. & Cauwenberghs, G.: Micropower Gradient Flow Acoustic Localizer, IEEE Transactions on Circuits and Systems-I: Regular Papers, Vol. 52., No. 10, October 2005, pp. 2148-2157.

[8] Trivedi, M. M., Gandhi, T. L., & Huang, K. S.: Homeland Security Distributed Interactive Video Arrays for Event Capture and Enhanced Situational Awareness, IEEE Intelligent Systems, September/October 2005, pp. 58-66.

[9] Tseng, Y.-C., Lin, T.-Y., Liu, Y.-K., & Lin, B.-R.: Event-Driven Messaging Services Over Integrated Cellular and Wireless Sensor Networks: Prototyping Experiences of a Visitor System, IEEE Journal on Selected Areas in Communications, Vol. 23, No. 6, June 2005, pp. 1133-1145.

[10] Valera, M. & Velastin, S.A.: Intelligent distributed surveillance systems: a review, IEE Proc.-Vis. Image Signal Process., Vol. 152, No. 2, April 2005, pp. 192-204.

[11] Velastin, S.B.: Special Section on Intelligent Distributed Surveillance Systems, IEE Proc.-Vis. Image Signal Process., Vol. 152, No. 2, April 2005.

0-7695-2796-5/07 $20.00 © 2007 IEEE