Smart Surveillance Systems and Their Applications

Andrei Braicov, Ivan Budanaev, Marco Cosentino, Walter Matta, Alessandro Mattiacci, Carlo Maria Medaglia, and Mircea Petic

1 Introduction

Information technology develops at a fast pace, and its progress influences the evolution of many other fields of science. It is difficult to say nowadays if there are any aspects of our modern world which have not yet been affected in some way by the IT revolution. One such area of today's society is the urban surveillance and security. Although security is paramount in its core concept, the importance of this area has substantially increased since the launch of the Global War on Terrorism military campaign in 2001. This can easily be observed with the shift of military technologies into domestic applications and the confluence of internal and external security [1].

Modern surveillance systems consist of many individual components, and represent a very complex architecture. Most common problems that arise when building such products are related with data transfer speed and reliability, data analysis, and automation of processes. The widely spread high bandwidth mobile networks and attack resistant cryptosystems provide solutions to the first two of the above requirements. Computer vision algorithms permit to analyze streams of data and detect predefined patterns to spot hostile or abnormal behavior and automatically send signals to supervisors at the monitoring stations.

This paper addresses this specific area of modern security—surveillance systems. This article is written in the framework of the Wide InTegration of sensor Networks to Enable Smart Surveillance (WITNESS) project which has the aim to design

A. Braicov · I. Budanaev · M. Petic (✉)
Tiraspol State University, Chisinau, Republic of Moldova

M. Cosentino · W. Matta · A. Mattiacci · C. M. Medaglia
Link Campus University, Rome, Italy

D. Cagáňová, N. Horňáková (eds.), *Mobility Internet of Things 2018*,
EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-030-30911-4_12

a system for urban surveillance and security to help detect, prevent, and give an efficient response to terrorist threats and attacks.

The aim of this paper is to describe the methodology of the research in the project, starting with the architecture of the surveillance system.

This article is structured as follows: First, we start with the state of the art of similar research topics. Then we will describe our main aspects of the system architecture. More details are given in the following sections, concerning sensor models.

2 Related Works

The topic of smart surveillance is very popular nowadays. Its idea came from the practical issues where video surveillance was used to monitor municipal buildings, banks, train stations, etc. Surveillance becomes more and more important because of increasing number of exceptional situations that require a high attention to the people and society [2]. Smart surveillance is the use of automatic video analysis technologies in video surveillance applications [3]. Automatic video analysis technologies usually take into account both GPS and telemetry data. As video data also contains noise, video sequences are usually divided to be processed into smaller pieces. A separate analysis of smaller video sequences allows one to create an overview of the whole video.

The current available smart surveillance infrastructure allows to configure and implement the algorithms for recording and filtering video data streams from interconnected objects on the Internet. One of the examples of state-of-the-art infrastructure are RFID frameworks. They are elaborated in such a way that they provide the functionality to monitor space (2D or 3D), identify suspicious events, and react by generating appropriate responses to the situation. RFID frameworks have been developed as a result of researchers' efforts [4] and commercial demands. Examples of open-source RFID frameworks include Mobitec [5], AspireRFID [6, 7], and the Fosstrak project [8, 9] that provide free infrastructure deployments.

Another approach would be to use Wireless Sensor Networks (WSNs). These were initially used as surveillance in military conflict zones. The first implementations of WSNs used distributed sensor networks (DSNs) technology. Just as the first sensors were quite large, their applicability was reduced as well as due to their limited wireless connectivity. Currently the sensors are significantly smaller and cheaper. This led to the implementation of sensor networks for monitoring apartments, the environment, and the use of body sensors. WSN is considered one of the most prospect technologies of the present century [6, 10].

The variety of WSNs platforms is great. There is a platform that only addresses the system as a network of sensors. Other platforms work with devices and other sensor networks connected to the WSNs. There are WSN development and monitoring systems that have limited extensibility, for example, Moteview [11] and [12]. The following tools provide development and/or programming environments for WSNs systems: Hourglass, SenseWeb, jWebDust [13], and GSN [14]. A more detailed description of the architectural particularities of the WSNs systems can be found in [13].

The effectiveness of WSNs in the surveillance process is acknowledged. However, there are approaches that seek to improve the use of WSNs by combining them with unmanned aerial vehicles (UAVs) in surveillance. UAV is a solution in situations where it is necessary to fly over dangerous areas without endangering people's lives.

Paper [15] presents a project example describing the interaction between WSNs technology and UAV tools used for border surveillance. The UAV in the given case is considered a quadcopter.

Research focused on the use of quadcopter in terrestrial surveillance is focused on identifying cost-effective solutions and preserving the same functionality. Usually a quadcopter is driven by the means of proprietary framework APIs from a laptop or a PC. A quadcopter is useful in reading the altitude to the ground, as well as in measuring air temperature, humidity, and gas composition [16].

3 Use Case Scenarios

WITNESS proposes an innovative technological solution to incidents and accidents that may occur in an unpredictable urban scenario characterized by crowded scenes with potentially complex structured man made surroundings. The typical scenarios WITNESS will cater for are those where an incident or accident has caused disruption in the normal 24/7 operation of a public space (for instance, a metro, a railway, or a bus station). In such environments a nominal flow of people can be expected and, therefore, normal behavior can be predicted. We also envisage that the public spaces of interest will be monitored by fixed cameras and by police forces.

Some examples of possible case studies are as follows:

- Natural disasters: A disaster is a serious disruption of the functioning of a community or a society involving widespread human, material, economic or environmental loss and impacts. Disasters caused by natural or technological reasons are identified as NaTech.
- General disruption of individuals: Public areas witness the presence of intoxicated individuals, usually disruptive in small groups. Such events may have an effect on the normal flow of people, for instance, in a metro or railway. Such individuals may start pushing one another and other people in the surroundings.
- Public events related to holidays, manifestations, or protests where there is an abnormal accumulation of people with high density. As noticed from latest terrorist attacks, these types of scenarios are a very attractive target for terrorists [17, 18].
- Accident: This describes a category of events that may be caused by the failure of electrical power, for instance, delaying metro or trains, or by physical accidents

happened to individuals, including suicide attempts. In such case an entire station may be closed and events may more or less slowly affect the entire area.
- Incident: This could be caused by a terrorist threat, even including hostage situations.

Specific use case scenarios of WITNESS system applications would include monitoring of the sport events, large-scale peaceful demonstrations, and violent protests. During these events, the abnormal behavior under study is sought to be well-organized groups of people who aim to destabilize public order by taking hostage among civilians, using guns, fumigants, or explosives. Depending on the event type, the size of monitored area can span between 10,000 and 300,000 m^2. The average occupancy of the monitored area is projected to be up to 20,000 people.

4 WITNESS Architecture

WITNESS implements a distributed multi-layered architecture to satisfy the operational requirements of a situational awareness and decision-making system. This approach facilitates building a flexible and pervasive enough product, ready to be automatically reconfigured and quickly redeployed when needed. The cornerstone of the system is the data, which is collected by a predefined set of sensors—wearable by police forces deployed on the grounds or sensors installed on UAVs and police vehicles. In this way, the layer responsible for collecting data in WITNESS system represents a sensor fusion grid that leverages data from multiple heterogeneous sensor nodes, including cameras, microphones, and drones. A schematic diagram of the system's architecture is depicted in Fig. 1.

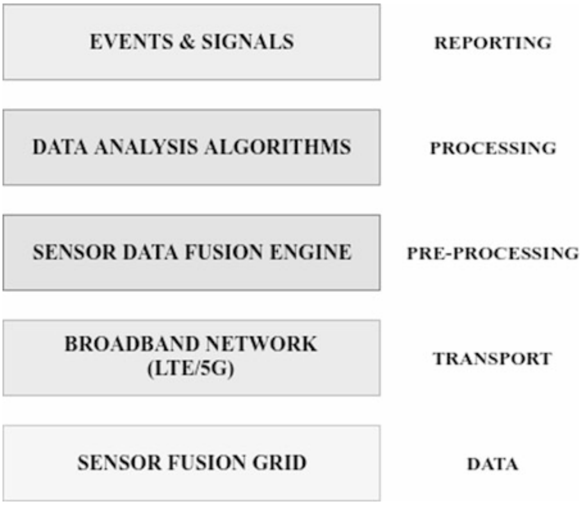

Fig. 1 WITNESS architecture

Data originating from different sources dispersed in multi-dimensional space (police forces on the field, quadcopters in the air, lags and losses during data transfer synchronization) needs to be gathered and pre-processed before it is submitted for analysis. This is a difficult task to address, since information received scales exponentially in terms of location, space, time, and means (multi-source information). Recent advances in ICT technologies can boost the efficient acquisition, fusion, and integration of information from the above sources. Sensor data fusion component will be implemented to address the above problem. Data fusion technologies involve the fusion of multi-sensory data to estimate the position, speed, attributes, and identity of the detected and flagged targets, e.g., a person, a vehicle, or an object in the operation area.

It is widely accepted that the data transfer between system components of the above architecture requires a dedicated broadband communication infrastructure (e.g., LTE, 5G technology) to be deployed in a very short time, so as to be promptly used to support the communications among security forces deployed on the field and used to gather and to process awareness data coming from monitoring devices (e.g., wearable sensors or mobile nodes) and to perform the command and coordination of the forces. In this regard, the underlying infrastructure plays a critical role in the security, processing, flow, supporting information requirements throughout the operational forces.

In particular, the proliferation of multi-purpose sensors provides ample room for sensing the physical world. For example, a host of visual processing algorithms can provide credible information about the context of a given actor (e.g., location, behavior). At the same time Wireless Sensor Networks (WSNs) provide the means for autonomic continuous information collection, in the scope of large-scale heterogeneous environments. However, even with these technologies at hand, there is need for the fusion of information captured by multiple sensors and modalities to the end of identifying situations, especially in the scope of highly distributed heterogeneous and volatile environments where people and entities (i.e., people, sensors, vehicle, etc.) may dynamically join and leave.

Within the proposed methodology, WITNESS ensures that data and information are delivered to the right place on time and optimally encoded for use by their intended recipients to take the appropriate actions at the right time. The security and safety of this information will be granted by the dedicated LTE cell. This architecture is a key enabler of Net-centric Enable Capability (NcEC) and is essential for “information superiority” and “decision superiority”: it will automatically enable the security units deployed in the area of interest to communicate with whom of interest and get an immediate perception of who and where suspects and security forces are.

WITNESS will adopt a breadboard architecture enabling plug and play integration of the various components. The architecture also enables the integration of third-party components. Furthermore, this architecture will give the possibility to assign a task to a UAV and to reallocate it to another one when the first drone will have low battery or any other malfunction scenario. This need arises for the known critical issue of the battery duration of the UAVs.

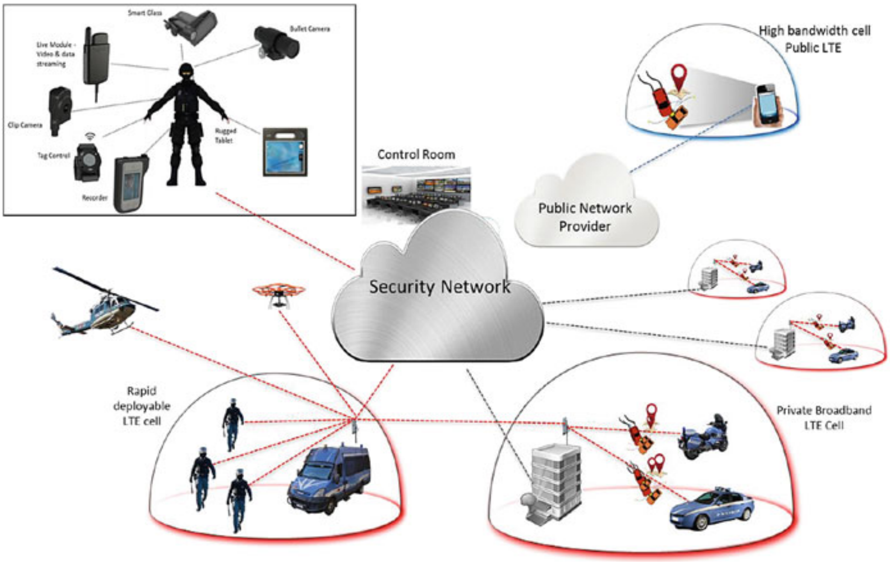

Fig. 2 WITNESS concept

This project aims to explore technological concepts and approaches already proposed for military operational fields for use in civilian security. Those concepts, and in particular the Network Enabled Capabilities (NEC), have practically never been applied in civilian applications, and are new even to the military sectors. At a global level, however, there are already focus groups questioning on how to apply the NEC philosophy to the security applications (especially in the USA), thus is imperative to start the development of a European blueprint on this topic. One of the technological impacts of WITNESS will be the generic Internet-of-Things approach towards creating a civil security C2 situation assessment and decision aiding framework (Fig. 2).

5 Methodology

Taking into account the current approaches in this field and the use cases for the system to be built the project WITNESS research will follow the scheme presented in Fig. 3.

The stages included in Fig. 3 are referred to the whole project. In this paper we refer to the following stages:

- Reference Scenarios and Operational Requirements,
- Architectural Design and Functional Description.

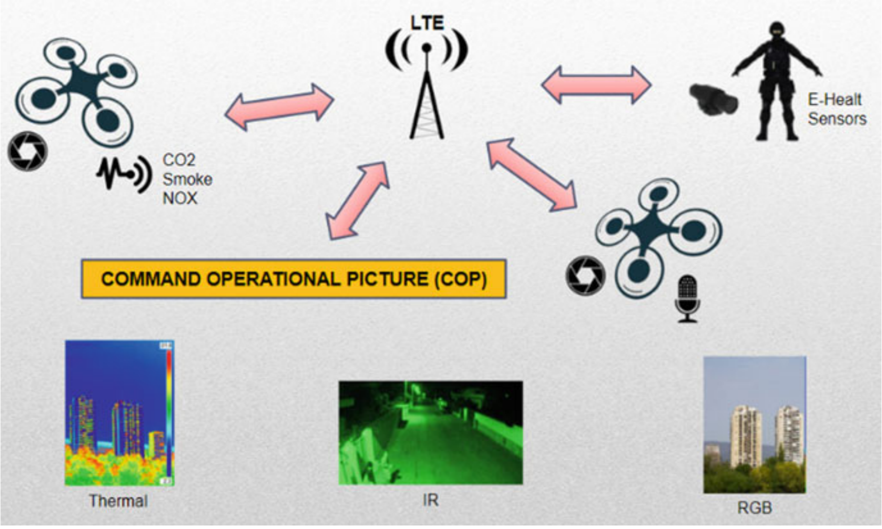

Fig. 3 WITNESS architecture details

Table 1 Parameters and devices

Parameters (sensors)	Devices
Optical sensor (video analysis)	RGB camera/thermal camera/infrared camera
Sound sensor	A microphone
Air quality sensor	SNS-MQ135

Each of the above scenarios was discussed in the corresponding sections of this paper. Below we will describe the solutions for architectural design and functional descriptions. The key elements of the system are quadcopters and different types of sensors.

In order to obtain a more accurate result we need a complete supply of important parameters for the proper determination of the instant situation. Therefore, the parameters to monitor are presented in Table 1.

The UAV solution for the architecture described can be a quadcopter, i.e., DYS D800 X4 Professional Multi-Rotor [19]. It has a maximum payload of up to 6.5 kg, which allows porting of several types of sensors. Flight time—up to 15 min. A platform NVIDIA Jetson [20] can be used to build the Artificial Intelligence application that will process the data provided by the sensors.

Another UAV solution candidate is Phantom2 [21]. Having a lower price, it provides higher flight time—up to 25 min. However, its maximum payload is only 1 kg.

Third candidate is a piloted quadcopter, with the A3-PRO flight controller [22]. Its flight time is 22 min, maximum payload is 1 kg, and its max speed is 22 m/s. Its advantages are the different available development platforms (Linux, ROS, QT) and the different programmable functionalities available.

The thermal camera is useful for detecting people in low visibility conditions (total darkness, fog, or smoke). It can see through smoke or light mist, it does not require additional lighting, the image being obtained due to temperature differences between the target object and the environment. The model FLIR LS-X can be a solution for project objectives [23]. It has a high resolution LCD display (640 × 480), good optical characteristics (spectrum: 7.5–13.5 μm, thermal sensitivity: <50 mK, Digital Detail Enhancement algorithm for image processing). Its operating time is between 4 and 6 h, at temperatures -20 to $+50$ °C.

As infrared sensor candidate can be used the ML8540 sensor [24]. It has a medium resolution (48 × 47).

Air pollution sensor is useful for gas detection (i.e., smoke detection).

Wearable sensors are used to monitor vital parameters of police agents and a wearable camera. Furthermore, system can use the data provided by a rugged smartphone. This way, the monitoring system relies on a numerous set of different types of sensors. The volume and complexity of data supplied by these sensors dictates the necessity to develop a data fusion algorithm, which will collect, serialize, and normalize the data, and pass it forward into the system pipeline.

6 Conclusions

WITNESS provides an opportunity for companies to increase the competitiveness of the WSN (wireless sensor network) industry by developing novel sensors so far never exploited in this field.

One of the project objectives is the definition of tools, technologies, and methods that will facilitate the countering to attacks and critical situations. This study will lead to some conclusions about the state-of-the-art resources and, hopefully, to the definition of new methods that will improve the ability to develop a monitoring solution in short time. The results obtained will be used in further stages of the WITNESS project.

Acknowledgements This research is sponsored by the NATO SPS Programme under the funding NATO SPS G5437—WITNESS—Wide InTegration of sensor Networks to Enable Smart Surveillance.

References

1. Wilson, D. (2012). Military surveillance. In *Routledge handbook of surveillance studies*. London: Routledge Taylor & Francis Group.
2. Sayantani, S., & Sarmistha, N. (2014). A case study on smart surveillance application system using WSN and IP webcam. In: *Proceedings of Applications and Innovations in Mobile Computing (AIMoC)*, Kolkata. ISBN: 978-1-4799-3880-3.

3. Hampapur, A., Brown, L., Connell, J., Pankanti, S., Senior, A., & Tian, Y. (2003). Smart surveillance: Applications, technologies and implications. In: *Fourth International Conference on Information, Communications and Signal Processing, 2003 and the Fourth Pacific Rim Conference on Multimedia, Proceedings of the 2003 Joint*, Singapore. ISBN: 0-7803-8185-8.
4. Prabhu, S., Xiaoyong, S., Harish, R., Chi-Cheng, C., & Rajit, G. (2006). WinRFID a middleware for the enablement of radio frequency Identification (RFID) based applications. In: R. Shorey, M. C. Chan, W. T. Ooi, & A. Ananda (Eds.), *Invited chapter in mobile, wireless and sensor networks: Technology, applications and future directions*. New York: Wiley.
5. *MobiTeC-open source RFID middleware 1.0. Mobile technology center*. http://mobitec.ie.cuhk.edu.hk/rfid/middleware/. Accessed 24 Sept 2018.
6. *AspireRFID OW2 project*. https://projects.ow2.org/view/aspire-rfid/. Accessed 24 Sept 2018.
7. Dimitropoulos, P., & Soldatos J. (2010). RFID-enabled fully automated warehouse management: Adding the Business Context. *International Journal of Manufacturing Technology and Management, 21*(3/4), 269–288.
8. *Fosstrak: Open Source RFID software platform*. http://www.fosstrak.org. Accessed 24 Sept 2018.
9. Floerkemeier, C., Roduner, C., & Lampe, M. (2007, December). RFID application development with the Accada middleware platform. *IEEE Systems Journal, 1*(2), 82–94.
10. Shu, Y., et al. (2014). *International Electrotechnical Commission: White Paper: Internet of Things: Wireless Sensor Networks: Wireless Sensor Networks Project Team*, Geneva (p. 78). http://www.iec.ch/whitepaper/pdf/iecWP-internetofthings-LR-en.pdf. Accessed 24 Sept 2018.
11. *MoteWorks getting started guide. Revision G* (2012, March). *Massachusetts: MEMSIC*. http://www.memsic.com/userfiles/files/User-Manuals/moteworks-getting-started-guide.pdf. Accessed 24 Sept 2018.
12. Ritter, H. (2018). *Short presentation of ScatterWeb software and hardware for next generation wireless networks*. http://files.messe.de/cmsdb/001/14916.pdf. Accessed 24 Sept 2018.
13. Chatzigiannakis, I., Mylonas, G., & Nikoletseas, S. (2005). jWebDust: A java-based generic application environment for wireless sensor networks. In: *Proceedings of the First International Conference on Distributed Computing in Sensor Systems (DCOSS 05)* (pp. 376–386).
14. Aberer, K., Hauswirth, M., & Salehi, A. (2006) *The global sensor networks middleware for efficient and flexible deployment and interconnection of sensor networks*. LSIR Report 2006-006.
15. Berrahal, S., Kim, J., Rekhis, S., Boudriga N., Wilkins, D., & Acevedo J. (2016, March). Border surveillance monitoring using Quadcopter UAV-Aided wireless sensor networks. *Journal of Communications Software and Systems, 12*(1), 67–82.
16. Borah, D. R., Debnath, L., & Gogoi, M. (2016). A review on Quadcopter Surveillance and Control. *Journal of Engineering Technology, 4*(1), 116–119. ISSN: 2348–7305.
17. *Country reports on terrorism 2016*. https://www.state.gov/j/ct/rls/crt/2016/. Accessed 24 Sept 2018.
18. *Global terrorism index 2016*. http://economicsandpeace.org/wp-content/uploads/2016/11/Global-Terrorism-Index-2016.2.pdf. Accessed 24 Sept 2018.
19. *DYS D800 X4 professional multi-rotor package for aerial photography and heavy lift*. https://www.unmannedtechshop.co.uk/dys-d800-x4-professional-multi-rotor-package-for-aerial-photography-and-heavy-lift-pnf/. Accessed 24 Sept 2018.
20. *NVIDIA Jetson TX2 module*. https://developer.nvidia.com/embedded/buy/jetson-tx2. Accessed 24 Sept 2018.
21. *Phantom 2 specifications*. https://www.dji.com/phantom-2. Accessed 24 Sept 2018.
22. *A3-PRO flight controller*. https://www.dji.com/a3. Accessed 24 Sept 2018.
23. *Tactical Handheld thermal monocular FLIR LSX model LS-X*. https://www.flir.com/products/lsx-r/. Accessed 24 Sept 2018.
24. *Lapis semiconductor infrared image sensor (IR sensor) ML8540*. http://www.lapis-semi.com/en/semicon/sensor/ir-sensor.html. Accessed 24 Sept 2018.