Wireless sensor network for mobile surveillance systems

Gert J.A. van Dijk[a], Marinus G. Maris[b]
Networked Embedded Systems department
TNO Physics and Electronics Laboratory
Oude Waalsdorperweg 63
2509 JG, The Hague, The Netherlands

ABSTRACT

Guarding safety and security within industrial, commercial and military areas is an important issue nowadays. A specific challenge lies in the design of portable surveillance systems that can be rapidly deployed, installed and easily operated. Conventional surveillance systems typically employ standalone sensors that transmit their data to a central control station for data-processing. One of the disadvantages of these kinds of systems is that they generate a lot of data that may induce processing or storage problems. Moreover, data from the sensors must be constantly observed and assessed by human operators. In this paper, a surveillance concept based on distributed intelligence in wireless sensor networks is proposed. In this concept, surveillance is automatically performed by means of many small sensing devices including cameras. The requirements for such surveillance systems are investigated. Experiments with a demonstration system were conducted to verify some of the claims made throughout this paper.

Keywords: Sensor networks, security, surveillance, unattended sensors.

1. INTRODUCTION

With increased technological developments, the demand for advanced security systems rises accordingly. In particular, mobile and unmanned surveillance systems have become a main focus. Such systems can easily be transported and quickly installed. At the same time, there is a tendency to reduce the number of personnel for maintenance and system operation. Hence, although a person is still required in the loop for final decision making, some traditional surveillance tasks can be taken over by unmanned surveillance systems. Typical tasks include support for securing compounds in hostile environments including protection of weapon storage depots and health monitoring, protection of provision routes, protection of forces in harbours, and monitoring activities of enemy troops.

In general, the desired functionality of an unmanned surveillance system is to provide situational awareness about the observed area. With situational awareness, hostile intrusions can be detected and assessed at an early stage to provide ample time to prepare countermeasures. However, military operations often take place in dangerous and unstructured terrains, which implies that the security systems cannot rely on local infrastructure. Conventional surveillance and security equipment is usually not suited for such demanding applications. They are typically based on the use of stand-alone sensors. A fundamental drawback of such systems is that they generate large amounts of data which imposes high demands on storage and processing, moreover they require continuous attention from human personnel.

For the protection of military compounds, a number of solutions currently exist. One solution is to bury mines around the compound. However, in peace-keeping operations (as mainly considered here) mines are not allowed. Another type of signalling method uses trip-wires. These can easily be detected and avoided by intruders. Therefore, trip-wires are not suitable for compound security. Yet another type is the battle-field radar. Battlefield radar is hardly mobile, difficult to install and to operate. It requires a high workload with specially trained operators and is very expensive. Furthermore it is rather vulnerable. Elimination of one device will make further observation

Unmanned/Unattended Sensors and Sensor Networks,
edited by Edward M. Carapezza, Proceedings of SPIE Vol. 5611
(SPIE, Bellingham, WA, 2004)0277-786X/04/$15 · doi: 10.1117/12.578046

impossible (single point of failure). Even (IR) cameras suffer from the fact that they require continuous human attention.

Generally speaking, most military systems suffer from similar shortcomings, in particular limited battery life time, single-point-of-failure, difficult to install, demanding specific know-how of trained personnel and continuous personnel attention (the concentration and attention level of a human operator will reduce typically strongly after only 20 minutes).

In this paper an alternative approach is described. Instead of on a single sensor, many small and light weight wireless sensor nodes are used, together forming a network. Wireless sensor networks have recently come within reach of practical applications due to new technological developments, particularly in the area of miniaturisation and device communication. These developments have enabled the creation of small devices consisting of a micro-controller, a radio front-end, a power supply and one or more sensors capable of sensing the environment. A number of such devices can together form a wireless sensor network.

In sensor networks, the nodes can communicate and cooperate with each other. An effective approach is to program the nodes such that they aid in interpreting their own data and present the extracted information to the operator. In this way, the operator has better situational awareness and consequently is better able to respond to the received information. Elimination of one of the nodes will not result in a break-down of the entire security system, but will only result in a marginal deterioration of the system's performance (graceful degradation). In addition, inter-sensor communication can reduce the vulnerability to false alarms. In that case, sensors that cover a large area can discuss and negotiate about the state of the object(s) they detect. Discrimination between different objects contributes to the prevention of false alarms.

A typical application of a large scale sensor network is the protection of premises or military compounds. For example, a compound for peace-keeping forces must be protected at all times. In such a case, it is vital that the area around the compound constantly monitors for intrusions and other threads. Suppose a large sensor network is employed, where each sensor can detect movement and knows its own position. The sensors are placed such that they can monitor the surrounding area in a satisfying manner. Because of the large number of sensors, it is impossible to send all information to a central node. Therefore, we need a system that performs local information extraction and information fusion.

The development of such cooperating systems for the gathering of information is one of the main topics of research within TNO. The research focuses on the combination of advanced wireless sensor networks with distributed sensor fusion methods. The work presented in this paper is part of this ongoing research. The challenge is to create cooperating sensor networks that can function without using a central control station while still processing information extracted from the environment.

2. RELATED WORK

Several research groups have identified the need for cooperating, information gathering systems as well. For example, wireless sensor systems have been discussed for tracking vehicles in a field[1] rather than for use in compound security. The problem of 100% field coverage by sensors[2] has also been discussed. Our question is whether 100% field coverage is always required. We tend to assume that this is not really necessary in multi-sensor object tracking systems. The relationship between data-aggregation and energy consumption[3] has also been touched upon. In the author's view, several nodes in the network should be used to fuse data from other sensor nodes. An optimization scheme provides overall energy consumption. We take the stance that local information processing should be optimized such that information fusion at other sensor nodes can be minimal. In another paper the author presents a system for multi-hop routing[4]. In many sensor network applications this is an important issue. However if used for sending signals over a large distance, for compound security that may not be very relevant, since the observed area is typically small enough such that all sensor nodes are within reach of each other.

Most research institutes are involved in the fundamental research on distributed sensor networks and systems. TNO aims to put more emphasis on the practical aspects of wireless sensor networks and has expertise in the different technology fields involved. In this article, compound security is discussed. In section 3 the typical system requirements will be discussed. Then, in section 4 our approach towards designing a system that meets those requirements will be presented, followed by a description of an experimental implementation in section 5. Finally, a discussion about this approach is given.

3. SYSTEM REQUIREMENTS

In this section, requirements for a compound security system are presented. For clarity, a compound security system is composed of a number of wireless communication nodes, each with one or more sensors attached. The type of sensor may vary per node. The nodes communicate and cooperate and must be able to operate in an outdoor environment for a long time.
The main requirements of such a system are listed below.

- **Rapid and easy deployment and installation**

In many situations, time to install a security system is limited. We assume a target installation time of 1 hour. Hence, light and wireless sensors that don't need cables to operate are strongly preferred.

- **Simple operation**

The system should not place many requirements on the type of operator (like training or special skills) and present clear information to the operator.

- **Robustness**

The system should be reliable and robust, in the sense that the system is still operational if some components do not function properly (graceful degradation).

- **Easy transportation**

The system should be easily transportable. This puts constraints on the size and weight of the system components.

- **Low occupancy of personnel**

The workload of the personnel should be minimal. This implies that the system has to operate partly autonomously. (Preferably only 1 person needed).

- **Self configuration**

The system must be capable of configuring itself, for example if a node is no longer active, an alternative routing path must be found. Ideally, the sensor nodes possess self-localisation capabilities to provide position information to the rest of the network.

- **Low false alarm rate**

The applicability of a surveillance system depends on its detection reliability. If there are many false alarms, personnel will not trust the system any more. Furthermore, false alarms demand a lot of effort from personnel. Of course, reduction of the false alarm rate may never be at the expense of reliability of the system.

- **Object discrimination and classification**

The system should be able to report the presence of people and vehicles, but ignore small animals. Therefore, discrimination between different objects is required.

- **Scalability**

The system must be scalable, i.e. it must be extendable with additional sensor nodes without much reconfiguration effort. In the ideal case, new devices automatically join the network.

- **Long (device) life-time**

Long lifetime is required in order to prevent the need for replacing batteries during operation. Low-power electronics and algorithms will help to realize this (target: 6 months autonomous operation).

- **Stealthiness**

Stealthiness is an important feature in order to prevent the opponent to detect and manipulate the surveillance system. Stealthiness of the physical components can be realized by applying specific housing. The detection of the transmitted signals is more difficult to prevent. Encryption needs to be used to avoid intrusion from hackers.

- **24 hour surveillance**

Besides the need for long battery endurance, fulltime operation (24 hour) requires that the security system stays operational during the replacement of modules that are defective or have run out of batteries.

- **Compatibility with existing systems**

The system should be able to cooperate with existing battle management and surveillance equipment of different military units. This puts demands on the type of platform and/or data-communication and protocols between the different systems.

- **Verification of alerts.**

By applying existing surveillance equipment like (IR) cameras, an alert can be verified before taking actions.

With the above requirements it is possible to come to the design of an autonomous surveillance system.

4. PROPOSED SYSTEM APPROACH

In this section a system approach for a compound surveillance, that can meet the system requirement mentioned in section 3, is proposed.

At TNO, several years of research have been focussed on the development of so-called Networked Intelligent Devices (NIDs). These are cooperating devices that share knowledge and negotiate about tasks and observations. This work has resulted in numerous applications. The most notable that we have presented described an autonomous cooling system on Navy ships[5]. Recently, TNO decided to move into the field of wireless sensor networks and to create its own system, since the combination of NIDs with wireless sensor technology is most promising.

The challenge is to combine the physical infrastructure of the wireless sensor network with suitable sensor fusion techniques in such a manner that the human operator receives enhanced situational awareness from the system. To accomplish this, the sensor nodes have to be positioned at strategic locations and communicate their extracted information to each other. This means that the sensor nodes must contain mechanisms for extracting useful information from their data. Useful information may be “motion detected” or even “human detected”. This kind of information is useful for other sensor nodes. This approach contrasts to more traditional solutions that focus on overlapping raw sensor data sets.

As stated above, information from one sensor node is sent to other sensor nodes. Each node belongs to a group of sensor nodes that fuse information related to a particular type of observation. The advantage of such “horizontal” communication is that better extraction of locally available information can be achieved. This is because the sensor

group can make assessments of the desired information hidden in their data. Particularly when sharing information between sensors, the reliability of such assessments can be greatly improved. Therefore, sensor networks implicitly posses the capability to deliver enhanced situational awareness to a human operator. Clearly, this is a substantial improvement compared to the previously mentioned data generation method in traditional multi-sensor systems.

We focus on exploiting heterogeneous sensors for security applications. There are two sensor groups proposed in our system. In one group, there is a number of motion detectors. They report object motion information to the camera group. The cameras pan towards the location(s) indicated by the motion detection group. With such a setup, the sensors can communicate directly with each other without the use of a central control system. Such a decentralized approach vastly increases the configuration flexibility and the number of sensors that may be used. Moreover it prevents a single point of failure, namely the central control node itself.

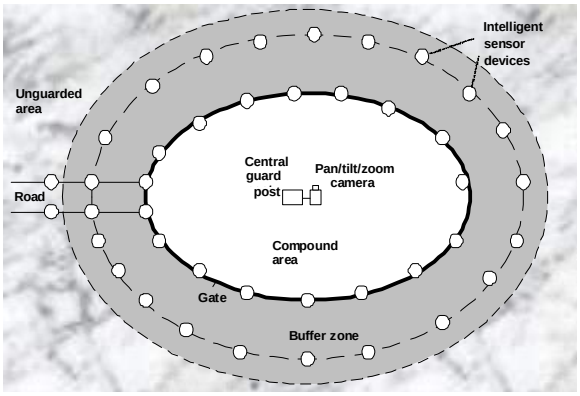

Figure 1. Basic Compound Security System

5. EXPERIMENTAL SETUP

To evaluate the surveillance concept described in the previous section, four wireless sensor nodes with passive infrared (PIR) sensors were placed on posts to detect motion (see Figure 2). A pan/tilt/zoom video camera was used for tracking and verification purposes, and a monitoring station containing the user interface for displaying status messages and camera images. The PIR detectors were placed in a row. The camera was placed in such a manner that it could observe the part of the area covered by the motion detectors. If one of the motion sensors observed movement, the camera would move and zoom to focus on the location indicated by that sensor. Therefore, the potential orientations of the camera had to correspond with the positions of each particular sensor. These orientations were coded prior to the experiments. Hence, the camera control software selected one out of four possible pan/tilt/zoom parameter settings. If no motion was detected, the camera would zoom out to provide an overview of the area. Other features include the capability to detect broken or removed nodes. This was implemented by monitoring a “heartbeat” from the sensor-nodes.

During operation, the motion detection nodes can be in one of the following 5 states, a sensor node could be in: *Active*, *Motion detected*, *Motion has gone*, *Sensor node not yet available* and *Sensor node no longer available.* The operator was permanently informed about the state of each sensor which was indicated by distinct colours on the user interface. Furthermore the “live” camera images were visible on the screen (see Figure 4). Several experiments with this setup have shown that that the system is able to reliably detect and track persons.

Figure 2. One PIR sensor and camera wireless node mounted on posts.

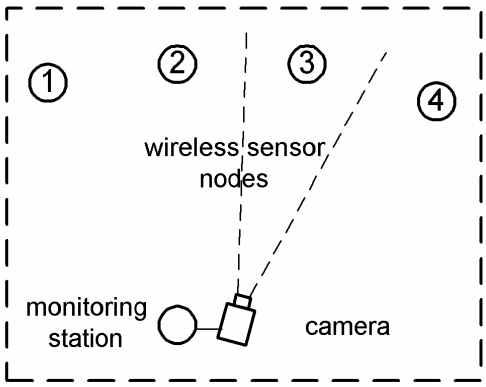

Figure 3. Experimental setup schematic

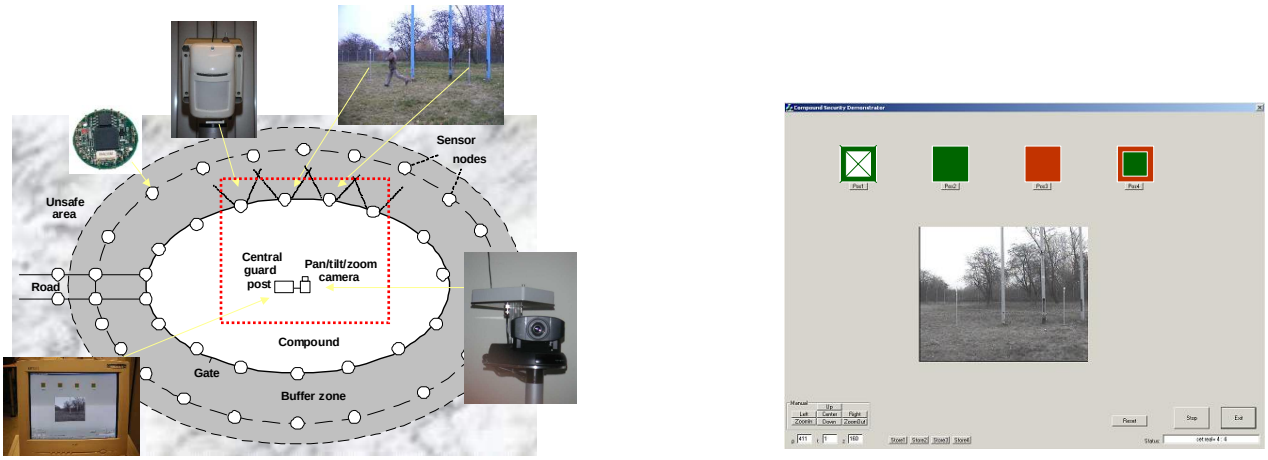

Figure 4. The demonstration system and user-interface

6. DISCUSSION AND FUTURE WORK

The experimental system presented in section 5 is an appropriate base system for evaluating intelligent sensor network technology and has proven to create applications, such as compound security support to detect and track intruders around a compound. However, before a true operational system can be developed, a number of extensions are still to be implemented. In section 2, a number of requirements were mentioned. The experimental system presented here, meets several of these requirements, but not all. From a network infrastructure point of view, some aspects that are still lacking are: low power operation, multi-hop routing and automated position estimation per node. Furthermore, operational requirements such as stealthiness and sensor-fusion are still to be improved.

At TNO, research is currently focusing on these issues. For example, in the SOWNet (Self Organising Wireless Networks) project a low power protocol (LP4) has been designed that reduces the current consumption of the circuitry to a level below the contribution of the battery leakage. Furthermore TNO has designed its own disposable sensor devices called TNOdes, that can randomly be distributed around a compound and can seamlessly join the network of the deployed sensor devices as described here.
Expectations are that soon most requirements will be met and that the system will be tested and evaluated in a true military setting.

7. REFERENCES

1. A. Arora et. al. “A line in the sand: A wireless sensor network for target detection, classification, and tracking”. *Technical report*, Ohio State University, 2003.
2. T. Yan et. al. “Differentiated Surveillance for sensor networks”. In *proceedings of the first international conference on Embedded networked sensor systems*, Los Angeles, CA. Nov. 2003.
3. B. Krishnamachari, D. Estrin, and S. Wicker, “Impact of Data Aggregation in Wireless Sensor Networks,” *International Workshop on Distributed Event-Based Systems*, Vienna, Austria, July 2002.
4. G.H. Ahn, A. T. Campbell, A. Veres, and L. H. Sun, “SWAN: Service Differentiation in Stateless Wireless Ad Hoc Networks,” *IEEE INFOCOM'2002*, New York, June 2002.
5. J.A.A.J. Janssen and M.G. Maris. “Self-Configurable Distributed Control Networks on Naval Ships”. In *proceedings of SCSS 2003*, Orlando, FL, 2003.

[a]G.vanDijk@fel.tno.nl; phone +31 70 3740602; www.tno.nl/instit/fel
[b]maris@fel.tno.nl; phone +31 70 3740593; www.tno.nl/instit/fel