Surveillance of mobile objects using coordinated wireless sensor nodes

Tony Larsson

DOI: http://dx.doi.org/10.1109/EFTA.2007.4416877
Copyright: IEEE

Surveillance of Mobile Objects using Coordinated Wireless Sensor Nodes

Tony Larsson
Halmstad University
Sweden
+46 35 167 168
tony.larsson@ide.hh.se

Abstract

Surveillance of mobile office assets is made by attaching wireless sensor nodes to assets and to their authorized users. The wireless sensor nodes are monitored via radio base access points connected to a distributed application framework for analysis and coordination of security events. By logic rules applied to the event information, temporarily stored and accessible in a distributed tuple space, security decisions, alarms and other actions are implemented.

1. Introduction

To simplify daily work an office should be as open as possible for employees and guests.

Security issues is traditionally dealt with by use of locks, keys, id-cards, passwords, active infra-red (IR) or passive infra-red (PIR) detectors. Such equipment for passage control or detection of motion patterns require proper placement. Video cameras with image recognition [1] can distinguish authorized persons but are regarded as intrusive from a personal integrity perspective.

In order to limit annoyance and intervention from a rigorous security system there is a need for solutions which, in a less awkward way, can identify suspicious events and behaviour patterns and prevent from theft.

Passive RFID tags, attached to assets, are used to identify and detect theft in shopping malls. This requires assets to pass close to a tag-reader due to their limited range often less than a meter. The reading can also be hindered by putting the tagged asset in a metal foil covered bag.

Surveillance using global positioning system (GPS), [2] is popular for tracking of larger assets such as boats, cars and containers where one can equip node with a processor, a GPS receiver and a wide area wireless link, such as GSM/GPRS or 3G. However, this is too energy ravenous and costly for small and cheap office assets.

For personal assets we need a solution that is both selective and that can work in an open environment visited by many persons and be yet less intrusive than video cameras from a personal integrity point of view.

Our solution, partly inspired by the active badge concept [3], is based on wireless sensor networks [4] used to detect and communicate location proximity or containment information combined with a middleware STITCH [5] for coordination of distributed activities.

The paper describes background and enabling technologies in section 2. Application solutions are presented in 3. Section 4 includes analysis, results and related work. Finally, the paper is summarized in 5.

2. Background

This work build on experiences from the “Open Secure Office” project [6] [7] [8] and from “T4 – Telematics for Totally Transparent Transports” [9].

2.1. Wireless Sensor Network Technology

Wireless sensor networks (WSN) consist of wireless sensor nodes, called motes, see figure 2.

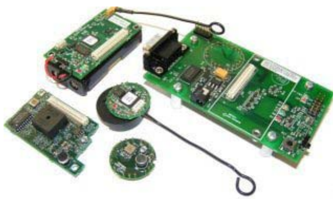

Figure 1. The hardware platform.

Motes are small miniaturized devices equipped with one or more sensors and/or actuators, a processor, memory and a low-power radio transceiver. As many others we used the Berkeley Mica2 and Mica2dot [10] and wrote NesC programs [11] supported by the TinyOS [12] since it meet basic requirements on the hardware, development and run-time software support.

2.2. Coordination Middleware

The solutions used a middleware STITCH – to coordinate events received from different networks via base stations, see figure 1.

1-4244-0826-1/07/$20.00 © 2007 IEEE

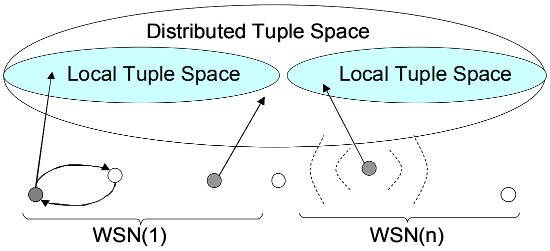

Figure 2. Events sent from sensor networks to the distributed tuple space on which rules for coordinated alarm decisions are applied.

STITCH is a tuple-space[1] technique [13], based on CLF/Mekano [14]. Resource managers control how tuples are inserted to, read and removed from a *resource* component. Tuples are made available via component services. Interaction among components is managed by specific *coordinator* components encapsulating *rules* stating conditions on resources in one component that trigger creation or change of resources in another. In our investigated solutions STITCH simplifies detection and coordination of security events received from more than one sensor network placed in different offices or floors. The following is an example of a rule:

```
['Asset_mote','isMoving']('true');
['Personal_mote','isAuthorized']('false')
  <>-
['AlarmSystem','triggerAlarm']('true').
```

3. Solutions

In this section alternative solutions for keeping track of the relation between assets and users are presented.

3.1. Location Area Containment

In this solution authorized users and assets equipped with motes are detected when contained in an area covered by a base station. If an asset is moved to an area together with its owner it is supposed to remain there or be moved from there only if it is in close proximity of its owner or other authorized person. An asset can be left alone but must then stay where it is. This requires base stations to cover and periodically poll the location areas. The coverage range can be dimensioned versus security requirements by the number of base stations and selection of signal strength threshold levels.

3.2. Location Proximity

To potentially save energy and still enable mobility in sparsely covered areas asset motes can be equipped with an accelerometer to detect if it is moved and then wake up the radio to check if it is in risk trying to get in contact with the user's personal mote, see figure 3.

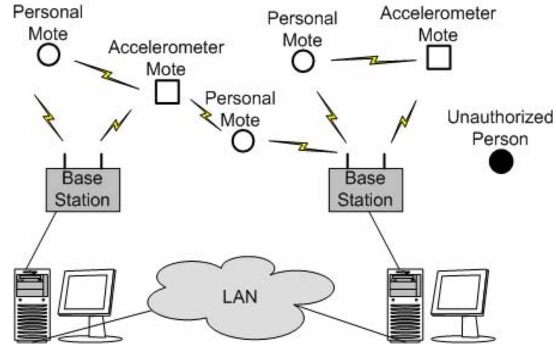

Figure 3. The different network nodes used in the open secure office solution.

If an asset is moved, it will send a notification to the user's personal mote. If acknowledge is not received it will send an alarm to a base station. If an asset mote can not reach its user or a base station it will send the alarm repeatedly[2] until it is reset. To make it robust the alarm is relayed and received by any other asset, personal motes or base station in range; flooding the network until all reachable nodes has been reached. To save energy one can limit the flooding by location based addressing. If an asset is moved it will be detected by the user's personal mote or other motes or when it approaches an exit covered by a base station, see figure 4.

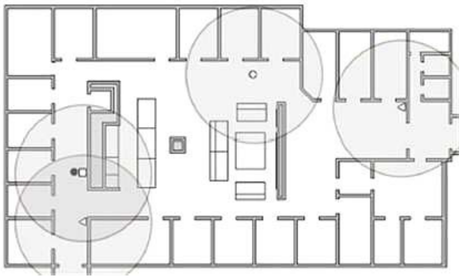

Figure 4. Thief (black dot) with asset (white circle) in range of a base (white triangle).

3.3. Location Proximity and Area Containment

In this solution proximity checks are combined with "I am alive" and containment checks communicated to the system via base stations. The security logic rules assert that: If a related asset and user are in contact in contiguous time and either of them can reach a base all is fine; else if asset and user can send "I am alive" to the same base (or other neighbouring bases) all is fine. The cooperation between an asset mote and an authorized user mote is supported by base stations covering important location areas integrated via the coordination framework.

[1] Tuple space techniques, in general, share many ideas with blackboards, real-time databases and concurrent objects.

[2] As a complement a piezoelectric beeper can send a sound signal.

4. Analysis

In this section pros and cons of the solutions and some remaining research problems are discussed.

4.1. The Coordination Framework

The use of a distributed coordination framework to integrate sensor networks covering different areas, adds overview of the security event information. It also makes it easy to add new features. Notifications to authorized users can be handled and sent in different ways depending on if the user is in the area or not. Extending the logic enables granting access to copying machines, turning on and off lights as the owner moves around in the office. Using the distributed coordination framework further enables local decisions to be made when more global coordination is not needed.

4.2. Combining Proximity and Containment

By combining proximity and containment checks a reliable and energy efficient solution is achieved. One or more WSNs can be attached via the coordination framework. There is no need to have coverage over an entire office area to implement acceptable surveillance. Though, the base stations must be properly placed, e.g. close to exits, to ensure that no mote leaves an area without having been able to send stored notifications. Further, the accelerometer, used to detect motion events and trigger proximity checks enables to extend the "I am alive" interval used for containment checks, uses much energy when active and the mote is also forced to send alarm notifications until any has reached the coordination framework before the alarm state can be reset. Location area containment leaves out the need for accelerometers but instead requires frequent polling or "I am alive" notifications as well as more base stations.

4.3. Experiment Results

To analyse the solutions three experiment scenarios were set up and performed in our own office spaces with a few motes and users; hence more tests should be made in other settings and in a larger scale.

Scenario 1 checks that the owner gets an alarm when an accelerometer mote equipped asset is moved, even in cases when the asset is out of range (10-40 meters) of an owner. This test also assures that the alarm message can be relayed to the owner via multi-hop broadcasting.

Scenario 2 verifies that the accelerometer mote must not be within direct range of a base station when an asset is moved illegally. This requires that a node can relay information indirectly via other nodes and also pervasively will send notifications until the node passes another node that can take care of the alarm.

Scenario 3 catches weaknesses of the system when an owner is within radio range of his asset but still can not see it physically due to a hiding wall or similar. To cause attention the owner's personal mote can send a discreet beep sound when the equipment is moved.

Though, the security logic has been analysed through variations of these scenarios in different physical spaces there are many potential situations of a malicious nature remaining to be verified. One can envision a thief that tries to move the equipment slowly or quickly and possibly get by, or tries to hide it from radio based detection by using a metal foiled enclosure. Security holes like these can be reduced by regular or random interval system sanity checks.

4.4. Dependability Issues

A surveillance network must be dependable. The system itself must be monitored that it is working. Logic rules with access to security events via the coordination framework make it possible to detect malicious behaviour patterns also when sensor nodes have failed to work, for example due to lack of battery energy or if it is hindered. If an asset mote is failing it is detected by lack of "I am alive" messages and the owner is alerted.

It is necessary to check that messages arrive within time limits, and that nodes are reachable by probes sent regularly, this especially when motes are put in sleep mode and only wake up sparsely on the occurrence of security events. Activation must be controlled by a synchronized clock time period or the nodes have to be waked up by a beacon signal. The timer period waking up the processor must be long, 1-5 seconds, and the active duty interval short, 5-10 ms, to save energy and yet the period short and the duty interval long enough to enable detection of susceptible patterns.

In order to make the system robust and to limit communication sensor data can be locally assessed, filtered and sanity checked against predefined thresholds and time intervals. This requires proper selection of measurement periods, interval lengths, threshold levels and filter functions. An accelerometer requires much energy when active, and thus needs to be turned on and off with a suitable duty ratio. But can be replaced by a simpler tilt/motion detector to turn the mote from sleep to active mode when moved.

A reason for allocating more of decision and configuration knowledge to motes is to increase battery lifetime by decreasing the need for radio communication. A drawback with this is that the advantage of centralized management is lost. It is however possible to change the configuration information even if it is located in the motes, but remote configuration raise demands on authentication and security over the radio links.

4.5. Related Work

Surveillance using wireless communication of alarm messages and compressed video streams is discussed in [15]. The energy needed for local signal analysis and compression is compared to the cost of moving the video data to a central processing node. In [16] wireless sensor devices to detect and track the positions of moving vehicles in an energy efficient way to enable sufficiently long unmanned military surveillance missions are investigated. In [17] neighbour monitoring, local decisions and coordination of decisions among neighbours of the surveillance system itself are discussed. ZebraNet [18] is a WSN for monitoring, logging, and tracking of wild animals, e.g. their position in the territory. It floods data to neighbours via short distance radio and then aggregate and relay this data via long distance radio to sparsely located base stations. System architecture, routing and duty cycle issues for monitoring of habitat climate and utilization using a WSN solution, called ESS, are discussed in [19]. CodeBlue [20] is a WSN for used both inside a hospital and in field. It supports transferring of medical data, e.g. from patients at an accident to the hospital without loss, using filtration and aggregation of events seen as a monitoring and prioritization process.

5. Conclusions

Surveillance using coordinated WSN enables valuable mobile assets to be used in open environments by employees and visitors and does not interfere with user integrity or equipment use. The energy efficiency can be improved but is promising allowing reasonable battery size and lifetimes; and needed hardware is affordable when produced in volume. However, to make this solution even more competitive there are things that can be improved, both at the system level and at the enabling technology level. Examples are the adaptation of the coordination middleware for embedded applications as well as more dependable and energy efficient low-duty-ratio motes for use in surveillance applications.

A pro with the proposed solution is that it can be selective when it comes to keeping track of authorized persons and their assets and almost blind about what the persons are doing. A traditional video based vision system that lacks abstraction simply sees too much.

Acknowledgements

This project was executed within CERES (Centre for Research on Embedded Systems) at Halmstad University supported by the Knowledge Foundation in Sweden, and Xerox Research Centre Europe.

References

[1] R. T. Collins et al. “Algorithms for Cooperative Multisensor Surveillance”, *Proceedings of the IEEE*, vol. 89, no. 10, pp. 1456-1477, October 2001.

[2] U. Leonhardt and J. Magee, “Multi-Sensor Location Tracking”, *MOBCOMP Int. Conf. on Mobile Computing and Networking,* pp. 203-214, Texas, October 1998.

[3] R. Want, A. Hopper, V. Falcao and J. Gibbons, “The Active Badge Location System, *ACM Transactions on Information Systems*, vol. 10, pp. 91-102, January 1992.

[4] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks", *IEEE Communications Magazine*, August 2002.

[5] D. Arregui, et al., “STITCH: middleware for ubiquitous applications”, *Smart Object Conference*, France, 2003.

[6] R. Andersson, M. Sandberg, and L. Urzuly, *The open secure office project – Wireless Sensor Network*, Master Thesis IDE0502, Halmstad University, Sweden, 2005.

[7] E. Nilsson, J. Olsson, and A. Ståhl, *Open secure office project - evaluating STITCH*, Master Thesis IDE0509, Halmstad University, Sweden, 2005.

[8] P. Srihari, *Open secure office project - Graceful Degradation in Distributed Embedded Systems*, Master Thesis IDE0508, Halmstad University, Sweden, 2005.

[9] T. Larsson et al., “T4 – Telematics for Totally Transparent Transports”, Proc. Int. IEEE Conf. on Intelligent Transportation Systems, Austria, September, 2005.

[10] J. L. Hill and D. E. Culler, 2MICA: a wireless platform for deeply embedded networks”, *IEEE Micro*, pp. 12-24, Nov.-Dec. 2002.

[11] D. Gay et al., “The nesC language: a holistic approach to networked embedded systems”, *Programming Language Design and Implementation*, June 9–11, USA, 2003.

[12] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler and K. Pister, “System architecture directions for network sensors”, *Proc. Architectural Support for Programming Languages and Operating Systems*, USA, 2000.

[13] N. Carriero and D. Gelernter, “Linda in context”, *Communications of the ACM*, vol. 32, no. 4, 1989.

[14] J-M. Andreoli, D. Arregui, F. Pacull, M. Riviere, J-Y. Vion-Dury and J. Williamowski, “CLF/Mekano: a framework for building virtual-enterprise applications, *Proc. Enterprise Distributed Object Computing Conference*, Germany, 1999.

[15] T. E. Boult, “Geo-spatial active visual surveillance on wireless networks”, *Proc. Applied Imagery Pattern Recognition Workshop,* Washington DC, USA, 2003.

[16] T. He et al., “Energy-efficient surveillance system using wireless sensor networks”, *Proc. Mobile Systems, Applications, and Services*, USA, June 2004.

[17] C-F. Hsin and M. Liu, “A distributed monitoring mechanism for wireless sensor networks”, *Proc. Wireless Security*, Atlanta, Georgia, USA, 2002.

[18] P. Juang et al., “Enery-efficient computing for wildlife tracking: design tradeoffs and early experiences with ZebraNet”, *Proc. Architecture Support for Programming Languages and Operating Systems*, San Jose, USA, 2002.

[19] R. Szewczyk et al., “Habitat monitoring with sensor networks”, *Communications of the ACM*, vol. 47, no. 6, pp. 34-40, June 2004.

[20] K. Lorincz et al., “Sensor networks for emergency response: challenges and opportunities”, *IEEE Pervasive Computing*, Oct-Dec 2004.