A Wireless Sensor Network For Border Surveillance

Denise Dudek, Christian Haas, Andreas Kuntz, Martina Zitterbart
Institute of Telematics
University of Kalrsruhe
dudek,haas,akuntz,zit@tm.uka.de

Daniela Krüger, Peter Rothenpieler, Dennis Pfisterer, Stefan Fischer
Institute of Telematics
University of Lübeck
krueger,rothenpieler,pfisterer,fischer@itm.uni-luebeck.de

Abstract

We will demonstrate a wireless sensor network system for the surveillance of critical areas and properties – e.g. borders. The system consists of up to 10 sensor nodes that monitor a small border area. The protocols we show focus on detecting trespassers across a predefined area and reporting the detection to a gateway node securely. There, the trespasser's path will be graphically diplayed on a border map. The demonstration features secure protocols for the detection of trespassers, node failure and network partitioning, along with a duty cycle protocol to ensure network longevity. All information pertaining to relevant events in the network or border area will be graphically displayed on a gateway computer.

Categories and Subject Descriptors

H.4 [**Information Systems Applications**]: Miscellaneous

General Terms

Security, Experimentation, Design

Keywords

Security, Area monitoring, Prototype

1 Motivation

Over the past years, wireless sensor networks (WSNs) and their applicability for a vast number of scenarios have been the focus of research worldwide. An interesting application scenario for WSNs is the domain of area monitoring systems. WSNs in this field can be used for the surveillance of critical areas such as borders, private properties or even rails. Their main objective is the detection and signalling of trespassers within a predefined area. Accessibility entails the presence of both malicious and non-malicious interference, thus imposing high demands regarding security and robustness in protocol design. Besides, the heavy restrictions in terms of power supply, memory capacity and processing power that are typical for WSNs imply the need for protocols efficient use of resources. The project FleGSens [3] realizes a WSN architecture for secure trespasser detection on green line borders. Our demonstrator shows a system for monitoring a small border area with up to 10 sensor nodes. It demonstrates the feasibility of our border monitoring system in a real world environment, running protocols for the detection of trespassers, node failure and partitions alongside a duty cycle protocol. As can be seen in Figure 1, the prototype was built and deployed in a public park in the city of Lübeck, Germany. The prototype has been extensively tested in an outdoor prototype consisting of 152 sensor nodes for monitoring a 300 m long and 20 m wide land strip.

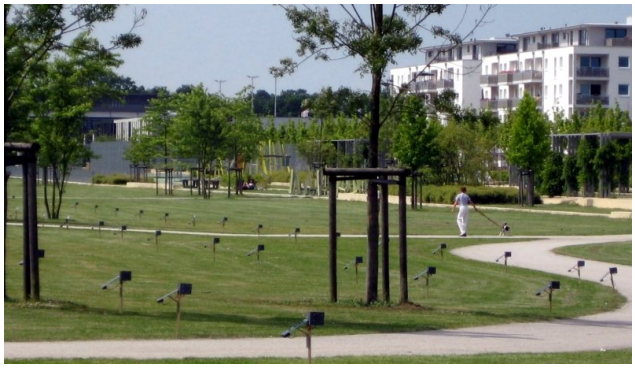

Figure 1. FleGSens Prototype in Lübeck

2 Demonstrator

For demonstration purposes, we built a small border monitoring system that is able to detect an illegal crossing of the monitored area. The demonstrator consists of up to 10 sensor nodes and 2 gateway computers which are used to control and manage the sensor network and to display possible trespasses, node failures and attacks on the network functionality. Each protocol that is shown in our demonstrator was designed and implemented according to a detailed security analysis within the scope of FleGSens. The security analysis has lead to an extension of the classical Dolev Yao [2] attacker that allows for a percentage of compromised nodes; this extended attacker model captures general and application-specific goals which a potential attacker would try to achieve. It thus defines the security hazards the demonstrated system must be able to defend against. We will show attacks on the network's functionality a potential attacker might perform in order to cross the border unrecognized. We demonstrate that the system is able to defend against the attacks successfully.

SenSys'09, November 4–6, 2009, Berkeley, CA, USA.
ACM 978-1-60558-748-6

2.1 Protocols

The protocols and mechanisms described in the following are part of our demonstration. They were specified according to the aforementioned attacker model. Protocol robustness was tested in simulations and real world scenarios accordingly. In order to detect an illegal crossing over the monitored area, a *trespasser detection protocol* has to be used. However, the successful detection of trespassers depends on full coverage of the monitored area. Therefore, it is necessary to detect the failure of nodes at runtime using a *node failure detection protocol*. Furthermore, it must be ensured that all messages arrive at their destination; alarm messages reporting a trespasser must reach at least one gateway. This can only be achieved if a path between any sending node and a gateway exists – which is not always the case once the network is partitioned. To detect and report partitioning of the network is the task of a *partition detection protocol*. Due to the limited capacity of the lithium ion battery and a requirement to guarantee network longevity, a *duty cycle protocol* managing sleeping and waking times of the nodes is necessary.

2.1.1 Trespasser Detection Protocol

A trespasser that moves within the range of a passive infrared (PIR) sensor creates a so-called *PIR event*. A PIR event is characterised by the timestamp of its registration and the location and ID of the node that detects the movement. The basic idea of the trespass detection protocol used in the FleGSens system is to collect PIR event messages locally before flooding an *aggregate* of local events into the network. This way, we can ensure resilience against sporadic PIR events caused by the environment – e.g. wind – and reduce the number of false alarms. Using message authentication codes (MACs), the gateway is able to detect forged or manipulated events, so that, on the whole, the attacker's possible influence is limited by the number and position of nodes they have compromised. During the demonstration, we will show how the trespasser's path is displayed on a border map at runtime, based upon the flooded aggregate reaching the gateways.

2.1.2 Node Failure Detection Protocol

The basic idea of the node failure detection protocol consists in the sensor nodes monitoring each other's liveness. To this end, they each send and listen for *heartbeats* from a set of nodes in their vicinity. This set of nodes – the monitoring node's *buddies* – is chosen randomly during network initialization. All messages contain a MAC for message integrity and authenticity protection and a timestamp to prevent an attacker from replaying messages to conceal a node failure. The buddies report the failure of a node given the absence of a preconfigured number of successively missing *heartbeats*. The *failure* message is then flooded to the gateway; there, the failed and reporting nodes are indicated on the border map. During our demonstration, we will switch off nodes arbitrarily and measure the time needed to detect the failure.

2.1.3 Partition Detection Protocol

It is the main idea of the Partition Detection Protocol that gateways periodically exchange messages and check if and via which nodes the message from the other gateway arrived. These messages – so called *ping messages* – are secured using an entry in a hash chain for each node that forwards the *ping message*. This way, we prevent the attacker from launching wormhole attacks in order to conceal a partition. The message body is secured using a MAC.

2.1.4 Duty Cycling

In order to minimize maintenance costs and maximize network lifetime, nodes alternate between two different operation modes: In sleep mode, only the PIR sensor is active, whereas in full operation mode, commands can be executed and messages sent or received. We use a TDMA medium access scheme that ensures non-varying energy consumption in terms of sending and receiving messages. This prevents exhaustion attacks such as the *sleep deprivation torture* attack.

2.2 Hardware

We use iSense sensor nodes [1] from coalesenses which are equipped with a JN5139 microcontroller and an IEEE 802.15.4 compliant radio interface with a data rate of 250 kbit/s and hardware AES encryption. We extended the core sensor node module by the Security Sensor Module comprising an AMN14112 PIR sensor which is capable of detecting moving objects in a 110° angle within a range of up to 15 m depending on temperature difference, speed and size of the objects.

3 Summary

This proposal presents a demonstrator for a wireless sensor network in a border monitoring scenario. The demonstrator represents a 10 node section of the 152 node outdoor prototype deployed within the FleGSens project. It shows the basic functionality of the network as well as its capability to defend against attackers. For this purpose, it runs protocols to detect trespassers, node failures and network partitioning alongside a duty cycle management to ensure network longevity. On the gateway computers, information pertaining to the state of the protocols is graphically displayed. Attendees at the workshop will be able to observe the border monitoring, node failures and attacks as well as the system's respective countermeasures.

4 Acknowledgments

This project was funded by the German Federal Office for Information Security (BSI).

5 References

[1] coalesenses. isense. `http://www.coalesenses.com`.

[2] D. Dolev and A. Yao. On the security of public key protocols. *IEEE Transactions on Information Theory*, 29(2):198–208, 1983. ISSN: 0018-9448.

[3] P. Rothenpieler, D. Krüger, D. Pfisterer, S. Fischer, D. Dudek, C. Haas, A. Kuntz, and M. Zitterbart. Flegsens - secure area monitoring using wireless sensor networks. In *Proceedings of the 4th Safety and Security Systems in Europe*, 2009. To appear.