Diss. ETH No. 18451

Safety-Critical Wireless Sensor Networks

A dissertation submitted to the

SWISS FEDERAL INSTITUTE OF TECHNOLOGY ZURICH

for the degree of Doctor of Sciences

presented by

Andreas Meier

Msc ETH in Electrical Engineering

born November 10, 1978

citizen of Luzern

accepted on the recommendation of

Prof. Dr. Lothar Thiele, examiner

Prof. Dr. Koen Langendoen, co-examiner

2009

Shaker Verlag, ISBN 978-3-8322-8563-0

Abstract

Safety-critical sensor networks are pervasively embedded in our surroundings. Such networks impose strong requirements in terms of reliability and latency of sensor readings and do for instance allow to monitor buildings for detecting fires and intrusions. The network requires a costly and cumbersome installation of wires for connecting the distributed sensors, which is sometimes not even possible. This suggests adopting the emerging technology of wireless sensor networks (WSN) to be used in a safety-critical context. With this technology, the wires connecting the sensors can be replaced by a radio and a battery pack.

A WSN is a collection of embedded sensor nodes with wireless networking capabilities. Collectively the sensor nodes establish a wireless ad-hoc network for transferring, processing and monitoring the sensed data. In order to ensure a small form factor, the sensor nodes are highly integrated and provide minor processing capabilities and limited memory. More stringent, the battery-powered nodes have to carefully orchestrate the power-hungry radio device if a yearlong independent operation is targeted. To make matters even worse, wireless communication is inherently unreliable and limited in range. Altogether this makes it a very demanding task to ensure a reliable, timely and energy efficient transport of the sensed data over possibly multiple hops.

Reliability is of utmost importance in a safety-critical environment. Additionally, there are often regulations imposing strong demands in terms of message latency and the availability of the sensor nodes. In particular, this thesis refers to the exemplary case of a wireless fire-alarm application, in which an alarm must be reported to a control station within 10 seconds, and a failed node has to be detected by the network within 5 minutes. These requirements are exacerbated by the fact that the nodes have to power off the radio more than 99% of the time, in order to enable an independent operation for several years with a small battery.

This thesis contributes towards adopting WSN technology for safety-critical applications. It focuses on communication aspects, and makes the following major contributions:

- The novel communication strategy, Dwarf, ensures a robust and timely forwarding of alarm messages, despite having the sensor nodes powered off most of the time. The maintenance protocol DiMo allows the monitoring of the nodes and the network topology with minimal communication overhead. In conjunction, Dwarf and DiMo enable safety-critical networking.
- This thesis contributes an analytical framework for analyzing and comparing WSN MAC protocols. The framework provides deep insight into the behavior of WSN MAC protocols and provides the first available solution for benchmarking. This provides the means for selecting the most suitable MAC protocol for an application at hand.
- This thesis contributes the NoSE protocol enhancement. NoSE allows for considerable energy savings while maintaining the sensor network and allows for a swift and dependable initialization. NoSE is beneficial for specialized applications and protocols like Dwarf and DiMo that are optimized for yearlong operation, but exhibit a reduced energy efficiency and responsiveness during maintenance and initialization.

Zusammenfassung

Sicherheitskritische Sensornetzwerke sind allgegenwärtig und werden beispielsweise eingesetzt um Brände oder Einbrüche zu detektieren. Solche Netzwerke erfordern eine zuverlässige Übermittlung der Sensormessungen mit einer minimalen zeitlichen Verzögerung. Bisher erforderte das eine aufwändige und kostspielige Verdrahtung der verteilten Sensoren. Es liegt daher auf der Hand, die neu entstehende Technologie der drahtlosen Sensornetzwerke auch für sicherheitskritische Anwendungen zu nutzen. Mit dieser Technologie können die Verbindungskabel der Sensorenknoten durch ein Funkmodul und eine Batterie ersetzt werden.

In einem drahtlosen Sensornetzwerk wird im Verbund ein Netzwerk aufgebaut, damit die Sensordaten transferiert und verarbeitet werden können. Um die Grösse und den Energieverbrauch zu minimieren sind die Sensorknoten hochintegrierte Systeme und verfügen daher nur über eingeschränkte Rechenleistung und Speicher. Zusätzlich ist es zwingend notwendig das Funkmodul als Hauptenergieverbraucher nur zu gezielten Zeitpunkten einzuschalten, um einen jahrelangen und unabhängigen Betrieb zu ermöglichen. Erschwerend kommt die Unzuverlässigkeit und limitierte Reichweite der drahtlosen Kommunikation dazu. Es ist daher eine äusserst schwierige Aufgabe einen zuverlässigen und energieeffizienten Datentransport innerhalb der vorgegebenen Zeit zu gewährleisten.

Zuverlässigkeit ist für sicherheitskritische Anwendungen von höchster Bedeutung. Zudem gibt es Vorschriften die Mindestanforderungen an die Latenz und Verfügbarkeit des Netzwerkes stellen. Diese Arbeit bezieht sich konkret auf das Beispiel eines Feuermeldenetzwerks mit der Vorgabe, ein detektiertes Feuer innert 10 Sekunden und einen beschädigten Sensorknoten innerhalb von 5 Minuten bei einer Kontrollstation zu melden. Diese Anforderungen werden verschärft, da das Funkmodul mehr als 99% der Zeit ausgeschaltet sein muss, um einen jahrelangen Betrieb ohne Batteriewechsel sicherzustellen.

Diese Dissertation befasst sich mit offenen Problemen, die es für die Anwendung drahtloser Technologie auf dem Gebiet von sicherheitskritischen Sensornetzwerke zu lösen gilt. Die Arbeit fokussiert sich auf das Themengebiet der Kommunikation und leistet folgende Hauptbeiträge:

- Mit der Kommunikationsstrategie Dwarf kann ein robustes und rechtzeitiges zustellen von Alarmnachrichten sichergestellt werden, auch wenn die Sensorknoten überwiegend ausgeschaltet sind. Das Überwachungsprotokoll DiMo stellt die kontinuierliche Überwachung der Knoten und der Netzwerktopologie sicher. Im Zusammenspiel ermöglichen Dwarf und DiMo sicherheitskritische drahtlose Sensornetzwerke.
- Diese Arbeit stellt ein analytisches Instrument für die Analyse und den Vergleich von MAC Protokollen für drahtlose Sensornetzwerke vor. Es ermöglicht einen tiefen Einblick in das Verhalten der Protokolle und bietet die erste verfügbare Lösung für Benchmarks. Damit ist es möglich das passende MAC Protokoll für eine bestimmte Anwendung auszuwählen.
- Mit der NoSE Protokollerweiterung kann das Sensornetzwerk energieeffizient unterhalten und zudem schnell und zuverlässig in Betrieb genommen werden. NoSE ist von besonderem Vorteil für spezialisierte Applikationen und Protokolle wie Dwarf und DiMo, die für einen langjährigen Betrieb optimiert sind, aber während dem Unterhalt und der Inbetriebnahme eine reduzierte Energieeffizienz und Ansprechverhalten zeigen.