Adaptive Multipath Key Reinforcement for Energy Harvesting Wireless Sensor Networks

Energy Harvesting - Wireless Sensor Networks (EH-WSNs) constitute systems of networked sensing nodes that are capable of extracting energy from the environment and that use the harvested energy to operate in a sustainable state. Sustainability, seen as design goal, has a significant impact on the design of the security protocols for such networks, as the nodes have to adapt and optimize their behaviour according to the available energy. Traditional key management schemes do not take energy into account, making them not suitable for EH-WSNs. In this paper we propose a new multipath key reinforcement scheme specifically designed for EH-WSNs. The proposed scheme allows each node to take into consideration and adapt to the amount of energy available in the system. In particular, we present two approaches, one static and one fully dynamic, and we discuss some experimental results.
Energy Harvesting Wireless Sensor Networks (EH-WSNs) represent an interesting new paradigm where individual nodes forming a network are powered by energy sources scavenged from the surrounding environment. This technique provides numerous advantages, but also new design challenges. Securing the communications under energy constraints represents one of these key challenges. The amount of energy available is theoretically infinite in the long run but highly variable over short periods of time, and managing it is a crucial aspect. In this paper we present an adaptive approach for security in multihop EH-WSNs which allows different nodes to dynamically choose the most appropriate energy-affecting parameters such as encryption algorithm and key size, providing in this way energy savings. In order to provide evidence of the approach’s feasibility in a real-world network, we have designed and implemented it as extension of on-demand medium access control (ODMAC), a receiver-initiated (RI) MAC protocol specifically designed and developed to address the foundational energy-related needs of Energy Harvesting Wireless Sensor Networks.


Energy Harvesting Wireless Sensor Networks (EH-WSNs) represent an interesting new paradigm where individual nodes forming a network are powered by energy sources scavenged from the surrounding environment. This technique provides numerous advantages, but also new design challenges. Securing the communications under energy constraints represents one of these key challenges. The amount of energy available is theoretically infinite in the long run but highly variable over short periods of time, and managing it is a crucial aspect. In this paper we present an adaptive approach for security in multihop EH-WSNs which allows different nodes to dynamically choose the most appropriate energy-affecting parameters such as encryption algorithm and key size, providing in this way energy savings. In order to provide evidence of the approach's feasibility in a real-world network, we have designed and implemented it as extension of on-demand medium access control (ODMAC), a receiver-initiated (RI) MAC protocol specifically designed and developed to address the foundational energy-related needs of Energy Harvesting Wireless Sensor Networks.

Given the continuous advancements in the technology of energy harvesting over the last few years, we are now starting to see wireless sensor networks (WSNs) powered by scavenged energy. This change in paradigm has major repercussions not only on the hardware engineering aspects, but also on the software side. The first protocols specifically designed to take advantage of the energy harvesting capabilities of a network have just recently appeared. At the same time, security remains one of the central points of WSNs development, because of their intrinsically unreliable nature that combines a readily accessible communication infrastructure such as wireless data exchange, to an often likewise readily accessible physical deployment. This dissertation provides a comprehensive look at how security can be improved by what energy harvesting has to offer. The main question asked is whether or not it is possible to provide better security in a WSN, by being aware of the fact that the amount of available energy is not going to monotonically decrease over time. The work covers different aspects and components of a WSN and focuses on what is arguably one the most important ones, medium access control (MAC) protocols. An energy-harvesting specific MAC protocol is introduced together with a related security suite. A new attack relevant to a whole class of MAC protocols is also introduced, along with a scheme that defeats it. A security approach for MAC protocols is discussed to provide an energy-aware solution. In order to address security bootstrapping, a new energy-adaptive key reinforcement scheme is presented. Finally an implementation and some experimental results are provided.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Embedded Systems Engineering
Authors: Di Mauro, A. (Intern), Dragoni, N. (Intern)
Number of pages: 144
Publication date: 2015

Publication information
Place of publication: Kgs. Lyngby
Publisher: Technical University of Denmark (DTU)
Original language: English

Series: DTU Compute PHD-2014
Number: 349
ISSN: 0909-3192
Main Research Area: Technical/natural sciences
Electronic versions:
phd349_Mauro_AD.pdf
Publication: Research › Ph.D. thesis – Annual report year: 2015

Receiver-initiated medium access control protocols for wireless sensor networks

One of the fundamental building blocks of a Wireless Sensor Network (WSN) is the Medium Access Control (MAC) protocol, that part of the system governing when and how two independent neighboring nodes activate their respective transceivers to directly interact. Historically, data exchange has always been initiated by the node willing to relay data, i.e. the sender. However, the Receiver-Initiated paradigm introduced by Lin et al. in 2004 with RICER and made popular by Sun et al. in 2008 with RI-MAC, has spawned a whole new stream of research, yielding tens of new MAC protocols. Within such paradigm, the receiver is the one in charge of starting a direct communication with an eligible sender. This allows for new useful properties to be satisfied, novel schemes to be introduced and new challenges to be tackled. In this paper, we present a survey comprising of all the MAC protocols released since the year 2004 that fall under the receiver-initiated category. In particular, keeping in mind the key challenges that receiver-initiated MAC protocols are meant to deal with, we analyze and discuss the different protocols according to common features and design goals. The aim of this paper is to provide a comprehensive and self-contained introduction to the fundamentals of the receiver-initiated paradigm, providing newcomers with a quick-start guide on the state of the art of this field and a palette of options, essential for implementing applications or designing new protocols.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Embedded Systems Engineering, Technical University of Denmark
Authors: Fafoutis, X. (Intern), Di Mauro, A. (Intern), Vithanage, M. D. (Ekstern), Dragoni, N. (Intern)
Detecting and Preventing Beacon Replay Attacks in Receiver-Initiated MAC Protocols for Energy Efficient WSNs

In receiver-initiated MAC protocols for Wireless Sensor Networks (WSNs), communication is initiated by the receiver of the data through beacons containing the receiver's identity. In this paper, we consider the case of a network intruder that captures and replays such beacons towards legitimate nodes, pretending to have a fake identity within the network. To prevent this attack we propose RAP, a challenge-response authentication protocol that is able to detect and prevent the beacon replay attack. The effectiveness of the protocol is formally verified using OFMC and ProVerif. Furthermore, we provide an analysis that highlights the trade-offs between the energy consumption and the level of security, defined as the resilience of the protocol to space exhaustion.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Embedded Systems Engineering, Language-Based Technology
Authors: Di Mauro, A. (Intern), Fafoutis, X. (Intern), Mödersheim, S. A. (Intern), Dragoni, N. (Intern)
Pages: 1-16
Publication date: 2013

Host publication information
Title of host publication: Secure IT Systems: 18th Nordic Conference, NordSec 2013, Ilulissat, Greenland, October 18-21, 2013, Proceedings
Publisher: Springer
ISBN (Print): 978-3-642-41487-9
ISBN (Electronic): 978-3-642-41488-6
Series: Lecture Notes in Computer Science
Volume: 8208
ISSN: 0302-9743
BFI conference series: Nordic Workshop on Secure IT-systems (5010160)
Main Research Area: Technical/natural sciences
Beacon Replay Attack, Receiver Initiated Medium Access Control, Wireless Sensor Network Security
DOIs: 10.1007/978-3-642-41488-6_1
Source: dtu
Source-ID: n:oai:DTIC-ART:inspec/426863031::35034
Publication: Research - peer-review › Article in proceedings – Annual report year: 2013

Sustainable medium access control: Implementation and evaluation of ODMAC
Harvesting small-scale ambient energy constitutes a promising source of power for wireless embedded devices. Due to the unpredictable nature of the harvested energy, adaptive radio duty cycling can lead to a long-term sustainable operation. In energy constrained conditions, very low duty cycles are vital to guarantee the sustainability of the system; whereas, in the opposite case, the system should use the energy surplus to increase the application performance. In this paper, we implement and evaluate On-Demand MAC (ODMAC), the first receiver-initiated MAC protocol specifically designed for energy harvesting applications. In particular, we provide a basic yet fully operational implementation of ODMAC for the Texas Instruments' MSP430 microprocessor family. Furthermore, we verify the theoretical results of our previous work by achieving sustainable operation of an energy harvesting node in various cases of energy input using a real test-bed.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Embedded Systems Engineering
Authors: Fafoutis, X. (Intern), Di Mauro, A. (Intern), Dragoni, N. (Intern)
Pages: 407 - 412
Publication date: 2013

Host publication information
Publisher: IEEE
ISBN (Print): 9781467357531
Main Research Area: Technical/natural sciences
Conference: IEEE International Conference on Communications (ICC 2013), Budapest, Hungary, 09/06/2013 - 09/06/2013
Sustainable Performance in Energy Harvesting - Wireless Sensor Networks
In this practical demo we illustrate the concept of "sustainable performance" in Energy-Harvesting Wireless Sensor Networks (EH-WSNs). In particular, for different classes of applications and under several energy harvesting scenarios, we show how it is possible to have sustainable performance when nodes in the network are powered by ambient energy.

Energy-Harvesting Wireless Sensor Networks
Energy Harvesting comprises a promising solution to one of the key problems faced by battery-powered Wireless Sensor Networks, namely the limited nature of the energy supply (finite battery capacity). By harvesting energy from the surrounding environment, the sensors can have a continuous lifetime without any needs for battery recharge or replacement. However, energy harvesting introduces a change to the fundamental principles based on which WSNs are designed and realized. In this poster we sketch some of the key research challenges as well as our ongoing work in designing and realizing Wireless Sensor Networks with energy harvesting capability.
Secure File Allocation and Caching in Large-scale Distributed Systems

In this paper, we present a file allocation and caching scheme that guarantees high assurance, availability, and load balancing in a large-scale distributed file system that can support dynamic updates of authorization policies. The scheme uses fragmentation and replication to store files with high security requirements in a system composed of a majority of low-security servers. We develop mechanisms to fragment files, to allocate them into multiple servers, and to cache them as close as possible to their readers while preserving the security requirement of the files, providing load-balancing, and reducing delay of read operations. The system offers a trade-off-between performance and security that is dynamically tunable according to the current level of threat. We validate our mechanisms with extensive simulations in an Internet-like network.

Security challenges for energy-harvesting wireless sensor networks

With the recent introduction of Energy-Harvesting nodes, security is gaining more and more importance in sensor networks. By exploiting the ability of scavenging energy from the surrounding environment, the lifespan of a node has drastically increased. This is one of the reason why security needs a new take in this topic. Traditional solutions may not work in this new field. Brand new challenges and threats may arise and new solutions have to be designed. In this paper we present a taxonomy of attacks, focusing on how they change in the energy harvesting scenario compared to regular sensor networks. Finally, we present and discuss existing security solutions for EH-WSNs.

Toward a Threat Model for Energy-Harvesting Wireless Sensor Networks

Security is a crucial matter for Wireless Sensor Networks. With the recent introduction of Energy-Harvesting nodes, it has gained even more importance. By exploiting the ability of scavenging energy from the surrounding environment, the
The lifespan of a node has drastically increased. This is one of the reasons why security needs a new take in this topic. Traditional solutions may not work in this new domain. Brand new challenges and threats may arise and new solutions have to be designed. In this paper we present a first taxonomy of attacks, focusing on how they change in the energy-harvesting context compared to regular sensor networks. We also discuss existing security solutions specific for the energy harvesting world and comment on the trend that this topic may follow in the future. Finally, we draw a comparison between the cyber-physical attacker we define in our model and adversary models belonging to security protocols verification literature.

General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling, Language-Based Technology, Embedded Systems Engineering
Authors: Di Mauro, A. (Intern), Papini, D. (Intern), Vigo, R. (Intern), Dragoni, N. (Intern)
Pages: 289-301
Publication date: 2012

Host publication information
Title of host publication: Networked Digital Technologies : 4th International Conference, NDT 2012 Dubai, UAE, April 24-26, 2012 Proceedings, Part II
Publisher: Springer
ISBN (Print): 978-3-642-30566-5
ISBN (Electronic): 978-3-642-30567-2
Series: Communications in Computer and Information Science
Volume: 294
ISSN: 1865-0929
BFI conference series: Networked Digital Technologies (5010629)
Main Research Area: Technical/natural sciences
Conference: 4th International Conference on Networked Digital Technologies (NDT 2012) , Dubai, United Arab Emirates, 24/04/2012 - 24/04/2012
DOIs:
10.1007/978-3-642-30567-2_24
Source: dtu
Source-ID: u::5212
Publication: Research - peer-review › Article in proceedings – Annual report year: 2012

Projects:

Technical University of Denmark
Period: 15/08/2011 → 19/12/2014
Number of participants: 6
Phd Student:
Di Mauro, Alessio (Intern)
Supervisor:
Probst, Christian W. (Intern)
Main Supervisor:
Dragoni, Nicola (Intern)
Examiner:
Schoeberl, Martin (Intern)
Gaspari, Mauro (Ekstern)
Mazzara, Manuel (Ekstern)

Financing sources
Source: Internal funding (public)
Name of research programme: Institut stipendie (DTU)
Project: PhD