Publications:

Quantitative modelling and analysis of a Chinese smart grid: a stochastic model checking case study

Cyber-physical systems integrate information and communication technology with the physical elements of a system, mainly for monitoring and controlling purposes. The conversion of traditional power grid into a smart grid, a fundamental example of a cyber-physical system, raises a number of issues that require novel methods and applications. One of the important issues in this context is the verification of certain quantitative properties of the system. In this paper, we consider a specific Chinese smart grid implementation as a case study and address the verification problem for performance and energy consumption. We employ stochastic model checking approach and present our modelling and analysis study using PRISM model checker.
Design-Efficiency in Security

In this document, we present our applied results on balancing security and performance using a running example, which is based on sensor networks. These results are forming a basis for a new approach to balance security and performance, and therefore provide design-efficiency of key updates. We employ probabilistic model checking approach and present our modelling and analysis study using PRISM model checker.

General information

State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology
Authors: Yuksel, E. (Intern), Nielson, H. R. (Intern), Nielson, F. (Intern)
Number of pages: 33
Publication date: 2013

Publication information

Place of publication: Kgs. Lyngby
Publisher: Technical University of Denmark (DTU)
Original language: English
Security Games for Cyber-Physical Systems
The development of quantitative security analyses that consider both active attackers and reactive defenders is a main challenge in the design of trustworthy Cyber-Physical Systems. We propose a game-theoretic approach where it is natural to model attacker’s and defender’s actions explicitly, associating costs to attacks and countermeasures. Cost considerations enable to contrast different strategies on the basis of their effectiveness and efficiency, paving the way to a multi-objective notion of optimality. Moreover, the framework allows expressing the probabilistic nature of the environment and of the attack detection process. Finally, a solver is presented to compute strategies and their costs, resorting to a recent combination of strategy iteration with linear programming.

Key Update Assistant for Resource-Constrained Networks
Key update is a challenging task in resource-constrained networks where limitations in terms of computation, memory, and energy restrict the proper use of security mechanisms. We present an automated tool that computes the optimal key update strategy for any given resource-constrained network. We developed a push-button solution - powered by stochastic model checking - that network designers can easily benefit from, and it paves the way for consumers to set up key update related security parameters. Key Update Assistant, as we named it, runs necessary model checking operations and determines the optimal key update strategy that satisfies given security and performance requirements.
**LBTool: A stochastic toolkit for leave-based key updates**

Quantitative techniques have been successfully employed in verification of information and communication systems. However, the use of such techniques are still rare in the area of security. In this paper, we present a toolkit that implements transient analysis on a key update method for wireless sensor networks. The analysis aims to find out the probability of a network key being compromised at a specific time point, which result in fluctuations over time for a specific key update method called Leave-based key update. For such a problem, the use of current tools is limited in many ways such as rapidly constructing a compact formal model, computing the time point where the risk is maximum, or terminating the transient analysis after the fluctuations disappear and system stabilizes. Our toolkit, LBTool, is not only resolving the above-mentioned issues, but also demonstrating how to construct models in an analytical way and how to speed up the analysis by eliminating redundant computations. The toolkit can be generalized to other key update methods by replacing the analytical model construction.

**Modelling and Analysis of Smart Grid: A Stochastic Model Checking Case Study**

Cyber-physical systems integrate information and communication technology functions to the physical elements of a system for monitoring and controlling purposes. The conversion of traditional power grid into a smart grid, a fundamental example of a cyber-physical system, raises a number of issues that require novel methods and applications. In this context, an important issue is the verification of certain quantitative properties of the system. In this paper, we consider a specific Chinese Smart Grid implementation as a case study and address the verification problem for performance and energy consumption. We employ stochastic model checking approach and present our modelling and analysis study using PRISM model checker.
Modelling Chinese Smart Grid: A Stochastic Model Checking Case Study

In this document, we consider a specific Chinese Smart Grid implementation and try to address the verification problem for certain quantitative properties including performance and battery consumption. We employ stochastic model checking approach and present our modelling and analysis study using PRISM model checker.

General information
State: Published
Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling, Wuxi SensingNet Industrialization Research Institute, East China Normal University
Authors: Yuksel, E. (Intern), Nielson, H. R. (Intern), Nielson, F. (Intern), Zhu, H. (Ekstern), Huang, H. (Ekstern)
Number of pages: 58
Publication date: 2012

Publication information
Place of publication: Kgs. Lyngby, Denmark
Publisher: Technical University of Denmark, DTU Informatics, Building 321
Original language: English
Number: 2012-02
ISSN: 1601-2321
Main Research Area: Technical/natural sciences
Electronic versions: tr12_02.pdf
Source: orbit
Source-ID: 318944
Publication: Research › Report – Annual report year: 2012

Smart Grid Security A Smart Meter-Centric Perspective

The electricity grid is a key infrastructure for our society, therefore its security is a critical public concern. This physical system is becoming more and more complex as it is coupled with a cyber layer carrying information about power usage and control instructions for intelligent appliances, leading to what is known as the Smart Grid. The development of this Cyber-Physical System introduces new security issues, thus calling for efforts in studying possible attacks and devising suitable countermeasures. In this paper, we review a generic model for the Smart Grid, and present possible attacks and countermeasures focusing on a key component of the Smart Grid: the Smart Meter.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Language-Based Technology
Authors: Vigo, R. (Intern), Yuksel, E. (Intern), Ramli, C. D. P. K. (Intern)
Pages: 127-130
Publication date: 2012
A ZigBee-based Automatic Meter Reading System

General information
State: Published
Organisations: Department of Informatics and Mathematical Modeling, Language-Based Technology, Istanbul University
Authors: Yüksel, E. (Ekstern), Zaim, A. H. (Ekstern), Yuksel, E. (Intern), Aydin, M. A. (Ekstern)
Publication date: 2011

Host publication information
Title of host publication: Proceedings of the International Conference on Networking and Future Internet (ICNFI 2011)
Main Research Area: Technical/natural sciences
Conference: International Conference on Networking and Future Internet, Paris, France, 01/01/2011
Electronic versions:
EnderICNFI2011-Zigbee_AMR.pdf
Source: orbit
Source-ID: 312748
Publication: Research - peer-review › Article in proceedings – Annual report year: 2011

Characteristics of Key Update Strategies for Wireless Sensor Networks
Wireless sensor networks offer the advantages of simple and low-resource communication. Challenged by this simplicity and low-resources, security is of particular importance in many cases such as transmission of sensitive data or strict requirements of tamper-resistance. Updating the security keys is one of the essential points in security, which restrict the amount of data that may be exposed when a key is compromised. In this paper, we investigate key update methods that may be used in wireless sensor networks, and benefiting from stochastic model checking we derive characteristics of these methods in security perspective.

General information
State: Published
Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling
Authors: Yuksel, E. (Intern), Nielson, H. R. (Intern), Nielson, F. (Intern)
Pages: 132-136
Publication date: 2011

Host publication information
Title of host publication: Proceedings of the International Conference on Network Communication and Computer (ICNCC 2011)
Main Research Area: Technical/natural sciences
Conference: International Conference on Network Communication and Computer, New Delhi, India, 01/01/2011
Security, Sensor networks, Verification, Key management
Electronic versions:
EnderICNCC2011-KU_characters.pdf
Links:
http://www.icncc.org/
Source: orbit
Source-ID: 312718
Publication: Research - peer-review › Article in proceedings – Annual report year: 2011

Optimizing Key Updates in Sensor Networks
Sensor networks offer the advantages of simple and low-resource communication. Nevertheless, security is of particular importance in many cases such as when sensitive data is communicated or tamper-resistance is required. Updating the security keys is one of the key points in security, which restrict the amount of data that may be exposed when a key is compromised. In this paper, we propose novel key update methods, and benefiting from stochastic model checking we propose a novel method for determining optimal key update strategies for custom network scenarios. We also present a case study where an application in commercial building automation is considered.

General information
State: Published
Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling, University of Oxford
Authors: Yuksel, E. (Intern), Nielson, H. R. (Intern), Nielson, F. (Intern), Fruth, M. (Ekstern), Kwiatkowska, M. (Ekstern)
Pages: 82-87
Publication date: 2011

Host publication information
Title of host publication: 2011 IEEE Sensors Applications Symposium (SAS)
Publisher: IEEE
ISBN (Print): 978-1-4244-8063-0
Main Research Area: Technical/natural sciences
Electronic versions:
EnderSAS2011-KU_optimize.pdf
DOIs:
10.1109/SAS.2011.5739805
Links:
http://2011.sensorapps.org/

Bibliographical note
Copyright 2011 IEEE. Personal use of this material is permitted. However, permission to reprint/republish this material for advertising or promotional purposes or for creating new collective works for resale or redistribution to servers or lists, or to reuse any copyrighted component of this work in other works must be obtained from the IEEE.
Source: orbit
Source-ID: 312746
Publication: Research - peer-review › Article in proceedings – Annual report year: 2011

Qualitative and Quantitative Security Analyses for ZigBee Wireless Sensor Networks
Wireless sensor networking is a challenging and emerging technology that will soon become an inevitable part of our modern society. Today wireless sensor networks are broadly used in industrial and civilian application areas including environmental monitoring, surveillance tasks, healthcare applications, home automation, and traffic control. The challenges for research in this area are due to the unique features of wireless sensor devices such as low processing power and associated low energy. On top of this, wireless sensor networks need secure communication as they operate in open fields or unprotected environments and communicate on broadcasting technology. As a result, such systems have to meet a multitude of quantitative constraints (e.g. timing, power consumption, memory usage, communication bandwidth) as well as security requirements (e.g. authenticity, confidentiality, integrity). One of the main challenges arise in dealing with the security needs of such systems where it is less likely that absolute security guarantees can be sustained - because of the need to balance security against energy consumption in wireless sensor network standards like ZigBee. This dissertation builds on existing methods and techniques in different areas and brings them together to create an efficient verification system. The overall ambition is to provide a wide range of powerful techniques for analyzing models with quantitative and qualitative security information. We stated a new approach that first verifies low level security protocols in a qualitative manner and guarantees absolute security, and then takes these verified protocols as actions of scenarios to be verified in a quantitative manner. Working on the emerging ZigBee wireless sensor networks, we used probabilistic verification that can return probabilistic results with respect to the trade-off between security and performance. In this sense, we have extended various existing ideas and also proposed new ideas to improve verification. Especially in the problem of key update, we believe we have contributed to the solution for not only wireless sensor networks but also many other types of systems that require key updates. Besides we produced automated tools that were intended to demonstrate what kind of tools can developed on different purposes and application domains.

General information
State: Published
Organisations: Language-Based Technology, Department of Informatics and Mathematical Modeling
Authors: Yuksel, E. (Intern), Nielson, H. R. (Intern), Nielson, F. (Intern)
Number of pages: 306
Publication date: 2011

Publication information
Place of publication: Kgs. Lyngby, Denmark
Publisher: Technical University of Denmark (DTU)
Original language: English
Series: IMM-PHD-2011
Number: 247
ISSN: 0909-3192
Main Research Area: Technical/natural sciences
Electronic versions:
Resilience Analysis of Key Update Strategies for Resource-Constrained Networks
Severe resource limitations in certain types of networks lead to various open issues in security. Since such networks usually operate in unattended or hostile environments, revoking the cryptographic keys and establishing (also distributing) new keys— which we refer to as key update— is a critical security issue. In this paper, we investigate the behaviour of different key update strategies under deviant network conditions. We consider resource-critical networks that employ symmetric cryptography and rely on (shared) network keys. We provide a methodology for quantitative security and performance analysis, and present a case study covering six different key update strategies.

A Secure Key Establishment Protocol for ZigBee Wireless Sensor Networks
ZigBee is a wireless sensor network standard that defines network and application layers on top of IEEE 802.15.4’s physical and medium access control layers. In the latest version of ZigBee, enhancements are prescribed for the security sublayer but we show in this paper that problems persist. In particular, we show that the end-to-end application key establishment protocol is flawed and we propose a secure protocol instead. We do so by using formal verification techniques based on static program analysis and process algebras. We present a way of using formal methods in wireless network security, and propose a secure key establishment protocol for ZigBee networks.
High Security at a Low Cost

In the future tiny devices with microcontrollers and sensors will be in charge of numerous activities in our lives. Tracking our energy consumption and CO2 emission, controlling our living conditions, enforcing security, and monitoring our health will be some examples of their functions. These devices will form wireless networks to communicate with one another, moreover their power consumption will be very low. It is not hard to predict that our modern society will depend on the correct operation of these devices, and the security of the network they are operating. Such sensor-based systems, also known as "cyber-physical systems", achieve security by means of cryptographic protocols. In a simplistic setting where the power consumption should be minimum and the processing power is limited, it is more likely that all devices in the network will share the same cryptographic key. In this study, we are working on the trade-off between two challenges: "the cryptographic key should be changed frequently to preserve security" and "the cryptographic key should be changed rarely to save power". We work on the ZigBee wireless sensor network standard, that offers the advantages of simple and low resource communication. We model the system as a continuous-time Markov chain, and analyze it by posing a number of questions shedding light on its behaviour. The properties we are interested in are expressed in continuous stochastic logic, and probabilistic model checker Prism is used in the analysis.

General information

State: E-pub ahead of print
Organisations: Department of Informatics and Mathematical Modeling
Authors: Yuksel, E. (Intern), Nielson, H. R. (Intern), Nielson, F. (Intern)
Publication date: 2010
Optimizing ZigBee Security using Stochastic Model Checking

A Secure Key Establishment Protocol for ZigBee Wireless Sensor Networks

Quantitative Security Analysis of ZigBee Key Updates
ZigBee-2007 Security Essentials

ZigBee is a fairly new but promising standard for wireless networks due to its low resource requirements. As in other wireless network standards, security is an important issue and each new version of the ZigBee Specification enhances the level of the ZigBee security. In this paper, we present the security essentials of the latest ZigBee Specification, ZigBee-2007. We explain the key concepts, protocols, and computations. In addition, we formulate the protocols using standard protocol narrations. Finally, we identify the key challenges to be considered for consolidating ZigBee.

A Secure Simplification of the PKMv2 Protocol in IEEE 802.16e-2005

Static analysis is successfully used for automatically validating security properties of classical cryptographic protocols. In this paper, we shall employ the same technique to a modern security protocol for wireless networks, namely the latest version of the Privacy and Key Management protocol for IEEE 802.16e, PKMv2. This protocol seems to have an exaggerated mixture of security features. Thus, we iteratively investigate which components are necessary for upholding the security properties and which can be omitted safely. This approach is based on the LySa process calculus and employs the corresponding automated analysis tool, the LySaTool.
Projects:

Qualitative and Quantitative Security Analyses for ZigBee Wireless Sensor Networks

Department of Informatics and Mathematical Modeling
Period: 01/09/2007 → 30/03/2011
Number of participants: 6
Phd Student:
Yuksel, Ender (Intern)
Supervisor:
Nielsen, Flemming (Intern)
Main Supervisor:
Nielsen, Hanne Riis (Intern)
Examiner:
Madsen, Jan (Intern)
Gilmore, Stephen (Ekstern)
Martinelli, Fabio (Ekstern)

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