available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

# Quantitative analysis of a certified e-mail protocol in mobile environments: A probabilistic model checking approach

*S. Basagiannis*, S. Petridou, N. Alexiou, G. Papadimitriou, P. Katsaros*

*Department of Informatics, Aristotle University of Thessaloniki, 54124 Thessaloniki, Greece*

ARTICLE INFO

*Article history:*
Received 14 July 2010
Received in revised form
27 December 2010
Accepted 6 February 2011

*Keywords:*
Certified e-mail
probabilistic model checking
CTMC
mobile environments

ABSTRACT

Formal analysis techniques, such as probabilistic model checking, offer an effective mechanism for model-based performance and verification studies of communication systems' behavior that can be abstractly described by a set of rules i.e., a protocol. This article presents an integrated approach for the quantitative analysis of the Certified E-mail Message Delivery (CEMD) protocol that provides security properties to electronic mail services. The proposed scheme employs a probabilistic model checking analysis and provides for the first time insights on the impact of CEMD's error tolerance on computational and transmission cost. It exploits an efficient combination of quantitative analysis and specific computational and communication parameters, i.e., the widely used Texas Instruments TMS320C55x Family operating in an High Speed Downlink Packet Access (HSDPA) mobile environment, where multiple CEMD participants execute parallel sessions with high bit error rates (BERs). Furthermore, it offers a tool-assistant approach for the protocol designers and analysts towards the verification of their products under varying parameters. Finally, this analysis can be also utilized towards reliably addressing cost-related issues of certain communication protocols and deciding on their cost-dependent viability, taking into account limitations that are introduced by hardware specifications of mobile devices and noisy mobile environments.



## 1. Introduction

During the last decades, the fact that a number of communication protocols have been published with security flaws (Lowe, 1996; Lowe and Roscoe, 1997; Basagiannis et al., 2008) urges the protocol designers to "strengthen" their products with additional cryptographic mechanisms (e.g., public key cryptography) that secure and guarantee the safe completion of protocol's sessions. But, the tradeoff of gaining in security is losing in terms of computational cost. Increased computational cost, in turn, entails that a protocol cannot be adopted by low-cost hardware equipment, such as mobile devices. Moreover, when discussing protocols' cost in mobile environments, parameters that determine transmission cost, such as the high bit error rate (BER), should be taken into consideration. However, predicting computational and transmission costs is often impossible, due to the presence of multiple participants executing parallel sessions. For example, nowadays, the widespread use of wireless and mobile communications (Miorandi et al., 2007; Bi et al., 2001; Zhang et al., 2010; Liaskos et al., 2010) along with the services and applications supported in new generation's mobile devices (Sklavos and

* *Corresponding author.*
E-mail addresses: basags@csd.auth.gr (S. Basagiannis), spetrido@csd.auth.gr (S. Petridou), nalexiou@csd.auth.gr (N. Alexiou), gp@csd.auth.gr (G. Papadimitriou), katsaros@csd.auth.gr (P. Katsaros).
0167-4048/$ – see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2011.02.001

Touliou, 2007) entails low-cost infrastructure operating in noisy environments. In fact, current WWANs (Wireless Wide Area Networks) are primarily based on second (2G) and third (3G) generation mobile technologies such as GSM (Global System for Mobile Communications) and HSDPA (High Speed Downlink Packet Access), respectively (Mouly and Paulet, 1992; Sohaib and Nordberg, 2006; Kliazovich et al., 2008). Thus, it is fundamental to define the conditions under which a secure protocol is suitable for mobile environments.

Nowadays, research in formal methods leads to the development of verification techniques that facilitate the early detection of software or hardware defects in Information and Communication Technology (ICT) systems (Baier and Katoen, 2008). Moreover, formal analysis techniques, such as probabilistic model checking, are considered to be an effective way for studying security failures in communication systems, since they can discover design flaws in protocols.

In this paper we propose the use of probabilistic model checking (Kwiatkowska et al., 2004) to analyze the Certified E-mail Message Delivery (CEMD) protocol (Nenadic et al., 2004; Ateniese and Nita-Rotaru, 2002). Current work aims at providing a quantitative analysis in mobile environments. Nowadays, one of the most dominant applications used by mobile devices, e.g., smart phones and PDAs, is the e-mail delivery service (Sklavos and Touliou, 2007). Given the popularity of e-mail service and the current trend for secure communications, analyzing the cost of security in e-mail service is an important issue. CEMD protocol provides all the anticipated security properties, i.e., fairness, confidentiality, timeliness and TTP invisibility (Nenadic et al., 2004) that an e-mail protocol ought to support. Moreover, it is a well accepted protocol in related bibliography based on the well known ANR protocol (Ateniese and Nita-Rotaru, 2002).

An abstract representation of the proposed analysis is presented in Fig. 1. As shown in the inner circle our analysis considers the security properties, i.e., fairness, timeliness, confidentiality and TTP invisibility, of CEMD. The CEMD protocol is modeled as a Continuous-Time Markov Chain (CTMC) (Stewart, 1994), while its properties are expressed as Continuous Stochastic Logic (CSL) formulas (Aziz et al., 2000). The PRISM framework (Prism Model Checker) performs automated analysis of the CEMD protocol and verifies the security guarantees it provides. Then, the aforementioned CTMC model is used for the quantitative analysis of the protocol's cost-related properties. These properties are twofold: computational cost imposed by low-cost participants, i.e., mobile devices, and transmission cost due to high BER in mobile environments. As a result, our study provides answers

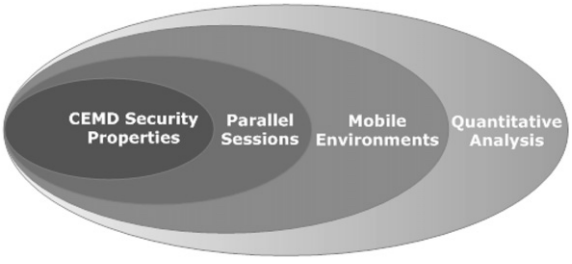


**Fig. 1 – An abstract representation of the proposed analysis.**

for whether or not the CEMD protocol can assure security guaranties for low-cost participants involved in multiple protocol sessions and operating in error-prone environments, and if so, at what cost. Thus, the next two circles of Fig. 1 represent the last contribution of our analysis which takes into consideration that CEMD protocol operates in noisy environments such those of mobile communications and involves multiple participants executing parallel protocol sessions. The outer circle of Fig. 1 represents the proposed quantitative analysis incorporating all the above components.

### 1.1. *Contribution*

To the best of our knowledge, this is the first work that applies probabilistic model checking for the quantitative analysis of a protocol under specific computational and communication parameters. The current paper considers the widely used Texas Instruments TMS320C55x Family operating at 200 MHz (Hwang et al., 2007; Hwang et al., 2003). Although, nowadays, mobile processors' speed up to 1 GHz, there are many CPU manufacturers who support products working on different modes. For example, Intel launched a Mobile Pentium III processor with two working modes, namely full power mode at 800 MHz and low power mode at 650 MHz (Prasithsangaree and Krishnamurthy, 2004). This characteristic is very important, since fundamental communication components, e.g., protocols, and their mechanisms, e.g., cryptographic operations, can be developed in a way that exploits their low power mode feature. This entails that protocol designers and analysts can verify their products considering them as operating in low power mode. In this way protocols and security services will be always fully supported contrary to other mobile functionalities in which energy scale-down techniques can be applied e.g., display scale down optimizations (background half or fully dim). Consequently, this paper exploits CPUs at the low corner of 200 MHz, since it is significant for CPU to provide critical services when it operates in low power mode. Works in (Sklavos and Touliou, 2007; Prasithsangaree and Krishnamurthy, 2004; Mayo and Ranganathan, 2003; Karri and Mishra, 2002) also pinpoint the necessity of minimizing CPU energy consumption in mobile devices.

Thus, in this work, we consider computational cost in line with the CPU cycles and the time required by the aforementioned mobile processors to perform RSA operations, i.e. encryption and decryption processes, required by the CEMD protocol. This actually means that the proposed computational cost analysis considers battery life through CPU cycles. Although display and applications, e.g., camera, mp3 and games, consume a great portion of battery life, it is found that CPU and memory are the dominant consuming subsystems in 3G mobile devices (Sklavos and Touliou 2007). In fact, the CPU power is consumed due to instructions' execution and their fetching from the memories or caches. This in conjunction with the fact that security protocols embed cryptographic mechanisms that, nowadays, require increasing bit size keys, e.g., greater than 512 bits, results in great deal of CPU expenditure.

The communication parameters that the proposed analysis takes into account is the presence of BER in mobile networks, which constitutes them as noisy environments, and the multiple CEMD participants executing parallel