Journal of Computer and System Sciences 81 (2015) 1464–1478

Contents lists available at ScienceDirect

Journal of Computer and System Sciences

www.elsevier.com/locate/jcss

Modeling energy-efficient secure communications in multi-mode wireless mobile devices

Arcangelo Castiglione [a], Francesco Palmieri [b,*], Ugo Fiore [c], Aniello Castiglione [a], Alfredo De Santis [a]

[a] *Dipartimento di Informatica, Università degli Studi di Salerno, Via Giovanni Paolo II, 132, I-84084, Fisciano (SA), Italy*
[b] *Dipartimento di Ingegneria Industriale e dell'Informazione, Seconda Università di Napoli, Via Roma, 29, Aversa (CE), I-81031, Italy*
[c] *C. S. I., Università degli Studi di Napoli "Federico II", Via Cintia, 21, I-80126, Napoli (NA), Italy*

ARTICLE INFO

Article history:
Received 1 July 2014
Received in revised form 14 December 2014
Accepted 14 December 2014
Available online 19 December 2014

Keywords:
Cryptographic algorithms
Multi-mode devices
Power optimization
Energy analysis and modeling
Energy-aware secure communications
Energy efficiency

ABSTRACT

Despite the wide deployment of advanced wireless coverage infrastructures, finding the best way for achieving secure mobile communication in every-day's life activities is still an open question. Indeed, a large number of mobile terminals, supporting multiple networking technologies, may be used to manage data from everywhere and at anytime. However, the effort required for achieving security, given the complexity of cryptographic algorithms, heavily affects the power consumption of terminals. Such energy demand, together with the one required to manage communication activities, makes energy-efficient secure communication among hardware-constrained handheld devices a challenging topic. In this work, we introduce an analytic energy model for secure communication among multi-mode terminals. This model describes the energy consumption of mobile terminals operating within a dynamic network scenario, considering both their interconnection and secure data exchange issues, in order to develop adaptive strategies for energy-efficient secure communications. Finally, the model has been validated through simulation.

1. Introduction

Because of the wide deployment of cellular networks and high capacity Wi-Fi coverage infrastructures, a large number of *Mobile Terminals (MTs)*, simultaneously supporting multiple networking technologies, may be used to store, access, manipulate, or communicate sensitive data from everywhere and at anytime. One of the main features of such MTs, is the support and inter-operation of multiple different mobile communication technologies, resulting into a heterogeneous multi-standard network coverage. In particular, when using multiple networking technologies opportunistically, each one supporting its specific security model, it is easy to note that ensuring content confidentiality and authentication becomes a real challenge. Furthermore, the computational efforts required for achieving security, due to the complexity of cryptographic algorithms, heavily affect the power consumption and consequently the energy demand of involved terminals, which are usually equipped with battery units of limited capacity, in order to contain their weight and size. Such energy demand, together with the amount of power required to manage communication activities carried out by using multiple network interfaces, makes energy-efficient secure communication among mobile hardware-constrained devices a non-trivial task.

[*] Corresponding author.
E-mail addresses: arccas@dia.unisa.it (A. Castiglione), francesco.palmieri@unina.it (F. Palmieri), ufiore@dia.unisa.it (U. Fiore), castiglione@acm.org (A. Castiglione), castiglione@ieee.org (A. Castiglione), ads@unisa.it (A. De Santis).

http://dx.doi.org/10.1016/j.jcss.2014.12.022
0022-0000/© 2014 Elsevier Inc. All rights reserved.

Accordingly, in this work we studied the energy-related dynamics of secure communications among MTs providing multiple and heterogeneous networking capabilities. In particular, we formulate a comprehensive analytic energy model, which can be used to describe and estimate the energy consumption of MTs operating within a continuously evolving network scenario, by considering both communication and security-enforcement activities, mainly accomplished through cryptographic techniques. Each MT is both an information source and sink, hence needing to send and receive multiple messages in a secure manner from any other MT in the same network. Such a model, may be particularly useful for adaptively choosing the best option among multiple available ones, with the final goal of minimizing the overall energy consumption of involved terminals. The fundamental factors affecting energy-efficiency in secure wireless communications are analyzed carefully, in order to evaluate their joint effects on battery lifetime.

Therefore, the energy consumption estimation resulting from the proposed model, becomes an objective function that can be considered for evaluating or implementing power optimization strategies. In order to model, estimate and possibly predict the energy consumption for secure communications in multi-mode devices, we considered both the energy needed for pure network communication activities and the one associated to the operations ensuring end-to-end security.

In addition, in order to be as realistic as possible, we also considered a set of other factors, such as the motion of MT, the distance of an MT from the corresponding endpoint (in case of ad-hoc communications), either from the *Base Station (BS)* or from any other kind of *Access Point (AP)* (when operating in the more traditional infrastructure mode), as well as the signal quality and strength. In doing this, the proposed model also takes into account the effects on energy consumption associated to user mobility, and in particular to the authentication and re-authentication operations that MTs perform during their motion. In detail, for modeling energy consumption of cryptographic operations performed by a MT, we consider several factors, including the individual network interface activities, as well as how many end-to-end data exchange sessions are simultaneously active for each interface. Indeed, it is important to emphasize that the number of cryptographic operations performed is also strongly related to the involved MTs' "*mobility profiles*", which given a set of interacting users, describe their behavior in a specific period of time. Clearly, only by knowing in advance all the mobility patterns associated to such mobility profiles, we can estimate, for each session, the number of *authentications*, *key exchanges* and *key updates* performed. Accordingly, we model the fixed contribution of authentication, key exchange and key setup operations for each session, by taking into account the number of operations resulting from the above mentioned mobility patterns.

It is also necessary to point out that the proposed model is specifically targeted on secure end-to-end communication activities, thus it does not consider all the other energy-draining factors associated to MT equipment, along with operations such as flash storage access, display and backlight usage, operating-system specific burden, routing protocol overhead, etc.

The proposed model has been validated through simulation, by comparing the obtained results with power consumption data available in the literature. The comparison confirmed that the basic concepts and assumptions underlying our proposal are correct, as well as the associated ideas are promising and worth to be exploited by future works.

This paper is structured as follows. Section 2 provides an overview of the most popular systems/solutions for modeling energy consumption in several networking scenarios. Section 3 defines and evaluates what are the factors that most influence the energy consumption required by secure communications. Section 4 describes the energy-efficient secure communication model, which is the main focus of this work. Section 5 shows the results obtained by analyzing the model through simulation and finally, Section 6 presents some conclusions and possible future developments.

2. Related work

Due to the ever-increasing diffusion of handheld devices with limited hardware and software characteristics, the problem of *energy-efficiency* is gaining importance, both from the academic and industrial point of view. In recent years, there have been many research efforts aiming at modeling energy consumption of such devices, by considering either communications or operations perspectives, but always in a separate way.

Two of the most relevant works in MTs' energy modeling were proposed in [1,2]. In particular, [1] describes several experiments carried out to obtain detailed energy consumption measurements of IEEE 802.11 wireless network interfaces, when operating in an ad-hoc networking environment. In [2], instead, a model for evaluating the energy consumption of ad-hoc networks is presented. Several other contributions concerning energy modeling in *Wireless Sensor Networks (WSN)* are available in the literature.

In [3], a three-tier architecture for collecting sensor data in sparse WSNs, which achieves substantial power savings from energy-awareness practices, has been defined and analyzed. Moreover, such work defines a simple analytic model for evaluating performance when system parameters are scaled.

Furthermore, [4] presents a scalable simulation environment for WSN, providing an accurate per-node energy consumption estimation. The work presented in [5], instead investigates the problem of irregular energy consumption in a large class of many-to-one WSNs. In detail, it proposes an analytic model addressing this problem, which may be helpful for understanding the relevance of different factors on energy consumption rates.

Other research efforts focus on modeling energy consumption of handheld devices. The most notable of them is the one proposed in [6], which evaluates the energy consumption characteristics of three widespread mobile networking technologies, namely 3G, GSM, and Wi-Fi. Such work points out that 3G and GSM require a high *tail energy* overhead, because of lingering in high power modes after completing a transfer. Based on these considerations, it models the energy consumption