2015 12th International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Services (TELSIKS)

TELSIKS 2015

Proceedings of Papers

Serbia, Niš, 14 - 17 October, 2015

2015 12th International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Services, Serbia (TELSIKS), Niš, 14-17 October, 2015

Proceedings of Papers

Editors: Prof. Dr. Bratislav D. Milovanović
Prof. Dr. Nebojša S. Dončov
Prof. Dr. Zoran Ž. Stanković

Technical Editors: Dr. Biljana P. Stošić
Dr. Tijana Ž. Dimitrijević

Published by: Institute of Electrical and Electronics Engineers (IEEE), and
Faculty of Electronic Engineering (FEE), University of Niš, Serbia

Printed by: UNIGRAF X-COPY, Niš

Number of copies printed: 100

Printing of this edition has been financially supported by
Ministry of Education, Science and Technological Development of Republic of Serbia

IEEE Catalog Number: CFP15488-CDR
ISBN: 978-1-4673-7514-6 (IEEE)
978-86-6125-148-1 (FEE)

CIP - Каталогизација у публикацији - Народна библиотека Србије, Београд

621.39(082)(0.034.2)
537.8(082)(0.034.2)
621.315:66.017(082)(0.034.2)
316.774:004(082)(0.034.2)
004(082)(0.034.2)
537.8(082)(0.034.2)

INTERNATIONAL Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Services - TELSIKS (12 ; 2015 ; Niš)
Proceedings of Papers [Elektronski izvor] / 12th International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Services - TELSIKS 2015, Niš, 14 - 17 October, 2015 ; [editor Bratislav D. Milovanović, Nebojša S. Dončov, Zoran Ž. Stanković]. - Niš : Faculty of Electronic Engineering ; Piscataway : Institute of Electrical and Electronic Engineers, 2015 (Niš : Unigraf X-Copy). - 1 elektronski optički disk (CD-ROM) ; 12 cm

Системски захтеви: Нису наведени. - Nasl. sa naslovne strane dokumenta. -
Tiraž 100. - Bibliografija uz svaki rad.

ISBN 978-86-6125-148-1 (FEE)
ISBN 978-1-4673-7514-6 (IEEE)

a) Телекомуникације - Зборници b) Електротехнички материјали - Зборници
c) Електромагнетизам - Математички модели d) Мултимедији - Зборници e)
Рачунарство - Зборници f) Микроталасна техника - Зборници
COBISS.SR-ID 218074124

Power Consumption Aware Software Architecture for M-Health Applications with Adaptive Security of Network Protocols

Vladimir Ciric*, Jovica Zlatanovic†, Emina Milovanovic‡, Nenad Stojanovic§

***Abstract*— The goal of this paper is development of software architecture for mobile devices, which is able to trade-off between security levels and power consumption. The analysis of the influence of different security protocols on power consumption is given. The proposed architecture is described in detail. Three different security levels with corresponding cipher suites are proposed: low, medium and high. The architecture is implemented on Android platform. The difference in power consumptions of the cipher suites in high and low security/power profiles is around 8.2% for WiFi, and 9.6% for 3G network. In order to further reduce the power consumption during network communication, the delay between sending two successive packets is analyzed. The proposed architecture is capable of stalling packets and sending them in burst-mode, letting the network interface to stay in low-power mode for a longer period of time. The power consumption in this mode is reduced for additional 25%.**

Keywords—Mobile applications, security protocols, battery life, power consumption.

I. Introduction

According to Gartner Inc., 48.61% of all computer devices shipped worldwide in 2014 had Android operating system, 11.04% were with iOS, 14% were under Windows, and 26.34% were with other operating systems [1]. With more than 60% of overall computer market share, mobile computers, smarthpones, and lately all kinds of wearable devices, set global, but very specific requirements in front of the developers and researchers [1].

Users expect to run most of computationally intensive applications on smart mobile devices in the same way as they do on powerful stationary computers. However, despite all the advancements in recent years, mobile devices still have relatively low computational capabilities. Mobile cloud computing is the latest practical solution for filling this gap by extending the services and resources of computational clouds to smart mobile devices on demand basis [2].

In the same manner, smart mobile devices can offload data to the cloud, either for permanent data storage, or for the later processing and analyzing of data acquired from one or many devices. One example of smart mobile application, which gets a lot of attention lately, is mobile-health (m-health) [3]. Modern smart mobile devices offer media-rich and context-aware features that are highly useful for electronic-health (e-health) applications. These apps either simply collect the patients data, or perform some minor functionality, but in almost all cases they communicate with some variant of ”the cloud” [3].

Having in mind that mobile communication is very power-consuming, as well as that data transmitted by m-health apps, or any other kind of m-app can be private and sensitive, two major challenges exist: battery life and security. The latest research have shown that power consumption and security level are inversely proportional, which makes them suitable for trading-off [4], [5], [6], [7]. Furthermore, the transition from one interface type to another, using specific characteristics of the communication channel can be used to further reduce the power consumption used for the communication [8], [9].

The goal of this paper is development of the software architecture for mobile devices, which is able to trade-off between security levels and power consumption. The analysis of the influence of different security protocols on power consumption is given, and the corresponding architecture is described in detail. Three different security levels with corresponding cipher suites are proposed: low, medium and high. In order to further reduce the power consumption during network communication, the delay between sending two successive packets is analyzed. The proposed architecture is capable of stalling packets and sending them in burst-mode, letting the network interface to stay in low-power mode for a longer period of time.

II. Communication Protocol Security and Power Consumption

With the aim to clarify the influence of encryption algorithms and interface type on the power consumption during secure communication, we give a brief survey of the research on communication protocols and power consumption.

The authors in [4] presented a performance evaluation of selected symmetric encryption algorithms. The selected algorithms are AES, DES, 3DES, RC6, Blowfish and RC2. Several performance metrics are collected: encryption time, CPU process time and clock cycles, and battery power. According to the obtained results, authors in [4] concluded that changing an encryption key size leads to clear change in the battery and time consumption. In case of AES, three different key sizes were considered, i.e., 128 bit, 192 bits and 256 bit keys. It was shown that going from 128 bits key to 192 bits causes increase in power and time consumption about 8%, and to 256 bit key causes an increase of 16% [4].

Similar research, but with the focus on asymmetrical algorithms has been presented in [5]. The paper presents an esti-

*Vladimir Ciric is with Faculty of Electronic Engineering, University of Nis, Aleksandra Medvedeva 14, 18000 Nis, Serbia, E-mail: *vladimir.ciric@elfak.ni.ac.rs*

†Jovica Zlatanovic is with Nissatech Innovation Centre d.o.o., Kajmakcalanska 8, 18000 Nis, Serbia, E-mail: *jovica.zlatanovic@nissatech.com*

‡Emina Milovanovic is with Faculty of Electronic Engineering, University of Nis, Aleksandra Medvedeva 14, 18000 Nis, Serbia, E-mail: *emina.milovanovic@elfak.ni.ac.rs*

§Nenad Stojanovic is with Nissatech Innovation Centre d.o.o., Kajmakcalanska 8, 18000 Nis, Serbia, E-mail: *nenad.stojanovic@nissatech.com*

978-1-4673-7514-6/15/$31.00

mate of the performance improvements that can be expected in SSL (Secure Socket Layer), by involving Elliptic Curve Cryptography (ECC). The 1024-bit RSA and 163-bit ECC keys are compared without client authentication. In terms of a throughput, it is shown that ECC is more than five times better than RSA on the two platforms that are considered. The experiments were repeated using 2048-bit RSA keys and 193-bit ECC keys.

In [6] a comprehensive analysis of the energy requirements of a wide range of cryptographic algorithms that are used as building blocks in security protocols is presented. It is shown that the SSL handshake protocol can be optimized depending on whether client authentication is performed or not, by choosing ECC algorithm in the former case, and RSA algorithm in the latter case. Usually, applications which require a high degree of security need client authentication. In case of applications where security requirements are not stringent, further energy savings can be obtained by switching to smaller keys. In order to account for all the factors on which the energy consumption of the SSL protocol depends, the formulation of an energy cost function is proposed in [6], which can be parameterized on a number of factors.

On the other hand, using a wireless radio to transfer data is potentially one of the most significant sources of battery drain. We will consider 3G and WiFi radio interfaces. Three major factors have influence on the WiFi interface power consumption [10]:

- *Scanning, connecting and control overhead* – This factor accounts for the power used to discover and connect devices, and to send and receive control packets.
- *Transmission and reception* – This accounts for the energy spent by a node in data receptions, and in data packet transmission.
- *Idle listening* – Refers to the power consumed when the radio of the node is waiting to receive potential packets but the media is idle.

IEEE 802.11 standard for WiFi suggests the usage of power-save mode (PSM), and move from Full-Power State (FPS) to Low-Power State (LPS) whenever the interface is in the idle mode. It wakes-up periodically to check whether there is a data waiting for the transmission. The energy required in this mode is much lower than the energy required for periodical scanning and connecting, which would happen if the interface is turned-off whenever the transmission burst is over [11].

In addition to two power levels of the WiFi, the state machine for a typical 3G network radio consists of three energy states [8], [9]:

- *Full power* – Used when a connection is active, allowing the device to transfer data at its highest possible rate.
- *Low power* – An intermediate state that uses around 50% of the battery power at the full state.
- *Standby* – The minimal energy state during which no network connection is active or required.

The states and the transitions of a typical 3G wireless radio state machine are shown in Fig. 1 [8].

While the low power and standby states significantly lower battery consumption, they introduce a latency while returning to full power from the low state of around 1.5 seconds, and of 2 seconds while moving from standby to full power state, which often can't be tolerated (Fig. 1). That is why the state machine delays the change of the state for a long period of

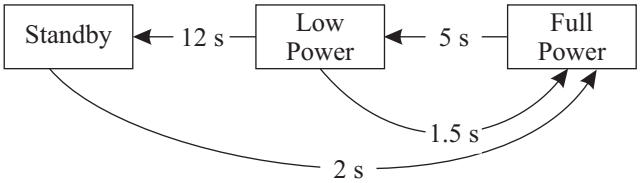

Fig. 1: Typical 3G wireless radio state machine

time, before it finally goes to the standby. Every time when a packet is sent, the interface moves to the full power state and resets the countdown timer. In the case described in Fig. 1, it will remain at full power for the duration of the transfer, plus an additional 5 seconds of tail time, followed by 12 seconds at the low energy state. Thus, for a typical 3G device, every data transfer session will cause the radio to draw energy for almost 20 seconds [8].

In practice, this means an app that transfers unbundled data for 1 second every 18 seconds will keep the wireless radio active, moving it back to high power just as it was about to become idle.

The main conclusion is that the power consumption characteristics of security protocols, along with the power consumption characteristics of radio interface should be considered while designing the software architecture of a mobile application that frequently communicates with the cloud over the wireless network.

III. Design of a Software Architecture with Ability to Trade-off Security and Power

The proposed architecture is designed in the form of software framework, which can be reused as a component in different environments. The primary target were m-health applications, in which the patients data should be transferred to the cloud in a secure manner, while keeping the battery live for a longer period of time. The data in m-health usually have a time stamp in order to track the status of the patient over the time. Thus, a delivery delayed for a less than a minute, if it can save the power, is acceptable. Security protocols should be involved in order to preserve patient privacy, but chances for attacks, concerning the type of the data in m-health apps are no that high. Thus, the security should be present all the time, but the efforts can be lowered if this is due to the battery preservation.

Having in mind the characteristics of security protocols, and the characteristics of radio interfaces, the following findings stand:

- Regarding algorithm performances and power consumption, AES and Blowfish are the best candidates, while AES is preferred if the keys should be often generated.
- ECC is preferred, particularly Elliptic curve Diffie-Hellman (ECDHE) with 163-bit keys.
- The size of data within a transaction should be 500 to 1024KB if data are sent via 3G [7].
- If a power level is low, and the communication is performed via 3G, packets buffering is required.

According to the requirements, we propose three security levels:

- *High* – the highest security level, and the highest power consumption,
- *Medium* – medium security level, average power consumption, and
- *Low* – low security level, the lowest power consumption.

The proposed collections of the algorithms for different security levels are given in Table I.

The software architecture is given in Fig. 2.

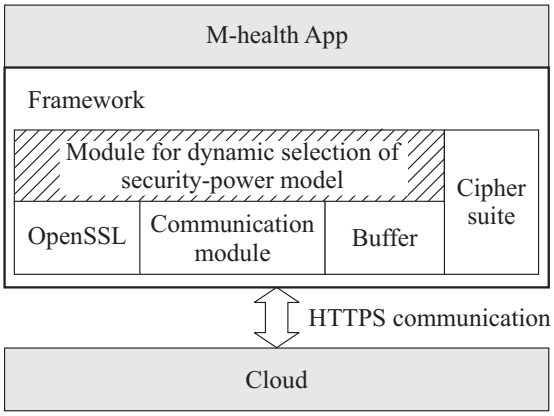

Fig. 2: Software architecture with ability to optimize a power consumption of a mobile device

The role of the Cipher suite in Fig. 2 is the implementation of different protocol suites from Table I. The buffer is able to stall the packets and release them in burst-mode, letting the interface to be in low power state for a longer period of time.

The algorithm implemented by the module for dynamic selection of security-power model from Fig. 2, which decides in real time which power model will be used is given in Fig. 3, where constants 1, 2, and 3, represent low, medium and high security levels, respectively. Battery low state is considered for the battery level below 15%.

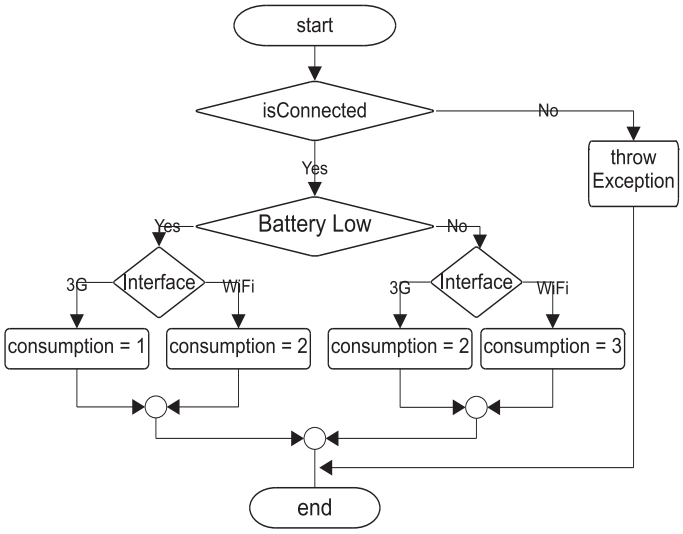

Fig. 3: Algorithm for dynamic selection of security-power model

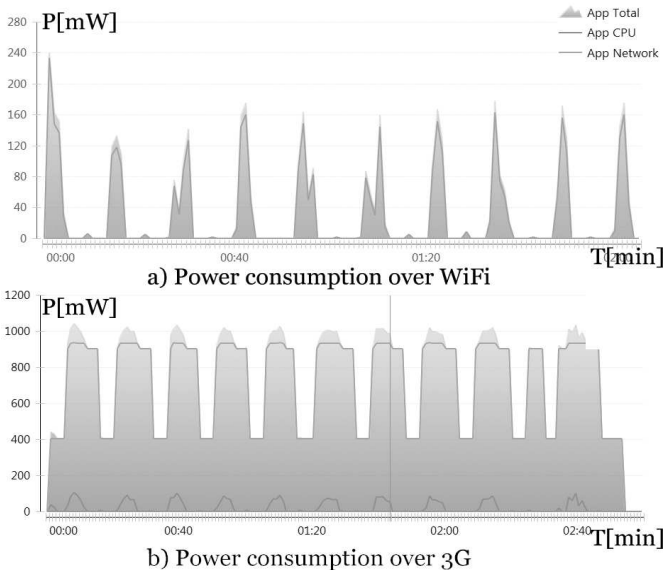

Fig. 4: Graphical representations of the power consumption for the measurement type T2: a) for WiFi network, b) for 3G network

IV. Implementation Results

The proposed framework is implemented on Android platform and tested on Sony WT19i platform. The evaluation is performed using *Little Eye Labs*$^{\text{TM}}$ performance measurement software [12].

Three types of measurements are performed:

T1 - Each of the proposed security levels from Table I was evaluated over 3G and WiFi interface for 100 successive packets/communication requests.

T2 - For the medium security and battery low level, 100 requests are made over both WiFi and 3G networks without buffering, in bursts of 10 requests with the delay between bursts of 10 seconds.

T3 - The same as T2, but with buffering.

The results of the measurement setting T1, given as a battery drain per packet, are given in Table II.

Graphical representations of the power consumption over time, for the measurement setting T2, for both 3G and WiFi networks are shown in Fig. 4. In both cases given in Fig. 4 the CPU power requirements for the preparation and securing the transmission are about 160mW, while WiFi interface consumes around 30mW (Fig. 4a). In the case of 3G (Fig. 4b), the network interface requires around 950mW, i.e. 1.100 mW for both CPU and the interface, Fig. 4b.

A graphical representation of the power consumption over the time, for the measurement setting T3 for 3G network is shown in Fig. 5. The battery drain measured for WiFi in T2 was $0.32mAh$, and $9.81mAh$ for 3G, while the drain in the case T3 was $0.30mAh$ for WiFi, and $7.19mAh$ for 3G. The reduction of power consumption in the case T2 was around 6.2%, while in the case T3 over 3G was more than 25% ($\frac{9.81-7.19}{9.81}$).

It should be noted that the presented reduction referees only to the analyzed aspect of battery drain, which is only one part of total power consumption of the mobile device.

TABLE I: The proposed cipher suites for different security levels

Sec. level	Cipher	Key exchange	Integrity	Cipher suite
High	AES_256_GCM	ECDHE	SHA386	TLS_ECDHE_RSA_AES_256_GCM_SHA384
	AES_256_CBC	ECDHE	SHA	TLS_ECDHE_RSA_AES_256_CBC_SHA
	AES_256_CBC	DHE	SHA	TLS_DHE_RSA_AES_256_CBC_SHA
Medium	AES_128_GCM	ECDHE	SHA256	TLS_ECDHE_RSA_AES_128_GCM_SHA256
	AES_128_CBC	ECDHE	SHA	TLS_ECDHE_RSA_AES_128_CBC_SHA
	AES_128_CBC	DHE	SHA	TLS_DHE_RSA_AES_128_CBC_SHA
Low	RC4_128	ECDHE	SHA	TLS_ECDHE_RSA_RC4_128_SHA
	RC4_128	-	SHA	TLS_RSA_RC4_128_SHA

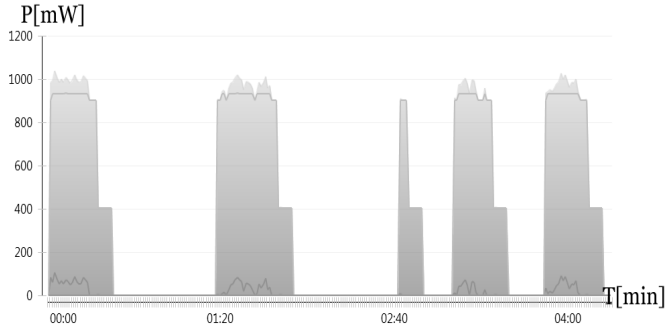

Fig. 5: Graphical representations of the power consumption for the measurement type T3 for 3G network

TABLE II: Battery drain per one sent packet in [μAh]

WiFi			3G		
Low	Medium	High	Low	Medium	High
2.775	2.975	3.025	47.10	47.50	52.15

V. Concluding Remarks

In this paper the software architecture for mobile devices, which is able to trade-off between security levels and power consumption, was proposed and described in detail. Three different security levels with corresponding cipher suites were proposed: low, medium and high. The architecture was implemented on Android platform. Measured differences between the power consumptions of the cipher suites in high and low security/power profiles is around 8.2% for WiFi, and 9.6% for 3G network. In order to further reduce the power consumption during network communication, the delay between sending two successive packets was analyzed. The proposed architecture is capable of stalling packets and sending them in burst-mode, letting the network interface to stay in low-power mode for a longer period of time. The power consumption in optimized 3G mode is reduced for additional 25%.

Acknowledgment

The research was supported in part by the Serbian Ministry of Education, Science and Technological Development (Project TR32012).

References

[1] J. Rivera, *Gartner Says Tablet Sales Continue to Be Slow in 2015*, Gartner Newsroom, Egham, UK, January 5, 2015.

[2] M. Shiraz, A. Gani, R.H. Khokhar, R. Buyya, *"A Review on Distributed Application Processing Frameworks in Smart Mobile Devices for Mobile Cloud Computing"*, IEEE Communications Surveys & Tutorials, vol. 15, no. 3, pp. 1294-1313, 2013.

[3] C. Liua, Q. Zhua, K. Holroydb, E. Sengb, *"Status and Trends of Mobile-health Applications for iOS Devices: A Developer's Perspective"*, The Journal of Systems and Software, Elsevier, vol. 84, no. 11, November 2011, pp. 2022-2033.

[4] D. Elminaam, H. Kader, M. Hadhoud, *Performance Evaluation of Symmetric Encryption Algorithms*, International Journal of Computer Science and Network Security, vol. 8, no. 12, pp. 280-286, 2008.

[5] V. Gupta, S. Gupta, S. Chang, *"Performance Analysis of Elliptic Curve Cryptography for SSL"*, Proceedings of the 1st ACM workshop on Wireless security - WiSE '02, ACM, New York, pp. 87-94, 2002.

[6] N. Potlapally, S. Ravi, A. Raghunathan, N. Jha, *"Analyzing the Energy Consumption of Security Protocols"*, Proceedings of the 2003 international symposium on Low power electronics and design - ISLPED '03, NY, USA, pp. 30-35, 2003.

[7] P. Miranda, M. Siekkinen, H. Waris, *"TLS and Energy Consumption on a Mobile Device: A Measurement Study"*, IEEE Symposium on Computers and Communications (ISCC), pp. 983-989, 2011.

[8] *"Optimizing Downloads for Efficient Network Access"* [Online] Available at: https://developer.android.com/training/efficient-downloads/efficient-network-access.html [Accessed: March 2015]

[9] R. Sims, C. Bauer, *"Handling a Device Changing from 3G to Wi-Fi Without Breaking Established Connections"*, New Trends in Networking, Computing, E-learning, Systems Sciences, and Engineering Lecture Notes in Electrical Engineering, Springer, vol. 312, pp 193-197, 2015.

[10] A. Gupta, P. Mohapatra, *"Energy Consumption and Conservation in WiFi Based Phones: A Measurement-Based Study"*, IEEE International Workshop on Wireless Ad-hoc and Sensor Networks - SECON 07, San Diego, California, USA, pp. 1-10, 2007.

[11] A. Sheth, R. Han, *"Adaptive Power Control and Selective Radio Activation For Low-Power Infrastructure-Mode 802.11 LANs"*, IEEE Workshop on Mobile and Wireless Networking, RI, USA, 2003.

[12] Little Eye Labs, *"How Little Eye Measures Power Consumption"* http://www.littleeye.co/blog/2013/07/ 30/how-little-eye-measures-power-consumption/ [Accessed: March 2015].