Performance Evaluation of an Enhanced Cryptography Solution for m-Health Applications in Cooperative Environments

Fabio Canelo[1], Bruno M.C. Silva[1], Joel J.P.C. Rodrigues[1], and Zuqing Zhu[2]

[1] Instituto de Telecomunicações, University of Beira Interior, Covilhã, Portugal
[2] School of Information Science and Technology, University of Science and Technology of China, Hefei, China

fabio.canelo@it.ubi.pt; bruno.silva@it.ubi.pt; joeljr@ieee.org; zqzhu@ieee.org

Abstract— **Mobile health (m-Health) applications delivers healthcare services through mobile applications regardless of time and place. An m-Health application makes use of wireless communications to sustain its health services and often providing a patient-doctor interaction. Therefore, m-Health applications present several challenging issues and constraints, such as, mobile devices battery and storage capacity, broadcast constraints, interferences, disconnections, noises, limited bandwidths, network delays, and of most importance, privacy and confidentiality concerns. This paper proposes a novel and enhanced cryptography solution in a cooperative environment considering a novel and early-proposed cooperation strategy for m-Health Applications. This proposal aims to face the challenges related to privacy and security issues of all forwarded and retrieved data concerning user sensitive information. Furthermore, it presents a performance evaluation of this proposal considering a comparison with an earlier proposed encryption strategy for the same cooperative environment.**

Keywords— Mobile Health; m-Health; Mobile computing; e-Health; Cooperation; Cryptography

I. INTRODUCTION

M-Health is considered the future of health telematics and a central point on healthcare innovation. It can be defined as the integration and application of health services in mobile technologies intended to deliver healthcare anywhere and anytime. Therefore, offering more ease of access to healthcare solutions overcoming issues like geographical, temporal, and even organizational barriers [1-2]. Hence, m-Health is commonly used in telemedicine allowing e.g., personal health care remote management and patient's health status monitoring [3]. Mobile devices and wireless communications support typical m-Health applications. However, these applications present several challenging issues and constraints, such as, battery and storage capacity, broadcast constraints, interferences, disconnections, noises, limited bandwidths, and network delays. Cooperation-based approaches are presented as a solution to solve such limitations and to improve wireless networks performance [4]. In the absence of a stable network infrastructure, mobile nodes cooperate with each other performing all networking functionalities [5].

A novel and early proposal of a reputation-based cooperation strategy for m-Health services, was presented in [6]. In its sense, this proposal allows and delivers access to health data despite connectivity state and availability. However, cooperation among mobile devices involves sensitive and private health data exchange, like personal health records or health treatment plans that are desirable to be kept private and undisclosed to unauthorized people. Health data privacy, integrity and authentication are major concerns when using m-Health applications. Cryptography algorithms are presented has a solution to the above mentioned security concerns. Due to the advent and evolution of current mobile devices, cryptographic algorithms are now capable of securing and exchanging data without the concern of mobile resources that could decrease cooperative gains and compromising the overall efficiency and effectiveness of the network or even degrading the mobile application user experience.

This paper presents a novel and enhanced cryptography strategy for m-Health applications in a cooperative environment called Enhanced Cryptography for Mobile Health Applications (eC4MHA). It focuses on assuring and guarantying the m-Health application data confidentiality, integrity, and authenticity. The performance assessment and evaluation of the proposal considers a comparison to a previous and early-proposed proposed encryption strategy for m-Health applications, called DE4MHA [7]. This evaluation studies the impact of the cryptography strategy on the performance of an m-Health application under the cooperative solution and environment. The evaluation was conducted using an m-Health application, named SapoFit, that aims obesity prevention and control [8-10].

The remainder of this paper is organized as follows. Section II elaborates on related work regarding health data privacy and security in a mobile environment that contributes to the proposed cryptography solution. Section III describes the proposed m-Health cryptography strategy in a cooperative environment while a performance evaluation and validation through a real m-Health application is presented in Section IV. Section V concludes the paper and points out further research suggestions.

II. RELATED WORK

Security is expected to be a central point in the evolution of pervasive m-Health applications towards mobile wireless networks. Energy saving in a mobile environment is a major concern that must be addressed carefully due to mobile

978-1-4799-1353-4/13/$31.00 ©2013 IEEE

devices limited resources. Often, typical m-Health network architectures require connectivity availability to operate with Web Services (WSs). This interaction is responsible for major energy consuming. Wi-Fi and Bluetooth transmissions are responsible for a significant consumption of battery power, specially Wi-Fi that can achieve up to 50% of the total energy unlikely Bluetooth which is believed to consume less than 10% battery power [11]. Furthermore, the mobile devices processing capability must be considered while developing mobile applications.

Cryptography algorithms are solutions to guarantee data confidentiality, integrity, and authenticity [12]. The use of these algorithms in mobile and wireless communications, represent time consuming and costly tasks to be executed. Therefore, a lightweight rather than complex approach is desired in such context. Securing e-Health data in a mobile environment has been a matter with high importance, mainly due to the data sensitivity associated exchanged between users [13]. In [14], it is proposed an architecture that allows exchanging patient's medical record in a secure way through existing infrastructure of mobile operators. Generic Bootstrapping Architecture (GBA) is used to enable user authentication while the other entity in the communication (service provider, hospital, and network operator) authenticates through usage of Public Key Infrastructure (PKI). To guarantee a secure communication, encryption and digital signature techniques are used. In [15], authors describe a new trend in security of e-health data presenting XML security solutions describing some selected solutions in health data. eXtensible Access Control Markup Language (XACML) and Security Assertion Markup Language (SAML) are presented enabling authentication and authorization in a large network space. Moreover, SAML enables transmission of authentication data between parties, namely between an identity provider and a service provider. XACML defines access control policies and a processing model describing how to evaluate authorization requests according to the rules defined in the policies.

The above-mentioned approaches present features required in an m-health scenario. However, some limitations arise, specifically the first one is the mobile operator dependency and the second one is focused towards systems exchanging data in XML format. Furthermore, cooperative scenarios present its own specific features and limitations, such as node misbehaviour or loss of connections requiring special care. Hence, an early-proposed encryption strategy for such cooperative scenarios was proposed in [7], called DE4MHA. This proposal addresses data privacy and protection achieved through a hybrid approach using both symmetric and asymmetric cryptography, not being confined to a specific mobile operator or a specific data file format. DE4MHA allows data exchange among nodes assuring data confidentiality through a symmetric algorithm, namely Advanced Encryption Standard (AES). An integrity and authenticity mechanism is achieved through usage of a combination of the Message Digest 5 (MD5) algorithm and the asymmetric algorithm Rivest, Shamir, Adleman (RSA). Afterwards, an output called message digest is calculated from the original message to be sent and then encrypted with RSA's private key. The result of the last operation (digital signature) is appended to the message, providing to the receiver the possibility of confirming if the received data is the original one and that it was sent from the expected source. This approach considers a peer-to-peer node-forwarding scheme based on node reputation, with message content aware, limiting WS access to nodes with low reputation value.

The cryptography strategy proposed in this paper overcomes the above-mentioned limitation that includes nodes forwarding messages with no content-aware other than strictly required information. Furthermore, mobile nodes act merely as messages forwarders. They do not perform encryption tasks, increasing the overall network performance in comparison to DE4MHA (demonstrated in section IV).

III. Cryptography Solution for m-Health Applications in Cooperative Environments

This section presents the reputation-based cooperation strategy for m-Health applications and the cooperative environment. Furthermore, it describes in detail, the novel cryptography solution for cooperative m-Health applications (eC4MHA).

A. Cooperation mechanisms

This reputation-based cooperation strategy relies on a WS to manage a fair access control to data and cooperation among nodes based on their reputation. According to the received reputation information, the WS decides if a requester node should have access to the requested data or not. Cooperating nodes with better reputation have priority over selfish nodes to access the m-Health application services.

This cooperation strategy for m-Health applications with service oriented architectures (SOAs) is based on two mobile and a remote module: *i*) the *node control message, ii*) the *requester control message*, and *iii*) the *cooperative Web service* (CWS).

The *node control messages* provide an awareness of the node status, i.e., if the node is willing to cooperate and in what conditions. It includes the node unique identifier, battery state, Internet connectivity status, as well the node cooperation status. The *requester control message* is first sent from the requester node (a mobile node without Internet connection and therefore without access to the m-Health application services) and it contains five main components: 1) the requester ID, the node unique identifier; 2) the service request, i.e., what the node is specifically requesting (e.g., the login token or its health profile); 3) the neighbors list; 4) the reputation list; and 5) the achieved cooperation time (ACT).

The *cooperative Web service* (*CWS*) is responsible for performing a fair access control to data, deciding if a node should be able to get the requested data or not. Thus, according to the received reputation information, the *CWS* holds the final reputation list in order to decide if a requester node should have access to the m-Health application Web service or not. The reputation list contains all the registered network nodes with their identifier and their respective reputation value.

B. *Enhanced Cryptography Solution for M-Health Applications: eC4MHA*

eC4MHA focuses on three major concerns on mobile and wireless communications, namely data confidentiality, integrity, and authenticity. Confidentiality assures that data is not made available or disclosed to unauthorized persons. However, guarantying data confidentiality may not be enough to ensure overall security and privacy of personal health information. Data integrity and authenticity assures that data has not been modified and its source is reliable.

Assuring Data Confidentiality

Two approaches were considered, 1) using only asymmetric cryptography, and 2) a hybrid approach using both asymmetric and symmetric cryptography. The first approach considered the usage of RSA algorithm with a 1024 bits key size on both mobile nodes and the WS itself. After public key exchange between the WS and a mobile node, all the exchanged information would be encrypted on the sender's side with the receiver's public key and decrypted with the receiver's private key. Although this option is completely valid to specific scenarios, it is necessary taking into account that RSA algorithm can only encrypt a limited amount of data that is directly related to the public key size. For instance, a 1024 public key can only encrypt 117 bytes, i.e., (1024/8) - 11 bytes.

eC4MHA aims any m-Health system, including applications that deal with different amounts of data. Therefore, this approach was not feasible and was discarded.

The second approach considered and applied in eC4MHA, is based on using a hybrid scheme to perform data confidentiality. The AES symmetric algorithm was chosen to encrypt all the data and the RSA asymmetric algorithm was used to exchange a random secret key used by the AES. It is assumed that an user is able to access directly (through Internet connectivity) the m-Health application WS (1). The reason for such assumption is the required exchange of the secret key between the WS and the mobile node (2,3) before encryption can be performed, followed by an acknowledgement sent by the WS (4), as may be seen in Figure 1. Therefore, the user is now able to securely retrieve health data, whether cooperation is required or not. Thus, the applied strategy assumes a secure transaction of data between nodes and the WS using the AES encryption algorithm in Cipher Feedback Mode (CFB), with a key size of 128 bits, and RSA algorithm with a 1024 bits keys size to exchange secret keys between nodes, and the WS.

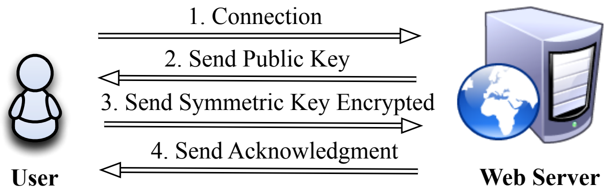

Figure 1 – Illustration of the Key exchange sequence on eC4MHA.

Integrity and authenticity

To assure authenticity, eC4MHA uses Message Digest 5 (MD5) algorithm in order to produce a 128 bits output, called message digest. To guarantee integrity, it uses the RSA algorithm to encrypt the message digest, commonly known as digital signature. The digital signature is then appended to the message that should be sent over the network.

Under this approach, cooperative mobile nodes should know their personal information that is being carried by messages sent all over the network, namely, the *requester control message* that contains user access credentials, such as username or password. A cooperative mobile node will merely act as a packet forwarder, until it reaches a mobile node with Internet connectivity. The mobile node is not aware of the packet content, other than required cooperative data such as node identification in order to forward back the response or reputation lists (RLs) determining and updating the level of cooperativeness of each mobile node. Through this proposal, it is assured that none of the sensitive information, such as login tokens or user's health information, is disclosed to unauthorized persons. Furthermore, it guarantees that information received is the original one as well as it comes from an expected and reliable source.

Key Management

Cryptography algorithms require encryption/decryption keys to operate. Therefore, it is vital to assure key's protection and privacy. This fundamentally depends on two factors, namely, where the keys are stored and who has access to them [16]. eC4MHA uses a *keystore* to store and assure key's protection and privacy. As above-mentioned, it is necessary to establish a previous connection to the WS in order to exchange a secret key for later communications. After a secret key generation, a *keystore* is created and the key is then securely stored and protected with a user password in the mobile device. To retrieve the secret key, the user must provide a password (in a transparent manner). Although the secret key is physically present in the device, it is not possible to access it from another application other than the application used to store the key. As for the WS, a *keystore* is also generated and used to store its own private key and each secret key needed for each node that requests data.

Figure 2 presents the overall and usual workflow of the eC4MHA in a cooperative environment. As may be seen, a requester node will try to discover and establish a connection to a mobile node through the above-mentioned cooperation mechanisms (1), receiving then a *node control message(2)*. Then, a *requester control message* is sent to the requested node (3) in order to define what information is it requiring. All the sensitive data is encrypted and signed. The requested node will then forward the request to the WS (4). The WS will receive the data, encrypting and signing it. The response is sent back to the request node (5) forwarding it to the requester node (6) that, after decryption, message integrity, and authentication verification will obtain the requested data (7).

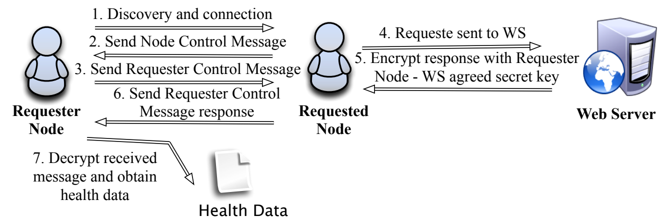
1. Discovery and connection
2. Send Node Control Message
3. Send Requester Control Message
6. Send Requester Control Message response
4. Requeste sent to WS
5. Encrypt response with Requester Node - WS agreed secret key
Requester Node
Requested Node
Web Server
7. Decrypt received message and obtain health data
Health Data

Figure 2 – Illustration of the eC4MHA overall workflow.

IV. Performance Evaluation

This section focuses on the performance evaluation and validation of the m-Health cryptography proposal. An m-Health application, called SapoFit, was used to evaluate the performance of the proposed cryptography approach. The network scenario and expected node behaviors are also presented. Then, the validation and feasibility of the proposal is evaluated through a comparison with an early-proposed cryptography strategy, called DE4MHA, above described in Section II.

A. *SapoFit Application*

SapoFit is a weight control mobile application that allows users to keep track of weight [8-10]. It allows users to control their weight, body mass index (BMI), basal metabolic rate (BMR), sports activity, and the possibility to follow food plans based on their needed calories. In this m-Health application all the users must be registered in a Web service. For performance evaluation of eC4MHA, it is considered a user without Internet connection requesting access to the *Login* and *Food Plans* services. Therefore, the user *Profile* will be fully obtained through cooperation among nodes.

B. *M-Health network scenario*

An illustration of the real network scenario used for the performance evaluation study of the eC4MHA may be seen in Figure 3. It includes seven mobile nodes (using SapoFit), where three of them are assumed to be uncooperative nodes. Node M is the only node with available connection to the SapoFit Web services. Although this scenario may present mobility issues, for evaluation purposes, it is considered that each mobile node assumes the position presented in the network scenario. The simulation environment can be summarized as follows: 7 mobile devices considering 3 uncooperative nodes, a requester node, and a single node with Internet connectivity.

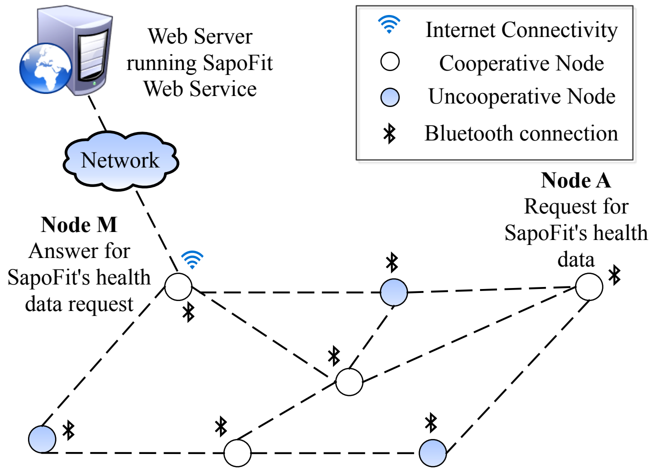
Web Server running SapoFit Web Service
Internet Connectivity
Cooperative Node
Uncooperative Node
Bluetooth connection
Network
Node A
Request for SapoFit's health data
Node M
Answer for SapoFit's health data request

Figure 3 - Illustration of the network scenario for performance evaluation of the eC4MHA.

The activity diagram of a mobile node is presented in Figure 4 It is subdivided into two logical parts: 1) Node discovery and connection and 2) *Cooperative Web Service*. The main goal consists in establishing a connection with the WS to obtain the required data. First, a node with no Internet connectivity and, therefore, unable to retrieve required data by itself, starts searching for neighbor nodes. If a node is found, cooperation information is exchanged among them, determining the cooperation status of the requested node as well what information it wants to retrieve. If the requested node is willing to cooperate, a *requester control message* is sent to the requested node. Sensitive information, e.g., passwords or health data, is encrypted with a secret key, shared uniquely between the requester node and the WS, and then signed with requester node’s private key. This way, the cooperative node will not be able to access unauthorized information, but only strictly required information necessary to forward the request to the WS. As soon as the request arrives at the WS, it verifies the authenticity and integrity of the request. If both are verified, the required data is obtained by the WS and then encrypted with the previous referred key. Furthermore, the content of the message is also signed by the server in order for the requester node to check its integrity and authenticity. Later the message is sent to the requested node, with only the required information to decrypt.

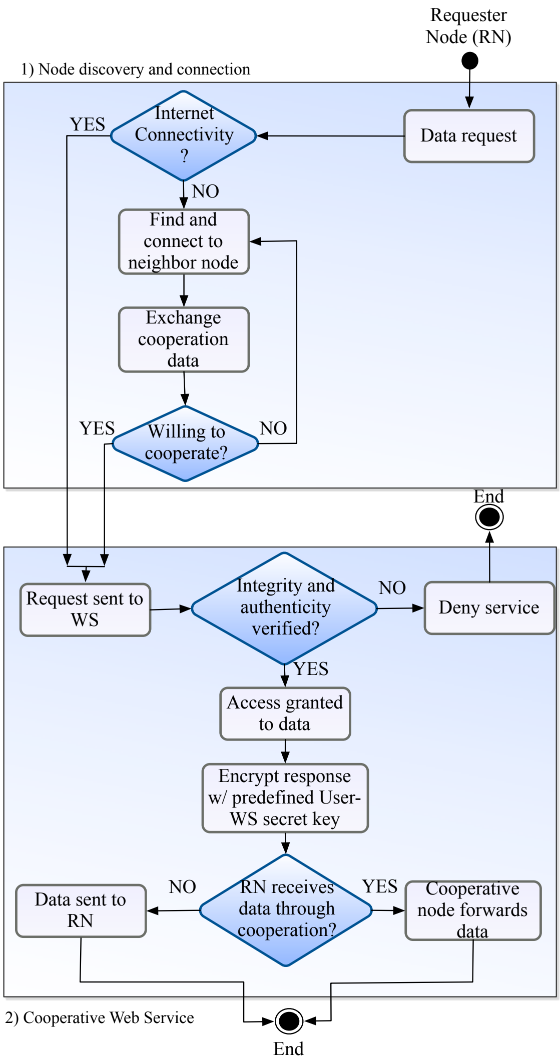
Requester Node (RN)
1) Node discovery and connection
Data request
Internet Connectivity ?
YES
NO
Find and connect to neighbor node
Exchange cooperation data
Willing to cooperate?
YES
NO
End
Request sent to WS
Integrity and authenticity verified?
NO
Deny service
YES
Access granted to data
Encrypt response w/ predefined User-WS secret key
RN receives data through cooperation?
NO
YES
Data sent to RN
Cooperative node forwards data
2) Cooperative Web Service
End

Figure 4 - Activity diagram of a mobile node representing a mobile device with SapoFit and a typical node behavior.

C. *Performance Analysis*

This section focuses on the performance analysis eC4MHA through a comparison with an early-proposed cryptography strategy, called DE4MHA, above described in Section II.

The study was performed through a real m-Health application, called SapoFit. The case study scenario included seven devices running the SapoFit application. Non-cooperative cases were controlled and measured to worst case-scenario of three uncooperative nodes, to guarantee the minimum service performance. However, uncooperative nodes affect directly the service delivery probability, the service average delay, and the overall network performance. Hence, the first analysis refers to the performance comparison of the m-Health application with and without the used cryptography mechanisms. To obtain a comparison of both cases, performance metrics were considered, namely the service delivery probability and the service average delay (in seconds). The service delay is measured as the time between the request and its corresponding response. The service delivery probability and the service average delay in function of the number of uncooperative mobile nodes in both scenarios (with and without cryptography algorithms) are presented in Figures 5 and 6. As may be seen, cryptography algorithms degrade slightly the overall performance, as expected, due to more time consuming tasks, such as encryption and decryption. Furthermore, the service delivery probability presents similar results with cryptography algorithms. The variance reflects the use of eC4MHA in cases where whether integrity or authenticity is not guaranteed, resulting in a denial of service to the initial request, therefore, contributing to the decrease of the service delivery probability.

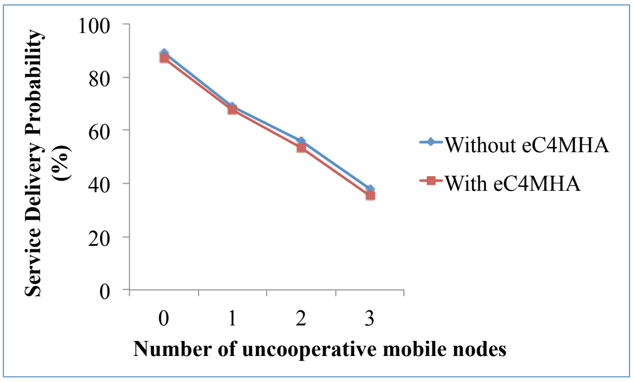

Figure 5 - Service delivery probability as function of the number of uncooperative nodes with and without eC4MHA.

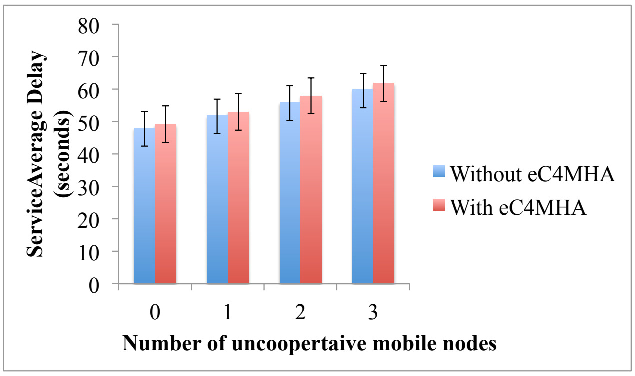

Figure 6 - Service average delay as function of the number of uncooperative nodes with and without eC4MHA.

The maximum service delay observed with three uncooperative nodes was about 59.8 seconds without eC4MHA with a standard deviation of 5.14 seconds, and about 61.8 seconds with eC4MHA, presenting a standard deviation of 5.57 seconds. These main variances were mostly caused by mobile devices constraints, such as loss of Bluetooth connection or distance variations among mobile nodes.

A performance evaluation analysis with the comparison to of both cryptography approaches for m-Health application, DE4MHA and eC4MHA was also considered and studied (Figure 7). Measuring the service average delay with both approaches it was demonstrated that eC4MHA is more effective and have better overall performance over DE4MHA. Significant changes were made to the previous proposed strategy considering that each cooperative node would be aware of message content by turning them acting uniquely as packet forwarders in this new approach. Results show a slight improvement in the performance of service average delay with the eC4MHA. In a worst case-scenario with three uncooperative nodes, the requester node would receive the response to the request in about 64.06 seconds with DE4MHA and a standard deviation of 5.57 seconds while with eC4MHA an average of 61.8 seconds would be necessary in order to receive the response, with a standard deviation of 5.56 seconds.

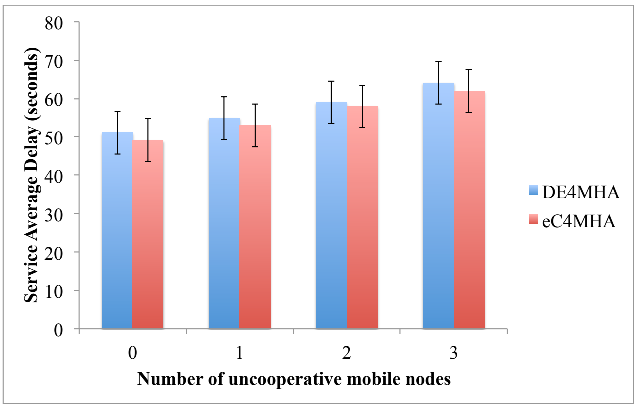

Figure 7 – Performance comparison of the service average delay in function of the number of uncooperative mobile nodes for DE4MHA and eC4MHA.

V. Conclusion and Future Work

This paper proposed a robust cryptography strategy for m-Health applications in a cooperative environment following a service-oriented architecture. This approach presented a solution where user health data is retrieved from a Web service through cooperation. It considers three main aspects: data confidentiality, data integrity, and data authenticity. The main objective of providing a cryptography solution for user's health data for m-Health applications in cooperative scenarios was fully accomplished. Another accomplished goal was the improvement of an earlier-proposed cryptography strategy, called DE4MHA, resulting in the eC4MHA.

The proposed solution was evaluated, demonstrated and validated through a real m-Health application, called SapoFit. Performance metrics were considered, such as service average delay and service delivery probability. The performance of the proposed eC4MHA was compared with DE4MHA. It was shown that it slightly increases service average delay and decreases service delivery probability. However, these results are totally feasible and tolerable in a real scenario and insignificant considering the assuring of privacy and security of the m-health data.

A comparison of both cryptography approaches and the respective performance evaluation through simulation, with different network scenarios and scalability, may be considered for future work.

Acknowledgments

This work has been partially supported by *Instituto de Telecomunicações*, Next Generation Networks and Applications Group (NetGNA), Portugal, by National Funding from the FCT - *Fundação para a Ciência e a Tecnologia* through the PEst-OE/EEI/LA0008/2013 Project, and by the AAL4ALL (Ambient Assisted Living for All), project co-funded by COMPETE under FEDER via QREN Programme.

References

[1] S. Tachakra, X. Wang, R. Istepanian and Y. Song, " Mobile e-Health: the Unwired Evolution of Telemedicine," Telemedicine Journal and e-Health, vol. 9, nº 3, 2003, pp. 247–257.

[2] S. Akter, and P. Ray, "mHealth - an Ultimate Platform to Serve the Unserved," IMIA Yearbook of Medical Informatics, 2010, pp. 94-100.

[3] I. Cubic, I. Markota, and I. Benc, "Application of session initiation protocol in mobile health systems," presented at the MIPRO, 2010 Proceedings of the 33rd International Convention, Opatija, Croatia, May 24-28, 2010, pp. 367–371.

[4] G. Kramer, I. Maric, and R. D. Yates, "Cooperative communications (Foundations and Trends in Networking)," Now Publishers Inc., June 2007, ISBN-10: 1601980264.

[5] L. Buttyan and J.-P. Hubaux, "Stimulating Cooperation in Self-Organizing Mobile Ad hoc Networks," Mobile Networks and Applications, vol. 8, nº 5, 2003, pp. 579–592.

[6] B.M.C. Silva, J.J.P.C. Rodrigues, I.M.C. Lopes, T.M.F. Machado, L. Zhou, "A Novel Cooperation Strategy for Mobile Health Applications," IEEE Journal on Selected Areas in Communications Special Issue on Emerging Technologies in Communications - eHealth, IEEE Communications Society (in press).

[7] B.M.C. Silva, J.J.P.C. Rodrigues, F. Canelo, I.C. Lopes, and L. Zhou, "A Data Encryption Solution for Mobile Health Applications in Cooperation Environments: DE4MHA", Journal of Medical Internet Research (JMIR), vol. 15, nº 3, 2013, DOI: 10.2196/jmir.2498.

[8] B.M.C. Silva, I.M. Lopes, P. Ray, and J.J.P.C. Rodrigues, "SapoFitness: A Mobile Health Application for continuous Monitoring Dietary Evaluation", 13th International Conference on E-Health Networking, Applications and Services (IEEE HEALTHCOM 2011), Columbia, MO, USA, June 13-15, 2011.

[9] J.J.P.C. Rodrigues, I.M.C. Lopes, B.M.C. Silva, and I. Torre, "A New Mobile Ubiquitous Computing Application to Control Obesity: SapoFit", in Informatics for Health and Social Care, Informa Healthcare, 2013, 38(1):37-53.

[10] SapoFit, https://itunes.apple.com/pt/app/sapo-fit/id438487775?mt=8, Accessed in March 2013.

[11] T. Pering, Y. Agarwal, R. Gupta and R. Want, "CoolSpots: reducing the power consumption of wireless mobile devices with multiple radio interfaces," in MobiSys '06: Proceedings of the 4th international conference on Mobile systems, applications and services, Uppsala, Sweden, June 19 - 22, 2006, pp. 220-232.

[12] K. Raychaudhuri and P. Ray, "Privacy Challenges in the Use of eHealth Systems for Public Health Management," International Journal of e-Health and Medical Communications, IGI-Global, vol. 1, no. 2, pp. 12–23, 2010.

[13] R. Sulaiman, D. Sharma, W. Ma, and D. Tran, "A Security Architecture for e-Health Services," 10th International Conference on Advanced Communication Technology, Korea, February 17-20, 2008, pp. 99-104.

[14] M. Shanmugam, S. Thiruvengadam, A. Khurat, and I. Maglogiannis, " Enabling Secure Mobile Access for Electronic Health Care Applications," Pervasive Health Conference and Workshops, Innsbruck, Austria, November 29-December 1, 2006, pp.1-8.

[15] D. Brechlerova, M. Candik, "New trends in security of electronic health documentation," 42nd Annual IEEE International Carnahan Conference on Security Technology, Prague, Czech Republic, October 13-16, 2008 pp.13-16.

[16] M. Krishna, M. Doja, "Symmetric key management and distribution techniques in wireless ad hoc networks," International Conference on Computational Intelligence and Communication Networks (CICN), Gwalior, India, October 7-9, 2011, pp.727-731.