Towards a Cooperative Security System for Mobile-Health Applications

Bruno M.C. Silva[1], Joel J. P. C. Rodrigues[1], Fábio Canelo[1] , Ivo M. C. Lopes [1] and Jaime Lloret[2]

[1]Instituto de Telecomunicações, University of Beira Interior,
Rua Marquês d'Ávila e Bolama, 6201-001 Covilhã, Portugal

[2] Integrated Management Coastal Research Institute, Universidad Politécnica de Valencia, C/Paranimf, n° 1, 46730, Grao de Gandia, Spain

E-mail: bruno.silva@it.ubi.pt, joeljr@ieee.org, {fabio.canelo; ivo.lopes}@it.ubi.pt, jlloret@dcom.upv.es

Abstract – Mobile Health (m-Health) system architectures are typically based on mobile and wireless communications, and use mobile devices with data exchange supported by Web Services (WS). Although m-Health systems offer mobility as a potential and precious resource they also present several challenged issues and constraints, such as, battery and storage capacity, broadcast constraints, interferences, disconnections, noises, limited bandwidths, and network delays. Furthermore, constant mobility and often-required Internet connectivity also exposes and compromises the privacy and confidentiality of the m-Health system information. This paper proposes a novel data encryption solution for mobile health systems, considering a novel and early-proposed cooperation strategy. This encryption solution, called data encryption for mobile health applications (DE4MHA), tries to guarantee the best confidentiality, integrity, and authenticity of m-health systems users data. The paper also presents a performance evaluation study comparing the performance an m-Health application with and without the DE4MHA.

Keywords: Mobile Health; m-Health; Mobile computing; e-Health; Cooperation; Cryptograph; Encryption; Security

1. Introduction

Mobile health (m-Health) is considered the future on Health telematics and a new edge on healthcare innovation. It proposes and aims to deliver healthcare anywhere and anytime, surpassing geographical, temporal, and even organizational barriers [2,64]. It offers more accessible and affordable healthcare solutions to patients that live in remote rural areas, that travel constantly or that for some reason are physically incapacitated [40, 1]. In the last decade m-Health has been an important area of research gathering and innovating important findings and contributions to several health topics, such as, cardiology [46, 22, 38], diabetes [34, 42, 31], obesity [70, 48,47,66], smoking cessation [67], and healthcare services for developing countries [17], among others.

Typical m-Health services include mobile devices and wireless communications. Figure 1 illustrates a typical architecture of an m-Health system interacting with a Web service (WS) that delivers and provides several health services. However, these services and architectures present several challenging issues and constraints, such as, battery and storage capacity, broadcast constraints, interferences, disconnections, noises, limited bandwidths, and network delays.

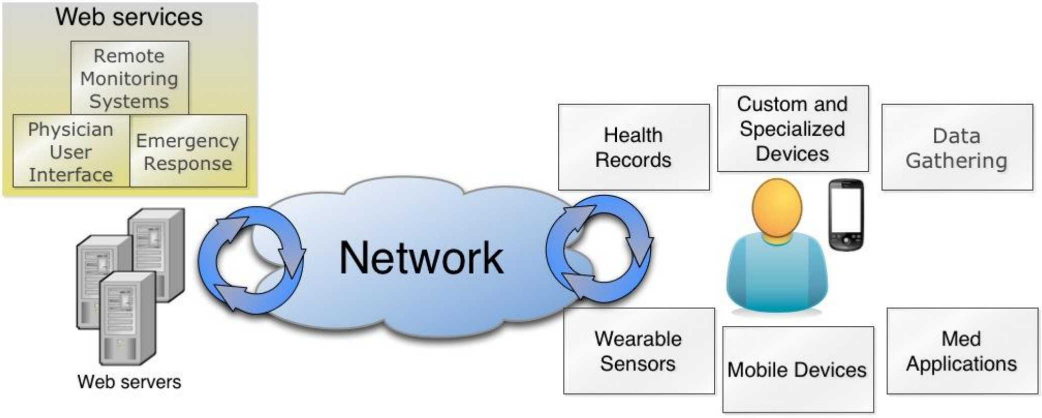


Figure 1. Illustration of a typical m-Health network architecture.

Several research studies present cooperation-based approaches as a solution to solve such limitations and also to improve wireless networks performance [33, 11]. In the healthcare context, cooperation among healthcare professionals has been studied and concluded that can improve their work and performance. Computer-supported cooperative work (CSCW) is usually used to share information through broadband and telecommunication networks (e-Mail or instant messaging) [5]. However, CSCW applied to healthcare information systems could enable patients and healthcare professionals to work together and share more efficiently health information even from remote locations [52,12].

Another challenging issue in m-Health services and applications is privacy and security. Moreover, security and privacy have been over the last year a point of interest in designing and researching IT solutions [3,13,25,29,35]. M-Health applications often save or access to sensitive and personal information. A patient or a healthcare professional that manages such information must assure its confidentiality**,** integrity, and authenticity**.** Therefore, cryptographic mechanisms can be seen as an excellent solution to guaranty health information privacy and protection [52].

This paper proposes a data encryption solution for mobile health applications (DE4MHA) for an early-proposed cooperation strategy presented in [60] considering m-Health systems to assure data confidentiality, integrity, and authenticity. The cooperation strategy and the DE4MHA are deployed and evaluated in a real m-Health application for obesity prevention and control, called SapoFit [61,55,56]. The DE4MHA includes the use of the RSA algorithm [32] for asymmetric encryption/decryption to assure Key exchange confidentiality and the Advanced Encryption Standard (AES) algorithm [50] for symmetric encryption/decryption assuring data confidentiality. To ensure data integrity a message digest is created with the generation of a hash of the transmitted data. Digital signature is used for data authenticity, encrypting the previous hash message with the RSA private Key. The HTTPS protocol is used to secure the communication with the SapoFit Web service (WS). The network performance assessment and validation of the proposal is also presented. This evaluation proves its feasibility and also studies the impact of the DE4MHA over the cooperation strategy for m-Health applications.

The main contributions of the paper are the following:

- Study of encryption/decryption algorithms for typical m-Healh network architectures;
- Proposal of an encryption/decryption hybrid approach using symmetric and asymmetric encryption algorithms for typical m-Healh network architectures;
- Proposal of a data encryption solution for mobile health applications (DE4MHA) in cooperation environments.

The remainder of this paper is organized as follows. Section II elaborates on related work about the topic focusing on cryptography approaches suitable for e-Health and m-Health applications. Section III summarizes the early-proposed cooperation strategy where the DE4MHA was applied and the cryptography proposal and its conceptual design is presented in Section IV. The performance evaluation and assessment of DE4MHA is presented in Section V. Finally, Section VI concludes the paper and points out further research works.

2. Related Work

One of the most known and to the best of authors knowledge the first definition of m-health comes from Istepanian and Lacal [28] when, in 2003, defined mobile health as “emerging mobile communications and networks technologies for healthcare”. In 2006, Laxminarayan *et al.* [37] presented an extensive study on the impact of mobility on the existing e-Health systems. In [16] authors define mobile health as “the provision of healthcare services through use of information and communication technologies (ICT) for mobile users”. Mobile health services are present in a large scale in the applications available to users allowing them to obtain useful information about their health care serving as well as awareness prevention. M-Health systems and applications use the Internet and Web Services to provide an authentic pervasive interaction between physicians and patients. Any healthcare professional or a patient can easily access the same medical record anytime and anywhere through his personal computer, tablet, or smartphone. With the proliferation of mobile devices [54], innumerous m-health applications have been developed and turned available to the public through online markets [49] giving users the possibility of monitoring their own health state, allowing them to create and maintain their own health records, treatments alerts, health goals establishment, just to name few of them.

2.1 Challenges in m-Health systems design

The use and the design of mobile applications and systems include several challenges, such as, limited computing power, storage space, and battery lifetime, among others [26]. Therefore, a lightweight computing approach rather than an intensive and complex approach is desired in such context [14]. Furthermore, mobile devices face several security issues summarized as follows [69]:

- **Message interception and falsification** – By monitoring and analysing wireless traffic introducing then false packets to achieve network access compromising communications.
- **Impersonation, identity theft and fraud** – When using technical or social engineering techniques, credentials of legitimate users may be obtained.
- **Mobile virus and devices hijacking** – A device can be fully exposed to attacks if viruses, Trojans, or worms are installed in a disguised form.
- **Spamming** – Sending a huge amount of unsolicited SMS messages or Instant Messages to users.

- **Phishing** – Term usually used to define the process that involves sensitive information acquisition, like usernames, passwords or, e.g., credit card details through trust agent personification on electronic communication. It is often accomplished by redirecting users to fake Websites that look exactly as the one they expected.

When creating and designing m-Health services, it is extremely important to give the appropriated attention to all the above-mentioned issues to assure that health data is secure and not compromised. The most appropriate and ideal solution to handle such security issues is cryptography [43].

2.2 Cryptography approaches suitable for e-Health and m-Health services and applications

Cryptography may be defined as a set of techniques and algorithms to assure safe communication between two agents, on an open network channel. Moreover, it answers numerous issues of a communication process, such as, confidentiality**,** integrity, and authenticity [24]**.**

2.2.1 Confidentiality

Confidentiality assumes that data is unavailable or disclosed to unauthorized persons [39]. Therefore, referring confidentiality implies dealing with encryption algorithms. Encryption is the process of encoding messages so that only authorized agents should be able to read them. Hence, several algorithms were developed over the past decades to deal with the increasing need of assuring data confidentiality and they may be divided into two main groups, (1) symmetric algorithms where both encryption and decryption is accomplished using the same key and (2) asymmetric algorithms where one key is used for encryption (public key) and another one is used for decryption (private key) [45].

As above-mentioned, symmetric algorithms use the same key for encryption and decryption. In this section, several encryption algorithms that are suitable for m-Health applications are considered. A typical symmetric encryption algorithm workflow is presented in Figure 2. A number of well-known symmetric key encryption algorithms suitable for e-Health systems enumerated in [10] have been studied, namely, the following: DES, 3DES, AES, Blowfish, IDEA, and RC4.

Data Encryption Standard (DES) [23] is an algorithm developed by IBM, in 1975, that as been adopted and published as a Federal Information Processing Standard (FIPS) in 1977. The algorithm operates on a 64 bits data block and a fixed key length of 56 bits size for 16 rounds. Nowadays, it is considered to be out-dated and it has been replaced by its successor 3DES.

TripleDES, or 3DES algorithm [27], was introduced in 1978 by IBM as an extension of DES. 3DES applies DES algorithm three times instead of just one, supporting 112 bits or 168 bits key length and a block size of 64 bits that operates on 48 rounds.

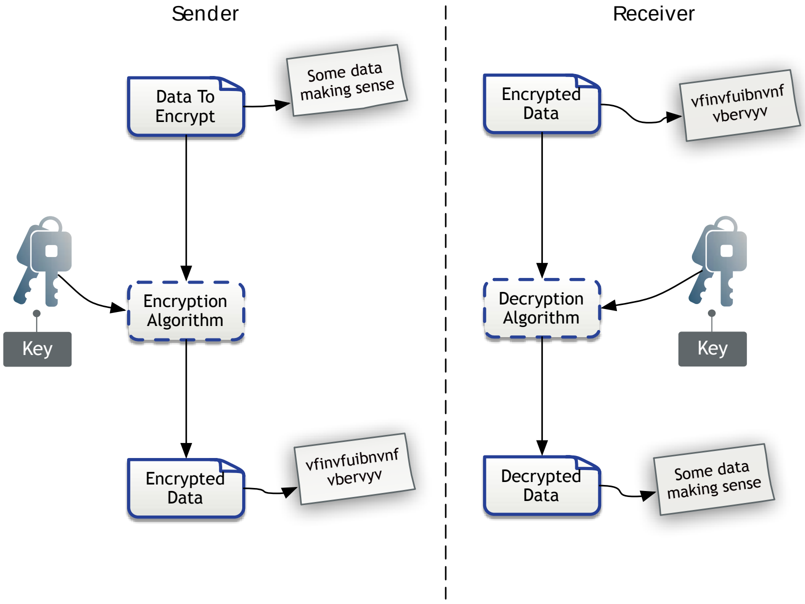


Figure 2. Illustration of a symmetric encryption algorithm workflow.

In 2001, in an open competition (known as Advanced Encryption Standard process), promoted by the National Institute of Standards and Technology (NIST), with the purpose of replacing the existing DES algorithm, two Belgian cryptographers proposed an algorithm originally named Rijndael that later became known as Advanced Encryption Standard (AES) [65]. It operates on a block cipher of 126 bits size and the key size is 128, 192, or 256 bits.

Another widely known symmetric algorithm is RC4 [30], also known as ARC4 or ARCFOUR and it was designed by Ron Rivest in 1987. This algorithm is applied to the Secure Socket Layer (SSL), WEP or PDF. It uses variable key length from 40 to 256 bits, as well as variable block sizes, changing its speed in encryption/decryption operations.

Blowfish [57] is another symmetric algorithm with worldwide acceptance and it was originally designed by Bruce Schneier, in 1993. The algorithm uses a variable key length between 32 and 448 bits (128 bits by default) and a 64 bits block size for operations on 16 rounds.

International Data Encryption Algorithm (IDEA) [7] is the best known for its use in Pretty Good Privacy (PGP) v2.0. It is an algorithm that operates on a 64 bits block size with a 128 bits key size. Asymmetric cryptography, more known as public key cryptography, can be used to assure confidentiality. A typical asymmetric encryption algorithm workflow is presented in Figure 3. In this type of algorithms, two keys are required in order to operate. One key, known as public key, is used to encrypt the content of a message and the other one (private) key is used to decrypt it. These type of algorithms solve some of the faults of the symmetric algorithms, although they are considered to be at least 1000 times slower than symmetric ones [6] and keys size must be significantly bigger (for example, a 1024 bits key of an asymmetric algorithm corresponds approximately to a 128 bits key of a symmetric algorithm), and it is usually harder to handle key management. These types of algorithms are usually used for identification purposes or to session key exchange without requiring a trust agent [18].

RSA is an example of an asymmetric algorithm and its name stands for **R**ivest, **S**hamir and **A**dleman, the founders of the referred algorithm. It is widely known by being appropriated to encrypt/decrypt as well to perform digital signature. It was proposed in the late 70’s but it is still used currently. Another example of asymmetric algorithm is Elgamal, described by Taher Elgamal in 1984 [21].

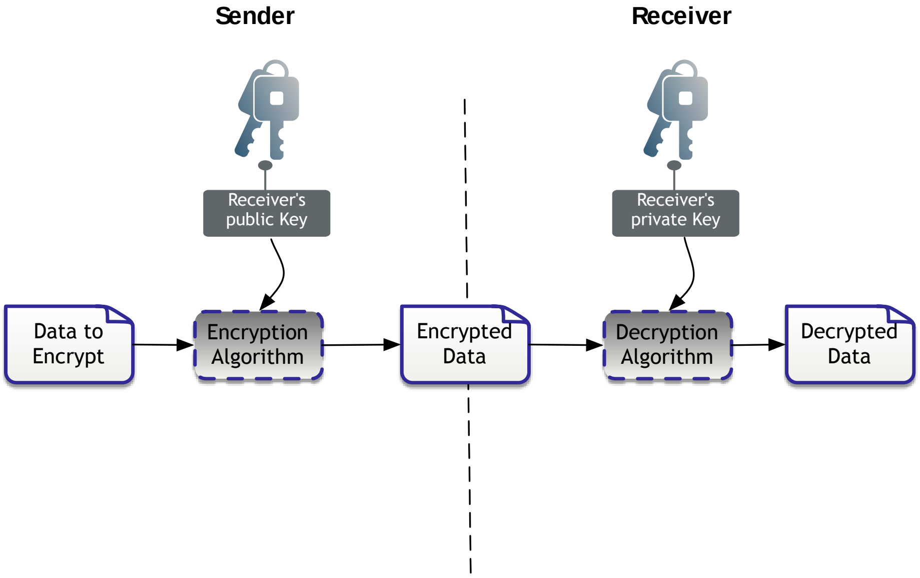


Figure 3. Illustration of asymmetric encryption algorithm workflow**.**

2.2.2 Integrity

Integrity is intended to provide users whether some data remains as it was when it was firstly created or if it has been changed [15, 58]. Health information is known as sensitive information in which a small change of the original information may have a negative outcome. Therefore, it is usually a good idea to use algorithms that can assure that users are handling unchanged and original information. Hence, cryptographic hash functions are used for that purpose.

As an example of a hash algorithm, Message Digest 5 can be named and it was designed by Ron Rivest, in 1991 [53], and it is largely used to check data integrity. It produces a 128-bit output, called message digest. In order to check data integrity, the same piece of data must always produce the same message digest as output, though in rare cases it may produce the same message digest for different piece of data [68]. For instance, given some data sent over the network, if it suffers any change when arriving at the end point, it will produce a different message digest, what makes possible to check data integrity.

Secure Hash Algorithm 1 (SHA-1) is an algorithm to assure data integrity, producing a 160 bit message digest. Both algorithms allow checking data integrity, by computing the message digest of a certain message. Any change of the message will almost certainly result in a different message digest, which allows to check if data integrity has been compromised or not [19].

2.2.3 Authenticity

Authenticity is another important concept when handling with security mechanisms. Nowadays, in every system, it is vital to assure that users send or receive information from the expected person or entity. Authenticity can be achieved using the above-mentioned RSA algorithm in combination with a hash function where the private key is used to encrypt the message digest. Then, the public key is used to decrypt the message digest and, when compared with the generated message digest on the sender side, both must be equal. Digital Signature Algorithm (DSA) [44] also provides digital signature capabilities. However, DSA can only sign and cannot encrypt information. Furthermore, it uses SHA-1 to generate the message digest as opposed to MD5 used by RSA. DSA was proposed by David Kravitz. In 1991, it was adopted by the National Institute of Standards and Technology (NIST).

2.3 Mobile health security approaches

Over the years securing e-Health data has been a matter with high importance, mainly due to the sensitivity data exchanged between users [63]. Many studies have been conducted in order to assure secure communications conveying e-Health data. In [62], a security model is presented focusing in identification, authentication, access control, integrity, confidentiality, and availability matters. For that purpose, cryptography has been widely used and studied in systems that share and transmit health data [9]. Furthermore, in [59], it is proposed an architecture that allows exchanging patients medical record in a secure way through the available 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 the usage of Public Key Infrastructure (PKI). Finally, to guarantee secure communication, encryption and digital signature techniques are used. Although the use of standard security mechanisms of mobile networks and service providers present benefits, such as easy utilization and implementation of proven secure solutions, it clearly introduces some issues including the service provider and mobile network provider cooperation as well defining privacy and security policies concerning patient’s private health data while transferred outside the source management. Since there are multiple mobile networks providers in each country and in order to turn health secure services available to all the potential users, it is clear that several agreements between multiple parties should be defined to turn this solution mobile operator dependent [59]. In

[41], the 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) languages are presented enabling authentication and authorization in a large network space. More specifically, SAML enables transmission of authentication data between parties, namely between an identity provider and a service provider. XACML defines access control policies as well as a processing model describing how to evaluate authorization requests according to the rules defined in the policies.

Lacuesta et al, presents in [36], a hybrid symmetric/asymmetric secure protocol for wireless ad hoc networks. This proposal also implements a trust scheme between users for data and secret key exchange. This scheme is based on the first visual contact between network nodes and its completely self-configured and able to create the entire network and exchange secure services.

3. Cooperation Strategy

This section describes, in detail, the early-proposed cooperation strategy for m-Healh applications [60]. This reputation-based strategy is based on the following three modules: *i*) *a node control message*, *ii*) a *cooperative list*, and *iii*) a *cooperative Web service* (*CWS*).

3.1. Nodes control message and cooperative list

The *node control message*, illustrated in Figure 4, contains a *node ID*, *node status* (storage capacity, energy, and Internet connectivity), and its *cooperation status* (cooperative or uncooperative). This *control message* is exchanged when a node establishes contact with a neighbor node. This *message* tries to provide an awareness control of all neighbor nodes knowing if they are willing to cooperate and in what conditions.

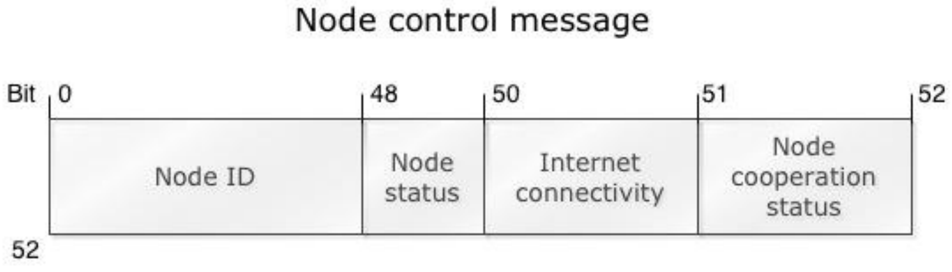


Figure 4. Node control message.

The *network cooperative list*, illustrated in Figure 5, registers all the cooperative and uncooperative network nodes throughout a service request. This *list* classifies all the neighbor nodes cooperative actions. It saves the *Node ID* and adds or subtracts a classification threshold according to the node *cooperation status*. When a service is requested from a node without Internet connectivity, all the nodes update their status in the *cooperative list*.

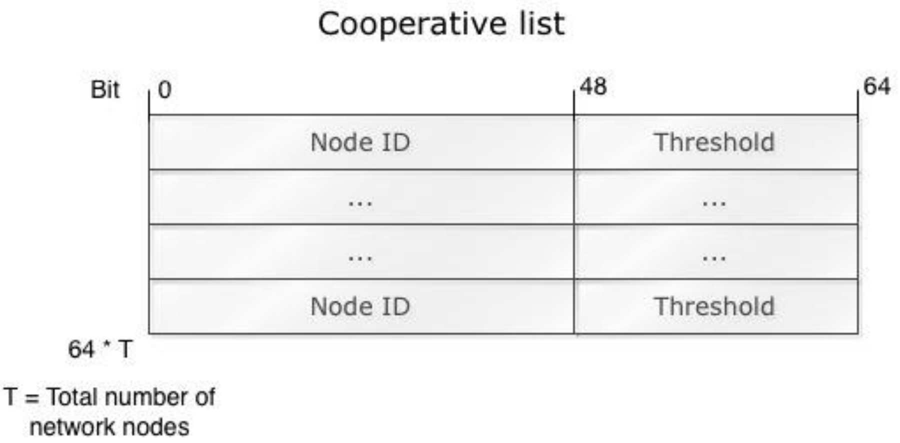


Figure 5. Node control message.

The *cooperative threshold list* (*CT*) influences directly the node reputation. The *list* starts at *0* (zero) and a unit (*1*) is added or subtracted according to the *node cooperation status* and *node status*. The correlation between the *node cooperation status*, the *node status*, its Internet connectivity, and the resultant CT is presented in Table I.

Table I. Correlation between the node cooperation status, the node status, its Internet connectivity, and the resultant CT classification.

Battery State		Internet Connectivity	Cooperation State	Reputation Value (RV)
Classification	0%-100%			
Critical	<15%	-	-	-
Poor	>= 15% and < 35%	0	0	-1
Poor		0	1	+3
Poor		1	0	-2
Poor		1	1	+4
Regular	>= 35% and < 70%	0	0	-2
Regular		0	1	+2
Regular		1	0	-3
Regular		1	1	+3

Excellent	>= 70%	0	0	-3
Excellent		0	1	+1
Excellent		1	0	-4
Excellent		1	1	+2

The node status is based on its storage capacity and energy lifetime. A node has three types of status: *poor*, *regular*, and *excellent*. A node with *poor* status occurs when the device storage capacity is over 95% or its available power energy is below 20%. The *regular* status comes when a node storage capacity is under 95% and its power energy is between 20% and 80%. A node is classified with an *excellent* status when the node storage capacity is under 95% and its available power energy is over 80%. The CT value guarantees that non-cooperative nodes are punished.

3.2 Cooperative Web service and reputation table

The *cooperative Web service* (*CWS*) includes and manages the *node reputation table*. To calculate nodes reputation, the *CWS* uses the *cooperative lists* deciding if the requesting node should have access to the m-Health application WS or not. Based on nodes reputation, the *CWS* will not grant access and release any resource from the WSs to *selfish* nodes. *Selfish* nodes are punished by the CWS with an order to cooperate until its reputation reaches a *cooperative* state. The CWS always release resources to *cooperative* nodes, however, *super-cooperative* nodes have a maximum priority in case of simultaneous requests. Figure 6 presents a user scenario of the m-Health cooperation approach. *User A* has network connectivity and cooperates, the status value is defined according to the battery status. *User B* has network connectivity and does not cooperate. Then, the status value will suffer a negative impact according to the battery status. *Users C* and *D* do not have network connectivity. *User C* queries *User A* for cooperation and receives a positive response and all the requested data. *User D* queries *User B* for cooperation and receives a negative response. Then, *User D* requests data from *User C* that answers this request, getting positive status by cooperating. Cooperating nodes have a better reputation, and have priority over selfish nodes to access the m-Health application services.

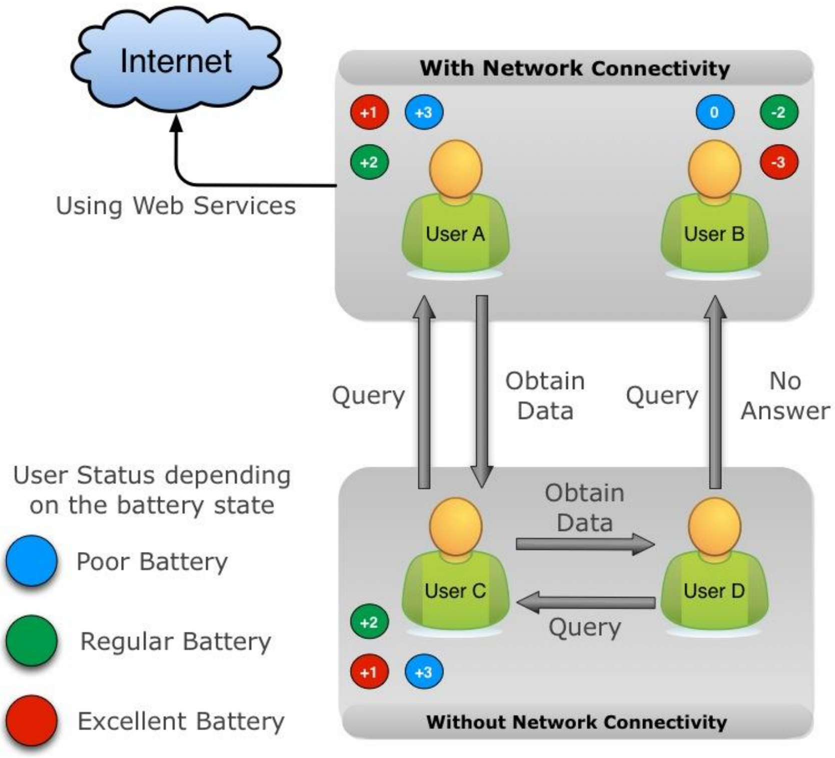


Figure 6. Illustration of the interaction for an m-Health application with the proposed cooperation approach for 4 users.

4. Data Encryption Mechanisms for Mobile Health Applications

This section presents the data encryption proposal for health applications (DE4MHA) in cooperation environments. The main goal aims to assure and guaranty m-Health data confidentiality, integrity, and authenticity in a cooperation environment where sensitive and personal data is exchanged through different agents. Figure 7 presents the use case diagram of the DE4MHA basic mechanisms and procedures.

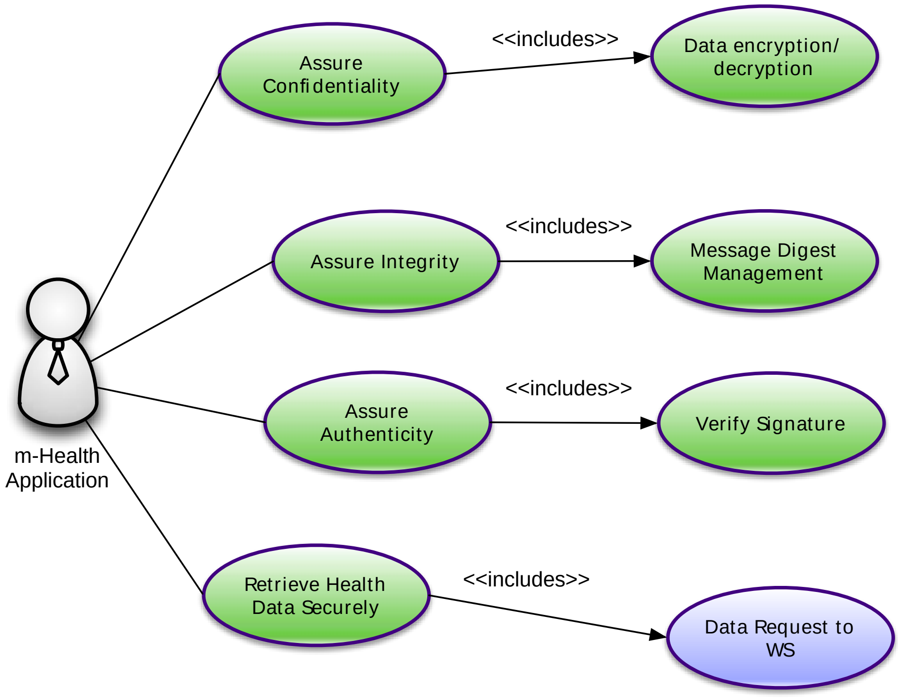


Figure 7. Use case diagram of the DE4MHA basic mechanisms and procedures.

Data confidentiality protects data that is exchanged through the network from unauthorized agents. There are two types of encryption algorithms to treat confidentiality: *i*) Symmetric Algorithms and *ii*) Asymmetric algorithms. Symmetric algorithms use the same key from encrypting and decrypting while asymmetric algorithms use one key for encryption (Public Key) and one for decryption (Private Key) [22]. Data confidentiality symmetric algorithms are widely used over asymmetric algorithms mainly because the last ones require a bigger encryption key that analogously increases the encryption time. In this paper, four distinct symmetric algorithms were considered to treat data confidentiality, namely, Advanced Encryption Standard (AES), Triple Data Encryption Standard (3DES), RC4, and Blowfish. Working and studying encryption algorithms implies a comprehensive understanding of the encryption key procedure once the encrypted data strongly depends on key's size [4]. All the four experimented algorithms use 168 bits key length except for AES, which uses 128 bits key length (additionally, it is possible to use a 192 or 256 bits key length).

Concerning the asymmetric encryption, two algorithms were considered, RSA and Diffie-Hellman, although, Diffie-Hellman might not be considered an encryption algorithm but a key exchange protocol [8].

4.1 Encryption strategy

The first issue addressed on the construction of the DE4MHA was the exchange key problem [18]. Therefore, DE4MHA uses a hybrid approach using asymmetric algorithms for session key exchange and symmetric ones for encrypting data being transferred among network nodes.

The DE4MHA procedures (illustrated in the activity diagram shown in Figure 8) begins with a mobile node (a person using SapoFit), trying to access the SapoFit Web service (WS) that contains the user profile, weight measures, fitness, and diet indications. A SapoFit user (mobile requester node) without network connectivity and without access to the SapoFit WS will try to obtain the required health information through cooperation. Another user with network connectivity (mobile requested node) will forward the requested health information from the SapoFit WS. Both the requested and requester nodes will exchange (through Bluetooth) a Public Key Message (PKM). After the public key exchange, the requested node creates a session key, encrypting it with the requester node's public key. Then, a signature of the whole message is created and appended to the Session Key Message (SKM) that is sent to the requester node. When the message containing the session key is received, if its integrity and authenticity is verified, the requester node sends an acknowledgement (Ack) to the requested node. This method guaranties safe communication between nodes, otherwise, if the integrity and authenticity is not verified the communication between nodes is finished (aborted). A mobile node with network connectivity will access the cooperative WS to obtain the required health information. To secure all the communication with the WS, the Secure Socket Layer (SSL) over the HTTP (also known as HTTPs) is used. Therefore, granting confidentiality, integrity, and authenticity of all the retrieved health data from the WS.

Figure 9 illustrates the overall behaviour of DE4MHA and the most fundamental messages exchanged between two mobile nodes that requires safe communication establishment in order to exchange information through cooperation. The procedure begins when a requester node needs to obtain data through cooperation, performing the process of node discovery and further connection through Bluetooth to a mobile node willing to cooperate (1). When both nodes are connected through Bluetooth, both nodes will generate a RSA key pair, exchanging their public key, so that each mobile node will be able to encrypt messages for further exchange (2). As soon as the requested node receives the requester node's public key, it proceeds to generate an AES session key encrypting it through the requester node's public key, appending then a digital signature to assure data integrity as well as authenticity (3). Finally, if the previous message is received by the requester node, its integrity and its authenticity will be checked and, if nothing wrong happened, the requester node will create a Ack message and a signature to guaranty that requested nodes know the requester node has received the session key (4). Therefore, all exchanged messages will be encrypted using the referred session key instead of the key pair used to exchange the session key, due to the superior time taken to encryption/decryption procedures by public key cryptography.

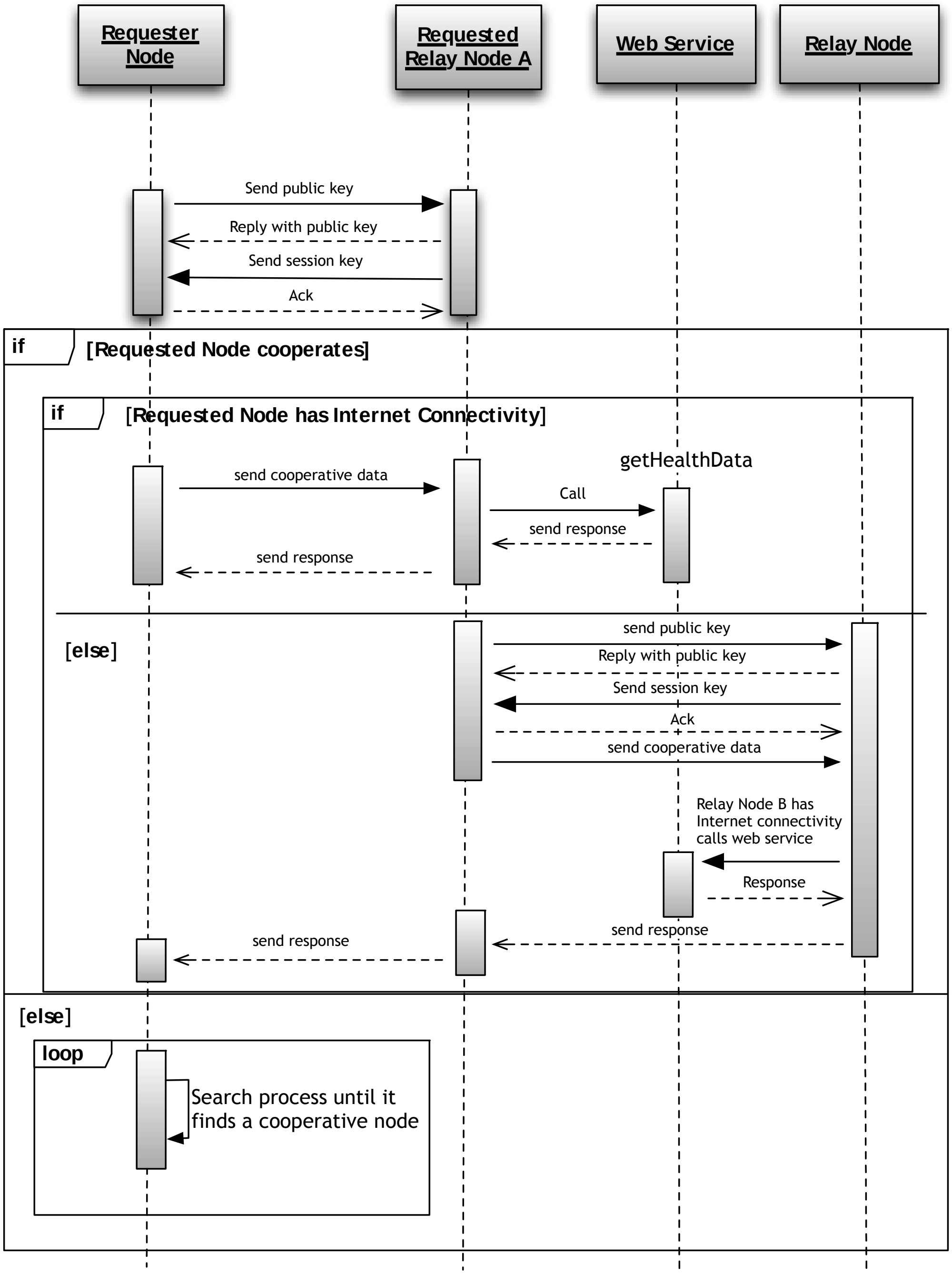


Figure 8. Activity diagram of the DE4MHA procedures.

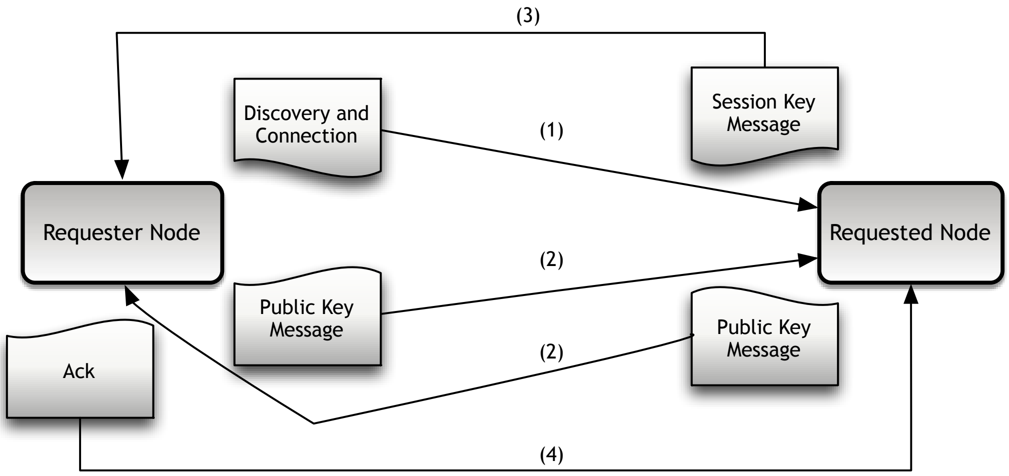


Figure 9. Data Exchange sequence

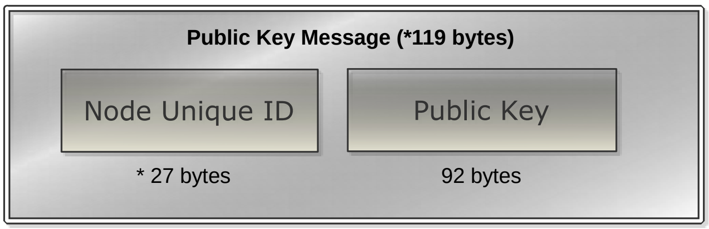
4.2 Public key message

Public key messages are sent from both requested and requester node, aiming to provide to each node their public key. In the future, this public key is used to encrypt a session key and it is used later to enable safe session key transfer.

Figure 10 illustrates a public key message. It has a maximum size of 119 bytes and the two following modules:

1. **Node unique ID:** This identifier is created through the aggregation of the mobile device Bluetooth mac address and the user unique identifier.
2. **Public Key:** This field will include the RSA public key previously generated along with the necessary private key.

These two elements comprise the public key message, which essentially enables safe public key exchange among mobile nodes on the network.



* Maximum size

Figure 10. Public Key Message.

4.3 Session key message

The requested node is the one who sends the *session key message*, and it comprises three main components: *i*) the requested ID, *ii*) the session key, and *iii*) the signature. The three main components of the session key message are illustrated in Figure 11 and may be described as follows:

1. **Requested ID**: as above-mentioned, the requested ID results from the aggregation of the mobile device Bluetooth mac address and the user unique identifier.
2. **Session Key**: this field includes the session key used to encrypt and decrypt all the data exchanged among mobile nodes, assuring that all sensitive data is kept safe and its content remains unknown to unwanted threats (ensuring **confidentiality**).
3. **Signature**: To every message exchanged between mobile nodes an hash of that message is generated and encrypted with the node's private key creating a signature of the message. In this particular case, the requester node, to assure the message is exactly as it was when it was sent remains intact (preserving its **integrity**), and at the same time it assures the message was sent from the expected person (mobile node) guaranteeing **authenticity**.

When the requester node receives the session key message from the requested node, it verifies its integrity and authenticity. If the message has not been corrupted neither sent by someone else then expected, both the requester and requested nodes can safely communicate and exchange messages using the session key that only both possess.

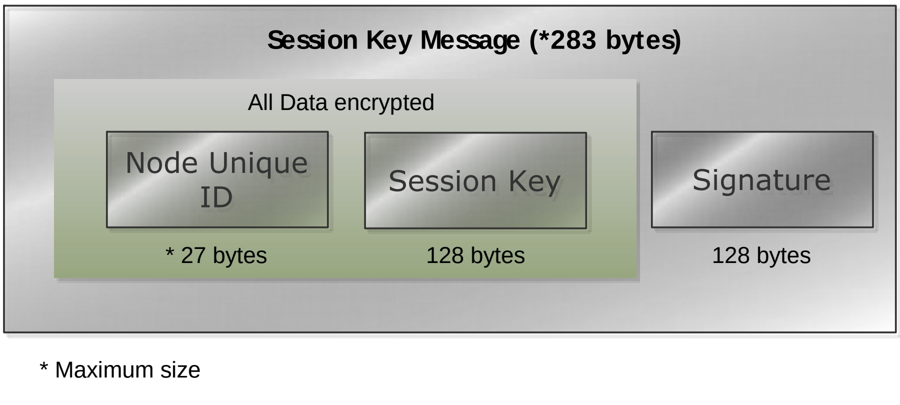


Figure 11. Session Key Message.

4.3 Symmetric and Asymmetric algorithm choice

In order to choose the most suitable symmetric encryption algorithm for DE4MHA, performance experiments were conducted using four different encryption algorithms, including AES, Triple Data Encryption Standard (3DES), RC4, and Blowfish. Given that DE4MHA aims any mobile health application in a cooperative environment, the amount of data that each application usually exchange is not known *a priori*. Therefore, in order to study several scenarios, different sizes of data that should be encrypted have been used as a performance metric.

Figure 12 presents the performance comparison of average encryption and decryption time as function of data size for the symmetric algorithms AES, 3DES, RC4, and Blowfish. As may be seen, results shown that when data size to encrypt increases, the encryption time (seconds) also increases, as expected. When comparing small amounts of data, all the four algorithms present similar results. However, AES algorithm presented better results, since the encryption time of bigger data tends to grow up very slowly. All the other three evaluated algorithms tend to grow up exponentially when data size to encrypt overcomes 1000 KB. The 3DES algorithm presented the maximum observed encryption time, encrypting 10,000 KB of data, which took on average 14.3 seconds. With the same amount of data, the AES encryption time was only about 0.0045 seconds. Regarding decryption process, the obtained results are nearly the same. AES algorithm decryption time is about 0.0038 seconds to decrypt 10,000 KB of data, in average. Given the observed results, AES algorithm was chosen for DE4MHA as a symmetric algorithm.

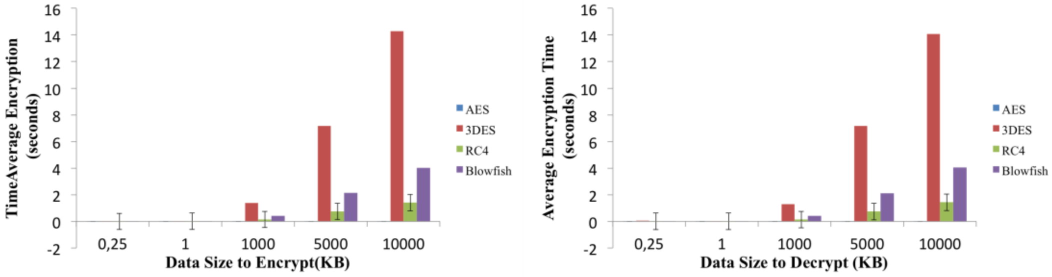


Figure 12. Performance comparison of average encryption and decryption time as function of data size for the symmetric algorithms AES, 3DES, RC4, and Blowfish.

Regarding the choice of an asymmetric algorithm to exchange session keys between mobile nodes, two options were considered, the RSA and the Diffie-Hellman algorithms. The RSA encrypts the session key for delivery and the Diffie-Hellman allows users to share a secret, generating then a session key based on the shared secret.

Several experiments were performed with both algorithms. It was observed that RSA presents better encryption times than Diffie-Hellman, due to the high amount of computation needed by Diffie-Hellman and the low processing capacity of mobile devices.

4.4 Integrity and authenticity

In order to assure integrity, Message-Digest 5 (MD5) algorithm was chosen. It takes a message of arbitrary length as input and produces a 128-bit “hash” value or “message digest” as output. When this method is used multiple times with the exactly same message, it should always produce the same hash value. Then, if a message is modified or corrupted, generating a hash value and comparing it with the original one, it is possible to verify if the message maintains its integrity.

To guarantee authenticity, two approaches were considered, (1) using RSA algorithm to encrypt the hash value previously generated with MD5 and (2) using Digital Signature Algorithm (DSA). RSA can only sign a message but cannot encrypt information. Since a hybrid approach has been chosen when AES is used for symmetric encryption and RSA used for asymmetric encryption, the last one was chosen to perform digital signature, considering the fact that RSA will be used both for session key exchange and digital signature performance. Thus, the generation of a pair of keys to exchange session keys and another one for digital signature is unnecessary.

5. Performance Evaluation

This section focuses on the performance evaluation and validation of the security mechanisms embedded in an m-Health application with cooperation mechanisms. First, the m-Health application (SapoFit) and corresponding network scenario used to evaluate and demonstrate the solution is introduced. Afterwards, the system validation and results are discussed.

5.1 SapoFit, an m-Health application

SapoFit is a weight control mobile application that allows users to keep track of weight in a healthier and more practical way [55, 56, 61]. SapoFit 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. Figure 13 presents the main activities screenshots of SapoFit application created for Android operating system.

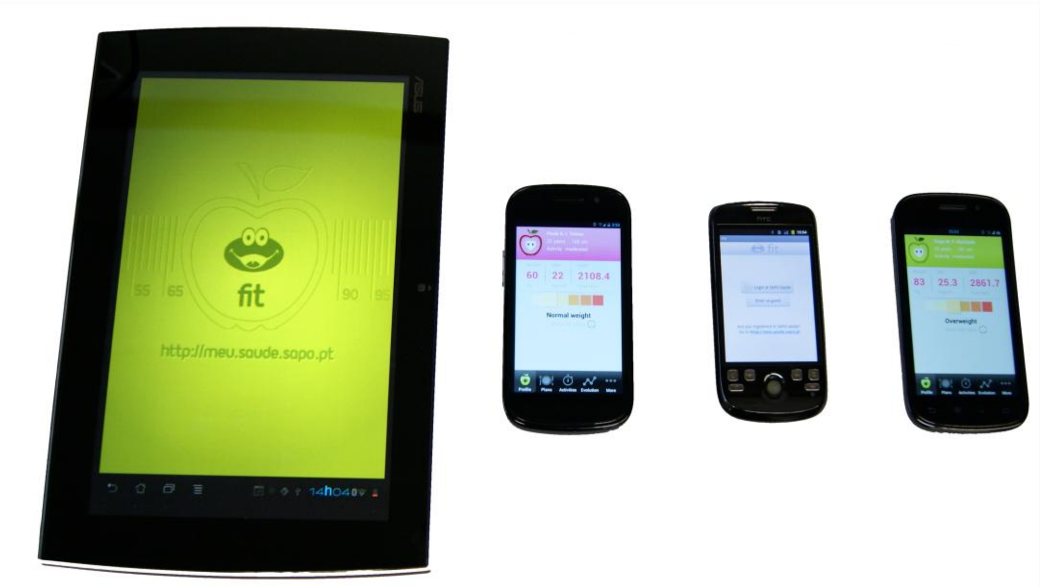


Figure 13. SapoFit Application.

The SapoFit application was used to evaluate and demonstrate DE4MHA and the cooperation strategy targets mobile devices running Google Android OS. The communication to the SapoFit Web service uses Simple Object Access protocol (SOAP) messages over Hypertext Transfer Protocol (HTTP). The information returns to the mobile application in JavaScript Object Notation (JSON) or Extensible Markup Language (XML).

5.2. Network scenario

Figure 14 presents the network scenario used to evaluate and demonstrate the proposed solution. It includes seven mobile devices with different hardware and software with SapoFit m-Health application. During five days, seven different users experimented the application. Non-cooperative cases where controlled and measured to a maximum of 4 to guarantee the minimum service performance. Through cooperation, all the devices can indeed use the m-Health application. However, uncooperative nodes affect directly the service delivery probability, service average delay, and the overall network performance. Performance metrics considered in this study are the request and response average time (in seconds). A performance comparison study of the m-Health application with and without the DE4MHA is presented.

In the presented scenario, all the devices carry Bluetooth class 2 modules, but only three devices have Internet connectivity. Users without Internet connectivity must use the integrated cooperation mechanisms in order to obtain the requested health information. When the number of uncooperative nodes increases, the average time of any request or response also naturally increases.

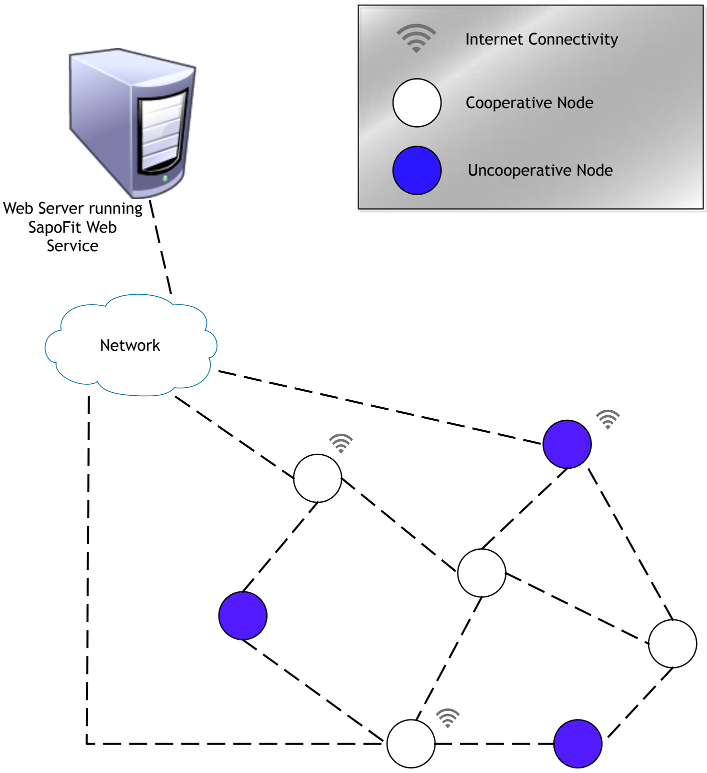
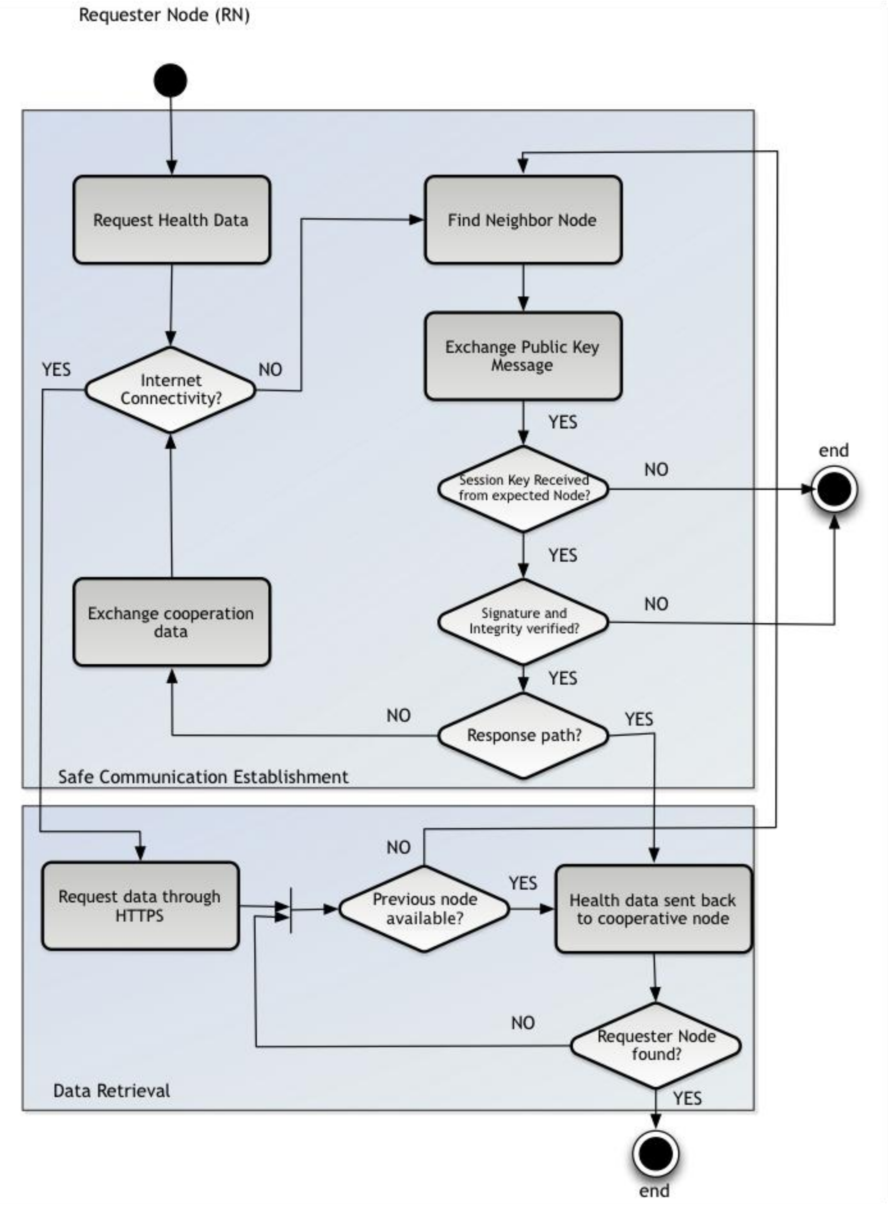


Figure 14. Network scenario of SapoFit in a cooperation enviorment.

Figure 15 shows how a request is handled when a mobile node desires to obtain determined health information. When a request is generated (required by the requester node), it initially checks if the device has Internet connectivity in order to obtain the desired information. In affirmative case, the requester node establishes a HTTPS connection (to assure data confidentiality) to the Web service that will try to obtain the information required by the device. On the other hand, when the requester node does not have Internet connectivity, a more complex scenario arises. In this scenario, in order to establish a secure channel through two mobile nodes, it is necessary to exchange public keys with the purpose of session key exchange assuring that nothing wrong happens in this procedure through authenticity and integrity properties. Thus, a message digest of the message to be sent is generated with MD5 algorithm, encrypting it with the receiver’s public key and then appending it to the referred message (as previously referred). Hence, the receiver is able to generate a message digest of the received message using MD5 algorithm as well as comparing it with the message digest appended by the sender and decrypted with the receiver’s private key, making it possible to check if the session key has not been modified and if it comes from the expected source. Although this methodology has been exemplified with the session key message exchange case, it is actually applied in every message type that is exchanged between two mobile nodes.



Requester Node (RN)
Request Health Data
Find Neighbor Node
Exchange Public Key Message
YES
Internet Connectivity?
NO
YES
Session Key Received from expected Node?
NO
end
YES
Exchange cooperation data
Signature and Integrity verified?
NO
YES
NO
Response path?
YES
Safe Communication Establishment
NO
Request data through HTTPS
Previous node available?
YES
Health data sent back to cooperative node
NO
Requester Node found?
Data Retrieval
YES
end

Figure 15 – Flowchart with request path activity.

At this moment, both mobile nodes might communicate safely, exchanging cooperative data so the requested node is aware of what the requester node desires to obtain. If the requested node has Internet connectivity and is willing to cooperate, it will establish a HTTPS connection to the cooperative Web service to obtain the required health data. Then, if the requester node is still within coverage, the health data is directly forwarded. If the requester is no longer within reach, due to devices displacement, it tries to find an alternative mobile node with cooperation mechanisms embedded that is, at the same time, neighbor from both mobile nodes. Then, the common neighbor is able to deliver the message to its final destination, i.e., the requester node. Finally, when anything wrong happens, i.e., integrity or confidentiality is not verified, the communication between two mobile nodes is immediately ended (aborted) in order to avoid information leakage and system compromising.

5.3 Performance Analysis

This section focuses on the performance analysis of the proposed encryption strategy in the above-mentioned cooperative environment and its impact on the overall network performance. The study was performed with the above-mentioned real users. The study refers to the comparison of the m-Health application performance with and without the cryptography strategy embedded. Results show a minimal increase of the overall time taken to accomplish cooperation tasks when encryption mechanisms are present, not compromising the overall network performance. Hence, due to DE4MHA incorporation, the average time added with encryption/decryption tasks corresponds to approximately 0,003557 seconds, and if compared with the average time taken by cooperation mechanisms shown in [60], it corresponds to an increase of 2% of the overall time. In this sense, the extra time required is perfectly acceptable since privacy and security is a concerning issue and must be included in every m-Health applications. This analysis focuses on the response service average time and request delay (in seconds). The delay is measured as the time between the request for the application service and the time that a response is received. Figure 16 shows results of the average request and response time delay in function of the number of uncooperative mobile nodes with and without the DE4MHA. Taking into account both approaches, with and without DE4MHA, it is observed that DE4MHA presents a slightly worse result in both request and response average time delay. However, as may be seen, this delay increase is almost insignificant.

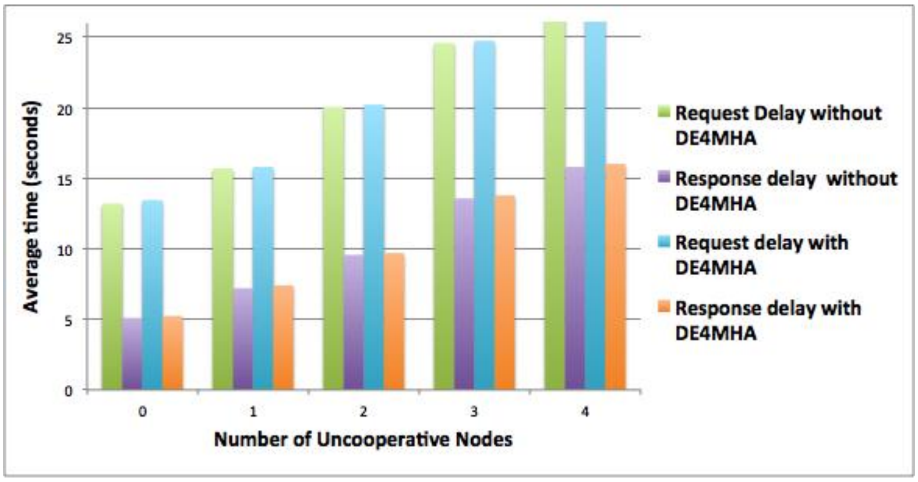


Figure 16. Average request and response time delay in function of the number of uncooperative mobile nodes with and without the DE4MHA.

6 – Conclusion and Future Work

This paper described, in detail, a data encryption solution for mobile health applications using a cooperation strategy proposed in [60], called DE4MHA. The data encryption algorithm DE4MHA with cooperation mechanisms embedded in mobile health applications allows users to safely obtain health information with data carried safely. DE4MHA uses a hybrid approach using symmetric and asymmetric encryption algorithms. From this study, it was concluded the most suited symmetric algorithm for m-Health network architecture is the AES algorithm. For the same network scenarios using typical m-Health architectures, this study concludes the most suited asymmetric algorithm is the RSA. For communication with Web services, the HTTPS protocol is the most suitable security mechanism.

The performance evaluation of this cryptography strategy shows that overall network and SapoFit performance was not degraded, maintaining slightly the same performance that without the encryption strategy. DE4MHA offers a robust and reliable increase of privacy, confidentiality, integrity, and authenticity on m-Health applications. Although it was experimented on a specific m-Health application, called SapoFit, both DE4MHA and the cooperation strategy can be deployed in a given m-Health application.

In future works we will test the impact of security attacks[71] in DE4MHA. Moreover, A performance evaluation study of DE4MHA in other m-Health applications to obtain comparison results with other health data types and length may be considered for further works. A comparison of a performance evaluation results obtained by simulation may also be considered.

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/LA0008/2011 Project, and by the AAL4ALL (Ambient Assisted Living for All), project co-funded by COMPETE under FEDER via QREN Programme.

References

[1] Akter, S., D'Ambra, J., and Ray, P. (2010). User Perceived Service Quality of mHealth Services in Developing Countries. European Conference on Information Systems (ECIS 2010). South Africa. 6-9 June 2010, pp 1-12.

[2] Akter, S. and Ray, P. (2010). mHealth - an Ultimate Platform to Serve the Unserved. IMIA Yearbook of Medical Informatics - Biomedical Informatics: Building Capacity Worldwide. Schattauer, Germany, pp 94-100.

[3] Antoniou, G., Batten, L. (2011). E-commerce: protecting purchaser privacy to enforce trust. Electronic Commerce Research, November 2011, Vol. 11, Issue 4, pp 421-456.

[4] Agrawal, M., and Mishra, P. (2012). A Comparative Survey on Symmetric Key Encryption Techniques. International Journal on Computer Science and Engineering, Vol. 4, pp 877–882.

[5] Bannon, L. and Hughes, J. (1993). The Context of CSCW. K. Schmidt (Ed.), Report of COST14 "CoTech". Working Group 4 (1991-1992).

[6] Batten, L. (2013). Public Key Cryptography: Wiley-IEEE Press.

[7] Biryukov A., Nakahara J., Preneel B., and Vandewalle J. (2002) New Weak Key Classes of IDEA. Lecture Notes In Computer Science. Vol. 2513, pp 315-326.

[8] Biswas, G. (2008) Diffie-Hellman technique: extended to multiple two-party keys and one multi-party key. IET Information Security. Vol. 2(1), pp 12-18.

[9] Bleumer, G. (1994). Security for decentralized health information systems. International Journal of Bio-Medical Computing. February 1994, pp 139-145

[10] Boonyarattaphan, A., Bai, Y., Chung , S. (2009) A security framework for e-Health service authentication and e-Health data transmission. 9th International Symposium on Communications and Information Technology (ISCIT 2009). 28-29 September, pp 1213-1218.

[11] Buttyán, L. and Hubaux , J.-P. (2003). Stimulating Cooperation in Self-Organizing Mobile Ad hoc Networks. Mobile Networks and Applications. Vol. 8(5), pp 579-592.

[12] Chan, V., Ray, P., and Parameswaran, N. (2008). Mobile e-Health monitoring: an agent-based approach. IET Communications. Vol. 2(2), pp 223-230.

[13] Chang, H. (2013). The security service rating design for IT convergence services. Electronic Commerce Research. Published Online: 15 May 2013. DOI: 10.1007/s10660-013-9115-2

[14] Chen, Y., and Ku, W. Self-encryption scheme for data security in mobile devices. Proceedings of the 6th IEEE Conference on Consumer Communications and Networking Conference, 850-854.

[15] Cochran, M. (2008). Cryptographic Hash Functions: ProQuest.

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

[17] Déglise, C., Suggs, L., and Odermatt, P. (2012) Short message service (SMS) applications for disease prevention in developing countries. Journal of Medical Internet Research, Vol. 14(1), http://www.jmir.org/2012/1/e3/.

[18] Diffie, W. (1988). The first ten years of public-key cryptography. Proceedings of the IEEE. Vol. 76(5),pp 560-577.

[19] Eastlake, D., and Jones, P. (2001). US Secure Hash Algorithm 1. http://www.ietf.org/rfc/rfc3174.txt. Accessed 12 January 2013.

[20] Elminaam, D., Kader, H., and Hadhoud, M. (2010). Evaluating the performance of symmetric encryption algorithms. International Journal of Network Security. Vol. 10(3), pp 213–219.

[21] Elgamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory. Vol. 31(4), pp 469- 472.

[22] Fayn, J., and Rubel, P. (2010). Towards a personal health society in cardiology. IEEE Transactions on Information Technology in Biomedicine. Vol. 14(2), pp 401-409.

[23] Federal Information Processing Standards Publication. Data Encryption Standard (Des). http://www.itl.nist.gov/fipspubs/fip46-2.htm. Accessed 12 January 2013.

[24] Ferguson, N., Schneier, B., and Kohno, T. (2012). Cryptography Engineering: Wiley. ISBN: 978-0-470-47424-2

[25] Gritzalis, S., Zhan, J., Z., Jeong, K. (2013). IT convergence and security. Electronic Commerce Research. Published Online: 9 May 2013. DOI: 10.1007/s10660-013-9114-3

[26] Gupta, A. (2008). Challenges of Mobile Computing. Proceedings of 2nd National Conference on Challenges and Opportunities in Information Technology. 29 March, pp 86-90.

[27] Housley, R. (2001). Triple-DES and RC2 Key Wrapping. http://www.ietf.org/rfc/rfc3217.txt. Accessed 12 January 2013.

[28] Istepanian, R., and Lacal, J. (2003). Emerging Mobile Communication Technologies for Health: Some Imperative notes on m-Health. Proceedings of the 25th Annual International Conference of the IEEE Engineering in Medicine and Biology Society. Vol. 2, pp 1414-1416.

[29] Isaac, J. T., Zeadally, S., Cámara J., S. (2012). A lightweight secure mobile Payment protocol for vehicular ad-hoc networks (VANETs). Electronic Commerce Research. March 2012, Vol. 12(1), pp 97-123.

[30] Jaganathan, K., Zhu, L., and Brezak, J. (2006). The RC4-HMAC Kerberos Encryption Types. http://tools.ietf.org/html/rfc4757 /. Accessed 12 January 2013.

[31] Jara, A., Zamora, M., Skarmeta, A. (2011). An Internet of things-based personal device for diabetes therapy management in ambient assisted living (AAL). Personal and Ubiquitous Computing. Vol. 15(4), pp 431-440.

[32] Jonsson, J. and Kaliski, B. (2003). Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1. http://tools.ietf.org/html/rfc3447. Accessed 12 January 2013.

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

[34] Kollmann, A., Riedl, M., Kastner, P., Schreier, G., and Ludvik, B. (2007). Feasibility of a mobile phone-based data service for functional insulin treatment of type 1 diabetes mellitus patients. Journal of Medical Internet Research. Vol. 9(5). http://www.jmir.org/2007/5/e36/.

[35] Koukopoulos, D., Styliaras, G. (2013). Design of trustworthy smartphone-based multimedia services in cultural environments. Electronic Commerce Research. May 2013, Vol. 13(2), pp 129-150.

[36] Lacuesta, R. Lloret, J. Garcia, M. Peñalver, L. (2013). A Secure Protocol for Spontaneous Wireless Ad Hoc Networks Creation. IEEE Transactions on Parallel and Distributed Systems. Vol. 24(4), pp. 629-64. DOI:10.1109/TPDS.2012.168.

[37] Laxminarayan S., Istepanian R., and Pattichis C. S. (2006). M-Health: Emerging Mobile Health Systems: Springer. ISBN-10: 0387265589**.**

[38] Lin, C. T., Chang, K. C., Lin, C. L., Chiang C.C., Lu, S.W., Chang, S. S., et al. (2010). An intelligent telecardiology system using a wearable and wireless ECG to detect atrial fibrillation. IEEE Transactions On Information Technology in Biomedicine. Vol. 14(3), pp 726-733.

[39] Martin, K. (2012). Everyday Cryptography: OUP Oxford. ISBN-10**:** 0199695598.

[40] Moullee, B., and Ray, P. (2009). Issues in E-Health Cost Impact Assessment. In IFMBE Proceeding of the World Congress on Medical Physics and Biomedical Engineering. Berlin: Springer, pp. 223-226.

[41] Mirkovic, J.; Bryhni, H.; Ruland, C. (2011). Secure solution for mobile access to patient's health care record. 13th IEEE International Conference on e-Health Networking Applications and Services. 13-15 June. Columbia, USA, pp 296-303.

[42] Mougiakakou, S., Bartsocas, C., Bozas, E., Chaniotakis, N., Iliopoulou, D., Kouris, I., et al. (2010). SMARTDIAB: a communication and information technology approach for the intelligent monitoring, management and follow-up of type 1 diabetes patients. IEEE Transactions On Information Technology in Biomedicine. Vol. 14(3), pp 622-33.

[43] O. Goldreich, O. (2005). Foundations of Cryptography: Now Publishers Inc. ISBN 10: 1933019026.

[44] Paar, C., and Pelzl, J., (2010) The Data Encryption Standard (DES) and Alternatives. Understanding Cryptography, A Textbook for Students and Practitioners: Springer. pp 55-86.

[45] Pachghare, V. K. (2009). Cryptography And Information Security: PHI Learning Pvt. Ltd. ISBN: 978-81-203-3521-9.

[46] Pare, G., Moqadem, K., Pineau, G., and St-Hilaire, C. (2010) Clinical effects of home telemonitoring in the context of diabetes, asthma, heart failure and hypertension: a systematic review. Journal of Medical Internet Research. Vol. 12(2). http://www.jmir.org/2010/2/e21/.

[47] Patrick, K., Raab, F., Adams, M., Dillon, L., Zabinski, M., Rock, C., Griswold, W., and Norman, G. (2009). A text message-based intervention for weight loss: randomized controlled trial. Journal of Medical Internet Research. Vol 11(1). http://www.jmir.org/article/citations/1100.

[48] Pollak, J., Gay, G., Byrne, S., Wagner, E., Retelny, D., and Humphreys, L. (2010). It's Time to Eat! Using Mobile Games to Promote Healthy Eating. IEEE Pervasive Computing. Vol. 9(2), pp 21-27.

[49] Qiang, Z., and Yamamichi, M. (2012). Mobile Applications for the Health Sector. http://siteresources.worldbank.org/INFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/Resources/mHealth_report.pdf. Accessed 12 January 2013.

[50] Raeburn K. (2005) Advanced Encryption Standard (AES) Encryption for Kerberos 5. http://www.ietf.org/rfc/rfc3962.txt. Accessed 12 January 2013.

[51] Ray, P., Parameswaran, N., Chan, V., and Yu, W. (2008). Awareness modeling in collaborative mobile e-health. Journal of Telemedine and Telecare. Vol. 14(7), pp 381-385.

[52] Raychaudhuri, K. and Ray, P. (2010) Privacy Challenges in the Use of eHealth Systems for Public Health Management. International Journal of e- Health and Medical Communications. Vol. 1(2), pp 12–23.

[53] Rivest, R. (1992). The MD5 Message-Digest Algorithm. http://www.ietf.org/rfc/rfc1321.txt. Accessed 12 January 2013.

[54] Rodrigues, J., Oliveira, M., and Vaidya B. (2010). New Trends on Ubiquitous Mobile Multimedia Applications. EURASIP Journal on Wireless Communications and Networking, Vol. 2010(10), pp 1-12.

[55] Rodrigues, J., Lopes I., Silva, B., and Torre, I. (2013) A new mobile ubiquitous computing application to control obesity: SapoFit. Informatics for Health and Social Care, Vol. 38(1), pp 37-53.

[56] SapoFit. http://itunes.apple.com/pt/app/sapo-fit/id438487775?mt=8. Accessed 12 January 2013.

[57] Schneier, B. (1994). The Blowfish encryption algorithm. Dr Dobb's Journal-Software Tools for the Professional Programmer. Vol. 19(4), pp 38-43.

[58] Schneier, B. (1996). Applied Cryptography: Protocols, Algorithms, and Source Code in C: Join Wiley and Sons, Inc. ISBN-10: 0471117099

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

[60] Silva, B., Rodrigues, J., Lopes, I., Machado, and T., Zhou, L. (2012). 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).

[61] Silva, B., Lopes, I., Rodrigues, J., and Ray, P. (2011) SapoFitness: A mobile health application for dietary evaluation. 13th IEEE International Conference on e-Health Networking Applications and Services (Healthcom 2011). 13-15 June. Columbia, Missouri, USA, pp 375-380.

[62] Smith, R. (2005). Introduction to multilevel security. Handbook of Information Security: Google Scholar.

[63] Sulaiman, R., Sharma, D., Ma, W., and Tran, D. (2008) A Security Architecture for e-Health Services. 10th International Conference on Advanced Communication Technology. Gangwon-Do, South Korea, Vol. 2, pp 99-104.

[64] Tachakra, S., Wang, X., Istepanian ,R., and Song, Y. (2003) Mobile e-Health: the Unwired Evolution of Telemedicine. Telemedicine Journal and e- Health. Vol. 9(3), pp 247–257.

[65] Tillich, S., and Herbst, C. (2008) Attacking State-of-the-Art Software Countermeasures—A Case Study for AES. Proceedings of the 10th international workshop on Cryptographic Hardware and Embedded Systems. 10-13 August. Washington, D.C., USA, pp 228-243.

[66] Watson, A., Bickmore, T., Cange, A., Kulshreshtha, A., and Kvedar, J. (2012). An internet-based virtual coach to promote physical activity adherence in overweight adults: randomized controlled trial. Journal of Medical Internet Research. Vol. 14(1). http://www.jmir.org/2012/1/e1/.

[67] Whittaker, R., Dorey, E., Bramley, D., Bullen, C., Denny, S., Elley, C. et al. (2011). A theory-based video messaging mobile phone intervention for smoking cessation: randomized controlled trial. Journal of Medical Internet Research. Vol. 13(1). http://www.jmir.org/2011/1/e10/.

[68] Yong-Xia, Z. and Ge, Z. (2010). MD5 Research. Second International Conference on Multimedia and Information Technology. 24-25 April. Kaifeng, China, Vol. 2, pp 271-273.

[69] Zheng, P., and Ni, L. (2005). Smart Phone and Next Generation Mobile Computing: Morgan Kaufmann. ISBN-10: 0120885603.

[70] Zhu, F., Bosch, M., Woo, I., Kim, S., Boushey, C., Ebert, D., and Delp, E. (2010). The Use of Mobile Devices in Aiding Dietary Assessment and Evaluation. IEEE Journal of Selected Topics in Signal Processing. Vol. 4(4), pp 756-766.

[71] Kuncha Sahadevaiah and Prasad Reddy P.V.G.D. (2011). Impact of Security Attacks on a New Security Protocol for Mobile Ad Hoc Networks, Network Protocols and Algorithms, Vol. 3(4), Pp. 122-140.

Bruno Silva received his BsC degree (licentiate) in 2008 in Informatics Engineering from University of Beira Interior, Portugal. In 2010, he received his MsC degree in Informatics Engineering from University of Beira Interior. He is currently a PhD student on Informatics Engineering at the University of Beira Interior under supervision of Prof. Joel J. P. C. Rodrigues. He is also a PhD student member of the Instituto de Telecomunicações, Portugal. His current research interests include Delay Tolerant Networks, Vehicular Networks, Mobile Computing, Ubiquitous Computing, e-Health but especially in mobile Health. He authors or co-authors 12 international conference papers and 4 International Journal publications.

Joel Rodrigues is a professor in the Department of Informatics of the University of Beira Interior, Covilhã, Portugal, and researcher at the Instituto de Telecomunicações, Portugal. He received a PhD degree in informatics engineering, an MSc degree from the University of Beira Interior, and a five-year BSc degree (licentiate) in informatics engineering from the University of Coimbra, Portugal. His main research interests include sensor networks, e-health, e-learning, vehicular delay-tolerant networks, and mobile and ubiquitous computing. He is the leader of NetGNA Research Group (http://netgna.it.ubi.pt), the Chair of the IEEE ComSoc Technical Committee on Communications Software, the Vice-Chair of the IEEE ComSoc Technical Committee on eHealth, and Member Representative of the IEEE Communications Society on the IEEE Biometrics Council. He is the editor-in-chief of the International Journal on E-Health and Medical Communications, the editor-in-chief of the Recent Patents on Telecommunications, and editorial board member of several journals. He has been general chair and TPC Chair of many international conferences. He is a member of many international TPCs and participated in several international conferences organization. He has authored or coauthored over 250 papers in refereed international journals and conferences, a book, and 2 patents. He had been awarded the Outstanding Leadership Award of IEEE GLOBECOM 2010 as CSSMA Symposium Co-Chair and several best papers awards. Prof. Rodrigues is a licensed professional engineer (as senior member), member of the Internet Society, an IARIA fellow, and a senior member of ACM and IEEE.

Fábio Canelo received his BSc degree (licenciate) in 2011 in Information Systems and Technologies from University of Beira Interior, Portugal. Currently, he is concluding his MSc degree in Informatics Engineering also from the University of Beira Interior. He is a student member of the Instituto de Telecomunicações, Portugal. His current research topics include Security Mechanisms, Mobile Computing, and Ubiquitous Computing. He has co-authored one journal publication.

Ivo Lopes is a PhD student on Informatics Engineering at the University of Beira Interior, Covilhã Portugal, under supervision of Prof. Joel J. P. C. Rodrigues. He received his Master degree in Informatics Engineering from University of Beira Interior, 2011. His research interests include mobile and ubiquitous computing, e-Health, Ambient Assisted Living, Web Services, and sensor networks. Currently he is affiliated with Instituto de Telecomunicações, Portugal since March 2009. He has authored or co-authored of several papers in international journals, books, and conferences.

Jaime Lloret (jlloret@dcom.upv.es) received his M.Sc. in Physics in 1997, his M.Sc. in electronic Engineering in 2003 and his Ph.D. in telecommunication engineering (Dr. Ing.) in 2006. He is a Cisco Certified Network Professional Instructor. He is currently Associate Professor in the Polytechnic University of Valencia. He is the head of the research group "communications and remote sensing" of the Integrated Management Coastal Research Institute and he is the head of the "Active and collaborative techniques and use of technologic resources in the education (EITACURTE)" Innovation Group. He is the director of the University Expert Certificate “Redes y Comunicaciones de Ordenadores”, the University Expert Certificate “Tecnologías Web y Comercio Electrónico”, and the University Master "Digital Post Production". He is currently Vice-chair of the Internet Technical Committee (IEEE Communications Society and Internet society). He has authored 12 books and has more than 240 research papers published in national and international conferences, international journals (more than 70 with ISI Thomson Impact Factor). He has been the co-editor of 15 conference proceedings and guest editor of several international books and journals. He is editor-in-chief of the international journal "Networks Protocols and Algorithms", IARIA Journals Board Chair (8 Journals) and he is associate editor of several international journals. He has been involved in more than 200 Program committees of international conferences and in many organization and steering committees. He led many national and international projects. He is currently the chair of the Working Group for the Standard IEEE 1907.1. He has been the general chair (or co-chair) of 18 International conferences. He is IEEE Senior and IARIA Fellow.