A New Framework for Ubiquitous Context-Aware Healthcare Applications

Georgios Mantas, *Member, IEEE,* Dimitrios Lymberopoulos, *Member, IEEE,* and Nikos Komninos, *Member, IEEE*

***Abstract*—Nowadays, there is a significant lack of generic application frameworks providing third party developers with the appropriate mechanisms for building ubiquitous contextaware healthcare applications over medical heterogeneous networks. In this paper, we propose a new framework integrating context-aware and security mechanisms with mechanisms that allow the ease exploitation of the core networks' functionality to enable third party developers to build reliable and secure ubiquitous context-aware healthcare applications over medical heterogeneous networks.**

Keywords: ubiquitous healthcare, contex-awareness, extended framework, security mechanisms, sensor networks mechanisms

I. Introduction

The current healthcare sector needs a shift towards the patient-centric healthcare approach to meet the rising demand for healthcare services of different population groups and at the same time to reduce the costs of delivering healthcare services. The main objective of the new approach in healthcare is not only the effective treatment of a large number of diseases but also the disease prevention, proactive actions and life quality improvement. The patient-centric healthcare approach emphasizes more on the provision of high quality personalized healthcare services at the right time, right place and right manner without limitations on time and location. In other words, the patient-centric approach is based on ubiquitous healthcare. However, despite the importance of ubiquitous healthcare in patientcentric approach, there is a lack of generic application frameworks providing third party developers with the appropriate mechanisms for reliable and rapid development of ubiquitous context-aware healthcare applications over heterogeneous medical networks. Especially, there are not generic frameworks to support the cross network development of ubiquitous context-aware healthcare applications in a flat and common way as well as to support the essential mechanisms for acquisition and management of contextual and bio information.

Hence, in this paper, we propose a generic application framework integrating context-aware and security mechanisms with mechanisms that enable any client application to access transparently the core network functionality and use it. The proposed framework aims at giving the ability to third party developers to build rapidly reliable ubiquitous context-aware healthcare applications over heterogeneous medical networks. Essentially, we adopt the OSA/Parlay architecture and propose a new framework that integrates the basic mechanisms of the OSA/Parlay Framework Interface with context-aware mechanisms derived from current context-aware frameworks (e.g. CMF, JCAF). The adoption of OSA/Parlay architecture is suggested since it allows the interworking between client applications and telecommunications capabilities through open standardized interfaces. Moreover, the new framework incorporates security mechanisms that are essential for healthcare applications. In other words, the new framework extends the OSA/Parlay architecture. The main objective of the proposed framework is to stimulate the deployment of innovative ubiquitous context-aware healthcare applications by third party providers, which may not be experts in the field of telecommunications and context-awareness but they have expertise in the enterprise market.

Following the introduction, this paper is organized as follows. In Section II, current context-aware frameworks are presented as well as an overview of the OSA/Parlay architecture and its components is given. In Section III, the extended OSA/Parlay architecture is discussed. Furthermore, the proposed framework, its mechanisms and interfaces are described. In Section IV, examples of security mechanisms that can be provided by the proposed framework are discussed. Finally, Section V concludes the paper.

Georgios Mantas is with the Electrical & Computer Engineering Department, University of Patras, Rio, Patras, GR-26504, Greece (e-mail: gman@ upatras.gr).

Dimitrios Lymberopoulos is with the Electrical & Computer Engineering Department, University of Patras, Rio, Patras, GR-26504, Greece (phone: 0030-2610996852; e-mail: dlympero@upatras.gr).

Nikos Komninos is with the Athens Information Technology, Peania, Athens, GR-190 02, Greece (e-mail: nkom@ait.edu.gr).

II. Related work

A. Context-Aware Frameworks

There is a wide range of different context-aware frameworks supporting mechanisms required for the development of ubiquitous healthcare applications. Each context-aware framework is characterized by its own strengths and weaknesses. Three well-known context-aware frameworks are the following; the CMF (Context Management Framework), the JCAF (Java ContextAwareness Framework) and the Context Toolkit.

The CMF is a framework supporting the management of context information on mobile terminals. It provides systematic methods for acquiring and processing useful context information from user's environment and providing it to the ubiquitous applications. The CMF permits semantic reasoning on context in real time and even in the presence of uncertain, noisy and rapidly changing information. Furthermore, the CMF enables the dissemination of the contextual information to applications using an event-based communication approach [2], [3].

The JCAF is a Java-based lightweight context-aware framework defining a compact and small set of interfaces for the development of context-aware applications. The JCAF consists of a set of components, called Context Services, which are connected in a peer-to-peer setup. Each Context Service is responsible to collect and handle context information in a specific environment [2], [4].

Finally, the Context Toolkit is another context-aware framework. The Context Toolkit follows a layered architecture approach that enables the separation of the context acquisition from its use in applications. Besides, this framework supports context interpretation, constant context availability, constant storage, resource discovery and distributed communication [1], [2].

B. OSA/Parlay Architecture

The European Telecommunications Standards Institute (ETSI), the Parlay Group and the 3rd Generation Partnership Project (3GPP) have collaborated and defined jointly the OSA/Parlay standard. The OSA/Parlay specifications define an architecture that enables third party client applications to access transparently the core network functionality and make use of it through an open, standardized and technologyindependent API, called OSA/Parlay API. The OSA/Parlay architecture is focused on Next Generation Networks (NGNs) and includes the following main components; the OSA/Parlay API, the Client Application and the Enterprise Operator. The OSA/Parlay API consists of two groups of interfaces; the Service Capability Features (SCFs) Interfaces and the interfaces included in the Framework Interface. Both groups of the interfaces are incorporated in Service Capability Servers (SCSs) located in the OSA/Parlay Gateway [5].

In the context of OSA/Parlay standard, the functionality of the core network is defined as a set of Service Capability Features (SCFs). The SCFs provide the total core network functionality including call control, user interaction, mobility, messaging, location and data connectivity to the client applications via abstract interfaces, called SCFs Interfaces. The SCFs Interfaces of the OSA/Parlay standard hide the heterogeneity and complexity of the underlying network from the developers of the client applications.

Finally, the Framework Interface, which mediates between the SCSs and the client applications, supports the basic mechanisms enabling applications to discover and use the required service capabilities of the network [5].

III. Design of the Extended OSA/PARLAY Architecture

The proposed framework is based on the OSA/Parlay architecture to provide a generic application framework for rapid and ease development of ubiquitous context-aware healthcare applications over heterogeneous medical networks. The main components of the proposed framework are the set of SCFs Interfaces and the Framework Interface.

However, in the proposed framework, the included set of SCFs Interfaces, called Extended Set of SCFs Interfaces, integrates not only the core network SCFs Interfaces but also the Sensor Networks SCFs Interfaces that enable the ubiquitous healthcare applications to access the sensing capabilities handled by the services provided by sensor networks. The sensing capabilities are associated with the different types of sensors incorporated in the possible networks that can be included in a ubiquitous context-aware healthcare application. In our case, we have assumed that the supported ubiquitous context-aware healthcare applications are going to require contextual information acquisition from sensors included in Home Networks and Vehicle Networks. In addition, the supported applications will be provided with bio information derived from sensors embedded in Body Area Networks.

Furthermore, the incorporated Framework Interface, called Extended Framework Interface, integrates a wide range of mechanisms to facilitate the realization of secure ubiquitous context-aware healthcare applications.

The proposed framework leads to an extension of the OSA/Parlay architecture. The extended architecture is shown in the following Fig. 1:

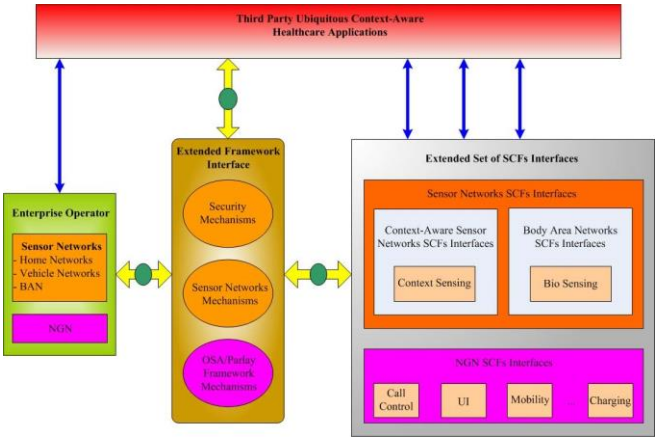

Fig. 1 The Extended OSA/Parlay Architecture

A. Extended Set of SCFs Interfaces

The Extended Set of SCFs Interfaces includes two categories of SCFs Interfaces; the NGN SCFs Interfaces and the Sensor Networks SCFs Interfaces.

The NGN SCFs Interfaces are the known SCFs Interfaces that we meet in the OSA/Parlay standard and they provide access to the underlying network capabilities handled by the corresponding network services. On the other hand, the Sensor Networks SCFs Interfaces are classified into two subsets based on the different types of gathered information; the Context-Aware Sensor Networks SCFs Interfaces and the Body Area Networks (BANs) SCFs Interfaces.

The Context-Aware Sensor Networks SCFs Interfaces enable an application to access context sensing capabilities supported by context-aware sensor networks. Moreover, the BANs SCFs Interfaces are responsible to enable an application to access biosignals sensing capabilities supported by BANs.

Context sensing is the process of collecting context information from the patient's environment. Context information can be collected by many different types of sensors included in many different types of networks. In our case, we have considered Home Networks and Vehicle Networks as the networks that incorporate context-aware sensors. These sensors can gather context information ranging from location and time to low-level types of physical context such as light level, temperature, humidity, sound, pressure and the concentration of gases (e.g., carbon dioxide). Furthermore, context sensing can provide information related to patient's activities.

On the other hand, biosignals sensing is the process of acquisition of various vital parameters (e.g. ECG signals, blood pressure, body core temperature, respiration rate) derived from the patient's body. Vital parameters are gathered by wearable biosensors of the BAN.

Finally, it is worthwhile to mention that the supported services by the Extended Set of SCFs Interfaces are considered as service components. In the world of service standards, these service components, called service enablers, can be bundled in order to create independent and reusable niche services targeted at specific markets, which concern specialized ubiquitous context-aware healthcare applications. Thus, the proposed framework creates a development environment allowing the proliferation of niche services rather than finding the next killer application. Furthermore, the niche services lead to shorter development cycles and decrease the efforts for application's development. Consequently, niche services generate considerable revenue to the developers and providers, mainly through economies of scale.

B. Extended Framework Interface

First of all, the Extended Framework Interface provides the applications with all the basic mechanisms, called OSA/Parlay Framework Mechanisms, supported by the standard OSA/Parlay Framework Interface. These mechanisms enable ubiquitous context-aware healthcare applications to discover and use the core network service capabilities. Besides, the OSA/Parlay Framework Mechanisms encompass management functions for handling fault and overload situations. Moreover, a number of the OSA/Parlay Framework Mechanisms are responsible to enable network operators to authenticate third party applications.

In addition, the Extended Framework Interface incorporates two mechanism categories; the Sensor Networks Mechanisms and the Security Mechanisms. The Sensor Networks Mechanisms are responsible for the management of the captured contextual and bio information as well as the deployment of ubiquitous context-aware healthcare applications. These mechanisms are derived from current context-aware frameworks such those that we mentioned in Section II. Even though these mechanisms are derived from frameworks that process and manage contextual information, we have supposed that the concept of these mechanisms can also be applied properly on bio information. The Sensor Networks Mechanisms supported between the Extended Framework Interface and the Application are described below.

Context and Bio Information Abstraction: This mechanism is used for context and bio information interpretation, since ubiquitous context-aware healthcare applications make use of many different types of sensors to perceive contextual and bio information. The main objective of this mechanism is to hide the heterogeneity of the sensored information providing a higher level of abstraction. Hence, this mechanism increases the independency of physical sensors as well as their reusability.

Context and Bio Information Storage and Management: This mechanism is responsible for the storage of contextual and bio information. Additionally, this mechanism is responsible for the management (e.g. retrieval, search, delete) of the stored information as well as its delivery using different types of approaches (e.g. request/response, subscription/notification). Besides, this mechanism is

essential for applications that require sensored vital data and sensored contextual data to be combined.

Reasoning: In ubiquitous context-aware healthcare applications the captured information is often unreliable due to the inaccuracy and lack of precision of sensors. For that reason, a reasoning mechanism is essential to address uncertainty of sensors' measurements making deductions for suitable adaptations without an explicit intervention from the user.

Devices and Resource Discovery: This mechanism is responsible to enable devices (e.g. bio-sensors) to be added or removed dynamically from the sensor networks without affecting the entire operation of the sensor networks.

Services Discovery: This mechanism is responsible to inform ubiquitous context-aware healthcare applications about the available supported services based on their requirements.

Furthermore, the Extended Framework Interface supports the registration mechanism of Sensor Networks SCFs at the Extended Framework Interface. This Sensor Network mechanism is supported between the Extended Framework Interface and the SCSs including the corresponding SCFs.

Finally, in ubiquitous context-aware healthcare applications, a wide spectrum of Security Mechanisms should be supported, since vital and contextual data captured from bio sensors and context-aware sensors respectively convey extremely sensitive information. Hence, the proposed framework provides third party developers with energy-efficient Security Mechanisms for sensor networks in order to achieve authenticity, confidentiality, integrity, nonrepudiation and availability in ubiquitous context-aware healthcare applications. Examples of such Security Mechanisms are given in Section IV.

IV. Security Mechanisms in the Extended Framework Interface

The proposed framework provides developers with a plethora of security mechanisms for sensor networks to properly select those mechanisms that fit well into the specific sensor network's constraints (e.g. low power processor, small memory and bandwidth, short battery life) and deployment cost.

In addition, the provided security mechanisms are considered by the developer as simple components that can be integrated to implement security mechanisms with multiple lines of defense against both known and unknown security threats. Thus, the deployed security mechanisms work well not only in the presence of designated attacks but also under new attacks. Moreover, the integrated security mechanisms are able to address not only malicious attacks but also other network faults due to misconfiguration, extreme sensor network overload, or operational failures [6].

For example, user authenticity, data confidentiality, integrity and availability mechanisms can be based on symmetric, asymmetric and/or hybrid techniques [6]. Besides, the Extended Framework Interface can support some security mechanisms designed by the authors in [7] and [8] to achieve strong security in a multilayer approach.

The efficient security mechanism proposed in [7] provides authenticity and data integrity for the communication among the sensors and the base station of a sensor network. This mechanism exploits a low-weight hash function, which is used in combination with a key to produce Message Authentication Codes (MACs), in a group communication model to prevent unauthorized data disclosure as well as to ensure that data have not been altered during transmission. This key, which is shared among the sensors and the base station, is frequently changed. Besides, the key is exchanged once, during the deployment of the sensor network, and specific steps are followed in order to secure the communication among the sensors and the base station.

In addition, the data integrity mechanism proposed in [8] can be used by the developer to achieve data integrity in the case of deployment an eHealth tele-monitoring system that operates in a smart home and supports transmission of medical data from the smart home to the healthcare center. In this data integrity mechanism, agent technology is proposed to ensure data integrity making use of MACs and cryptographic smart cards connected to the Residential Gateway of the smart home and the PC of the caregiver. Each smart card stores a pair of secret keys. The one is for encryption/decryption processes executed on the smart card and the other for computing MACs on the smart card. Finally, for computing MACs on sensors and the Body Gateway, each of them uses a secret key which is the XOR result of its MAC-address and a secret pre-shared key.

V. Conclusion & Future Work

In this paper, we have proposed a generic application framework integrating context-aware mechanisms derived from well-known context-aware frameworks with the basic mechanisms of the OSA/Parlay Framework Interface. Furthermore, a set of essential security mechanisms are integrated in the proposed framework. The inspiration of the proposed framework originates from the lack of current generic frameworks that support developers to build rapidly reliable and secure ubiquitous context-aware healthcare applications over heterogeneous medical networks.

Finally, as future work, we plan to design and implement a wizard that will help third party developers on how to deploy efficiently secure ubiquitous context-aware healthcare applications, where sensor networks mechanisms and security mechanisms will be essential.

References

[1] M. Baldauf, S. Dustdar, and F. Rosenberg, "A survey on contextaware systems," *Int. J. of Ad Hoc and Ubiquitous Computing*, vol. 2, no. 4, pp. 263-277, 2007.

[2] M. Miraoui, C. Tadj, and C. Ben Amar, "Architectural Survey of Context-Aware Systems in Pervasive Computing Environment," *Ubiquitous Computing and Communication J.*, vol. 3, no. 3, 2008.

[3] P. Korpipaa et al., "Managing Context Information in Mobile Devices," *IEEE Pervasive Computing*, vol. 2, no. 3, pp. 42–51, Sept. 2003.

[4] J. E. Bardram, “The Java Context Awareness Framework (JCAF) – A Service Infrastructure and Programming Framework for ContextAware Applications,” in *Pervasive 2005*, LNCS, vol. 3468, H. Gellersen, R. Want, and A. Schmidt, Eds. Munich: Springer Verlag, 2005, pp. 98-115.

[5] D. Lymberopoulos, “The State of the Art of Distributed Architecture for Supporting Value-Added Services in Next Generation Networks (NGNs),” *Book Chapter in Heterogeneous Next Generation Networking: Innovations and Platforms*, S. Kotsopoulos and K. Ioannou, Eds., IGI Global, 2008, pp. 134-157, ISBN: 978-1-60566108-7.

[6] N. Komninos, D. Vergados, and C. Douligeris, “Layered security design for mobile ad hoc networks,” *Computers and Security J.*, Elsevier, vol. 25, no. 2, pp. 121-130, March 2006.

[7] I. Kolokouris, N. Zarokostas, and N. Komninos, “Integrity and Authenticity Mechanisms in Sensor Networks,” *International Journal on Computer Research*, vol. 15, no. 1, pp. 57-72, 2007.

[8] G. Mantas, D. Lymberopoulos, and N. Komninos, “Integrity Mechanism for eHealth Tele-monitoring System in Smart Home Environment,” in *Proc. 31st Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, Minneapolis, Minnesota, 2009, pp. 3509-3512.