This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the WCNC 2008 proceedings.

A Presence-based Architecture for the Integration of the Sensing Capabilities of Wireless Sensor Networks in the IP Multimedia Subsystem

May El Barachi, Arif Kadiwal
Concordia University, Montreal, Canada

Roch Glitho
Ericsson and Concordia University, Montreal, Canada

Ferhat Khendek, Rachida Dssouli
Concordia University, Montreal, Canada

***Abstract* --- Wireless Sensor Networks (WSN) are made up of small devices that can sense context information (e.g. space, physiology, and environment). The IP Multimedia System (IMS) aims at the convergence of Internet and cellular networks. It enables the delivery of multimedia services to end-users. Integrating the sensing capabilities of WSN in the IP multimedia subsystem will open the door to a wide range of novel multimedia services. This paper proposes a presence based architecture for the integration, focusing on how the information is conveyed from the WSN to the presence infrastructure (i.e the inbound interface). Presence is an integral part of IMS. It enables the distribution of end-user presence information (e.g. location, availability), a sub-set of context information, to interested parties, generally applications. We introduce the architecture and elaborate some of the required extensions to the 3GPP presence service. The proof of concept prototype is also described.**

Keywords — The IP multimedia subsystem, wireless sensor networks, integration, presence, context, pervasive games

I. INTRODUCTION

The IP Multimedia Subsystem (IMS) is one of the key components of third generation (3G) networks [1]. It can be seen as an overlay control layer that is deployed on top of IP-based mobile and fixed networks, in order to enable the seamless provision of IP multimedia services to end users. Wireless Sensor Networks (WSNs) are an emerging type of networks formed by a set of distributed devices (sensor nodes) that collaborate to monitor physical and environmental conditions [2]. Due to their ability to capture a rich set of contextual information (e,g. spatial, physiological, and environmental data), WSNs can be used for a wide range of applications [2].

This paper focuses on the integration of the sensing capabilities of WSNs in the IMS, as means to provide new and personalized services to end users. Examples of such services include: pervasive gaming, enhanced emergency services, wireless healthcare applications, and asset monitoring applications. The solution we propose for the integration is based on the extension of the presence framework proposed for 3G networks [3]. This framework focuses on the management and the dissemination of user presence information (which constitutes a subset of contextual information) to interested parties (usually applications). The architecture proposed is presented, and the extensions made to the presence framework are discussed. The implementation of a proof-of-concept prototype is also described.

The next section provides the necessary background information, followed by motivating scenarios and justifications for a presence-based approach. The proposed architecture is then discussed, along with some of the extensions made to the 3GPP presence framework. This is followed by a presentation of the prototype and a discussion of related work. We end the paper with our conclusions.

II. BACKGROUND

This section introduces wireless sensor networks and gives an overview of the 3GPP IMS architecture and the associated presence framework.

A. Wireless Sensor Networks

Sensors are electronic devices that can detect physical phenomena or stimuli from the environment and produce an electric signal. A WSN consists of a set of small sensors equipped with processors, memory, and short range wireless communication capabilities. The sensor nodes collaborate to collect and aggregate data about the phenomena under observation. Figure 1 illustrates a typical WSN architecture. It consists of three main types of nodes: sensors, sinks, and gateways. The sensors do the actual sensing, while the sinks collect data from all the sensors, and interact with applications via the gateway. This last has a dual network interface, and acts as a link between the WSN and the outside world by performing the needed mapping and protocol conversions. Usually, the sink and the gateway are co-located and simply referred to as either sink or gateway. Reference [2] provides a detailed overview of WSNs.

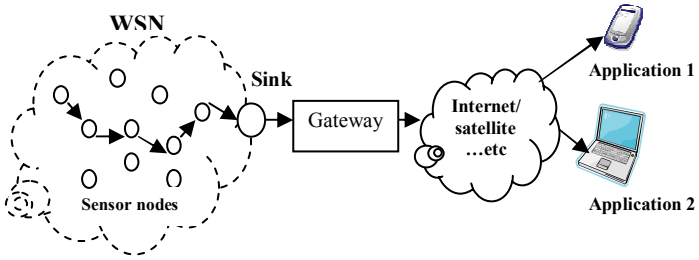

Figure 1. A typical wireless sensor network architecture

Due the availability of smaller, more powerful, and cheaper sensor nodes, and the ability of WSNs to capture a rich set of contextual information, this type of networks is increasingly used in a wide variety of applications. Typical applications include: environment/habitat monitoring, healthcare applications, home automation, and traffic control.

B. The IMS and presence

The IMS, which is standardized by 3GPP (the Third Generation Partnership Project), is rapidly becoming the de-facto standard for IP-based multimedia communication services. Figure 2 illustrates a simplification of the 3GPP IMS architecture, specified in [4].

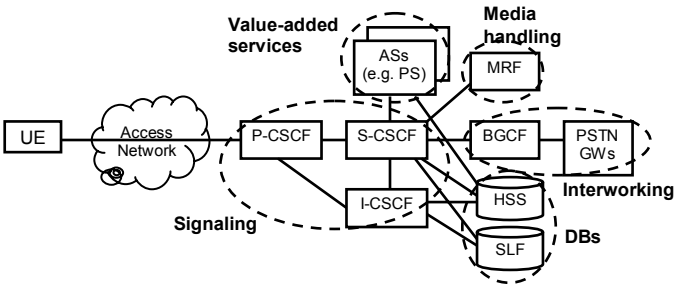

Figure 2. A simplified illustration of the 3GPP IMS architecture

The architecture consists of five main types of functional entities: databases, signaling entities, media handling entities, interworking entities, and entities providing value-added services. Of special interest to us are the databases, the signaling entities, and the entities providing value-added services. There are two main types of databases: The Home Subscriber Service (HSS) containing all the user-related subscription, authorization, and authentication information; and the Subscriber Location Function (SLF) which maps users' addresses to HSSs (in case more than one exits). In terms of signaling, several SIP servers, collectively known as Call/Session Control Functions (CSCFs), handle signaling operations in the IMS. There are three types of CSCFs: The Proxy-CSCF (P-CSCF), the Serving-CSCF (S-CSCF), and the Interrogating-CSCF (I-CSCF). The P-CSCF is the first point of contact between the User Equipment (UE) and the network, acting as inbound/outbound proxy and authorizing media resources. Located at the edge of the administrative domain, the I-CSCF assigns S-CSCFs to users performing SIP registration and routes messages to the appropriate S-CSCF. The S-CSCF acts as registrar, enforces network and user-related policies, and triggers the appropriate services at the application servers (which host and execute value added services). An example of standardized application servers is the Presence Server (PS), which constitutes a key component of the 3GPP presence architecture depicted in figure 3.

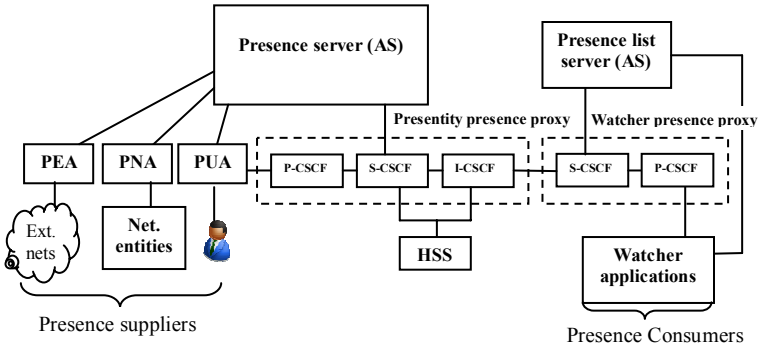

Figure 3. The 3GPP presence architecture

This 3GPP presence architecture is based on the IETF presence model [5], in which presence is referred to as information published by users (presentities – short for presence entities) to other users (watchers) to indicate their ability and willingness to communicate. The 3GPP architecture distinguishes between three types of presentities: Presence User Agents (PUAs) publishing information provided by users; Presence Network Agents (PNAs) publishing information provided by network entities about the user; and Presence External Agents (PEAs) publishing information provided by external entities/networks about the user. In addition to presence agents (which basically represent a layer of abstraction on top of information sources), there are four other types of entities in the 3GPP presence architecture: the presence server, the presence server list, presence proxies, and watcher applications. The presence server is responsible for the management of presence information published by agents, and the fusion of data from multiple sources into a single presence document, while the presence list server is responsible for group list management. Presence proxies (e.g. presentity presence proxies and watcher presence proxies) act as inbound/outbound proxies to the presence network, performing routing, security, and charging functions. The roles of presence proxies are assumed by CSCFs, as shown in figure 3. As for watcher applications, they subscribe to presence information of interest, therefore acting as presence information consumers.

III. MOTIVATIONS

Context-awareness is the ability to use contextual information to provide relevant information and/or services to the user [6]. By integrating the sensing capabilities of WSNs in the IMS, a rich set of contextual information can be exploited to provide new and personalized services to IMS users. In this section, we present two examples of services that could be provided and motivate the use of a presence-based approach for WSNs/IMS integration.

A. Motivating scenarios for integrating the sensing capabilities of WSNs in the IMS

Wireless healthcare is one of the application areas that could benefit from the availability of contextual information, (provided by WSNs) in the IMS network. We give as example a health monitoring application that tracks heart patients' health conditions, and automatically establishes a 911 call between the patient and the PSAP (Public Safety Answering Point), upon the detection of an incoming stroke. The application scenario could be described as follows: After a first heart stroke, the risk of suffering a second one increases. Therefore, the patient's heart rhythm and pulse are continuously monitored using biometric sensors (forming a body sensor network) and conveyed to the network. When an oncoming stroke is predicted, the health monitoring application (to which the user has subscribed) automatically establishes a 911 call between the user and the appropriate PSAP, which is determined based on the user's location and his/her terminal's media capabilities. After the call

establishment, the PSAP call taker dispatches the nearest ambulance to the user's location and the ambulance paramedic is added to the call (conferencing) by the health monitoring application. Furthermore, the patient's biometric data/vital signs are conveyed to the ambulance paramedic team. Upon the arrival of the ambulance, the conference is automatically terminated by the application, which determines the nearest hospital with an available ER unit and heart specialist, establishes a call between the hospital and the ambulance, and transfers the patient's file to the hospital.

Another potential application area is pervasive gaming. We give as example the Big Urban Game (BUG), originally designed by the University of Minnesota Design Institute [7], and examine its deployment in a WSN-enabled IMS environment. The idea of the game is a five day race through a city, as means to encourage the players to explore the city. The game is originally played via online voting and physical participation in the race. In a WSN-enabled IMS environment, the game scenario can be described as follows: Three teams must each move one giant inflatable object through a series of checkpoints. WSNs are used to detect and convey the location of inflatable objects and their presence at checkpoints, to the network. Each day, players get notified via IMS messaging about two possible routes to their object's next checkpoint. Players choose the route they feel is the fastest, voting via IMS messaging. Each evening, a team of volunteers move the inflatable object according to the chosen route, while getting notifications about their status in the game, and they are timed by the system. The team with the least cumulative time over the five days is declared the winner.

B. *Requirements and motivations for a presence-based approach*

In this section, we first derive a set of requirements for the integration of WSNs and the IMS, then evaluate the existing presence framework with respect to those requirements.

The first requirement is that the approach should make all possible WSN sensing capabilities (e.g. spatial, physiological, and environmental data) available in the IMS. Second, the approach should be capable of handling information about different types of entities (e.g. users, objects, places…etc), to enable a wide range of applications. Furthermore, the sensed data should be represented in an IMS-compatible format. As a fourth requirement, the approach should support standard IMS communication protocols when interacting with IMS entities, and enable both synchronous and asynchronous modes of communication. Finally, the approach should accommodate the business model in which the WSN infrastructure is owned by the IMS service provider, as well as the one in which the infrastructure is owned by a third party.

Our motivation for a presence-based approach stems from the fact that the existing presence framework has the potential of meeting all those requirements, after the proper extensions. In fact, the existing presence model already supports spatial information (e.g. location), and rudiments of environmental information (e.g. place properties). Physiological information could also be supported after the proper extensions to the model. Furthermore, although the presence model only handles information about user entities, it could be extended to handle non-user entities related information, as we will demonstrate in the coming section. In terms of information representation and information exchange model, the presence framework relies on a standard XML-based information model (the PIDF) and a standard IMS protocol (i.e. SIP) for synchronous and asynchronous information exchange. Presence information can also accessed via standard APIs, such as the Parlay-X APIs [8]. Furthermore, the presence architecture considers the case of external entities/networks as information sources, although the needed authentication, authorization, and charging mechanisms remain to be defined.

IV. ARCHITECTURAL COMPONENTS AND EXTENSIONS TO THE 3GPP PRESENCE SERVICE

In order to enable the integration of WSNs in the IMS, we assign the role of Presence External Agent (PEA) to the WSN gateway, which will publish information provided by the WSN about different entities (user and non-user entities) to an extended presence server, capable of managing the different types of information provided. Other entities such as IMS application servers (e.g. game servers), IMS core network entities (e.g. CSCFs), and IMS user applications can act as watchers to the information published in the presence server, and use this information to provide value-added services to end users. Figure 4 depicts the proposed architecture.

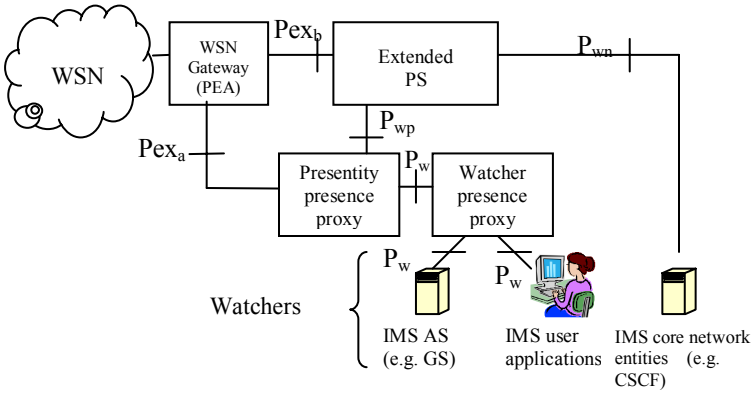

Figure 4. WSN/IMS integrated architecture

It should be noted that we divide the inbound interface (interface between the WSN gateway and the PS) into two sub-interfaces: Pex_a, and Pex_b. Pex_a is used for the exchange of contextual information between the gateway and the PS, via a trusted node (a presence proxy). This indirect interaction between the gateway and the PS is motivated by the fact that several support functions (e.g. identification and charging, authentication/authorization, service discovery, and the establishment of security associations) are needed for information exchange. Some of these functions are already supported by the presentity presence proxy, and therefore could be leveraged by including the proxy as intermediary node between the gateway and the PS. As for the Pex_b interface, it is used for direct interactions between the gateway

and the PS, in relation to the management of subscription policies (enabling information access control). In addition to the inbound interfaces, figure 4 depicts two outbound interfaces (interfaces between the PS and watchers): the P_w and the P_{wn} interfaces. P_w is an enhancement of the existing 3GPP interface which enables end user applications and IMS application servers to access presence information managed by the PS, via presence proxies. P_{wn} is a new interface we define to enable network entities acting as watchers to get direct access to presence information from the presence server. In this case, no intermediary trusted nodes are needed between the network entities (acting as watchers) and the PS, since those entities are owned and trusted by the network.

This mapping of the WSN architecture onto the presence framework entails several issues, such as: the existence of non-user entities in the IMS world (i.e. how will non-user entities be identified in the IMS, and how is charging in relation to their information publication to be performed); the extension of the presence information model to accommodate additional types of information; the definition of the reasoning mechanisms needed for information processing (e.g. the generation of high level information from low level data); and the identification of the communication protocols to be used on the inbound and outbound interfaces. In this paper, we focus on the first two issues, as well as the definition of the communication protocol to be used on one of the inbound interfaces (the Pex_a interface), leaving the remaining issues for future work.

A. Identification and charging related issues

As shown in the motivating scenarios, information about different types of entities (i.e. user entities and non-user entities such as inflatable objects, hospitals…etc) need to be handled in order to enable context-aware value added services. User entities are the norm in the IMS, and the publication of their information is already covered by the existing presence solution. However, the problem is how to deal with non-user entities in the IMS world (i.e. in terms of identification, authentication/authorization, and charging).

There are two potential solutions to this problem. The first solution is to uniquely identify those non-user entities in the IMS. Although simple to conceive, this solution is problematic, since it raises the following issues: who will be responsible of billing/charging (an object or place not being legal entities), and how will each object be associated with a SIM card allowing its identification by the network.

The second alternative which we propose is to create identities for non-user entities (e.g. objects and places) and associate those identities with the identity of an IMS corporate entity. To explain this idea, we introduce the concept of IMS corporate identity as follows: Game providers, enterprises, and corporations could have IMS corporate accounts, and thus be known as IMS subscribers (each corporation/enterprise would then be assigned one public corporate identity and one or more private corporate identities). Furthermore, separate (but dependant) public identities are created for each object/place managed by the IMS corporate client. We also assume the existence of a corporate user registration process, which is responsible for registering the IMS corporate client and all its dependant non-user identities with the network. This process could be optimized using the existing concept of implicitly registered public identities, which requires only one registration using the main identity and results in the registration of this identity and all its associated identities. As for charging/billing, it is made for the IMS corporate entity (not for the dependant entities), who is responsible for settling the bills. Figure 5 illustrates the concept of IMS corporate identity and its associated non-user identities.

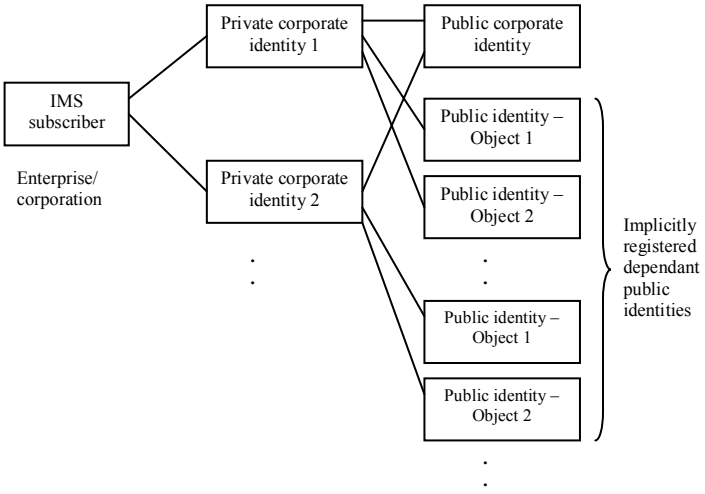

Figure 5. IMS corporate identity and its associated non-user identities

It should be noted that corporate public identities could serve as contact information on business cards (similar to companies e-mail addresses), and are used for routing of SIP traffic. Furthermore, corporate public identities can either be SIP URIs or TEL URIs, while public object identities can only be SIP URIs (TEL URIs not being relevant in this case). Figure 6 illustrates a possible SIP URI scheme. As for private identities, they are used for identification and authentication purposes only, and are not know by the corporate user. In fact, each private identity is associated with a SIM card on which it is stored. Since each organization may manage several branches/locations, it may be necessary to have several private identities (for each corporate client), each associated with a SIM card that will be used for registering all the objects related to a certain branch. Private identities take the form of network access identifiers, such as: username@operator.com.

Public corporate identity:
CompanyName.Country@operator.com

Public object identity:
ObjectID.CompanyName.Branch.Country@operator.com
Examples:
- Hospital room status:
  ER201.RoyalVicHospital.Montreal.Canada@operator.com
- Inflatable object in a pervasive game:
  IFO100.GameProviderX.MontrealDownTown.Canada@operator.com

Figure 6. SIP URI scheme for public corporate and object identities

B. *Extended presence information model and information exchange protocol*

The 3GPP presence architecture mandates the use of the XML-based PIDF [9], defined by the IETF, as presence information model. The PIDF defines only basic status and contact information, but can be extended. In fact, several extensions have already been proposed, such as: the RPID [10] which provides additional presence information about persons and their devices and services (e.g. activities, mood, place type and place properties…etc); the CIPID [11] which provides contact information related extensions; and the GEOPRIV [12] which provides geographical location related extensions. To enable the integration of WSNs in the IMS, other extensions need to be defined to accommodate additional types of information provided by WSNs, namely: physiological/biometric data, and environmental data. Furthermore, the information model should enable the distinction between user and non-user related information.

Focusing on this last enhancement, and taking the pervasive gaming scenario as example, we propose a simple extension to the GEOPRIV model, in order to identity the type of entity (e.g. inflatable object) to which the location presence information relates. This extension is achieved by adding two new attributes "entityType" and "entityDescription" to the existing presence element, as illustrated in figure 7. This distinction between the information related to user and non-user entities could offer more flexibility in terms of charging, as corporations may wish to negotiate a special charging rate for the publication of their managed objects related information. Furthermore, the privacy requirements may not be the same when it comes to objects related info (e.g. location).

```
<presence entity="pres: IFO100.BugProvider.Montreal.Canada@ericsson.com"
entityType = "object" entityDescription = "inflatable  piece" >
<tuple id="sg89ae">
<status>
  <gp:geopriv> <gp:location-info>
    <cl:civicAddress>
      <cl:country>Canada</cl:country>
      <cl:A1>Montreal</cl:A1>
            <cl:LOC>CheckPoint1</cl:LOC>
    </cl:civicAddress>
  </gp:location-info> </gp:geopriv>
 </status>
<timestamp>2007-10-1T10:57:19Z</timestamp>
</tuple> </presence>
```

Figure 7. GEOPRIV information model usage for pervasive gaming

As for the information exchange protocol to be used on the Pex_a interface, it must satisfy a set of requirements defined by 3GPP, namely: it must not impose any limits on the size of the information transported; it should support full and partial update notifications; and should support the transport of information formatted according to the PIDF. The IETF-defined SIMPLE (SIP for Instant Messaging and Presence Leveraging Extensions) protocol suite [13] satisfies all those requirements. Therefore, we believe it can be used for the transport of WSN related information over the Pex_a interface. However, some optimizations may be needed. For instance, a publish-upon-request mechanism could be added to trigger a certain sensor to publish information, only when requested. This can be useful to control the amount of information generated by environmental sensors, which typically generate large amounts of information that can overload the network.

V. PROTOTYPE

We leveraged the JAIN presence server [14] and a web service-based WSN gateway previously developed in our group [15], to build a proof-of-concept prototype of our architecture. We extended the presence server's XML schema with the enhanced GEOPRIV data elements. Furthermore, due to the lack of an IMS infrastructure in our lab, we decided to co-locate the CSCFs and HSS with the presence server. In fact, the JAIN presence server was already augmented with SIP registrar and SIP proxy functionalities, which we enhanced to emulate very simple CSCF and HSS components, in the same node. As for the existing WSN gateway, it was remodeled to act as presence external agent, by replacing the original web service communication interface by a SIMPLE interface, and adding the PEA related logic.

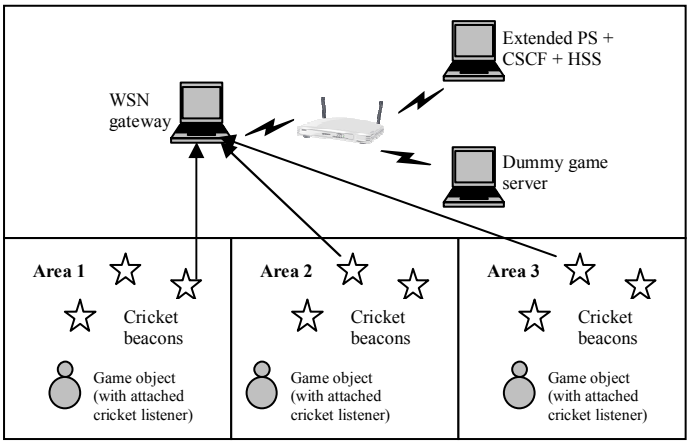

Figure 8. Prototype setting

As shown in figure 8, the WSN/IMS integrated environment was simulated using three laptops forming a WLAN, and a set of MIT Cricket location sensors [16]. One of the laptops hosted the IMS functional entities (i.e. the combined presence server/ CSCF/ HSS), while the other hosted the WSN gateway interfacing with the MIT Crickets. The third laptop hosted a dummy game server, acting as information consumer. Then, some of the interactions related to the pervasive gaming scenario were tested as follows: first, the game server was used to register as an IMS corporate user, then cricket beacons mounted to the ceiling were used to detect the location of three game objects (each with an attached cricket listener) which we moved around the room, and this information was conveyed to the WSN gateway, which publishes it (after proper formatting) in the extended presence server. The published information was then accessed by the game server, via subscription/notification. The three types of interactions mentioned (IMS corporate user registration, information

publication by the WSN gateway, and information subscription/notification between the GS and the PS) were carried successfully, therefore demonstrating the feasibility of the integration solution proposed.

VI. Related work

The e-SENSE architecture [17] aims at making ambient intelligence available to beyond 3G networks, to enhance their service provisioning capabilities. This solution focuses on info acquisition aspects, defining the protocol stack to be implemented by sensor nodes as well as a generic architecture for the WSN gateway. However, the integration of the e-SENSE architecture with the IMS is not addressed in this work, although the authors mention the possibility to interface their system with the IMS GUP (Generic User Profile) server, as means for the integration.

Alarm-Net [18] and CodeBlue [19] are examples of solutions for the integration of WSNs in the internet. Alarm-Net is used for monitoring patients in homes and nursing residencies, while CodeBlue is used for monitoring victims of mass casualty events. Similarly, MetroSense [20] is an architecture proposed to enable urban sensing using the Internet. None of these solutions uses IMS standard data formats nor standard protocols. Furthermore, Alarm-Net and MetroSense do not provide any charging mechanisms.

The work presented in [21] introduces the idea of service discovery gateways as means to connect a local network (with non-IMS devices) to the IMS infrastructure. Although sensors could be considered as non-IMS devices that could be integrated with the IMS, this work focuses on service discovery and remote invocation of services via the IMS, while we focus on making WSNs an integral part of the IMS by formatting the information they provide into an IMS-compliant format, and exchanging this information using IMS protocols, in addition to tackling other issues such as identification and charging in relation to information access.

The work presented in [22] addresses the issue of the use of IMS communication services by enterprises, and proposes four possible deployment scenarios: the standalone scenario (the enterprise managing its own IMS infrastructure); the fully hosted scenario (the enterprise communication system completely residing in the public IMS network); the intermediate scenario (the enterprise maintaining its own application severs and relying on the IMS service provider for signaling and control functions); and the virtual network operator scenario (the enterprise managing its own IMS infrastructure while relying on the mobile operator for management of mobility and roaming issues). In general, our solution fits within the second deployment scenario. However, the nature of the IMS services targeted is different (IMS communication services vs. info management and dissemination services). Furthermore, the solution presented in [22] focuses on user entities (i.e employees) as consumers of the IMS services, while we also address non-user entities, which raises the level of complexity of the problem.

VII. Conclusions

WSNs are seen as a major source of contextual information, and their integration with the IMS can lead to a wide range of context-aware value added services. In this paper, we have proposed a solution for the integration of WSNs sensing capabilities in the IMS. This solution is based on an extension of the 3GPP presence architecture. Some of the issues related to the integration were addressed in the paper, namely: issues related to identification and charging; as well as information exchange over the inbound interface. Furthermore, a proof of concept prototype, showcasing a pervasive gaming scenario, was presented. For future work, we plan to investigate the remaining issues related to WSNs/IMS integration, namely: information modeling and processing, the discovery of WSN gateways by the PS, and the definition of the outbound interfaces' related protocols and interactions. We also plan to work on a generic WSN/IMS gateway solution.

References

[1] G. Camarillo and M. Garcia-Martin, "The 3G IP Multimedia Subsystem", Wiley & Sons Ltd., August 2004

[2] I. Akyildiz et al., "Wireless Sensor Networks: A Survey", IEEE Communications Magazine, August 2002.

[3] 3GPP TS 23.141, "Presence service: architecture and functional description (Release 7 – v.7.0.0)", September 2005

[4] 3GPP TS 23.228, "IP multimedia subsystem (v.7.3.0)", March 2006

[5] M. Day, J. Rosenberg, and H. Sugano, "A model for presence and instant messaging", RFC 2778, February 2000

[6] G. Abowd et al., "Towards a better understanding of context and context-awareness", *HUC'99*, Germany, 1999.

[7] The university of Minnesota Design Institute website, accessible at: http://design.umn.edu/go/project/TCDC03.2.BUG

[8] The Parlay Group, Parlay X web services specification, V. 3.0, accessible at: http://www.parlay.org/en/specifications/pxws.asp

[9] H. Sugano et al., "Presence information data format (PIDF)", RFC 3863, August 2004

[10] H. Schulzrinne et al., "RPID: Rich presence extensions to the PIDF", RFC 4480, July 2006

[11] H. Schulzrinne, "CIPID: Contact information in PIDF", RFC 4482, 2006

[12] J. Peterson, "A presence-based GEOPRIV location object format", RFC 4119, December 2005

[13] B. Campbell et al., "SIP extension for instant messaging", RFC 3428, December 2002

[14] JAIN-SIP-PRESENCE-PROXY, available at: http://www-x.antd.nist.gov/proj/iptel/nist-sip-downloads.html

[15] Truong Ta, Nuru Othman, Roch Glitho, and Ferhat Khendek., "Using web services for bridging end user applicationas and wireless sensor networks", ISCC'06, Italy, 2006.

[16] Adam Smith et al., "Tracking moving devices with the cricket location system", MOBISYS, Boston, 2004.

[17] A. Gluhak et al. "e-SENSE Reference Model for Sensor Networks in B3G Mobile Communication Systems", Information society technologies (IST) 2006.

[18] V. Wood et al. "Alarm-Net: Wireless Sensor Networks for Assisted-Living and Residential Monitoring", Technical Report CS-2006-13, Department of Computer Science, University of Virginia, 2006.

[19] F. Malan, and M. Welsh, "CodeBlue: an Ad Hoc Sensor Network Infrastructure for Emergency Medical Care", International Workshop on Wearable and Implantable Body Sensor Networks, April 2004.

[20] A. Campbell et al., "People-centric urban sensing", WICON-06, Boston, August 2006

[21] A. Haber, M. Gerdes, F. Reichert, and R. Kumar, "Remote service usage through SIP with multimedia access as a use case", PIMRC 2007, Greece, September 2007

[22] H. Khlifi, and J-C. Gregoire, "IMS for enterprises", IEEE Communications Magazine, July 2007