Integration of eHealth Service in IPv6 Vehicular Networks

Sofiane Imadali[1], Athanasia Karanasiou[2], Alexandru Petrescu[1], Ioannis Sifniadis[2], Eleftheria Vellidou[2], and Pantelis Angelidis[3]

[1] CEA, LIST, Communicating Systems Laboratory, 91191 Gif-sur-Yvette CEDEX, France
{sofiane.imadali,alexandru.petrescu}@cea.fr,
[2] Vidavo Technical Department, Vidavo S.A., Thermi, Thessaloniki 57001, Greece
{it,helpdesk,projects}@vidavo.gr
[3] Wireless Sensors Laboratory, University of Western Macedonia, Karamanli & Lygeris, Str Kozani 50100, Greece
pantelis@vidavo.gr

Abstract. Several convenience and efficiency applications have been proposed as part of recent vehicular networks (a.k.a. VANET) activities. Among these proposals, eHealth has often been studied as a time-critical application to emulate an ambulance. The Vehicle-To-Infrastructure (V2I) setting is the typical communication scenario to carry out the data in this case. From a user perspective, combining vehicular networking and eHealth to record and transmit a patient's vital signs is a special telemedicine application that helps hospital resident professionals to optimally prepare the patient's admittance. The current proposal provides an IPv6 vehicular platform which integrates eHealth devices and allows sending captured user health-related data to a Personal Health Record (PHR) application server in the IPv6 Internet. The collected data is viewed remotely by a doctor and supports his diagnostic decision. The resulting platform is then compared to the state-of-the-art related architectures.

Key words: Vehicular networks, eHealth, IPv6, Testbed Integration, Remote diagnosis

1 Introduction

Intelligent Transportation Systems (ITSs) [5] are envisioned to play a significant role in the future, making transportation safer and more efficient. As it was concisely stated at the Intelligent Transportation System World Congress in 2008: save time, save lives [1]. In order to achieve these objectives, V2I interactions have evolved to include various applications, some of which are safety-related and others user-oriented (infotainment).

1.1 M2M devices proliferation

According to some estimates, the size of the Internet doubles every 5.32 years, which will lead to an average of 6.58 connected devices per person by 2020 [6]. These 50 billion things [7] connect to the network in order to gather and spread information for various and unattended applications supporting new markets [8]. From an addressing perspective, these new and exciting opportunities come with the requirement of a larger addressing space. The current IPv4 addressing pool is nearly exhausted [9], which urges the transition to the new version of Internet Protocol (IPv6) giving the important numbering space it comes with(2^{96} times bigger than IPv4's) [10].

In the wide field of health informatics, eHealth is about the use of the Internet to disseminate health related information [11]. The World Health Organization (WHO) defines eHealth as "the transfer of health resources and healthcare by electronic means". This activity includes the delivery of health information to health professionals and health consumers through the Internet and telecommunications in order to improve public health services. To be accurate, another term, mHealth, is defined as the subset of eHealth that concerns health services by means of mobile technologies such as mobile phones and PDAs (personal digital assistants) [2]. Health-related information is captured by small and various M2M devices and stored in large databases to be further processed in order to support diagnostics. The final goal is to improve efficiency and save lives [12].

1.2 IPv6 vehicular networking

Several years of research initiatives in the field of automotive applications proved the considerable improvement of traffic safety and new unattended market opportunities these applications could provide. EHealth is only one application example that could apply to the vehicular paradigm. V2I and V2V environments include several other examples of safety and service or infotainment applications support. Basically, we can classify these applications in two major categories: safety-oriented or user-oriented [13]. Safety applications are clearly time-critical tasks, where message delivery with short delay guarantee is the first design goal. To satisfy the time stringent requirement, non-IP (radio) communication technologies are often preferred over best-effort networks (Internet) for their reliability and reduced overhead[14]. Radio communications are initiated on dedicated channels [1]. In contrast, user-oriented applications are non-time-critical tasks, in which falls infotainment and other prevention on road applications. The use of Internet Protocol (best effort) to extend the supported geographic area for these applications is possible [15].

As we experience an upgrade in the Internet Protocol from version 4 to 6, the use of IPv6 in current standardization work for vehicular communications technologies guarantees a better integration in the Future Internet and ensures a better compatibility with unattended applications. For example, UMTS and LTE technologies support IPv6 according to 3GPP specifications [16], which opens new V2I services perspective using the deployed infrastructure, and this before the wide adoption and deployment of dedicated Roadside Units (RSUs) [17]. In recent ETSI activities, a GeoNetworking protocol combined with IPv6 has been experimented and standardized [15]. In the GeoNet project, a safety oriented application using broadcast has been defined. GeoBroadcasting is the use of relay messages from vehicle to vehicle (V2V) in a certain geographic neighbourhood (zone or area) over IEEE 802.11p radio technology.

1.3 Heterogeneous technologies

Wireless communication technologies such as ZigBee, Bluetooth, and WiFi are already widely used in the M2M industry and expected to be widely deployed in near future automotive communications. Limited computing and networking capabilities devices (including eHealth devices) are expected to use such means of communication with the outside world. These short range communication technologies are much more common use for "small" devices because of the reduced amount of overhead (compared to IPv6, for example) and demands less energy to transmit data when compared to long range standards (UMTS, LTE or WiMax) [3].

For these reasons, with a client-server application design in mind, an additional functional element (the gateway (GW)) translates between both short and long range communication technologies and helps expending the boundaries of the current Internet. From an addressing perspective, these gateways are called Address Translation Gateways [18] due to their dual addressing function (IP and IEEE 802.15.4 in 6LoWPAN, for instance).

This paper focuses on the use of eHealth technologies in an IPv6 vehicular setting as a special V2I non-time-critical application. The operational scenario studied involves the use of an eHealth device, Electrocardiograph (ECG), Spirometer, Oximeter or Blood Glucose meter sending health-related measurements over Bluetooth to an IPv6-ready phone application. The phone is attached to an IPv6 Mobile Router (second part of the testbed). When the phone application (Android based) sends these measurements after user review and comments, to an application server in the IPv6 Internet, the Mobile Router ensures the right path is selected. Upon delivery, the gathered data is viewed remotely by the user's physician on his/her personal terminal.

The remainder of this paper is structured as follows. Section 2 describes the IPv6 communications requirements that apply to the M2M world. Section 3 presents the overall integrated platform and details its functional elements along with the considered scenario. Section 4 covers the default route configuration with an extension to Dynamic Host Configuration Protocol version 6 (DHCPv6) proposed at the Internet Engineering Task Force (IETF). Section 5 describes the hardware specifications and the integration process of the prototype used in experimentation. Section 6 covers the related work and position our platform among state-of-the-art solutions. Section 7 concludes the paper and gives some envisaged perspectives to our platform.

2 M2M IPv6 communications

As stated earlier, in the longer term, large-scale deployments of various M2M appliances will bring hundreds of millions of communicating devices to the currently deployed network. This perspective assumes that newly deployed devices will communicate in an unattended manner. In this scenario, the Internet Protocol family could glue all the parts of the heterogeneous wireless communication technologies used during the deployment. Hence the importance of auto-configuration mechanisms (with no human intervention) of network parameters to build an end-to-end model from the application server to the endpoint. Two indivisible parts of the configuration process are studied below: addressing and routing.

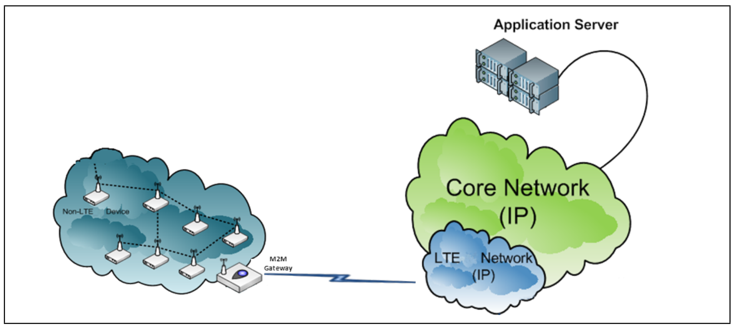

Fig. 1. M2M general system architecture. When the M2M gateway attaches to the network, the M2M gateway sets the PDN Gateway as its first hop towards the Internet and configures its IPv6 address using IPv6 stateless auto-configuration. An additional IPv6 prefix for the internal network is requested via DHCPv6 Prefix delegation.

2.1 Addressing

In order to configure a device with the necessary settings allowing it to communicate on a network, two types of mechanisms exist: stateful and stateless. The state here refers to the management information kept at the gateway level and the device. The configuration parameters usually include the address, mask, and a default route. DHCPv6 protocol falls within a *stateful* group since it maintains a database with all the assigned addresses to a specific device (leases file) at the DHCPv6 Server. Neighbor discovery protocol (NDP) on the other hand, which belongs to the *stateless* group, does not maintain such information: a Router provides a prefix to device and the device forms an address for itself without further assistance from other entities.

In the vehicular-eHealth scenario we are studying, IP devices are deployed in a vehicle equipped with a Gateway offering long-range connectivity. Hence, auto-configuration mechanisms are needed. As depicted in Figure 1, the Gateway in addition to its egress interface address, requires a set of addresses (one or several prefixes) for the IP eHealth devices. The query is made through *Prefix Delegation*, an extension to the DHCPv6 protocol [23]. Basically, this extension allows the assignment of a set of prefixes to a Client. The DHCPv6 protocol is specified to work with Relay and Server entities several hopes away from the client, as described in this recent reference [24].

As vehicular gateways are designed for moving networks, Prefix Delegation for Network Mobility [25] has been specified and defines the behaviour for the above DHCPv6 Prefix Delegation in the context of network mobility. In this work, focus is made on integration and the experimentations occur on table. Mobility scenarios could be part of future work.

2.2 Routing

In addition to assigning IPv6 addresses to the phone handling the eHealth devices in a vehicular network, routing must be set up. Discovering and configuring routes for large networks may quickly become a communication- and computing-intensive task, overcoming the capacity of the existing network. The concept of *default* route (gateway of last resort) provides partial resolution to this problem: it is sufficient for Gateway to hold a single default route (the IP address of the next hop) instead of detailed routes towards specific destinations. Default route auto-configuration mechanisms exist basically under two distinct forms. The first is Router Advertisement-based (the use of stateless address auto-configuration) and the second is a dynamic routing protocol such as OSPF [26]. Currently these two mechanisms are the only IETF mechanisms to assign a default route to an end node.

Whereas NDP address auto-configuration offers a default route to an end device, it does not offer a set of prefixes. Similarly, the DHCPv6 Prefix Delegation part of the stateful address auto-configuration does offer a set of addresses to the Gateway (in order to further deliver them to the IP eHealth devices) but does not offer a default route.

For a limited capacity device (a constrained vehicular Gateway, a Phone, or a constrained IP-eHealth device), it is advantageous to use a lightweight auto-configuration protocol offering both parameters:

- An IPv6 route to be used as a default route in the routing table of the Gateway.
- A set of IPv6 addresses, to be used for address auto-configuration on the IP eHealth devices on-board the vehicle.

3 Platform integration

The objective of the platform described in this paper is to create a vehicular setting that integrates eHealth technology and improves current phone connectivity using next-generation communication capabilities. This section describes the functional elements involved in our architecture resulting from the integration phase both testbeds. The hardware specifications and the current state of the joint testbed are further detailed in the implementation section.

Figure 7 depicts the overall picture of the integrated testbed. The system includes 4 functional elements and 2 types of interactions (short and long-range).

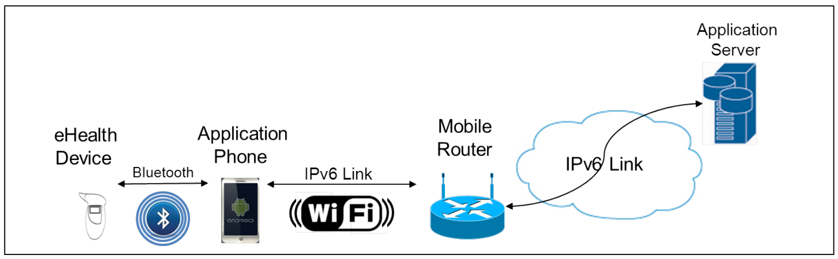

Fig. 2. Overall picture of the platform after integration. The eHealth devices communicate with the server through the phone application. The phone peers with the device over Bluetooth on one side, and attaches to the gateway over WiFi on the other. The gateway routes any traffic originated by the application to the PHR server in the infrastructure.

3.1 Functional elements

On the Figure 7, from left to right, the functional elements are as follows.

- **The eHealth Device** provides real time health-related measurements. These measurements can be of different nature such as blood glucose levels or oxygen saturation levels. Recorded data is sent over Bluetooth to another authorized peer and presented to the patient through a user interface.
- **The Application Phone** is in the middle of two different communication technologies. On one hand, short-range Bluetooth technology to communicate with M2M Devices, capture the eHealth data and present it to the patient and on the other hand, mid-range WiFi technology to send secure IPv6 packets to the server via the Gateway. The phone allows to process the gathered data before sending it to the server along with user comments, which is not possible with a standalone gateway.
- **The Mobile Router (MR)** provides IPv6 connectivity to in-vehicle devices and a default-route towards the server in the Internet. The gateway uses WiFi to advertise internal IPv6 prefix to the attached nodes. For the long-range communication technology (path towards the server), UMTS or LTE provide an IPv6 path from end to end. For testbed purposes, we demonstrate the concept over Ethernet (IEEE 802.3). The MR has a powerful CPU and provides some resource-demanding networking applications, not available to run on a limited battery power device like a smartphone. Besides, it is possible

to request a higher Quality of Service upon network attachment for the MR that could benefit to the phone and other attached devices.

- **The Application Server** collects the data captured on patients and provides a web interface for doctors to support their diagnostic decisions. The software running on the server includes a web server accessed over a secure connection (over SSL) and a limited-access database server to gather the data issued by patients.

3.2 Operational scenario

Vehicular networking and eHealth technologies are combined in the form of an ambulance equipped with special telemedicine devices that can record as well as transmit the patient's vital signs (body temperature, pulse rate, respiration rate, blood pressure) and critical physiological parameters (ECG, blood glucose levels, oxygen saturation levels) to the nearest hospital in order for the resident health professionals to optimally prepare the patient's admittance. This typical V2I scenario that is already possible with state-of-the-art technologies (IPv4 gateways) can be enhanced and tested in an IPv6 deployed architecture. This

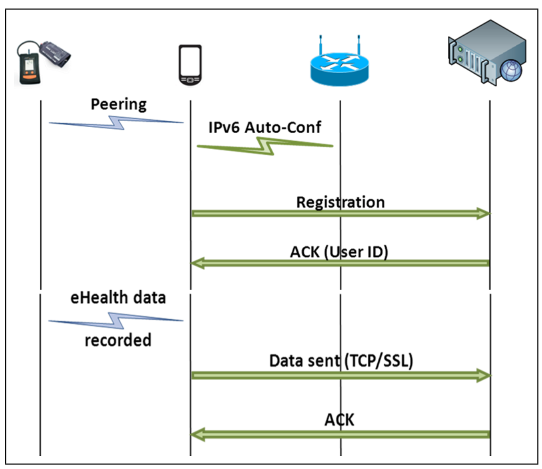

Fig. 3. Message exchange for the eHealth Operational Scenario. Vital signs recorded by the patient are sent to the expert for diagnosis.

scenario could be applied to a situation where a road accident involving serious trauma is to be taken into consideration. The ambulance crew has in its disposition a set of handheld lightweight devices (as demonstrated in the prototyping section) that can transfer emergency data to the hospital. The objective in such a situation is to maximize clinical value through a limited set of measurements. All involved devices communicate via Bluetooth to an Android smart phone providing for IPv6 connectivity to the vehicular gateway that has reserved network resources to achieve certain QoS.

However in an emergency situation (natural disaster, road accidents) where numerous vehicles of different functions (ambulances, fire brigade, police cars) are involved, the scenario could be enriched to accommodate for the optimum data transfer to the interested parties (health care provision, law enforcement) via V2V communications. This topic is out of scope of this paper.

4 Default route configuration with DHCPv6

As described in section 2, in order to configure in-vehicle devices we need to provide them with IPv6 prefixes requested from the infrastructure (PDN-GW) through DHCPv6 Prefix Delegation. In addition, the configuration of the attached gateway with an egress global address and a default route requires the use of NDP.

The proposal [27] depicted in the message exchange of Figure 4 shows the replacement of NDP by a DHCPv6 extension in the communications between the gateway and the infrastructure. The draft describes a new DHCPv6 option, Option Request Option (ORO) that allows to request, among other parameters, the default route. Figure 4 summarizes the extended message exchange performed by the vehicular Gateway and the DHCPv6 entities in the infrastructure. The

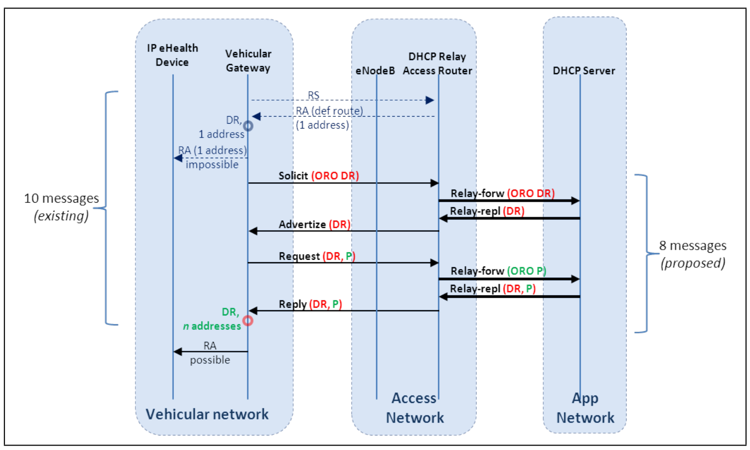

Fig. 4. Auto-configuration Protocol Messages. A comparison of the number of messages between current auto-configuration methods and the proposed one. DR stands for Default Route, P for prefix, and ORO for Option-Request Option.

original DHCPv6 protocol uses up to 10 messages in order for the gateway to obtain a set of addresses and a default route (that includes NDP interactions). In detail, the initial RS (Router Solicitation)/RA (Router Advertisement) offer the default route whereas the subsequent DHCP Solicit/Advertize/Request/Reply offer the set of addresses to the Gateway (to advertise for the eHealth devices).

Our proposal uses DHCPv6 messages only to provide the default route in addition to the set of addresses. The total number of messages of the earlier exchange is decreased from 10 to 8. The overall overhead due to control messages is reduced to optimize the bandwidth and the number of Round Trip Time (RTT) reduced. The practical gain depends on the quality of the link between the gateway and the infrastructure which cannot measured in our testbed conditions.

The draft [27] details the operations executed by involved parties in the protocol. In a Solicit/Request packet a client lists the wanted options in the Option Request Option (ORO), composed of a list of option codes. The DHCPv6 Server answers those packets with Advertise/Reply packets containing values for the options asked by the Client.

The relay receives the message from the client and forwards it to the server in a Relay-forward message. The server replies to the relay with an advertise/reply message encapsulated in a Relay-reply message. The content of this message is extracted by the relay and sent to the client.

In its DHCPv6 requests, the client sends a list of required options in the option request option (ORO). This option contains 3 mandatory fields: OPTION_ORO, option-len and requested-option-code, followed by new option fields.

The proposed option is named here OPTION_DEFAULT_ROUTER_LIST. It is possible to concatenate this value with several other existing requested-option-codes. The value of this code in this option is to be assigned. Obviously, this option needs to be understood by the server as well.

In the server side, the default router list option of DHCPv6 contains: OPTION_DEFAULT_ROUTER_LIST, option-len, router-address, router-lifetime, lla_len (link-layer address length) and optionally router_link_layer_address. As this option contains a list, the pattern containing router_address, router_lifetime, lla_len and optionally router_link_layer_address can be repeated.

5 Prototype implementation

This section describes technical aspects of the experimentation relating to testbed integration performed recently.[1] The high level goal is to demonstrate the capability of eHealth devices to communicate their specific data on the next-generation Internet from a vehicular setting. The underlying network communication protocols used were relying exclusively on IPv6. The application-layer protocols included, but were not limited to, HTTP and HTTPS.

5.1 Hardware specification

Figure 5 depicts the M2M Gateway used in the experimentations. The Kerlink Wirma Road is an energy-efficient ARM926EJ-S platform provided with a 2.6.27 Linux kernel. In embedded computing field, the ARM926EJ-S processor is one of

[1] Authors present early results from the ongoing FP7 EXALTED (EXpAnding LTE for Devices) project. More details here: http://www.ict-exalted.eu/project.

the most popular ARM processors, as it combines energy efficiency with enough CPU performance for most networking applications. The Brick (M2M GW) platform provides several communication capabilities. An integrated chipset provides only GSM/GPRS Cellular network service. An integrated WiFi module provides IEEE 802.11b/g connection. An integrated GPS module provides accurate geographic coordinates. GPRS, WiFi and GPS antennas are unified in one vehicle roof antenna as depicted in Figure 5. In the front panel, an Ethernet Hub and Serial connections (CAN, RS 232) are present. According to the manufacturer, 10% of the regional buses company in Paris (France) are equipped with this gateway. For testbed purposes, an additional NETGEAR Access Point (AP) is

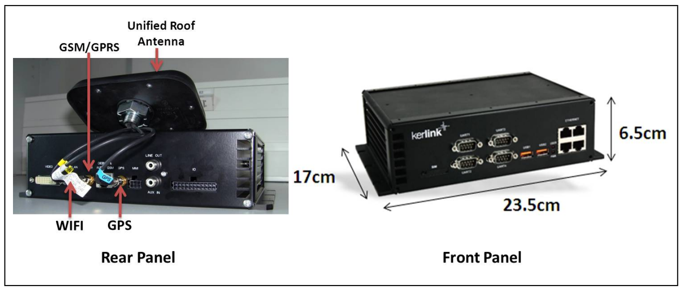

Fig. 5. Kerlink Wirma Road M2M Gateway. Factory settings propose M2M applications over IPv4-only networks. A kernel recompiling by cross-compilation has been performed to upgrade the capabilities of the platform in order to support next-generation protocols and include new drivers

plugged into the Brick with a USB-Ethernet converter. Its purpose is to ease mobile phones attachment to the network advertised by the AP protected by a WEP Key.

The eHealth devices (Figure 6) used for the testbed are manufactured by CardGuard[28] while the Android phone application is provided by Vidavo. The oxygen saturation level is measured by OxyPro, a wireless pulse oximeter. It provides for real time measurements and can be operated in continuous mode. It also provides for pulse monitoring. It displays oxygen saturation and pulse rate averages with the absolute maximum and minimum measurements.

The blood glucose and pressure measurement is performed by Easy2Check device. Blood glucose is measured with the use of an amperometric biosensor where fresh capillary blood is deposited. Its accuracy ranges from ±15mg/dL when glucose <75mg/dL to ±20% when glucose >75mg/dL. Accordingly for the pressure measurements the accuracy is ±3mmHg or ±2% of reading.

Self-check ECG offers 1 to 12 leads ECG events monitoring. It is intended for monitoring symptoms that may suggest abnormal heart function: skipped beats, palpitations, racing heart, irregular pulse, faintness, lightheadedness, or a history of arrhythmia. The recording period is set at 32 seconds while the bandwidth is 0.05 - 35 Hz for the 12 Leads and 0.4 - 35 Hz for the 1 Lead.

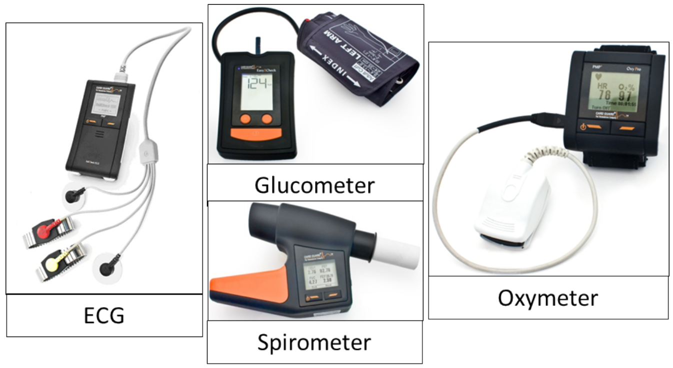

Fig. 6. Vidavo eHealth Devices. Different vital signs with different clinical value are observed. Captured data is sent over Bluetooth to the application.

Spiro Pro is a spirometer that records Volume (Time and Volume) Flow curves according to international performance standards. It measures lung ventilatory functions during Forced Vital Capacity (FVC) tests. The recording lasts for 17 seconds and its accuracy for the FVC and FEV 1 is +5% or +0.1L. It is mostly used for asthma or COPD monitoring.

A medical application is installed on an Android smart phone (IPv6-capable) which receives the vital signs from the portable monitoring devices via Bluetooth. The recorded data from the devices are transferred automatically (in the absence of the Mobile Router) through the smartphone via GPRS, Ethernet or WiFi to a designated web centre (over IPv4). The application provides a simple Electronic Health Record (EHR) for disease management and treatment and initiates patients' active involvement in healthcare. Analytically, it features browsing on the exams history, viewing of the recorded data, downloading of a diagnosis or advice from a doctor, comments addition and more. The final destination of these data is the EHR of the patient who uses the devices and it is resident in a dedicated server from where it is accessible for reviewing under secure credentials by the treating physicians.

5.2 Detailed integration process

Although the experimentation was performed in a laboratory setting, the hardware equipment is deployable in a vehicle as is: Kerlink's Wirma Road (IPv6 Gateway) is a low-consumption PC platform dedicated to vehicles, whereas eHealth devices are used by professionals for health periodic check-up and continuous monitoring. The kernel support of IPv6 and its associated extensions has been implemented in the gateway during the initial phase of the testbed integration. The overall architecture is summarized in Figure 7. In the joint testbed, the Brick runs Router ADVertisement Daemon (radvd), version 1.8.5 compiled for ARM platforms and available for Debian distributions[29]. The radvd is configured to advertise at regular intervals or immediately on solicitations, two different prefixes for two different interfaces. On the Air Interface (AP), which is bridged to the Brick, the 2001:DB8:B:2::/64 prefix is advertised for the devices which connect to the advertised essid. This is the Ingress Interface of the Brick. On the Ethernet side, the 2001:DB8:A:1::/64 prefix is announced for the connected devices. This is the Egress Interface of the Brick. The server is connected on this side of the Brick, and the traffic is routed through the gateway from one end to the other. These devices form the basis of what will be deployed in a vehicle such as an ambulance.

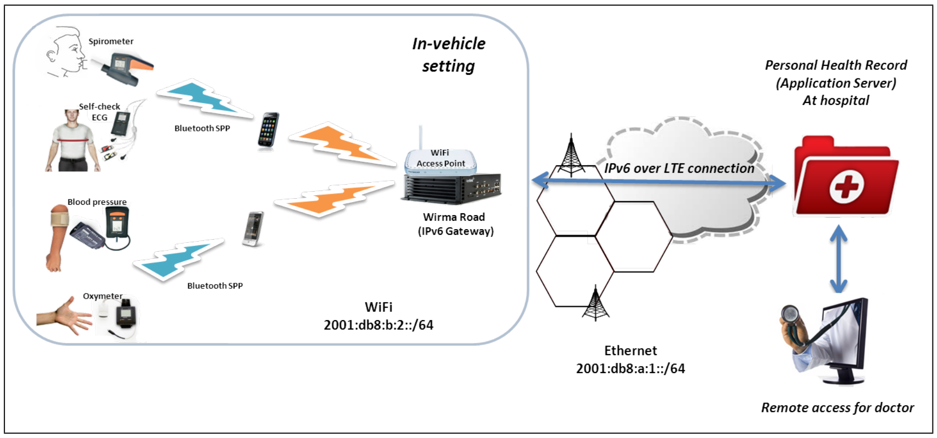

Fig. 7. eHalth and Vehicular testbeds integration. Future work includes replacing server-mobile router Ethernet link by LTE radio link.

As illustrated in Figure 7, on the vehicle side (ingress interface) two phone brands are used. (1) Samsung Galaxy 3 which runs Android 2.2 system. This phone is peered with the ECG and Spirometer devices over Bluetooth. (2) HTC Hero which runs Android 2.3 system. This phone is peered with the Glucometer and the oximeter over Bluetooth as well. Both phones are attached to the AP and configure IPv6 addresses on the 2001:DB8:B:2::/64 prefix. The devices are then used with the Vidavo Android Application that collects the data before sending it to the server over HTTPS along with a user comment (optional).

The server, which is located in the Internet side (Egress interface), configures an IPv6 address on the 2001:DB8:A:1::/64 prefix. The server is then ready to receive the data. The server application runs over Java (tomcat webserver) and includes a MySQL database, where the collected data is stored and organized per user ID. The physician can then issue a remote access to the server in order to observe the data as depicted in Figure 8. In order to observe these measurements (path from the viewer to the server), IPv4 and IPv6 access to the application server are possible.

Fig. 8. Web Interface for remote viewer. The health care specialist will have access to the collected information along with patient comments.

6 Related work

Generally speaking, eHealth protocol messages carry sensitive data and require integrity, confidentiality and availability. Privacy is also one major security concerns. Pseudonymization of medical data is the typical solution that addresses this issue [19]. The proposed platform relies on an encrypted channel of communication originating from the application towards the server. Access to the information database (EHR) is reserved to the parties owning the right credentials.

The WEHealth platform [20] covers the topic of embedding eHealth sytems in vehicular network. Basically, WEHealth provides eHealth service for medical needs on roads and enhances security and privacy by the use of the NOTICE framework (a secure and privacy-aware architecture for the notification of traffic incidents). The infrastructure of this proposal includes short-range communication capable sensorbelts deployed along the road. The infrastructure in NOTICE uses embedded sensor belts on the road put at regular intervals (e.g., every mile or so). Each belt is composed of a collection of pressure sensors and a few small transceivers. The pressure sensors in each belt allow every message to be associated with a physical vehicle passing over the belt, eliminating the need to uniquely identify vehicles in order to interact with them. The sensor belts do not communicate with each other directly and rely on passing cars to carry and forward a message between adjacent belts. Check station belts (authentication centres) and pseudonyming proxies complete the overall architecture design. These elements deployed on the roadside and attached to Base Stations have access the PHR (Personal Health Record) server in the Internet. Medical queries or accident alarms can be disseminated through the system to provide health records of the patients. In addition to wireless communications with external sensor nodes on the road, WEHealth platform assumes an underlying IPv4 Internet and the server side (PHR server) is accessible through Base transceivers. The platform presented in this paper does not rely on external interactions with sensors to carry the health-related data to the server, and is proposed for the next-generation networks.

eCall [21] is a recent European standard that brings the possibility of dialling the EU emergency number (112) in case of a serious road accident automatically without vehicle occupants' intervention. The European Commission adopted measures to ensure eCall will be available in new car models from 2015. Due to typical eSafety applications stringent delay requirements, eCall is to operate only on radio networks (24GHz) on a reserved channel. The platform described in this paper involves non-time-critical eHealth applications and does not belong to eSafety category, therefore recorded data can be transported over IP (best-effort) as the rest of user data.

Monitoring and dealing with a large number of casualties is an important key parameter to disaster response scenarios. The CodeBlue platform [22] provides a protocol and a software framework integrating eHealth devices such as wearable vital sign sensors, handheld computers, and location-tracking tags to handle disaster response and emergency care scenarios. The prototype proposes to integrate device discovery, robust routing, traffic prioritization, security, and RF-based location tracking. In a disaster scenario, handheld computers carried by first responders receive and visualize multiple patients vital signs on the implemented application. Based on these observations, triage operation can help optimizing the chances of survival. Along with these objectives, security and privacy are studied according to legal ramifications specific to the USA regulations. The platform presented in this paper does not focus on a disaster scenario and considers a more general use case. In addition, Internet next-generation communication standards are used (IPv6).

7 Conclusion and future work

The infrastructure of the Internet is continuously evolving to support new services. Intelligent Transportation Systems activities integrate the vision of future networks. The deployed applications should help to preserve lives and make transportation safer and efficient. EHealth, if supported by vehicular networks could be one of the applications improving vehicle passengers safety.

This paper describes the integration process of vehicular and eHealth testbeds. The vehicular network is designed to work over a fully deployed IPv6 network. EHealth testbed collects, stores and sends health-related measurements to a PHR Server located in the infrastructure where the results can be viewed by a doctor. Performed experimentation demonstrates the capability of eHealth specific data to be sent on the next-generation Internet from a vehicular setting. The underlying network communication protocols used were relying exclusively on IPv6. The application-layer protocols included, but were not limited to, HTTP and HTTPS. The hardware used in this configuration is deployable, as it is, in a vehicle.

Next steps ahead include quality and performance measurements. Actual in-vehicle integration and demonstration of cellular capabilities of the Brick are next. In the near future, a method for IPv6 Vehicle-to-Vehicle-to-Infrastructure (V2V2I) communications based on DHCPv6 and Neighbour Discovery extensions, as detailed in the Auto-configuration Protocol section will be described along with a set of experiment results.

Acknowledgement

This work has been performed in the framework of the ICT project ICT-258512 EXALTED, which is partly funded by the European Union. Authors would like to thank involved partners for the technical support. A special thank to Vidavo team for their participation and for hosting initial testbed integration. The authors would also like to thank, M. Mouton (internship 2011) for his implementation of the default router list with DHCPv6, A. Kaiser and S. Descremps, for their valuable support.

References

1. H. Hartenstein and K.P. Laberteaux. *VANET: Vehicular Applications and Inter-Networking Technologies*, chapter 1, "Introduction". pp. 1-19. John Wiley & sons, 2010.
2. Kai-Lik Foh. *Integrating Healthcare: The Role and Value of Mobile Operators in eHealth*, GSM Association mHealth Programme, Online 03/10/2012 at: http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2012/05/Role-and-Value-of-MNOs-in-eHealth1.pdf.
3. Ahmed Abdel-Rahim. *Intelligent Transportation Systems*, chapter 6, "Deploying Wireless Sensor Devices in Intelligent Transportation System Applications". pp. 143-168. InTech Design Team, 2012.
4. James Roberts. *The clean-slate approach to future Internet design: a survey of research initiatives.* Annals of Telecommunications (Annales Des Télécommunications), Springer, 64(5-6):271–276, 2009.
5. ETSI Intelligent Transport Systems (ITS), Online on 07 May 2012 at: http://etsi.org/WebSite/Technologies/IntelligentTransportSystems.aspx.
6. D. Evans. *The Internet of Things, The Next Evolution Of The Internet*, Cisco IBSG (Internet Business Solutions Group), Online on 03 October 2012 at: http://www.slideshare.net/CiscoIBSG/internet-of-things-8470978.
7. B. Raunio. *The Internet of things.* A report from the November 5, 2009 seminar, .SE:s Internet guide, nr. 16, English edition, Sweden 2009.
8. L. Heuser, Z. Nochta, and N-C. Trunk. *ICT Shaping The World: A Scientific View*, chapter 5, "Towards The Internet of Things". John Wiley & sons, 2008.
9. The IANA IPv4 Address Free Pool is Now Depleted, American Registry for Internet Numbers (ARIN), Online on 03 October 2012 at: https://www.arin.net/announcements/2011/20110203.html.

10. World IPv6 Launch, The Internet Society, Online on 03 October 2012 at: http://www.worldipv6launch.org/.
11. D. H. Gustafson and J. C. Wyatt. *Evaluation of ehealth systems and services.* British Medical Journal, 328:1150–1150, 2004.
12. C. Pagliari, D. Sloan, P. Gregor, F. Sullivan, D. Detmer, J.P. Kahan, W. Oortwijn, and S. MacGillivray. *What is eHealth (4): a scoping exercise to map the field.* J Med Internet Res, 7(1):e9, 2005.
13. Y. Toor, P. Muhlethaler, and A. Laouiti. *Vehicle Ad Hoc networks: applications and related technical issues.* Communications Surveys & Tutorials, IEEE, 10(3):74–88, 2008.
14. D.D. Stancil, F. Bai and L. Cheng. *Vehicular Networking, Automotive applications and beyond*, chapter 3, "Communication systems for Car-2-X Networks", pp 45–81, Wiley, 2010.
15. Geographic addressing and routing for vehicular communications (GeoNet), FP7 ICT, Online on 03 October 2012 at: http://www.geonet-project.eu/?page_id=9
16. 3GPP Long Term Evolution, Online on 03 October at: http://ipv6.com/articles/wireless/3GPP-Long-Term-Evolution.htm
17. K. Gosse et al. *Vehicular Networking, Automotive applications and beyond*, chapter 8, "Standardization of vehicle-to-Infrastructure Communication", pp 171–201, Wiley, 2010.
18. Geoff Mulligan. *The 6LoWPAN architecture*, In Proceeding of EmNets '07, Cork, Ireland, 2007.
19. D. Slamanig and C. Stingl. *Privacy aspects of ehealth.* Third International Conference on Availability, Reliability and Security (ARES), 0:1226–1233, 2008.
20. Gongjun Yan, Ye Wang, Michele C. Weigle, Stephan Olariu, and Khaled Ibrahim. *WEHealth: A Secure and Privacy Preserving eHealth Using NOTICE.* In Proceedings of the International Conference on Wireless Access in Vehicular Environments (WAVE), Dearborn, MI, dec 2008.
21. eSafety : eCall | emergency call for car accident | Europa-Information Society, Online on 03 October 2012 at: http://ec.europa.eu/information_society/activities/esafety/ecall/index_en.htm
22. K. Lorincz, D.J. Malan, T.R.F. Fulford-Jones, A. Nawoj, A. Clavel, V. Shnayder, G. Mainland, M. Welsh, and S. Moulton. *Sensor networks for emergency response: challenges and opportunities.* Pervasive Computing, IEEE, 3(4):16 – 23, oct.-dec. 2004.
23. O.Troan and R. Droms. *IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6.* IETF, 2003.
24. L. Yeh, T.Tsou, M. Boucadair, J. Schoenwaelder and J. Hu. *Prefix Pool Option for DHCPv6 Relay Agents on Provider Edge Routers.* IETF (Internet Draft), draft-yeh-dhc-dhcpv6-prefix-pool-opt-05, 2011.
25. R. Droms, P. Thubert, F. Dupont, W. Haddad and C. Bernardos. *Request for Comments: 6276, DHCPv6 Prefix Delegation for Network Mobility (NEMO).* IETF, 2011.
26. A. Lindem and J. Arkko. *OSPFv3 Auto-Configuration.* IETF (Internet Draft), draft-acee-ospf-ospv3-autoconfig-00, 2011
27. A. Petrescu, C. Janneteau and M. Mouton. *Default Router List Option for DHCPv6 (DRLO).* IETF (Internet-Draft), draft-mouton-mif-dhcpv6-drlo-01, 2012.
28. Card Guard Products & Technologies, Online on 03 October 2012 at: http://www.cardguard.com/cardguard
29. Linux IPv6 Router Advertisement Daemon (radvd), Online on 03 October 2012 at: http://www.litech.org/radvd/