End to end secure communication in ad-hoc assistive medical environments using secure paths

D. Vassis[1] P.Belsis[1] C.Skourlas[2] S. Gritzalis[1]
divas@aegean.gr pbelsis@aegean.gr cskourlas@teiath.gr sgritz@aegean.gr

[1]Department of Communications and Information Systems Engineering
University of the Aegean
Karlovassi GR-83200 Samos, Greece
[2]Department of Informatics
Technological Education Institute of Athens
Ag.Spyridonos GR-12210 Aigaleo, Greece

ABSTRACT

Recent advances in technology introduce many new capabilities for several sectors. Among else, the continuous improvement and integration of new features in mobile devices, allow their interoperation and integration to a large number of environments; primarily the medical sector may suffice from their utilization in order to monitor efficiently the condition of patients and provide feedback to specialists, especially in cases of absence of a stable (wired) network infrastructure. Strict security requirements emerge due to the sensitivity of data being transmitted, often imposed by different international legislation processes. We present an architecture that allows secure dissemination of medical information in a secure manner in the absence of stable topologies and infrastructures built upon resource efficient devices. The presented architecture utilizes advanced management techniques, achieving secure and privacy-preserving transmission of sensitive data. A number of initial measurements show the effective operation of our architecture in presence of an adequately large number of users participating in the performance test-bed scenario.

Categories and Subject Descriptors

H.3. [**Information Storage and Retrieval**]: Systems and Software. H.4. [**Information Systems Applications:** Communications Applications. .

Keywords

Medical Information Systems, security and privacy, Information Retrieval, wireless environments.

1. INTRODUCTION

As mobile devices become continuously more efficient, new paradigms in information sharing gain continuous acceptance daily. Among else, mobile ad hoc networks, pervasive and ubiquitous computing, introduce new possibilities and challenges for many sectors. Medical environments fall into this category, due to the demand for immediate access to information independently of location. Still the sensitivity of data being transferred impose a number of security related requirements.

PETRA'09, July 12-13, 2009, Corfu, Greece.

Conventional wireless networks require the presence of a fixed infrastructure and centralized management for their operation. In contrast, ad hoc and pervasive environments lack these capabilities. Therefore there is a need for advanced dynamic management that allows node identification and discovery of secure paths over which information may flow in a secure manner.

In many occasions, setting up a wireless environment with fixed access points is not feasible. Such a case may emerge in an emergency situation or in general in places and times that cost or other limitations make a stable infrastructure infeasible. In such a case we can still achieve the benefits of an e-health supportive environment by deploying an ad hoc network or by using wearable devices and through an advanced dynamic management platform to handle the network management and security challenges.

The remainder of the paper is organized as follows: Section 2 presents related work in context. Section 3 outlines the proposed remote medical services provided to patients, while Section 4 presents the modular components of our architecture. Section 5 discusses implementation and performance evaluation details; finally, Section 6 concludes the paper.

2. RELATED WORK

Pervasive and ad hoc networks bring new possibilities in the health sector. Remote patient monitoring attracts lately a lot of research and industrial interest [7][9][10]. A lot of internationally funded projects focus on the several aspects of security over these wireless environments which also are characterized by the presence of handheld, low resource devices. Legislation also in US and EU countries imposes strict restrictions concerning the management of data and the security measures taken to protect patient's privacy [3].

Different wireless technologies and different types of communication interfaces have been utilized in medical environments. Among else, Bluetooth, cellular phones (GSM) [8], handheld devices using the wireless application protocol (WAP) [6], wireless local area networks (WLAN) [5], are only a few examples of different technologies in different use case scenarios. Other studies describe an integration of wearable technologies to monitor different medical parameters of patients, as well as wired and wireless infrastructures to transmit and collect the patient related information [12].

In [14] several vital parameters are recorded using wearable devices for patients with chronic cardiac and respiratory illnesses. Medical data are collected on specific time intervals and are sent to medical databases for further utilization by authorized personnel using GPRS technologies.

In the MobiCare project [15] the patient's condition is monitored both in house as well as in open areas using GPRS.

In [13] a campus wide Mobile Information Management System is described that allows incident reporting and retrieval of medical information in a university campus, using a wireless LAN that spans the campus area.

Another prototype that focuses on vital parameters of patients using wearable devices is described in [17]. The project covers the area of a city. Several access points have been set up in a wide area, which collect and transmit the data so as to monitor the patient's condition continuously. Initial testing and an evaluation questionnaire have showed an adequate acceptance from the participating users. Medical information is sent by patients through several service points where the user may log on and manage transmission of data. Doctors also have to subscribe to a network service to view the data.

In [4] the authors describe a prototype that uses wearable devices to record several body parameters such as glucose for patients with diabetes. The transmission is made using mobile phones and the Zigbee protocol. The users have to log on to a web service while being at home using a simple access service and can easily send the various recorded physiological parameters to a medical database updating thus continuously his/her personal health file. Beyond collecting uploaded public health data from public gateways and home gateways, the medical gateway also provided a portal site allowing users to both access their personal file as well as to communicate with their family doctors.

Our approach focuses on providing a remote monitoring medical architecture, that records -using wearable devices- several physical parameters and transmits them through wireless unstable topologies, identifying first a secure path. We describe a mechanism that allows the identification of trusted nodes and then describe an architecture that enables medical personnel to access wirelessly and in a secure manner these data.

3. PROVIDED SERVICES

Our architecture focuses on providing a number of distinct medical treatment services to patients. The following section focuses on the description of the provided services.

3.1 Monitoring medical parameters

Monitoring of medical parameters is achieved through sensor devices attached to the patient's body. Each sensor is responsible for collecting one or more values from vital parameters regarding the patient's health. The most important of them are temperature, blood pressure, heart-beats and blood-oxygen ratio. Moreover, sensors should monitor other area-specific parameters such as temperature and humidity values. All these values are recorded by sensors in specific time intervals (e.g. every 1 minute) and transmitted to the medical center. There a special database is responsible to receive and store this information applying specific encryption standards in compliance with HIPAA (US medical health informatics information security standard) or the relevant ISO/TC 215, or CEN/TC251 standards form the ISO organization or the EU legislative framework respectively. Detailed information about the transmission of sensor information to the hospital is described in the next section.

3.2 Alarm triggering

When one of the monitored values goes above or below a threshold, the hospital's service is responsible of triggering an alarm. When an alarm is triggered, the associated doctor or nurse should be informed and proceed to the appropriate action.

Actions that can be taken when an alarm is triggered are for example to call the patient on his/her mobile or to send help at the patient's location.

3.3 Help on demand

The patient should have the ability to request for help by pressing specific keys of his/her hand held device. In this case, a message is automatically generated and sent to the hospital's server. The server is responsible for generating an alarm that will be forwarded to the appropriate doctor. The doctor will then proceed to the appropriate action. Several different levels of request may exist, depending on the features of his/her hand held device; e.g. by pressing key '**#' of the mobile phone / PDA means that he/she wants to contact with a nurse on the hospital in order to ask something. By pressing key '#**' means that he/she wants immediate help because he/she is not feeling very well.

3.4 Location-based monitoring

Many wireless devices nowadays are equipped with a GPS. This enables the support of location-based monitoring of a patient, which is very helpful for patients suffering from Alzheimer. If such a patient is lost, his/her family can contact with the hospital and find out his/her exact position. Moreover, patient's relatives can request from the hospital service to register a specific cellular phone number so location information about the patient could be automatically sent to this mobile through SMS, whenever requested, enabling thus easily tracing of the patient when necessary.

From another point of view, the patient can request information about the nearest place of medical assistance by pressing a key combination in his/her hand held device. The hospital's service is responsible to detect its location and send him/her information (e.g. hospital name or doctor's office) about medical assistance existed near the device's location.

3.5 Security

The unstable nature of a wireless infrastructure built over mobile nodes comprising of devices with low resources, demands innovative management techniques from a security perspective. In dynamic network formations such as those built over wireless

environments the absence of a certification authority that would enable key verification should be taken for granted.

In a given scenario supporting a similar infrastructure, such as the one described which enables the provision of health services within a given area (hospital, WLAN), the number of users will be upper limited (not extremely big). Thus, two main actions are of prime importance in order to allow interaction with the network for a user: first, we need to consider mainly the validity of a user's key and to verify that it has not been misused (stolen); second, we need to verify the level of trust associated with a specific user (key bound to a user), assigned to a user the moment a certificate is provided to him/her (by an already acknowledged user). For authentication purposes and considering the capabilities of modern devices, we accept that an adequate number of public keys can be stored within the device's memory. Thus, the authenticity of a given message as well as its sender could be verified for a limited number of senders. This means that a given device can identify a number of trusted nodes on the network; this technique may be used also to expand the list of trusted users in a network if a number of trusted nodes assign to them a high level of trust. Then, the list of known users can be expanded and the new public key can be inserted in the list of known keys. If on the contrary a node becomes compromised due to a stolen device, the validity of the key could be revoked if two other nodes sign and send an appropriate message to all the other nodes on the network. Therefore using electronic signatures a flexible framework can be provided that allows dynamic determination of trusted paths, over which secure transmission may be established. We need to address at this point that end to end communication between two nodes using asymmetric cryptography is feasible; current devices ensure that 128-bit key length is not a burden. Modern devices handle effectively at least 128-bit encryption. Still since such a strong encryption algorithm would demand excessive resources, it is used only to authenticate the two terminal nodes and in order the two nodes to exchange a shared key which will be further used to encrypt all communications. We also need to ensure that the path over which the information will flow will be trusted on grounds of two parameters: trust over given nodes, and node reliability.

Using the PGP web of trust algorithm [18] [16] we can identify for a given community a number of trusted users. Thus, each time we can identify all the valid keys starting from a node which is considered as source. By knowing the number of valid keys and the level of trust assigned to each of them we can identify trusted paths in order to allow secure information flow.

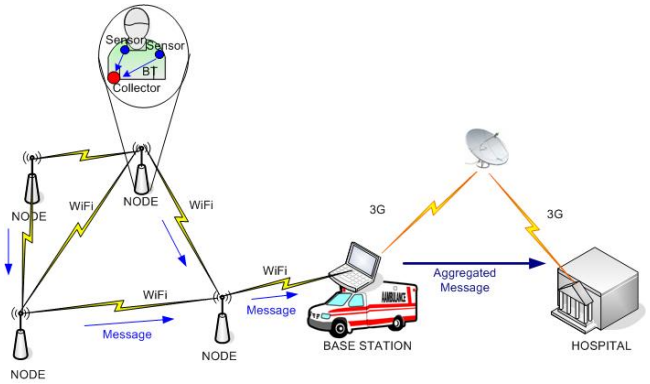

Fig. 1 : Hospital to patient interaction

4. THE PROPOSED ARCHITECTURE

This section describes the proposed architecture that supports the provision of the aforementioned services. We can consider the total architecture as a composition of two distinguished modules: A module that handles the interaction between the patient's equipment and the medical center's database, and a module that is responsible to manage the interaction between the database and the doctors' devices.

4.1 Hospital to patient interaction

Concerning the architecture on the patients' location, we consider a wireless ad hoc network interconnecting all the patients. Part of the ad hoc network is also a central node collecting all the information from patients and sending it to the hospital's database.

The whole architecture (depicted in Figure 1) combines three widely used wireless protocols; Bluetooth, WiFi and UMTS (3G). We use Bluetooth in order for the sensors attached to the patient's body to send data to a unit carried by the patient, a unit equipped with Bluetooth and WiFi interface. We call this unit a "collector", which can be a mobile phone, a PDA or another device with special characteristics. All collectors set up a WiFi ad hoc network, exchanging information with each other. Each collector sends the collected information from its sensors to the centralized node, called "Base Station". The Base Station is equipped with a WiFi and a 3G interface, and can be a laptop, a PDA or a 3G mobile phone. The Base Station communicates through 3G with the hospital's database in order to send the aggregate information concerning the patients' condition.

With the architecture described above, considering a network of 10 nodes and a WiFi range of 100m, we can cover an area of $0.5Km^2$, which about the same as the area covered by 100 football fields.

However, due to mobility, coverage and interference issues, the performance of an ad hoc network is much worse than this of a wireless network with fixed access points (less than 30%), so efficient routing protocols and message exchanging algorithms must be used, in order reliable information delivery to be achieved between the nodes and the Base Station. For this purpose, and more precisely, for eliminating the number of messages exchanged between the Base Station and the nodes, we define a broadcast-based policy for information delivery from the nodes to the Base Station.

The delivery of information is enabled from the Base Station. In ordinary time instances (e.g. 1minute or 5 minutes, depending on the network load) the Base Station sends a message to the nodes in order for the latter to send sensor information. Instead of sending a separate message to the collector of each node, it sends one broadcast message to all nodes. For this purpose, we use the DSR ad hoc routing protocol with multicast extension, as defined in [1]. When the collector of a node receives such a message, (which, as defined in [1], is sent through a routing update message), it also updates its routing table. Moreover, each node knows which nodes use this as a relay node for delivering information to the Base Station. Hence, when it receives the information message from other nodes, instead of relaying it to

the next node, it adds its information to the message and relays it. On the other hand, if a node is used as a relay node between other nodes and the Base Station, it will not send its information before it receives the information from the other nodes. The whole procedure can be depicted in Figure 2, where the black lines show the existence of WiFi link between collectors and the blue arrows depict the optimal paths from each node to the Base Station.

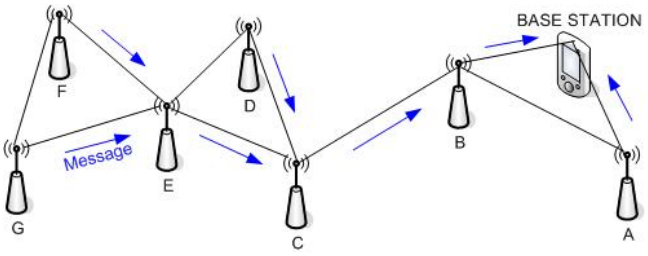

Figure 2: The proposed architecture

After the broadcast message is sent from the base station, each collector collects the necessary information from its sensors. Nodes F and G send the information messages to Node E, in order to be relayed to the Base Station. Node E will not send its message to Node C, before it receives the messages of Node F and G. When the messages are received, the collector of node E constructs an aggregated message (consisted of the information of its sensors and the information received from the collectors of Node F and G) and relays it to Node C. Similarly, Node C receives the messages of Node D and E, constructs an aggregated message (adding its information as well) and relays it to Node B. Finally, Node B relays the aggregated message to the Base Station, which contains the information of nodes C, D, E, F and G. Of course, Node A will sent its own message to the Base Station directly, as a direct route exists to the latter.

Using the policy described above, the following advantages are achieved:

- The information request messages sent from the Base Station to the nodes are eliminated to one broadcast message.
- The information messages sent from the nodes to the Base Station are eliminated to one aggregated message, thus eliminating the probability for a message to get lost or eavesdropped.
- The information request procedure is performed simultaneously with the routing update procedure, thus eliminating the network overhead.

4.1.1 Securing the ad hoc network

Wireless communications suffer from eavesdropping, so secure communication must be ensured between the entities of the ad hoc network described above. Concerning Bluetooth communication, the wireless range is less than 10m, so eavesdropping is difficult to occur. Concerning the communication between the Base Station and the hospital's gateway, UMTS supports a strong level of encryption, where decryption of eavesdropped packets is almost unachievable. The problem arises in the case of WiFi communication in ad hoc-connected collectors. If the network topology was stable, there would be no problem, as the wireless links would be secured through the WPA protocol that has a strong level of encryption. However, in our case, the network topology can change; wireless links can be broken while others can be created. The problem that arises is that, when a wireless link is created between two nodes, these nodes cannot know that they are trusted to each other and, secondly, if they know, they cannot setup an encryption through key exchange in a secure manner.

Our proposed solution to the above two problems uses a combination of IEEE 802.1x, WPA and asymmetric crypotgraphy protocols. IEEE 802.1x provides port based authentication in a WiFi network, thus preventing sensitive data exchange between two nodes before they are authenticated. WPA is the most common encryption mechanism used today in WiFi networks in order to secure the wireless links. Asymmetric cryptography, also known as Public Key cryptography is a technique for providing strong authentication and encryption services between two nodes that have not previously interacted with each other.

We consider that each collector (including the Base Station) is equipped with a public key / private key pair. When two trusted nodes want to setup a wireless link with each other, they perform a public key / private key message exchange using 802.1x, in order to authenticate each other. The message contains encrypted a shared key which will be used to setup a WPA encryption which will be used for securing the wireless link. The whole procedure is cleared through the following example.

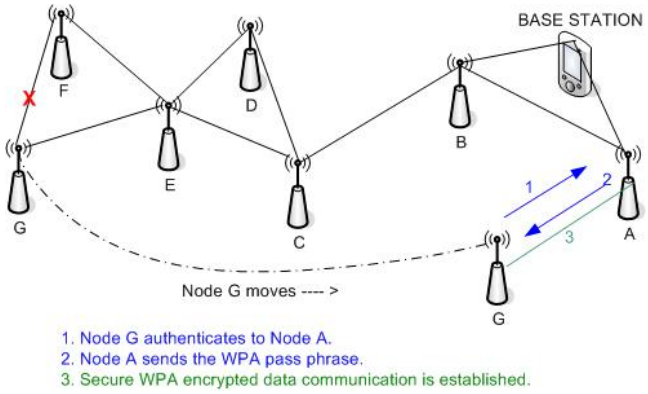

Figure 3: Link establishment procedure

In Figure 3, suppose that Node G moves near Node A. When node G detects a wireless link to Node A, the former sends an "authentication request" message to the latter, signed with Node G's private key and A's public key. This message will be recognized from Node A as an 802.1x/EAP message, meaning a message from a node asking for authentication. All other messages from node G will be rejected, as for the moment G is a non-trusted node to node A. Node A will then decrypt the message and check if G's public key is in the trusted list. If it is then it considers the identification of G as trusted successful and they can proceed to the establishment of a trusted path between them.

Now it is essential to verify that all the intermediate nodes (if any) also can be trusted. Therefore Node G needs to maintain a list of public keys with the intermediate nodes and examine which of these are valid. The queue for each node that contains a number of known trusted keys may be constantly updated using the PGP web of trust algorithm [18][16]. The exact details of this

technique as well as the principles of the PGP web of trust algorithm are out of the scope of this paper and for more details the reader may refer to [16][18].

Having identified a trusted path, the communication phase may begin between the two nodes.

Then Node A sends an "authentication success" message to Node A, encrypted with the public key. This message also contains the WPA shared key (pass phrase) that will be used to encrypt the wireless link. Note that only Node G (or similarly another trusted node of the ad hoc network that has been authenticated) can decrypt the message. When Node G decrypts the message using its private key, it sets up the WPA encryption mechanism using the pass phrase provided and a secure WPA connection with Node A is set up.

Using the mechanism described above, the following advantages are achieved:

- A non trusted collector (meaning a collector that does not belong to any of the trusted nodes) can not pretend to be a node of the medical wireless network.
- The WPA encryption pass phrase is created dynamically between two nodes, without the need of the existence of a higher layer trusted authority and is passed between two nodes in secure manner.
- No data link is established before two nodes are verified to be trusted to each other.

4.2 Medical center to doctor interaction

At the medical center's side, the recorded values from a patient's vital functions are encoded in a medical database that keeps all the medical history and personal details of the patient. The doctor while being in the broader area covered wirelessly around the medical center, may be notified through the WLAN that spans the area about the condition of a patient that needs specific attention; the doctor then queries the database using a PDA for more specific details related to the patient, to help him/her identify shortly the medical background of the patient that needs treatment. An agent based module installed at the doctors PDA is responsible to retrieve the patient's medical record and to perform all the necessary tasks related to access control enforcement.

The application on the doctor's device utilizes two agents; one for retrieving the medical record of the patient and one that acts as authorization delegate on behalf of the doctor, using the doctor's private key. More specifically, the doctor using a PIN code initiates the application on his/her PDA. Accordingly the Authorization Agent (Auth-Agent) that is responsible to perform all necessary authentication and access control tasks retrieves the doctor's private key from the smart card inserted in the PDA in order to initiate the authentication process with the system. All communications between the wireless devices and the system are encrypted in order to satisfy the privacy and security requirements imposed by European Union (EU) legislation.

The encryption scheme adopted is based on a combination of private key and shared key encryption; Private-key encryption has been used at the initiation of the communication between the system and the doctor's device. Thus the two parties exchange a shared key that will be used to encrypt all further messages. This choice was made, since the computational and power resources of a PDA are limited, resulting in big delays for encryption/decryption of messages and large resource consumption in case private key encryption was used to encrypt all messages. Still, It is essential to verify the shared key should is transmitted using a safe channel, which explains the use of private-key encryption to exchange the shared key. The shared key is sent from the medical database server to the doctor's PDA encrypted using the doctor's public key. Next, the shared key is being decrypted using the doctor's private key. Then the Search Agent (S-Agent) queries the database to identify medical information related to the patient. Accordingly the access control module is invoked which evaluates the doctor's credentials provided by the Auth-Agent; in case of a positive evaluation, it allows the Auth-Agent to transfer the patient's medical information at the doctor's PDA (fig. 4). For the software agents development we have used the JADE [19] software agent management software and more specifically the LEAP component (Lightweight Extensible Agent Platform) especially targeted for mobile devices with low resources.

4.3 Case study scenario

4.3.1 Patient to medical center interaction

We consider the following scenario: A patient using wearable devices that monitor specific vital parameters (ex. Heartbeats) is moving in an area covered by the ad hoc network. The data from these observations ought to be sent to a medical center. Such a medical center may be a hospital or a medical camp set-up in an area after an emergency situation. Patient monitoring data are sent through wireless links to a medical database. Most medical database systems lately tend to adopt the HL7 standard for encoding of medical information. For compliance with these demands we used the HL7Comm [19] application with J2ME installed on the mobile devices. J2ME as well as HL7COmm were chosen since they leave a small memory footprint on portable devices, such as the ones used to evaluate our prototype.

We consider at first that there exists a path which allows a message to be sent wirelessly to the Medical Center; then, we need to ensure that this path is trusted. We consider that several of the participating devices in the ad hoc network contain invalid keys or cannot be trusted. The existence of a secure path can be done by verifying that all the keys in the chain between the base and destination node are valid. This verification is achieved as explained in previous section. By calculating also the sum of the trust level of each intermediate key we can identify the maximum sum of trustworthiness and therefore we can choose the more trusted path between when there exist different paths to select form (Fig. 4). If a node is compromised and starts acting maliciously, its certificate can be revoked if at least two trusted nodes send a message (flood) to the rest nodes of the network (signed from both) that revokes the validity of the key associated with it.

After a secure path has been identified and a shared key has been exchanged between two terminal nodes, medical information may be securely transmitted end to end.

4.3.2 *Doctor to medical center interaction*

At the medical center, the doctor needs to be notified for serious updates to a patient's condition (ex. when certain physical parameters exceed certain thresholds). For this purpose there is a need for the doctor to be able to receive fast medical information. We consider that the doctor is most of the time within the range of an access point. The main challenges are to be able to provide efficient and secure access to the medical database in a transparent to the doctor manner. For this purpose we have used a software agent application the modules of which are being in brief described next.

When the doctor receives notification about a patient's condition he/she sends a request from his/her PDA to retrieve the data from the medical database. In order to authorize the request, the server needs to identify the doctor's identity as well as to evaluate the permissions which have been granted to the doctor. First it requests a validation of the doctor's id. This can be done by signing an appropriate message using the doctor's private key, stored in a smart card inserted in the PDA. Using the doctor's public key and the server's private key, the two parties may authenticate each other and they can exchange a (shared) session key which will be used to encrypt all further communications. The reasons for this selection are again related with the fact that public key encryption techniques for the transmission of all messages would demand a lot of valuable, still limited computational resources.

The doctor's device in addition –due to its importance among other resources in the network - is able to identify whether it resides within the medical center's wireless network (or whether it resides in an unknown environment) with the aid of a beacon which sends signed messages. These messages are identifiable by the doctor's device when compared to a (small) number of stored - within the smart card - signed messages. Thus, we prevent unauthorized transmission or reception from the device when it resides outside pre-settled space boundaries. After authentication has been performed and the session key has been exchanged, all communication can be encrypted end to end from the medical database to the doctor's device using SSL. When a new request is sent to the medical database, it is authorized or not depending on the authorization policies, the request and the requester's privileges.

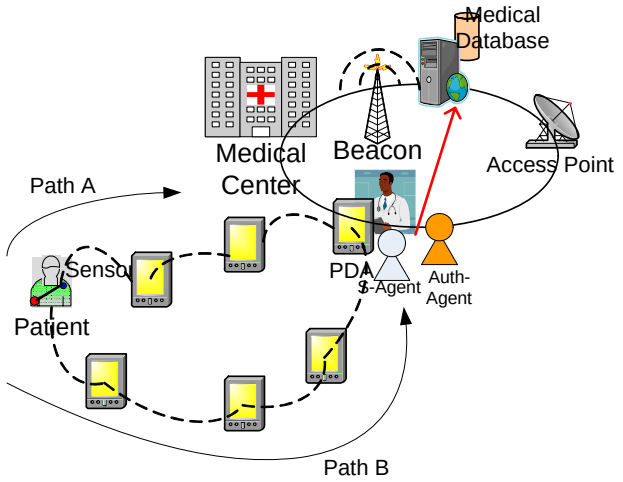

Figure 4: Patient to Medical Center (MC) and MC to doctor interaction

5. Performance Evaluation

We proceeded in an initial evaluation of the architecture proposed; this evaluation was performed in two distinct phases.

The first phase concerns the performance evaluation of the architecture related to the doctor-medical center interaction. For this purpose, a simple prototype was constructed as follows:

The HP IPAQ 111 model was used as the doctor's PDA, which has an integrated WLAN interface supporting WPA, and is based on the Windows Mobile 6 OS, allowing easy installation of the aforemnetioned applications. A regular desktop PC was used as the hospital's database with Ubuntu OS installed. The MySQL database server was used as the default database. The PC was equipped with a WiFi and a UMTS interface for communicating with the doctors' devices and the Base Station respectively. A custom made with small memory footprint Java application was created, that was able to send a message to the doctor's PDA when an alarm is triggered from the Base Station. As a Base Station, a Compaq nx 7400 laptop was used, equipped with 802.11G and UMTS interfaces, while a 1Mb/s 3G connection was leased from an ISP for communication between the Base Station and the hospital's database.

Concerning the hospital to patient interaction, excluding the Base Station, due to cost limitations, we were unable to build a prototype with hardware devices. Hence, we evaluated the performance of the architecture through simulation in the Pamvotis WLAN Simulator [2]. More precisely, the information of each sensor corresponds to data traffic of 4KBytes. We assume that each collector collects information from three sensors every one minute. Hence, each collector generates traffic of 12KBytes, every 1 minute. We extended Pamvotis in order to support WPA encryption, while we implemented the DSR routing protocol with multicast extension. Next, we simulated the topology depicted in Figure 2, and we measured the delay of 30 messages from Node G to the Base Station. We repeated the same experiment without our proposed broadcast and aggregation approach, where each node sends its own message to the Base Station. Figure 5 depicts the delay of the messages for both cases. Note that, in this metric, processing overhead due to reception of messages from sensors and due to construction and aggregation of IEEE 802.11 messages is not included.

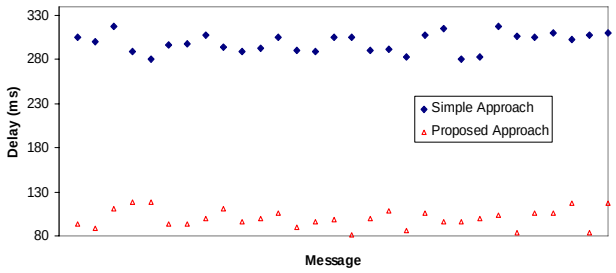

Figure 5: Information message delay

The mean value of the delay with the simple communication is 291ms, while the mean value of the delay using the proposed approach is 104ms, which about three times less.

Another experiment concerns the delay of the authentication procedure when a new WiFi link is created. For this purpose, we changed the topology during the simulation, in order new links to be created and we measured the time needed from the detection of the new link, until its secure establishment. Figure 6 depicts the delay for 20 new link creations.

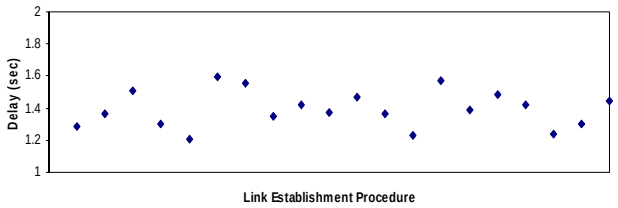

Figure 6: Link establishment delay

The mean value of the delay is 1.4sec, which is an acceptable value, considering that the topology does not change more frequently than 1min. Note that processing overhead concerning encryption / decryption is not included.

A final experiment concerns the whole architecture and, especially, the duration of an alarm, which is the time from the generation of the alarm until the receipt of the notification to the doctor's PDA. For this purpose, we first measured through simulation the duration of an alarm message from Node G to the Base Station. Next, using our prototype, we measured the duration of the alarm from the Base Station to the corresponding doctor's PDA. The total duration of the alarm message is approximately the sum of the two separate values we measured. Figure 7 depicts the duration of 30 alarms as measured by the procedure described above.

Figure 7: Alarm delay

The mean value of the delay is 4.2sec, which is acceptable, considering the various devices that are included from the generation of the alarm until the notification of the doctor.

6. Conclusions

In many occasions, setting up an assistive wireless infrastructure with fixed access points is not feasible. Such a case may arise in an emergency situation or in general in places where cost or other limitations make a fixed infrastructure temporarily infeasible. In such a case we can still achieve the benefits of an e-health supportive environment by deploying an ad hoc network; in addition, using wearable devices and through an advanced dynamic management platform we can achieve secure medical information management in compliance with the high security standards imposed by legislation.

In this paper, a secure network architecture is presented that enables the provision of patient monitoring services in areas where fixed wireless infrastructures are difficult to implement. Using sensor devices and wireless ad hoc nodes and combining wireless technologies, an end to end secure path between patients and medical centers is created. Using combination of encryption techniques secure transmission of information is achieved.

A prototype was implemented to ensure the validity of the proposed approach; part of the validation process was simulated in a WLAN simulator. An initial performance evaluation was also performed; the results so far seem encouraging. A number of parameters such as end to end delays have been measured. We plan to perform more thorough experimentation in the near future.

7. REFERENCES

[1] J. Jetcheva et. al., "A Simple Protocol for Multicast and Broadcast in Mobile Ad Hoc Networks", IETF MANET Working Group Internet Draft, Jul. 2001.

[2] "Pamvotis WLAN Simulator", Information available online at http://www.pamvotis.org

[3] Vassis D., Belsis P., Skourlas C., Pantziou G.: A pervasive architectural framework for providing remote medical treatment, proceedings of 1st International Conference on PErvasive Technologies Related to Assistive Environments, June 2008, Greece, ACM.

[4] H.J. Lee et al, Ubiquitous healthcare service using Zigbee and mobile phone for elderly patients Int J Med Inform. 2009 Mar, 78(3), pp. 193-198, Elsevier.

[5] K. Hung, Y.T. Zhang, Implementation of a WAP-based telemedicine system for patient monitoring, IEEE Trans. Inf. Technol. Biomed. 7 (2) (2003) pp. 101–107.

[6] Y.H. Lin, I.C. Jan, P.C. Ko, Y.Y. Chen, J.M. Wong, G.J. Jan, A wireless PDA-based physiological monitoring system for patient transport, IEEE Trans. Inf. Technol. Biomed. 8 (4) (2004) pp. 439–447.

[7] S. Fischer, T.E. Stewart, S. Mehta, R. Wax, S.E. Lapinsky,Handheld computing in medicine, J. Am. Med. Inf. Assoc. 10 (2003) pp. 139–149.

[8] R.G. Lee, C.C. Hsiao, C.C. Chen, M.H. Liu, A mobile-care system integrated with Bluetooth blood pressure and pulse monitor, and cellular phone, IEICE Trans. Inf. Syst. E89-D (5) (2006) pp. 1702–1711.

[9] http://www.pervasivehealthcare.dk/projects/index.html

[10] http://www.eecs.harvard.edu/~mdw/proj/codeblue

[11] Tentori, M., Favela, J and González, V, "Designing for Privacy in Ubiquitous Computing Environments," *Proceedings of UCAMI '05*, Granada, España.

[12] Sharmin, M., Ahmed, S., Khan, A. "Healthcare Aide: Towards a Virtual Assistant for Doctors Using Pervasive

Middleware”, Proc. of IEEE PerCom Workshops 2006, pp. 490-495.

[13] L’ Hereux, B., McHugh, M., Privett, B., Kinicki, R.E., Agu E., “A Campus-Wide Mobile EMS Information Management System”, Proc. of IEEE PerCom Workshops 2006, pp. 522-526.

[14] U. Anliker, J. A. Ward, P. Lukowitcz, et. al. AMON: A Wearable Multiparameter Medical Monitoring and Alert System. *IEEE Transactions on Information Technology in Biomedicine*, 8(4), pp. 415-427, 2004.

[15] R. Chakravorty. “Mobicare: A Programmable Service Architecture for Mobile Medical Care” Proc. of IEEE PerCom Workshop 2006, pp. 532-536.

[16] G. Theodorakopoulos and J. S. Baras, "On Trust Models and Trust Evaluation Metrics for Ad-Hoc Networks," *IEEE Journal on Selected Areas in Communications (JSAC)*, Feb. 2006

[17] C.-C. Lin, et al., A pervasive health monitoring service system based on ubiquitous network technology, Int. J. Med. Inform. (2009), Elsevier (in press).

[18] P. Zimmerman, The PGP user guide, MIT Press, 1994 Cambridge.

[19] JADE Software Agent Development Platform, http://jade.tilab.com/

[20] HL7COmm application website: http://nule.org