Wireless Pers Commun (2011) 57:431–439
DOI 10.1007/s11277-010-0078-5

Remote Patient Monitoring Within a Future 5G Infrastructure

Vladimir Oleshchuk · Rune Fensli

Published online: 15 July 2010
© Springer Science+Business Media, LLC. 2010

Abstract Systems of wearable or implantable medical devices (IMD), sensor systems for monitoring and transmitting physiological recorded signals, will in future health care services be used for purposes of remote monitoring. Today, there exist several constraints, probably preventing the adoption of such services in clinical routine work. Within a future 5G infrastructure, new possibilities will be available due to improved addressing solutions and extended security services in addition to higher bandwidth in the wireless communication link. Thus 5G solutions can represent a paradigm shift regarding remote patient's monitoring and tracking possibilities, with enhancement in transmitting information between patients and health care services. Some aspects of new possibilities are highlighted in describing a realistic scenario within a future 5G framework.

Keywords Wearable sensors · Implantable medical devices · Remote monitoring · Mobile communication · Security · Telemedicine

1 Introduction

Remote monitoring of patients using a wireless Body Area Network (BAN) has been described in several papers and research projects, since the first introduction of a Personal Area Network solution by Jovanov et al. in 2001 [12]. The idea is to monitor several vital signs parameters recorded by different sensors placed on the body surface, or even by implanted sensors; and that all signals are collected by a wearable receiver or wireless gateway to transmit the recordings to the doctor.

V. Oleshchuk (✉) · R. Fensli
Faculty of Engineering and Science, University of Agder, Grimstad, Norway
e-mail: vladimir.oleshchuk@uia.no

R. Fensli
e-mail: rune.fensli@uia.no

Despite of intensive research [2,3] efforts such solutions are not commonly used in routine medical investigations today, even if some promising products are launched to the marked, such as the Toumaz Sensium^{TM} technology and the V-patch system [15,16]. There might be several reasons for not adopting such solutions to be used in medical routine investigations. The technology is still not mature, and there exists several constraints limiting the clinical possibilities. Some new improved functionality might possibly be implemented within a future 5G infrastructure, which will open for higher communication bandwidth, improved addressing solutions and improved security.

In this paper, we will highlight some of today's limitations in the use of a BAN-solution in a mobile communication context, and try to sketch possible new approaches that may become feasible within context of 5G infrastructure. We present possible security and privacy preserving architecture for two-ways remote communication with patient's BAN containing both wearable sensors and IMD.

2 Motivation

We will use a typical scenario description to focus on limitations in existing systems, and based on this give a description of a future 5G solution. By comparing those two solutions, it is possible to evaluate future improvements and give recommendations on actual innovative actions to be followed up in future research efforts.

Current monitoring of patient is based mostly on one-way communication: data collected by sensors and are sent via gateway to a central server and made available to health care personal. As gateways the patient may use mobile devices like smart phones and communication between the gateway and a central server can be made secure by using conventional cryptographic methods. However current bandwidth limitations may put some limitations on amount of data that can be collected in real-time. In addition, the security and privacy are much more difficult to provide on the link between the gateway and sensors/IMD. This is because they communicate via wireless short-range links and devices have limited resources (both computational and energy). In this setting traditional cryptographic solutions cannot be fully utilized.

In the future, wearable sensors and IMD's will be used to support many lifesaving functions (pacemakers, implantable cardiac defibrillators (ICDs), drug delivery systems, neurostimulators, etc.), which require two-ways communication. In many cases health care personnel will need to access BAN devices in order to change setting that depends on selected medical treatment like adjusting insulin doses etc. It means such devices need to be addressable and the authentication/authorization issues need to be resolved. Currently [11] such access is implemented based on short-range communication. It simplifies authentication/authorization because to access these devices one needs to be located close to the patient within proximity of 1–3 dm. However, since authentication and authorization problems are not solved as it shown in [11], it is still possible to break into the system. A proper solution is difficult to achieve because of constraints on sensor/IMD side, but also because of needs to handle emergency cases in life-critical situations. Even without considering constraints of sensors/IMDs, currently existing authorization approaches are not developed to handle emergency situations.

In presence of a 5G infrastructure, the access to a BAN can be done remotely; however, it will create new security and privacy threats for patients. Therefore, a framework to deal with such remote authorization should be created. The problem is, however, in the limited capabilities of such devices.

Consider for example a Role Based Access Control (RBAC) system [7]. Roles describe permissions, and users will be given permissions to perform operations based on assigned roles. Handling emergency situations means that someone without having assigned a role with actual permissions should be able to perform some operations in specific cases (for example, life saving actions). The suggested solution requires emergency teams connected to Internet [10]. In this solution, it is suggested to send sensor/IMD's id or serial number to a trusted authority (manufacturer, prime-care hospital etc.) in order to receive needed credential for emergency authorization. However even if a 5G infrastructure is available, this could be too slow for emergency situations.

3 Remote Monitoring of Patients

When patients are monitored remotely by wearable sensors and communication equipments, the automatically recorded information is important for the doctors to make the correct diagnosis of the patient's actual condition, and it is an important part of the personalized health care concept [1,18]. In an overview and evaluation of different telecom solutions for remote cardiac patients, it is suggested that next-generation telecardiology network architecture should incorporate a signal processing module for local analysis of recorded physiological measurements, and only transmit detected events which are out of defined thresholds values. The systems should be able to use multiple wireless interfaces and include location-aware services [13]. It has been proposed to use a local signal processing solution, and transmission of periodic reports with detected alerts to a central server as an entry for the professional staff to monitor the recorded data [4].

3.1 Today's Limitations

Remote monitoring of patients will require high bandwidth and high quality of service in the mobile communication systems. Today, there are several obstacles which may prevent wide deployment of advanced monitoring solutions. Limitations in a standard GPRS system will normally prevent real-time transmission of medical waveforms from a recording system on a patient freely moving around during physical exercise like outdoor jogging; thus the clinical diagnostic procedures need to be carried out within a hospitals environment with the patient running on a treadmill. Wearable monitoring solutions within a hospital's buildings use old-fashioned radio systems (telemetry), with dedicated antenna systems and limitation on covered area.

New wearable recording solutions can be based on a BAN with a plurality of dedicated sensing/recording sensors planed on the patient. This can be non-invasive sensors (fastened to the patient's skin) or invasive sensors (implantable medical devices).

Wearable sensors to be used during physical exercise can be of importance when it comes to parameters that can be influenced by the patient's activities. For instance when monitoring ECG for arrhythmia detection purposes, it can be difficult to record rarely occurrences of arrhythmia episodes. We know that existing Holter recorders today represent unfortunate obstacles to the patients, thus perhaps preventing the patient from doing normal daily activities that can be the cause of arrhythmia events. If new sensors can be designed in a way where arrhythmias can be detected in all daily living situations even without the patient's notice, they could be useful for a quicker detection of arrhythmia events [5].

3.2 Possibilities in a Future 5G Infrastructure

Following up patients in a Tele-home-care situation gives possibilities for continuous monitoring of ECG, with an automatic arrhythmia detection alarm system, which can give alarms to the emergency department at a hospital.

In case of normal medical condition of the patient, a plurality of wireless sensors can be used for recordings of medical parameters as ECG recordings, Pulse waveform and Blood pressure waveform. Those recordings need to be recorded and properly transmitted to the PEHR [14] database and synchronization within a timeframe of only a few milliseconds. This will require time stamped recordings from each sensor and streaming functionality to view the on-line recorded information.

If abnormal conditions are encountered, there might be a need of instant collecting of more information from the different sensors, thus requiring dynamic bandwidth allocations. We can anticipate that high quality medical parameters will require a high sampling frequency and the need of transmission capacity can be a critical factor.

It is possible to develop data collection on-demand from a remote hospital having two-way communication to the actual sensors at the patient's body using pull mechanisms. In addition, push technology solutions can automatically give a direct warning to the doctor's mobile phone display if a wireless sensor detects abnormal situations [17].

Health care services are facing tremendous challenges in the rapid growth of elderly population. It is reasonable to believe that home-based hospitals will be a normally used solution for patents after a short hospital stay initializing treatment procedures [18]. Remote monitoring solutions need to be efficient and reliable; thus development of good and beneficial wireless sensors and systems should be accelerated, and they should be implemented into routinely clinical procedures.

New 5G network solutions can give possibilities of entirely new ways of patient monitoring, data analyzes and action control. As an example the prevalence of cardiac illness will in the future have a significant increase, and patient follow-up and medication treatment can be administered in new ways because of the new communication possibilities in a future 5G network. It will be possible to have a continuously transmission of recorded biomedical data to a cardiology specialist centre, which will have processing capacity for advanced pattern recognition and expert systems detecting critical situations and sophisticated detections of cardiac arrhythmias. The system can automatically steer the sensor on the patient by remote control to record different parameters and set up a faster transmission schema, in order to instantly follow-up the detected situation.

When needed, the system can push important information and instant waveforms to the doctor's mobile device for necessary actions. He will be able to have a near real-time view of the medical condition of the patient, and in addition he will be able to instantly set up a videoconference with the patient in order to gain necessary control of the situation. Of course he may know the position of the patient that may be displayed on a map when needed. The doctor will be able to share all this information with a rescuing team; thus new ways of advanced teamwork will be possible. Such applications can be of great importance in future health care services.

Another important application can be an advanced solution for individually tailored medication adjustment. Today, the medication is given in doses based on experience and maybe regular interval-based measurements as e.g. insulin doses for diabetic patients. In future, cardiac patients can achieve better control of arrhythmia episodes if implantable dose-reservoirs can be remotely controlled. The regulation system should be a closed loop from the actual recording sensors, with some rough estimates calculated within the Body Area Network

(BAN). However, for fine-tuning the system, the raw data should be continuously transmitted to a cardiology specialist with dedicated computation of the regulation parameters according to adaptive simulation models, and predictive calculations of optimal medication dose for the next minutes or hours. Necessary feedback can be given wirelessly to the actual medication doses adjustments in the implanted regulation system. Of course this will require a high degree of security and data integrity in the transmission loop.

Recently emerging concept of cloud computing will improve availability and reliability of health care services, and make them more convenient [19]. The availability of 5G infrastructure will play an important role in development of cloud computing since one of most useful cases for cloud computing is availability of high bandwidth Internet and constant and reliable connectivity.

4 Future Scenario Description

Generally speaking 5G will provide high-bandwidth for two ways communications between health care professionals and a central server and for patient to a Personal Trusted Gateway (PTG).

Let us consider possible scenarios that will show why we may need different approaches to authentication and authorization. We will propose an approach where the emergency authorization may be given based on a specific context. Access to such devices within a BAN can be done via gateways (in normal case). The gateway is a more powerful device that can handle both authentication and authorization mechanisms within a 5G context. All devices in the BAN will need to have established trust relations with the gateway at initialization phase.

There are three possible situations when access to devices of a BAN may require different approaches to authentication and authorization:

1. Emergency conditions;
2. Non-emergency access via Patient Trusted Gateway by explicitly authorized entity;
3. Non-emergency access via Patient Trusted Gateway by implicitly authorized entity based on predefined context (location, presence of specific devices/equipments, BAN identifiable patient condition, etc.);

It can for example take place when the BAN discovers that:

1. A patient needs emergency help (not breathing, no pulse, etc.). We assume that such kind of conditions can be discovered by the BAN sensors, and PTG will give permissions without explicit authentication.
2. In less severe situation (from BAN point of view) PTG can also decide to give authorization without explicit authentication, but under some contextual conditions (for example when a patient is located near some specific medical equipment, in emergency room, in hospital, in ambulance cars etc.)

We assume that in these cases there is no need for authorization since not getting or delayed authorization may result in patient death. However in the case of non-emergent need for access (for device test, auditing, routing setting adjustment, etc.) we would expect that contact with the BAN from outside will be done when a patient is in more or less in normal condition (no needs for emergency actions). In this case we assume that some adjustments will be done by authorized actors (health personal, device manufacturer, etc.). To increase security and privacy protection in this case, we would expect such procedures to be performed by someone that the patient might need to give his consent for the actual access. It

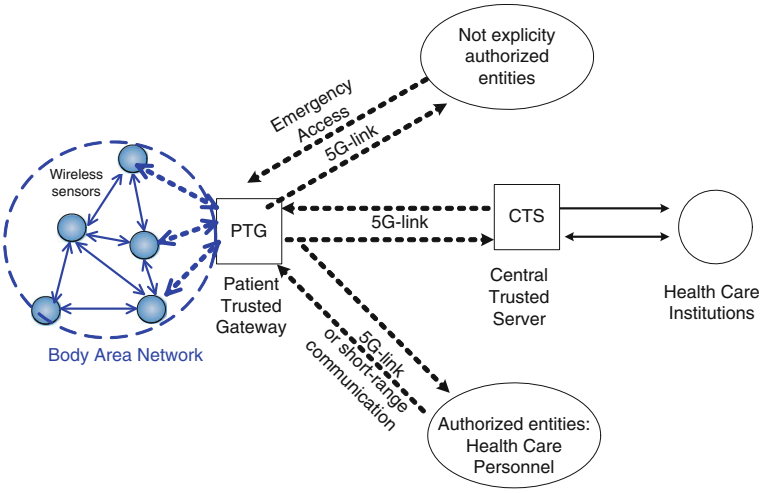

Fig. 1 System architecture for remote patient monitoring

may depend on what kind access and what kind of operations that need to be performed. It can be done remotely via Internet/wireless 5G. It means that the actor having a specific role will be assigned one-time credentials that can be sent together with operations directly to device. Verification of such credentials may be done fast, but generation can be more resource demanding.

5 Systems Architecture

In this section we describe briefly a system architecture that is aimed to address challenges described in previous sections. The general architecture is presented on the Fig. 1.

The proposed architecture consists of following elements: BAN that formed by patient sensors (both wearable and implanted); Patient trusted gateway (PTG) which is responsible for access control to BAN of external actors. It provides short-range communications with sensors in BAN and communications with external actors via wireless link. External actors can be both trusted entities like Central Trusted Server (CTS) or predefined healthcare personnel. CTS is a part that may be associated with patient's health care institution like hospital. PTG handles communication with actors (people and/or devices) that will be involved in emergency cases, and presented on the Fig. 1 as Non-explicitly authorized entities (NAEs). NAEs represent those actors who will need to communicate with BAN in emergency cases but cannot be explicitly authenticated and therefore authorized by PTG in non-emergency situation (like external emergency teams).

6 Emergency Aware Role-Based Access Control

In this section we propose a new solution to access control based on RBAC with extension to handle emergency situations. It is worth to mention that an approach to handle emergencies in medical context have been proposed recently [8,9]. The proposed approach is based on enforcement of "Breaking the glass" principle. However it may only partly solve

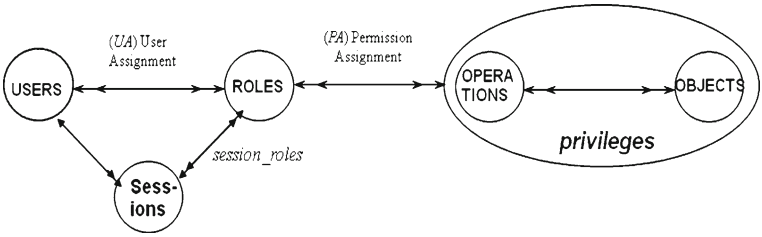

Fig. 2 The core RBAC model

the authorization problem considered in this paper. The main difference from our approach is that authors of earlier proposed approaches require that all users need to be registered in the system in advance since only authenticated users may be permitted to "break the glass". However, in the setting considered in this paper even unauthenticated user that may save the patient's life will be granted access. In this section we describe an approach that may help to handle such situations.

We assume that RBAC based access is performed at PTG device. In practice it means that when anyone wants to access BAN devices he will first be authenticated by PTG and then PTG will perform operations on behalf of this entity and with respect of permissions associated with roles assigned to the entity. However in emergency cases (we assume that such cases can be recognized as emergency and reported to PTG by BAN) the PTG should be able to permit actions on behalf of the entity without proper authentication.

The core RBAC model is presented on Fig. 2. For the sake of clarity in context of this paper we consider only core RBAC model (according RBAC reference model classification [11]). Our approach can be directly extended to more complex models that include hierarchies and separation of duty relations.

The core RBAC model [7] presented in Fig. 2 consists of five basic elements, which are *USERS, ROLES*, *Sessions*, *OPERATIONS* and *OBJECTS*. *USERS* is set of authorized users that can be authenticated by the system. *ROLES* is a set of roles that can be assigned to the users from *USERS*. Each role r from *ROLES* is defined by a set of privileges that defines what operations from *OPERATIONS* can be performed on what objects from *OBJECTS*.

In the context of this paper objects are members of BAN and operations are access to these members. Sessions are mapping between a user from *USERS* and an activated subset of roles from *ROLES* assigned to that user. There are also five relations defined within core RBAC model. User Assignment $UA \subseteq USER \times ROLES$ is a many-to-many relation between *USERS* and *ROLES*. Similarly, *privileges* are defined as relation between *OPERATIONS* and *OBJECTS*, that is $privileges \subseteq 2^{OPERATIONS \times OBJECTS}$. The permission assignment is a many-to-many relation *PA* between *ROLES* and *privileges*, $PA \subseteq ROLES \times privileges$.

However, in order to handle emergency cases, the core RBAC model should be extended. We propose to define a special emergency role r_e that will be activated each time BAN recognizes that the patient is in critical condition. We also define an emergency handler user *EH* that can be activated without any authentication with permissions needed give necessary heath care to the patient. These necessary permissions define the role r_e and the only role assigned to the *EH* user is the emergency role r_e.

Following the informal description above, we can expand existing core RBAC model to handle emergency situations as following: $USERS_E = USERS \cup \{EH\}$ and $ROLES_E = ROLES \cup \{r_e\}$, where $USERS_E$ and $ROLES_E$ define correspondently the sets of users and

roles in our emergency aware RBAC. The corresponding user assignment relation will be defined as $UA_E = UA \cup \{(EH, r_e)\}$.

Assuming that BAN can give more elaborated reports $c_1, c_2, \ldots, c_t$ on emergency types and levels of severity of the patient condition we could define a set of emergency roles which may be associated with different sets of permissions that *EH* can be assigned in different emergency situations. In general case it can be presented as $ROLES_E = ROLES \cup \{r_{e1}, r_{e2}, \ldots, r_{et}\}$, and role r_{ei} can be activated by *EH* only when condition c_i is reposted be BAN to PTG.

7 Conclusion

In this paper we considered possible scenario and related security and privacy challenges that may appear in context of 5G telecommunication networks. One of the new challenges comparing with current situation is ability of direct accessibility of devices within BAN. In the case of medical applications we have to balance patient security and privacy against required safety and utility with solutions to handle emergency situations. However existing authentication and authorization methods are not developed with these kind scenarios in mind. In this paper we have proposed a new approach based on enhancement of RBAC model to handle emergency situations that may appear in medical context.

References

1. Aziz, O., Lo, B., Pansiot, J., Atallah, L., Yang, G. Z., Darzi, A. (2008). From computers to ubiquitous computing by 2010: Health care. *Philosophical Transactions. Series A, Mathematical, Physical, and Engineering Sciences, 366*(1881), 3805–3811.
2. Barlow, J., Wright, C., Sheasby, J., Turner, A., & Hainsworth, J. (2002). Self-management approaches for people with chronic conditions: A review. *Patient Education and Counseling, 48*(2), 177–187.
3. CEN/ISSS eHealth Standardization Focus Group. (2005). Current and future standardization issues in the eHealth domain: Achieving interoperability. Executive summary. Retrieved 10 06, 2008, from ftp://ftp.cenorm.be/PUBLIC/Reports/eHealth/eHealthStandardizationExecutive%20summaryFinalversion2005-03-01.pdf.
4. Dagtas, S., Pekhteryev, G., Sahinoglu, Z., Çam, H., & Challa, N. (2008). Real-time and secure wireless health monitoring. *International Journal of Telemedicine and Applications*, p. 10.
5. Fensli, R., Dale, J. G., O'Reilly, P., O'Donoghue, J., Sammon, D., & Gundersen T. (2009). Towards improved healthcare performance: Examining technological possibilities and patient satisfaction with wireless body area networks. *Journal of Medical Systems.*
6. Ferraiolo, D. F., Kuhn, D. R., & Chandramouli, R. (2007). Role based access control, artech house, 2003, 2nd ed.
7. Ferraiolo, D.F., Sandhu, R., Gavrila, S., Kuhn, D. R., & Chandramouli, R. (2001). Proposed NIST standard for role-based access control. *ACM Transaction on Information and System Security, 4*(3), 224–274.
8. Ferreira, A., et al. (2009). How to Securely Break into RBAC: The BTG-RBAC Model. In *2009 Annual Computer Security Applications Conference* (presented at the 2009 Annual Computer Security Applications Conference (ACSAC) (pp. 23–31), Honolulu, Hawaii, USA.
9. Ferreira, A., et al. (2006). How to break access control in a controlled manner. In *Proceedings of the 19th IEEE Symposium on Computer-based Medical Systems* (pp. 847–854). IEEE Computer Society.
10. Halperin, D., et al. (2008). Security and privacy for implantable medical devices. *Pervasive Computing, IEEE, 7*(1), 30–39.
11. Halperin, D., et al. (2008). Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In *IEEE Symposium on Security and Privacy* (pp. 129–142).
12. Jovanov, E., Raskovic, D., Price, J., Chapman, J., Moore, A., & Krishnamurthy, A. (2001). Patient monitoring using personal area networks of wireless intelligent sensors. *Biomedical Sciences Instrumentation, 37*, 373–378.

13. Kumar, S., Kambhatla, K., Hu, F., Lifson, M., & Xiao, Y. (2008). Ubiquitous computing for remote cardiac patient monitoring: A survey. *International Journal of Telemedicine and Applications*.
14. Tang, P. C., Ash, J. S., Bates, D. W., Overhage, J. M., & Sands, D. Z. (2006). Personal health records: Definitions, benefits, and strategies for overcoming barriers to adoption. *Journal of the American Medical Informatics Association, 13*(2), 121–126.
15. Toumaz Technology Ltd. (2009). Retrieved December 6, 2009 from http://www.toumaz.com/.
16. V-Patch. (2008). Wireless. Retrieved December 06, 2009, from http://www.vpatchmedical.com/.
17. Wald, H. S., Dube, C. E., & Anthony, D. C. (2007). Untangling the web—The impact of internet use on health care and the physician–patient relationship. *Patient Education and Counseling, 68*(3), 218–224.
18. Wootton, R., & Kvedar, J. C. (2006). *Home telehealth: Connecting care within the community*. London: RSM Press.
19. Rolim, C. O., Koch, F. L., Westphall, C. B., Werner, J., Fracalossi, A., & Salvador, G. S. (2010). A cloud computing solution for patient's data collection in health care institutions. In *Second International Conference on eHealth, Elemedicine, and Social Medicine* (pp. 95–99), (ETELEMED '10), 2010.

Author Biographies

Vladimir Oleshchuk is Professor of Computer Science at University of Agder, Norway. He received his M.Sc. in Applied Mathematics (1981) and Ph.D. in Computer Science (1988) from the Taras Shevchenko Kiev State University, Kiev, Ukraine, and his M.Sc. in Innovations and Entrepreneurship (2007) from the Norwegian University of Science and Technology (NTNU). From 1987 to 1991 he was Assistant Professor and then Associate Professor at the Taras Shevchenko Kiev State University. He has been working at University of Agder since 1992. He is a member of IEEE and a senior member of ACM. His current research interests include formal methods and information security, privacy and trust with special focus on telecommunication systems.

Rune Fensli was born in 1950 in Arendal, Norway. He received his M.Sc. in Electrical Engineering with specialization in Biocybernetics from the Norwegian University of Science and Technology (NTNU) in Trondheim of 1976. From 1976 he was employed as manager of the Department of Biomedical Technology at the University Hospital in Tromsø. From 1985 until the end of 1996 he was Chief of the Technical Department at Aust-Agder Central Hospital in Arendal. After some years as Managing Director of two innovative high-tech companies in Grimstad, he started his academic career in 1999 at the University of Agder, where he teaches Computer Network Security and Health Informatics. He was Head of the Department of ICT from 2000 to 2003. From 1984 to 1991 he was Chief Editor of the Norwegian journal of Medical Technology. He is one of the founders of two Norwegian companies, where he is a board member and holds equity interests: SANUM AS and WPR Medical AS. He also holds a patent within wireless ECG. He graduated his Ph.D. at Aalborg University in 2008, with a research area of wireless ECG sensor systems.