A Proposed System of Trust Based ECG Monitoring for Ubiquitous Healthcare Applications

Sachin Bhardwaj¹, Dae Seok Lee² & Wan Young Chung³
³Dept. of CSE & IT, Institute of Technology and Management, HUDA, Gurgaon, India
²Dept. of Ubiquitous IT, Graduate School of Design & IT, Dongseo University, Busan, Korea
³Division of Computer & Information Engineering, Dongseo University, Busan 617-716, Korea

ABSTRACT

Ubiquitous computing technologies can be used to provide better solutions for healthcare of patients at home or hospital. Moreover, ubiquitous computing is also characterized by partial views over the state of the global environment, implying that we cannot guarantee that an environment can always verify the properties of the mobile entity that it has just received. Secure in this context encompasses both the need for cryptographic security and the need for trust, on the part of both parties, that the interaction is functioning as expected. In this paper, we propose a trust-based system of ECG Monitoring for ubiquitous healthcare applications. A ubiquitous trust domain is introduced to collaborate entities making of autonomous trust-based decision for ECG monitoring using wireless sensors. Wireless controller that can send monitored information to the service centre and provide a feedback, if necessary, to the patient from medic. If an emergency is detected the monitoring services gives alarm condition to doctor’s personal digital assistant.

Keywords: Trust, ECG Monitoring, BAN, Ubiquitous Trust Domain, Wireless Sensor Network, Ubiquitous Healthcare

1. INTRODUCTION

Future large-scale health-care will involve many different organizations cooperating in patient care, including hospitals, patient body area network, dentists, pharmacies, drug companies, and insurance companies. With the advent of new wireless healthcare products, it is becoming feasible to contemplate new applications that offer real-time healthcare to patients, and involve complex interactions between many services in many organizations. Key to their design is the issue of trust, where we want trust-based decisions relating to the interactions between entities – which entity to interact with, what resources should the entity have access to, what information should be released to the entity, how to configure the mechanisms needed to make the interaction secure and how trust levels change over time, based on experience and reputation. Large-scale applications cannot rely on the traditional person in the trust decision loop, but must make use of automated trust decisions. A trust domain is a dynamic set of collaborating entities capable of making autonomous trust-based decisions. Trust domains, with varying trust relationships between them, can be grouped in compositional, hierarchic and ad-hoc peer-to-peer relationships. Examples include a body-area network monitoring the health of a patient, care worker responsible for a patient, a hospital or a regional health authority.

Several international projects, which concentrate on using wireless sensors as a framework of a standardized body area network (BAN), are focusing on improving new technology solutions. Though, few of them have possibilities of extended healthcare parameter analysis within the trusted ubiquitous healthcare system. The European community’s MobiHealth System (2002-2004) demonstrates the Body Area Network (BAN) [1]. Code blue [2] is a wireless infrastructure for deployment in emergency medical care. Another health monitoring system is Coach’s Companion [3], which allows the monitoring of physical activity and low power, wireless two lead ECG [4]. Long term ECG analysis plays a key role in heart disease or chronic disease analysis. The long term objective, however, is to automate the ECG event classification in order to further enhance medical treatment. In order to classify the ECG signal, a reliable extraction of the characteristic ECG parameter is needed.

The component of Ubiquitous Healthcare system consists of sensing, monitoring, analyzing and the feedback of behavior modification, disease classification, and Emergency alert. In our system, emphasis is placed on recent advances in wireless ECG system for cardiac event monitoring with trusted environment for ubiquitous healthcare system. The components of trust and ubiquitous healthcare system are shown in...
Figure 1. Out of several definitions of trust, one definition that we would like to mention here is by Grambetta [5]. Grambetta relates trust to future expectation. He defines trust as a probability of a trusted entity doing something beneficial for the trusting entity. In other words, if Bob does something which Alice expects (assuming that this expectation is driven by the fact that the result will be beneficial to Alice) then Alice can trust Bob. If the result is not what Alice expects then Alice cannot trust Bob.

2. TRUST BASED SYSTEM CHALLENGES TOWARDS UBQUITOUS HEALTHCARE SYSTEM

Consider a simple scenario where a patient with an acute heart condition subscribes to a monitoring service that provides wearable sensors and a small wireless controller that can send monitored information to the service centre and provide feedback, if necessary, to the patient from a medic. If an emergency is detected the monitoring service calls an ambulance. The monitoring service needs access to patient cardiac history from the patient’s body area network and from the hospital where the patient had treatment and so liaises with the emergency services and the hospital to which he will be taken for emergency treatment. Assume the monitoring service also provides anonymised monitoring records for medical research. Hospitals need to interact with the patient’s body area network and possibly social services about caring for a patient after treatment. In a small hospital, there may not be local expertise to evaluate patient information such ECG readings and so these needs to be sent to a remote expert over the network. Perhaps the patient’s usual consultant is not available and a new trusted one has to be chosen which is a form of trust-based choice of service. A consultant evaluating an ECG may wish to search for similar examples via a medical services grid but then the question of trust in the source of the examples arises.

There are many different aspects of trust in all the above interactions. Will the monitoring service detect actual problems without false alarms? Can the wireless infrastructure being used be trusted with respect to confidentiality? If not, can this lack of trust, ensure that data is communicated over a secure channel. Can the monitoring service be trusted to pass on monitored information for research while still maintaining patient privacy and can they guarantee that the information will be used only for medical research. Can the patient (if he so wishes) agree to information being sold to insurance companies in exchange for a lower monitoring service charge or insurance premium? In cases of emergency, can we ensure that privacy issues may be over-ruled and the patient’s doctor should have access to detailed monitored information? Trust with respect to interactions between organizations (e.g. a hospital using a blood analysis service) will change over time based on experience, recommendations, or reputations [6]. There is a need to collect this evidence for use in making decisions based on trust, for example in health workflow systems to aid medical procedures or patient care, where the entities participating in the workflow, change dynamically because of workload, availability etc and may have varying levels of trust between them. Trust may also depend on current context, particularly for mobile applications. Privacy – an individual’s right to control the collection and use of personal information plays a crucial role in building trust, particularly in healthcare applications.

Research in trust issues is at an early stage. There is not much work on the integration of automated trust decision support within a potentially large-scale, multi-domain distributed system architecture, taking application context into account. The concept of trust domain is novel and important. The dynamic creation of trust domains, and interactions between trust domains, with the need to dynamically construct appropriate policies for trust based-decisions, and gather the evidence required to make those decisions while maintaining privacy has not been addressed in the literature.

We can classify security considerations in ubiquitous sensor network for the proposed system at three different levels of implementation.

- **Data Privacy at Acquiring Level (Non invasive):** At this level the Sensor nodes would acquire medical measurement and send these data to the sink device (SD). Also if there is any data to be sent to any of the sensor nodes such as
configuration settings for a sensor, it can be done at this level. Any data that has been acquired must be done in a non-invasive manner and must not be accessed by sensor devices on a different user. This can be achieved by authentication at the MAC layer level for a particular user. When the WSN is deployed all sensor can be identified and their distinct MAC addresses stored in the sink device [7]. Whenever a sensor needs to send some data it can request connection by sending a request with its own MAC address. The sink device can identify the incoming request by matching MAC address with the ones stored in its memory.

- **Data Security at Transmission Level**: At this level we assume that all data has been collected by the SD and is ready to be transmitted. A users SD is assumed to be roaming in a foreign network and therefore needs to connect to the healthcare provider’s device (HD) [8] by either accessing the Home Authentication Server (HAS) or the Foreign Authentication Server (FAS) depending on its current location, either in home network or a foreign network. In either case it will authenticate with the required server using a challenge/response mechanism by encrypting all correspondence with mutual sharable keys. If the HD allows the user to be registered it will authenticate the session for further data transmission. Figure 1 shows our proposed model.

- **Data Security at Healthcare Provider Level**: At this level the data is stored in the HD’s databases and can be access by authorized experts for analysis [9]. Application level security can be implemented at this level to guarantee privacy and security.

### 3. A TRUST BASED ECG ANALYSIS FOR UBQUITOUS HEALTHCARE APPLICATIONS

In our system, emphasis is placed on recent advances in wireless ECG system with trust-based environment for cardiac event monitoring in-patient for ubiquitous healthcare system. The system also provides an application for recording activities, events and potentially important medical symptoms. The hardware allows data to be transmitted wirelessly from on-body sensor to the base system and then to PC/PDA. Wireless Sensor nodes are small sized hardware modules, which have strong capabilities of sensing, computing and bi-directional communication. These sensor nodes can be programmed using TinyOS [10] and operates on low power batteries. The sensor measures ECG-signals with a sampling frequency of 200 Hz. The signal is digitalized with 10 bits resolution, and continuously transmitted it to a receiver-module attached to PC/PDA, using a modulated RF-radio link of radio chip CC2420 (Chipcon Inc., Norway). The sensors are sticky and attached to the patient’s chest. It will continuously measure and wirelessly transmit sampled ECG-recordings using of a built-in-RF-radio transmitter to the base station and then to PC/PDA through a RS-232 connector. Server/Client software programs were developed in C# based on .Net compiler for monitoring and analyzing the ECG-recordings [11]. The overall objective of our proposed system is to develop the necessary support for building e-science autonomous trust domains, with healthcare as a demonstrator. The specific objectives related to ubiquitous trust domain of the system include:

- Autonomous trust domains that make decisions based on evidence, trust and privacy requirements and trust negotiation and are capable of scaling down to body-area networks as well as scaling up for grid application.
- Techniques for the formation, management and interoperation of ad-hoc trust domains. This includes techniques for federating and composing trust domains to support large scale applications and inter-organisational interactions.
- An evidence service that collects, filters, synthesises and anonymises experience, risk, recommendation and reputation data that can be used as evidence for trust evaluation. Note that evidence may have to be archived for audit and statistical evaluations.
- Trust-based decision support for security adaptation, privacy or service selection.
- Techniques for protection against attacks on the trust infrastructure
- A healthcare demonstrator based on the scenarios described above.
Requests for trusted interactions are forwarded to the local ubiquitous trust domain, which is responsible for determining whether the interaction should succeed or fail. The Ubiquitous Trust Domain is also capable of providing a signed statement of the reasoning for success or failure (useful for debugging and repudiation). In this example, if a request succeeds, the Ubiquitous Trust Domain will establish a new secure channel and trigger any necessary security adaptations, e.g. access control systems. Although the architecture of the ubiquitous trust domain implied in Figure 2 is preliminary and over-simplified, it indicates some of the functionality and data that will be required. Functionality like secure communications is well understood with accepted standards (e.g. SSL/TLS), although most middleware communications services do not yet consider trust issues. Trust languages and trust negotiation protocols have few implementations and little acceptance. There is a need to federate (i.e. to form ad-hoc dynamic coalitions) and compose trust domains (e.g. nested hierarchies) to support more complex scenarios. This requires protocols for group-membership and trust negotiation, as well as an overarching architecture that is self-managing.

After receiving data from patient’s body then it will continuously measure and wirelessly transmit sampled ECG-recordings using of a built-in-RF-radio transmitter to the base station and then to PC/PDA through a RS-232 connector. Then the data is transfer for calculating trusted value for trusted environment and to give authentication to system for further processing. After calculating all parameter of ECG signal then can classify shape and beat of ECG and can diagnose heart related diseases. Then the data must be transfer to the ubiquitous trust domain for trust value calculation. It is processed by authorization policy is concerned with controlling access to services and the visibility of data on service/method invocation at the application level. But data is routinely recorded by a (trusted) audit service at the system level, to satisfy legal requirements. It is need to be classify different privacy requirements, different degrees of anonymisation that might be enforced, and how they affect the basic trust model and trust computation. After the result of trust values calculation then it can be decide whether the query should proceed for further processing or not. If any abnormality occur at server then it can transfer alarm condition to doctor’s PDA.

4. RESEARCH ISSUES RELATED TO TRUST BASED UBQUITOUS HEALTHCARE SYSTEM

Most of the emphasis of existing work in trust systems has been on exploring the very wide range of possible models for defining and formally reasoning about trust. We will concentrate on the research issues to deploy trust-based infrastructure for ubiquitous healthcare system. The research issues to be addressed therefore include:

- What trust model is most appropriate? This includes issues of how to specify trust requirements to enable use by trust decision algorithms? How to use policies to govern the behaviour of the trust infrastructure?
- How to scale down to simple wireless devices as well as scale up to large inter-organisation applications?
- What privacy models to use and how to specify privacy requirements in policies which combine trust and privacy?
- How to summarise historical evidence taking into account disparate, classified, patterns of behaviour? How to identify evidence as being specific to a particular trust related activity and how to correlate evidence related to different activities? How to anonymise evidence to satisfy privacy requirements? This includes the requirements for vertical studies of populations as well as for evidence distribution in recommendations.
- When and how to exchange evidence and trust information across trust domains? How to define trust relationships between domains? How to use such relationships in trust interactions?
- How to assess the trustworthiness and risks in using trusted interactions, which includes identification of potential attacks and vulnerabilities of the trust infrastructure? What countermeasures are possible and how to evaluate user confidence in proposed solutions?

Trust-based systems may be compromised by attacks based on generating incorrect information and collusion against the trust-models and trust-implementations used. There is also need to evaluate threats, characterise existing attack techniques and identify new ones (c.f. cryptanalysis).

5. CONCLUSIONS

A proposed system of trust based ECG monitoring for ubiquitous healthcare applications is discussed with implementation scenario and research issues. Our proposed system can acts as a continuous event recorder, which can be used to follow up patients who have survived heart diseases in both home and in hospitals. After analyzing ECG signals of patient at server with trusted value calculation can provide informative details to the doctors using PDA/PC, and simultaneously alert the doctor of any emergencies. Thus, the proposed system makes correct diagnosis even under situations
where the patient is unconscious or unaware of cardiac diseases and provides a capability for real time (software) monitoring of ECG signal at server with trusted ubiquitous environment and then notify to the doctor’s PDA.

Eventually, we believe that there is lots of work to do in the implementation area. As a future work we are going to build up the proposed trust evaluation and access control policy modules for ECG monitoring using wireless sensors that put our findings into practice, allowing people to differentiate exposure their resources by trust estimation.

REFERENCES