Vesta: A Secure and Autonomic System for Pervasive Healthcare

Yanmin Zhu[†‡], Morris Sloman[†], Emil Lupu[†], Sye Loong Keoh[†]
[†]*Imperial College London;* [‡]*Shanghai Jiao Tong University*
{yzhu, m.sloman, e.c.lupu}@doc.ic.ac.uk, sye.loong.keoh@gmail.com

Abstract—The proliferation of low-power wireless communications and handheld devices has facilitated the development of pervasive systems for healthcare applications. This paper describes a body sensor network comprising a personal controller, various biosensors and actuators for pervasive healthcare. Various physiological parameters such as heart rate or blood oxygen level can be continuously monitored. The growing complexity of such systems, however, poses challenges for system management and security. In this paper we present a secure autonomic body sensor network called Vesta which makes use of the extensible architecture pattern of a self managed cell (SMC). A policy-driven management paradigm supports adaptability to contextual changes by applying event-condition-action rules. Fine-grained access control of the system is realized through authorization policies. Experimental evaluation shows that it is viable and practical for real-world pervasive healthcare.

I. INTRODUCTION

With the advent of miniaturized biosensors [1] and low-power wireless communications, it has become increasingly practical to develop pervasive systems [2, 3] for healthcare applications [4, 5]. This paper focuses on a pervasive system that comprises biosensors, actuators, and a portable processing device such as smartphone. Wearable or even implantable biosensors are able to continuously monitor physiological parameters including heart rate, body temperature and oxygen saturation for healthcare purposes. Body sensor networks simplify sensor interconnection for in-hosptial monitoring and enables home monitoring of patients which facilitates early release from hospitals and automated emergency alert. Healthcare practitioners can also better understand a patient's condition, and limited hospital resources can be utilized more efficiently [2].

However, operating such a pervasive healthcare system is non-trivial, as it requires considerable computing expertise to configure as it includes heterogeneous devices and many different types of software. There is also a need to reconfigure the system to accommodate context changes over time and allow easy dynamic reconfiguration of the set of sensors for a patient. The system therefore needs to discover the new components and make them available to provide new services, or components may leave so should be cleanly removed from the system. To overcome these challenges, autonomic computing [6] can be used to enable self-configuring, self-healing, self-optimising, and self-protection to enable autonomous system operation with minimal human involvement.

For healthcare applications, data confidentiality and user privacy becomes an important issue, since the data may contain sensitive information about a patient, particularly when politicians or celebrities are involved. Wireless communication enables flexible configuration but exposes security weakness to an adversary. Data communication may be eavesdropped or an adversary may use compromised biosensors to join a patient's network to access sensitive user data.

Access control or authorization also becomes a necessity. For example, in a hospital environment, nurses or doctors often need to access resources, or even invoke operations, on a patient's system. Only legitimate users should be allowed to interact with a patient's system, but there is also a need to grant different access privileges to different users such as nurses, doctors, consultants etc. This is very important since an incorrect action may result in serious consequences.

Considerable research has addressed autonomic computing issues [6]. For example, many protocols have been developed for service discovery, including UPnP [7], Jini [8], Bluetooth SDP [9] and SLP [10]. Other traditional network and system management techniques have also been proposed for event dissemination, fault diagnosis and policy-based management. However, they are intended for enterprise networks and thus are not suitable for personal healthcare systems where computational resources are usually constrained.

In this paper, we propose a secure autonomic system called Vesta for managing pervasive healthcare systems. We extend the initial work done in the Amuse Project [3] by providing support for security and policy management on very simple biosensors. We use the Amuse Self-Managed Cell (SMC) architectural pattern for software components and devices which form a healthcare body sensor network. The SMC supports dynamic component addition and departure; interactions among components within a cell by making use of an event service. A policy service effectively implements a feedback control loop. Adaptation is enabled through deploying, removing, enabling and disabling policies.

Vesta incorporates a number of security measures to secure a self-managed cell. First, we propose a simple yet effective method to admit new sensors. Second, data communication between sensors and the controller are secured by symmetric cryptography that is appropriate for resource-constrained sensors. Finally, to realize fine-grained access control, authorization policies define what actions a subject can perform on a target when specified conditions hold. Adapter objects act as

Digital Object Identifier: 10.4108/ICST.PERVASIVEHEALTH2009.5939
http://dx.doi.org/10.4108/ICST.PERVASIVEHEALTH2009.5939

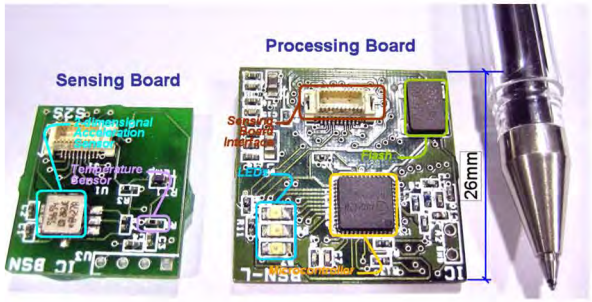

Figure 1: A biosensor node consisting of a processing board and a pluggable sensing board, compared to the size of a ballpoint pen.

proxies for remote components and can perform protocol specific adaptation.

This paper is structured as follows. The background and a motivating example are presented in Section 2. The system overview of Vesta is described in Section 3. The following section details the design of several important components. We conducted experiments and performance results are introduced in Section 5. Finally, the paper is concluded and future research directions are mentioned in Section 7.

II. Background and Motivation

This section introduces the basic components of a body network and gives a motivating example. Although there can be many application scenarios, we focus on the scenario of a hospital ward involving patients, nurses and doctors to exemplify the use of pervasive healthcare systems.

The patient's body network is usually composed of a handheld device such as a PDA, smart phone or gumstix as the personal controller plus a number of wearable or even implantable wireless biosensors and actuators. Figure 1 shows a typical body sensor node (BSN) with connected biosensors developed at Imperial College London [11]. These biosensors continuously monitor various physiological parameters of the patient. For example, ECG sensors can monitor the heart status and accelerometers can be used to determine activities. A feedback control loop could incorporate an actuator such as a drug pump. All biosensors, actuators and the personal controller communicate with each other through wireless communications, such as IEEE 802.15.4 or Bluetooth. The patient's body network is likely to evolve over time as new devices may be added to monitor emerging symptoms or sensors no longer needed are removed.

The configuration of the pervasive system often needs to adapt. New devices need to be configured when added and the system should be updated when devices are removed. The devices within the system should also be reconfigured when patient context changes. For example, when the patient is in the ward, an emergency is reported directly to a medic through local wireless communication such as WiFi. However, when the patient is outside of the hospital, the emergency should be reported to the doctor or the emergency services via the GPRS/3G channel of the patient's mobile phone.

The process of associating a biosensor to the body network of the patient is non-trivial and critical. In the environment of a hospital, there are many patient body networks. If a biosensor is physically attached to one patient but associates with the network of a neighboring patient, the reported data would be incorrect and this may lead to wrong medical decisions. Furthermore, an adversary may intentionally try to capture such biosensors in an attempt to access the data of a patient.

Wireless communication is one of the main strengths of pervasive computing, removing the burden of wiring different devices. However, it exposes security weakness. The biosensors communicate with the personal controller via short-range radios. A patient may communicate with medics through a wireless channel. An adversary may eavesdrop on the communications and compromise confidentiality of the data and hence patient privacy, particularly for prominent politicians or celebrities. The adversary may even launch active attacks by replaying or modifying messages to harm the patient.

Patients need to interact with nurses and doctors. A nurse reads the sensor data on a patient on a regular basis to ensure the wellbeing of the patient. A doctor may look at the logged physiological data to determine medical treatment. It is apparent that different medics have privileges of different levels. For example, a doctor is entitled to invoke a drug-pump operation on a patient, but a nurse is not allowed to do so. This highlights that, on the one hand, it is necessary to authenticate different users, and on the other hand, access control should permit only legitimate users to perform authorized operations.

Note that a nurse or doctor may also have a personal network, consisting of a portable computer/smart phone and various kinds of additional monitoring devices to access the patient's body network to perform specific tests or determine current state form the patient's sensors.

In summary, from the motivating example, we can see that the following functionalities are required for a pervasive healthcare system.

- **Autonomous management.** The system must be self-managing with little human intervention or configuration input and should be adaptive to context changes.
- **Access control** needs to differentiate different user roles, and only allow legitimate users to perform authorized operations.
- **Data confidentiality** must be ensured to minimize the security vulnerability of wireless communication.

III. Vesta Overview

In this section, we present the architecture overview of Vesta and describe the major components. Vesta makes use of the SMC architectural pattern, depicted in Figure 2 [3] to represent a Patient's or Medic's personal network. Vesta extends Amuse [3] by 1) securing the Discovery Service, 2) providing a new Authentication Service, and 3) including access control. For the completeness of describing the whole system, we introduce all of the main components in this section, and describe the design of the new components in the next section. The body network is by nature a distributed environment containing heterogeneous components and devices. Sensor nodes

Digital Object Identifier: 10.4108/ICST.PERVASIVEHEALTH2009.5939
http://dx.doi.org/10.4108/ICST.PERVASIVEHEALTH2009.5939

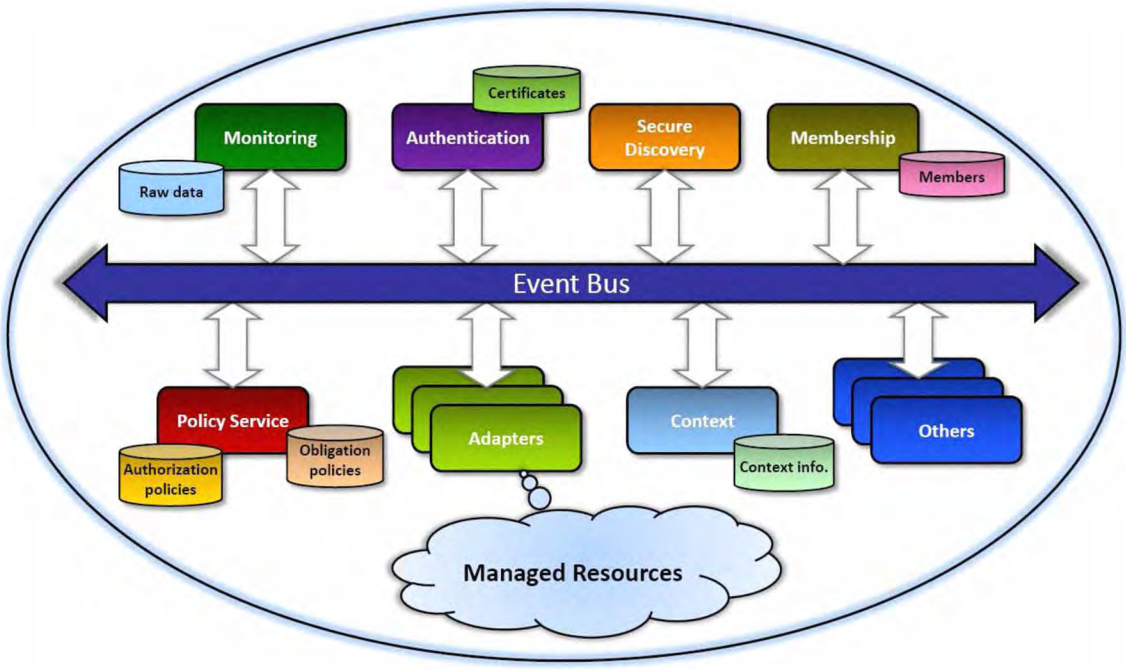

Figure 2. The Vesta architecture which extends the Self Managed Cell (SMC) architectural pattern. Components within the cell are connected through an event bus. Adapters are created for software components or devices that reside outside of the personal controller.

typically communicate using IEEE 802.15.4 while a smart phone has a Bluetooth radio. Vesta must support a unified view and allow all these components to interact with a unified interface. As management systems are usually event driven, Vesta uses a publish/subscribe event bus which ensures in-order and reliable delivery of events [12]. This decouples interacting components, allows multiple components to subscribe to the same events, and hides communication heterogeneity. However, we do not insist that all interaction is via the event bus but also support direct invocations.

The discovery service is responsible for discovering new services and devices. As discussed in the previous section, new biosensors may be added to a patient when new physiological parameters need to be monitored. It is also used to discover approaching nurses and doctors. When new services or devices are added into the network, corresponding adapters are automatically created and deployed to receive and relay both events on the event bus and packets between the personal controller and the devices. After new services or devices are admitted, the membership service continuously monitors the availability of these components. If a service leaves the system, resources like the adapters should be released. In addition, other components within the system should be informed of the departures so that they do not try to interact with components that have left. The discovery and admission procedure must be secure and guarantee that a biosensor is associated with the intended patient. The procedure must be easy to operate for nurses. This requires the procedure to be simple and efficient.

The policy service implements a policy-based management framework for adaptation. There are typically two types of policies. An obligation policy is an event-condition-action rule specifying the action that must be performed when the event occurs if the condition evaluates to be true. An authorization policy specifies whether a subject is permitted to perform specific operations on the target if the condition holds. This can be used to realize access control and effectively protect resources from unauthorized access. The lightweight policy system of Ponder2 [13] is deployed for the policy service.

A policy-based feedback loop is realized [3]. Context changes are indicated by events and disseminated through the event bus. The policy service uses these events to trigger obligation policies and if the policy condition evaluates to true, the corresponding policy action will be invoked. All actions are governed by authorization policies [14]. Before an action is actually performed, the policy system searches for an authorization policy which permits the action otherwise it is blocked. We also need to authenticate subjects performing an action on a target component and have developed an authentication protocol based on a public key infrastructure (PKI). As described in the next section. Adaptation is realized by loading, removing, enabling and disabling policies.

IV. Design Details and Analysis

This section describes three major components which extend the SMC architecture developed in the Amuse project: *secure sensor discovery*, *authentication module* and *access control*. With the secure sensor discovery module, a new sensor is guaranteed to be associated to the intended patient and only valid sensors can be admitted into the system. Wireless data transmission between sensors and the controller is en-

Digital Object Identifier: 10.4108/ICST.PERVASIVEHEALTH2009.5939
http://dx.doi.org/10.4108/ICST.PERVASIVEHEALTH2009.5939

crypted. A pairwise key is created when the sensor is admitted. Interacting users can authenticate each other, and subsequent communications between them are kept confidential. Fine-grained access control to resources at the target system must be performed for authenticated user.

A. Authentication Protocol

We developed an authentication protocol based on the public key infrastructure (PKI). It is assumed that there is a certificate authority (CA) within the hospital, which assigns a public key certificate to every user. The certificate is signed by the CA, and encloses the public key and other attributes of the user, such as the name, and identification.

The nurse controller broadcasts (*e.g.*, through WiFi) HELLO messages periodically in order for patients to be aware of its presence. On receipt of a HELLO message from a new nurse, a patient initiates the mutual authentication procedure as shown in Figure 3 The protocol procedure is exemplified with the authentication between a nurse, Alice, and a patient, Bob. Bob responds to Alice's HELLO with a REQ, which initiates the authentication protocol. Next, Alice sends her certificate C_a to Bob who checks the validity of C_a. If the certificate is valid, Bob sends his certificate C_b to Alice who also checks its validity. The exchange of Diffie-Hellman (DH) parameters enables generation of a pairwise key for Bob and Alice for a secure communication channel. On completion of DH key creation, each side has authenticated the other.

Due to the unreliable nature of wireless communications, it is possible that messages may be lost or corrupted in the process of packet exchange. Thus, it is important to ensure that no deadlock is introduced. To overcome this issue, a timer is started, at the start of the authentication protocol. When the timer fires, the process stops and the state is reset to INIT, *i.e.*, it is now ready to start a new authentication process.

A nurse may interact with multiple patients at the same time. Thus, each time the nurse discovers a new patient it starts a separate process for patient discovery and authentication. The resultant advantage is that different patients do not interference with each other during authentication.

B. Access Control

The Ponder2 policy system used in Vesta supports authorization polices [14] and is able to resolve conflicts among authorization policies. In the following we explain how access control regulates access from authorized doctors and nurses

In Ponder2, services and resources to be managed are represented as managed objects. An invocation from one managed object to another can be regulated by an authorization policy – an invocation is permitted only if a policy exists to grant access, otherwise, this invocation is denied. Managed objects are grouped into domains which can be nested. A domain structure is created and maintained at each user, as shown in Figure 4. With the availability of domain structures, authorization policies can be flexibly specified in terms of domain paths instead of individual managed objects. The consequent advantage is that even if individual managed object change, authorization policies do not have to be changed.

To control accesses from a nurse, the patient makes use of the adapter that represents the nurse. An adapter is created and put in the domain structure upon completion of mutual authentication. This adapter is a managed object in the patient's Ponder2 environment and represents the nurse. Java Remote Method Invocation (RMI) is used for interaction and the adapter implements a Java RMI interface, which defines all actions that may be invoked on the patient. On the nurse side, a mirror object is created, which is essentially the proxy of the remote adapter at the patient. To invoke operations on the patient, the nurse invokes operations directly on the mirror

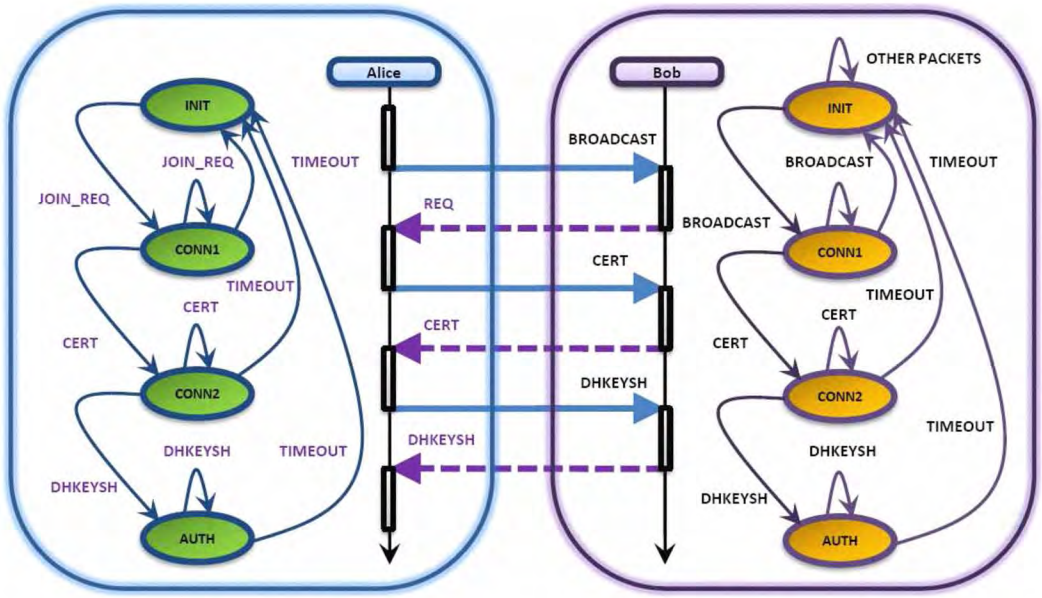

Figure 3. The mutual authentication protocol for a patient Bob and a nurse Alice. The protocol messages and their timing are shown. The state transition diagrams are along with the timing.

Digital Object Identifier: 10.4108/ICST.PERVASIVEHEALTH2009.5939
http://dx.doi.org/10.4108/ICST.PERVASIVEHEALTH2009.5939

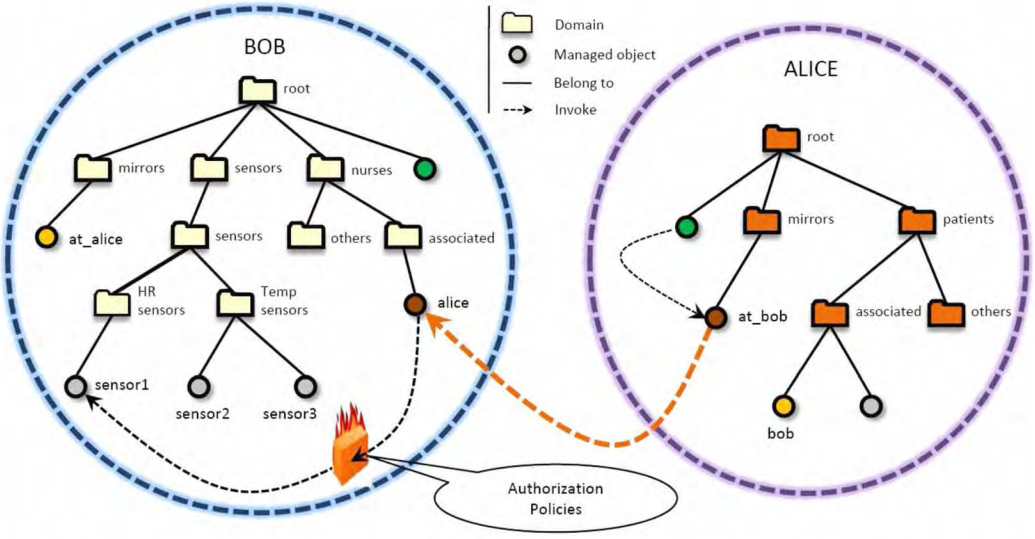

Figure 4: The domain structures of Bob and Alice. The procedure of Alice invoking a sensor operation on Bob is illustrated.

proxy. All requests are then forwarded to the adapter at the patient. The advantage of using RMI is that no proprietary protocol need be developed for communication between the patient and the nurse. The adapter then invokes the request operation at the target managed object on behalf of the nurse. This invocation can be effectively governed by authorization policies at the patient.

As an example, suppose nurse Alice wants to check the current status of the heart sensor at patient Bob, so she enters a request via her user interface. This request is received by the mirror proxy and is forwarded to the nurse adapter at Bob. As a result, this request reaches the Alice adapter that immediately invokes the requested operation at the managed object of the heart sensor. The invocation is intercepted by the authorization interpreter that checks if there is an authorization policy permitting this invocation. For example, the following authorization policy permits this invocation.

auth+ /nurses/associated/ → /sensors/HRsenors/

This policy specifies that all associated nurses are allowed to do any operations on hear rate sensors.

C. *Secure Sensor Discovery*

New sensors may have to be added to a hospital patient's body network fairly frequently. A nurse, or a doctor, can usually be authorized to perform new sensor association. These new sensors must be cleared of any previous states and re-initialized. The key challenge is to ensure secure association via simple mechanisms. Our secure discovery procedure avoids wireless interaction as this is more vulnerable to eavesdropping and capturing encryption keys. A newly initialized sensor node cannot easily distinguish between valid or unauthorized communication partners and has no encryption keys to secure communication.

We devise a physical secure channel for admitting new sensors. In the prototype implementation, we have used an ASUS EEE PC [15] as the personal controller as shown in Figure 5. Two of its USB ports are used. One port is connected to a BSN node acting as a gateway for IEEE 802.15.4 wireless communication with other nodes. In essence, it forwards packets from the controller to the intended sensor and packets from sensors to the controller. The second port is connected to a programming board and is exclusively used as a secure physical channel for admitting new sensors.

On the personal controller of the patient, a discovery manager is responsible for admitting new sensors. This manager monitors the activity on the admission port and accepts joining requests of new sensors. The procedure of associating a new sensor to a patient is shown in Table 1.

First, the nurse who wants to associate a new sensor to a patient must send an association request to the target patient. In essence, the request is forwarded to the discovery manager and the requested action is to open the admission port. The action request is then checked against authorization policies to ensure that only authorized nurses or doctors can add new sensors to a patient. If authorized, the action results in the admission port being opened for a time window size w –

Figure 5. The prototype of a personal controller (ASUS EEE PC) that operates two USB sensor ports, one acting as a gateway to wireless biosensors and one as the secure physical channel of new sensor admission.

Digital Object Identifier: 10.4108/ICST.PERVASIVEHEALTH2009.5939
http://dx.doi.org/10.4108/ICST.PERVASIVEHEALTH2009.5939

determined by the practical time required for the nurse to plug a new sensor into the port and the sensor then to communicate with the controller. When the new sensor is plugged into the admission port on the nurse's personal controller, it is powered up and starts functioning. Next, the sensor sends a JOIN message to the discovery manager via the admission port. On receiving this message, the discovery service is aware of the new sensor and admits it into the system. It prepares a pairwise session key and the group key. The two keys, in addition to other necessary information about the system, such as network ID, are enclosed in a CONFIRM message sent to the sensor. The discovery service also creates an adapter for the sensor, which will later interface interactions between the sensor and other components within the system. After the sensor has received the message, it stores the information in its non-volatile memory such as the external flash memory. Then, the sensor is removed from the port and is supplied with its own battery. On startup, it has been associated with a specific controller and hence a specific patient's network. All further communications to the controller is via wireless, relayed by the gateway.

The admission procedure of new sensors is secure. All communication during the admission procedure is through the physical channel that is essentially the serial communication channel emulated by the USB port. This channel is the only way that a new sensor is admitted to the system. The group key and the pairwise key define the membership of a sensor. The only way to obtain the two keys is to undergo the admission procedure. Note that although the EEE PC is adopted as the prototype implementation, Vesta is not limited to it and can be implemented on any device that can host a Java virtual machine environment and have a host USB port. Current smart phones do not support host USB ports so we would need to develop a smart cable to emulate the host to both phone and connected BSN node.

TABLE 1
THE PROCEDURE FOR NEW SENSOR ADMISSION.

Step 1: the nurse who wants to associate a new sensor sends an action request of new node association to the intended patient;
Step 2: the patient makes the authorization decision based on authorization policies. If authorizing the action, the discovery manager opens a small time window *w* during which the admission port opens.
Step 3: the new sensor is plugged into the nurse's admission port;
Step 4: the new sensor sends a JOIN message to the discovery manager through the USB port;
Step 5: the controller responds with a CONFIRM message which contains a pairwise key and the group key;
Step 6: upon reception of the CONFIRM message, the sensor retrieves the keys and store them in non-volatile storage;
Step 7: the new sensor is removed from the port and starts communication with the controller using the assigned keys;
Step 8: the controller creates an adapter that represents the new sensor.

V. IMPLEMENTATION AND EVALUATION

This section discusses several implementation details. Experimental results of the performance of Vesta are presented.

A. Data Encryption

Wireless communications take place in two places. One is between the controller and biosensors, and the other between the patient and a nurse or doctor. To achieve data confidentiality and combat passive eavesdropping, data packets should be encrypted before they are transmitted. To encrypt data transmitted between the controller and a sensor, we used the readily available Skipjack, implemented in TinySec [16], for symmetric encryption with a 160 bit key length. Skipjack is a block-cipher with the block size of 8 bytes. We use the Cipher Block Chaining (CBC) operation mode with non-repeating Initialisation Vector (IV). The battery level or sensor readings can be used as the seed of a pseudo-random number generator to generate the initial IV.

For encryption of data between the patient and the nurse, we could use asymmetric cryptography based on public and private keys of each user. However, a computing device acting as the personal controller typically has limited computational capability. This suggests that asymmetric cryptography would introduce significant latency. Therefore, a pairwise session key is created during the authentication process and is used for encryption of all data exchanged between the nurse and the patient.

B. Time Stamping

It is very important to guarantee the freshness of a delivered packet. An adversary may launch active attacks such as replaying previous sessions. This kind of attack may result in serious consequences. For example, an attacker could record the whole request packets from the nurse to the patient, which causes the pump to inject an amount of a drug. The attacker could send this request to the patient multiple times and hence endanger or kill the patient.

The effective counter measure is to ensure the freshness of a request. It is assumed that the clocks of all users are synchronized. Then every packet is attached with a time stamp of packet delivery off the source node. Note that the user data together with the time stamp are encrypted. Upon receiving a packet, the controller checks the difference between the current time and the time stamp. If the time difference exceeds a predefined threshold, this packet is dropped.

C. Performance Evaluation

We conduct experiments to study the performance of Vesta. In practice, the personal controller typically has limited resources and low computational power. Therefore, we are interested in studying the performance in terms of memory footprint and processing times of various operations. Small footprint and short processing latency are desirable.

To perform experiments and collect performance data, we implemented the patient and the nurse systems on two ASUS EEE PCs separately. An EEE PC has a 7 inch display. The processor adopts the Intel Celeron-M ULV 353 model that runs at 900 MHz. For the storage system, the PC has 512

Digital Object Identifier: 10.4108/ICST.PERVASIVEHEALTH2009.5939
http://dx.doi.org/10.4108/ICST.PERVASIVEHEALTH2009.5939

DDR2 SRAM and 4G HDD-SSG permanent storage. The operating system is Windows XP SP2. We deploy J2SE 5 as the Java virtual machine environment. During experiments, the systems are not running other applications. The communication between the patient system and the nurse system is implemented in ad hoc mode using IEEE 802.11b network interface cards available the EEE PCs.

On the patient system, a BSN node acts as the gateway. The new sensor is also a BSN node. A BSN node is equipped with an 8MHz TI MISP 16 bit processor. It has 2K RAM for data stack and 60K ROM for binary code. With a Chipcon CC2420 radio transceiver, it transmits data with bandwidth of up to 250 kbps.

We look at the footprints of Vesta at both the patient and the nurse. The system takes 1.39 MB RAM on the nurse and 1.25 MB RAM on the patient. The footprint on the nurse is larger than that on the patient because the system on the nurse embodies additional software components, such as HELLO broadcasting module and patient discovery module. We also investigate the footprint on the sensor node Which will depend on the specific applications installed. In the experiment, the new biosensor implements a basic function that regularly measures the heart rate and reports to the personal controller. In addition, it also deploys the modules enabling it to be securely admitted into a network. The software on the biosensor only uses 0.82 KB RAM and 7.23 KB ROM.

We determined the time overheads required by primitive operations as listed in Table 2. From the table, we can see that most operations except the startup process are efficient. In our implementation, we have used the Ant utility tool to manage the software compilation and execution. Each time the user tries to start the system, the Ant tool checks whether any source files have been changed and then the system is actually started. This slows down the system startup process. After the system is mature and put into real application, this management tool can be removed and the startup process can be speeded up.

Next we compare the secure sensor association of Vesta to a sensor discovery protocol that we have previously proposed [17]. In that protocol, it is assumed that all healthcare workers are authorized to perform the sensor association. In addition, each sensor is assumed to be preloaded with a public/private key pair. This is a strong assumption and increases the management burden of biosensors. To ensure that the given new sensor is associated with the intended patient, the LEDs on the new sensor and the gateway sensor are required to blink in the same pattern. When seeing such synchronized pattern, the healthcare worker sends an explicit authorization message to the patient which will then include the new sensor. In the process, the sensor needs to perform decryption operations which are very time-consuming for resource constrained sensors. As a result, the protocol developed in this paper accelerates the process of secure sensor association.

TABLE 2
TIMES REQUIRED BY DIFFERENT OPERATIONS

Operation	Host	Time
System startup	Nurse	13.6 s
System startup	Patient	13.5 s
DH Parameters generation	Nurse	110 ms
Secret key generation	Nurse	828 ms
Secret key generation	Patient	310 ms
Signing message	Nurse	125 ms
Signing message	Patient	78 ms
Symmetric encryption	Nurse	311 ms
Symmetric encryption	Patient	328 ms
Symmetric decryption	Nurse	235 ms
Symmetric decryption	Patient	198 ms
Data encryption	Biosensor	150 μs
Data decryption	Biosensor	90 μs

VI. RELATED WORK

With the proliferation of wireless communication, miniaturized sensors, and portable devices, pervasive computing systems have increasingly been introduced to the healthcare industry [4, 5]. In this paper, we focus on a small scale personal body networks within an overall pervasive system. A few researchers have studied issues such as Quality of Service (QoS) [18] and interoperability of data communications between different body sensor networks [19].

Autonomic computing [6] is a promising paradigm to address the complexity of large scale computer networks and pervasive systems. It enables self-configuring, self-healing, self-optimising, and self-protecting of a complex system. In [20], a good survey discusses existing technologies to realize different degrees of autonomic computing. Policy based management is a very flexible approach to adapting autonomic strategy as it is divorced from mechanisms and can be easily changed at run-time.

As discussed previously, Amuse [3] is a management framework for pervasive healthcare systems. It proposes the self-managed cell as the architectural pattern that is applicable for systems at different scales. Vesta complements Amuse by providing a working system that integrates autonomic management and security mechanisms.

There have been a number of papers on security issues of pervasive healthcare systems. In [21], concerns on user privacy raised when mobile technologies are used to communicate with a body area network are identified. A method is proposed for device-to-device authentication where a pair of small devices want to communicate with each other over wireless networks but have no prior knowledge [22]. The idea is to make use of the similar acceleration data generated by simultaneous shaking. This method is convenient but relies on the existence of accelerometers. Moreover, it is still possible for active attackers to hack new devices.

In summary, although much progress have been made for autonomic management in the aspects of discovery and adaptation, little work has been done for secure discovery and access control that are suitable for resource-constrained pervasive systems in healthcare scenarios. Vesta fills this gap.

Digital Object Identifier: 10.4108/ICST.PERVASIVEHEALTH2009.5939
http://dx.doi.org/10.4108/ICST.PERVASIVEHEALTH2009.5939

VII. Conclusions and Future Work

In response to the increasing need for practical pervasive healthcare, this paper has presented a secure and autonomous system called Vesta that manages personal-area healthcare systems. Such pervasive systems are usually composed of various devices such as wireless biosensors. Vesta caters for the autonomous and adaptive requirements of these systems by extending the extensible SMC architectural pattern. It features a practical and easy-to-use secure discovery mechanism for wireless sensors. In addition, it implements a fine-grained access control mechanism by making use of authorization policies in Ponder2.

This paper focuses on implementation aspects of a secure healthcare system that is practical for real applications. The future work needs to integrate the BSN into an overall healthcare monitoring for logging and analyzing monitored information.

Acknowledgement

This research is supported in part by UK EPSRC BiosensorNet Grant EP/C547586/1, and by China 973 Program through Grant 2006CB303000.

References

[1] L. Schwiebert, S. Gupta, J. Weinmann, A. Salhieh, V. Shankar, V. Annamalai, M. Kochhal, and G. Auner, "Research Challenges in Wireless Networks of Biomedical Sensors," *Proc. ACM MobiCom*, 2001.

[2] G.-Z. Yang, "Body Sensor Network," Springer-Verlag, 2006.

[3] E. Lupu, N. Dulay, M. Sloman, J. Sventek, S. Heeps, S. Strowes, S. L. Keoh, A. Schaeffer-Filho, and K. Twidle, "AMUSE: Autonomic Management of Ubiquitous e-Health Systems," *Concurrency and Computation: Practice and Experience,* 2007.

[4] U. Varshney, "Pervasive Healthcare and Wireless Health Monitoring," *Mobile Networks and Applications (MONET),* vol. 12, pp. 113-127, 2007.

[5] U. Varshney, "Pervasive Healthcare," *IEEE Computer,* vol. 36, pp. 138-140, 2003.

[6] O. K. Jeffrey and M. C. David, "The Vision of Autonomic Computing," *Computer,* vol. 36, pp. 41-50, 2003.

[7] The Universal Plug and Play Forum, http://www.upnp.org/.

[8] Jini Network Technology at Sun Microsystem, http://www.sun.com/software/jini/.

[9] The Bluetooth Technology, http://www.bluetooth.com/.

[10] E. Guttman, C. Perkins, J. Veizades, and M. Day, "RFC2608 - Service Location Protocol, Version 2," 1999.

[11] The BSN Specification, http://ubimon.doc.ic.ac.uk/bsn/.

[12] S. Strowes, N. Badr, N. Dulay, S. Heeps, E. L. M. Sloman, and J. Sventek, "An Event Service Supporting Autonomic Management of Ubiquitous Systems for e-Health," *Proc. International Workshop on Distributed Event-Based Sytems*, 2006.

[13] Ponder2, http://www.ponder2.net/.

[14] G. Russello, C. Dong, and N. Dulay, "Authorisation and Conflict Resolution for Hierarchical Domains," *Proc. IEEE Policy*, 2007.

[15] ASUS EEE PC, http://eeepc.asus.com/.

[16] K. Chris, S. Naveen, and W. David, "TinySec: a Link Layer Security Architecture for Wireless Sensor Networks," *Proc. ACM SenSys*, 2004.

[17] S. L. Keoh, E. Lupu, and M. Sloman, "Securing Body Sensor Network: Sensor Association and Key Management," *Submitted for publication*, 2008.

[18] G. Zhou, J. Lu, C.-Y. Wan, M. Yarvis, and J. Stankovic, "BodyQoS: Adaptive and Radio-Agnostic QoS for Body Sensor Networks," *Proc. IEEE INFOCOM*, 2008.

[19] A. Triantafyllidis, V. Koutkias, I. Chouvarda, and N. Maglaveras, "An Open and Reconfigurable Wireless Sensor Network for Pervasive Health Monitoring," *Proc. International Conference on Pervasive Computing Technologies for Healthcare*, 2008.

[20] M. C. Huebscher and J. A. McCann, "A Survey of Autonomic Computing: Degrees, Models, and Applications," *ACM Computing Survey,* vol. 40, pp. 1-28, 2008.

[21] J. A. MacDonald, "Authentication Considerations for Mobile e-health Applications," *Proc. International Conference on Pervasive Computing Technologies for Healthcare*, 2008.

[22] R. Mayrhofer and H. Gellersen, "Shake Well Before Use: Authentication Based on Accelerometer Data," *Proc. International Conference on Pervasive Computing*, 2007.

Digital Object Identifier: 10.4108/ICST.PERVASIVEHEALTH2009.5939
http://dx.doi.org/10.4108/ICST.PERVASIVEHEALTH2009.5939