Securing Medical Sensor Network with HIP

Dmitriy Kuptsov[1,2], Boris Nechaev[1,2], and Andrei Gurtov[1,3]

[1] Helsinki Institute for Information Technology HIIT
[2] Department of Computer Science and Engineering, Aalto University
[3] Centre for Wireless Communications, University of Oulu
firstname.lastname@hiit.fi

Abstract. Recent developments of embedded wireless technologies, such as low-cost low-power wireless sensor platforms, uncovered big potential for novel applications. Health care and well-being are examples of two applications that can have large impact on society. Medical sensor networks via continuous monitoring of vital health parameters over a long period of time, can enable physicians to make more accurate diagnosis and provide better treatment. Such network allow emergency services to react fast to dangerous patient's conditions and perhaps save more lives. For such applications to become viable, their design has to consider fail-safe mode of operation, protection of sensitive user data, and especially provide solution for efficient access control. Given the specifics of these applications, in this work we identify communication pattern that will guarantee the most secure way to exchange medical data, propose a standard based security protocol enabling authentication and data protection, and introduce a mechanism for access control—a crucial building block in privacy sensitive applications. To validate our design we implement a prototype on a wireless sensor platform.

Keywords: medical sensor network, security, embedded wireless Internet, network architectures, energy consumption.

1 Introduction

With proliferation of advanced wireless sensor platforms they found numerous applications in medicine. The vast list of applications includes invasive and non-invasive monitoring of blood pressure, ECG, temperature, oxygen saturation, etc. Wireless medical sensors worn by patients can form a *medical sensor network* (MSN) accessible to medical personnel. The patients need not be at the hospital, monitoring can be done remotely with patients staying at home or traveling in a vehicle. Specifics of health care field impose several requirements on such networks: reliability, ease of deployment and maintenance, device mobility, security and privacy. Without underestimating importance of other requirements, one can argue that security and privacy are crucial for modern medical applications.

Medical ethics requires that all medical records are kept private. This lays strict security requirements on all hardware and software used for medical purposes. Not only data collection and transfer in an MSN must be kept private, but there should also be strict access control. Breaches in security may have grievous consequences: from leaks of

K.S. Nikita et al. (Eds.): MobiHealth 2011, LNICST 83, pp. 150–157, 2012.

personal medical records to fatal outcomes. Since life of a patient may depend on adequate doctor's response time to abnormal sensor readings, a malicious person may want to try to undermine timely transmission of sensor measurements or replace alarming readings with benignly looking ones, thus potentially putting patient's life in danger.

In this paper we propose a medical sensor network framework which focuses on security and privacy. We consider several usage scenarios described in detail in the next section, involving sensors having and lacking Internet connection, different locations of doctor and patient, etc. The framework is aimed at providing confidentiality of data transmission over insecure network, access control and user authorization including temporary role delegation, authenticity and integrity of communications between patients and medical personnel.

Our framework heavily relies on Host Identify Protocol (HIP) [1,2,3]—a protocol proposed to overcome the problem of using IP addresses both for host identification and routing. HIP defines a new cryptographic *Host Identity* name space, thereby splitting the double meaning of IP addresses. In HIP, Host Identities (HI) are used instead of IP addresses in the transport protocol headers for establishing connections. Prior to communication over HIP, two hosts must establish a HIP association. This process is known as HIP base exchange (BEX) [2] and it consists of four messages transferred between initiator (I) and responder (R). A successful BEX authenticates hosts to each other and generates a Diffie-Hellman shared secret key used in creation of two IPsec Encapsulated Security Payload (ESP) Security Associations (SAs), one for each direction. All subsequent traffic between communicating nodes is encrypted by IPsec.

The task of designing a medical sensor network was already explored by other researchers. In [4] the authors propose a system which allows post cardiac surgery patients to be monitored remotely. In their system ECG signals collected from patients staying at home are uploaded to a server and automatically analyzed for possible arrhythmia. [5] and [6] describe medical sensors developed by the authors and routing, discovery and query protocols together forming an MSN. Neither of the above projects are concerned with security. [7] proposes a security scheme relying on Elliptic Curve Cryptography (ECC) which only focuses on protecting communication between sensors and a base station. In [8] authors go further and define access control for secure pervasive health care systems. The work in [9], which is the closest to ours, proposes a new protocol for communication between all parties in MSNs. Our solution is different from all the above in considering various realistic communication modes and proposing more general solution which covers all essential aspects of secure medical applications. Another advantage of our approach is in using a standardized protocol (HIP) which is more reliable, versatile and flexible than ad-hoc custom solutions.

The rest of the paper is structured as follows. In Section 2 we outline communication model, assumptions and requirements for our system. Section 3 describes our protocol in detail. Feasibility evaluation of our system is discussed in Section 4. Finally, Section 5 concludes the paper.

2 Model and Requirements

Our system for medical monitoring comprises several key components: (a) **Personal Area Network (PAN)** which includes multiple low-power **medical sensors** placed on

or implanted into a patient's body and performing long-term reading of vital health parameters (e.g., blood pressure, pulse, etc.) and a single **on-body gateway** serving as a full-functional node for medical sensors and which has two wireless interfaces (one short range wireless interface, e.g., 802.15.4 for maintaining connection with medical sensors, and one long-range wireless interface, e.g., UMTS or 802.11, for maintaining Internet connection); (b) a **trusted authority (TA)** which is a node trusted by all other nodes belonging to the system and responsible for managing identities, revocation statuses, and access rights; (c) a **backend server** responsible for storing collected patient's sensor readings (a PAN gateway when connected to the Internet always establishes a secure channel to a backend server and uploads sensor readings to it periodically); and (d) a **backend terminal** with a graphical interface used by accredited personnel (this does not necessary need to be only patient's doctor, but may include any emergency services such as paramedics or police, having various access rights for reading patient's data); a backend terminal can retrieve patients' sensor readings from backend service, or accept readings directly from the gateway node after establishing security association with the sensor. The last is needed in emergency situations when no Internet connection is available.

In our medical application we consider the following communication patterns. Initially, medical sensors and patient's gateway node should establish a long term security association, or perform **initial pairing**. In its basic form this is achieved with a HIP handshake between a medical sensor node and the gateway. However, mutual authentication between two nodes can differ and depends on how the protocol is configured (we discuss two alternatives in Section 3). No node, other than the patient's gateway, can have a security association with medical sensors. Depending on the logic implemented, gateway node may perform various sophisticated tasks with sensor readings, such as preprocessing, adaptations, anomaly detection analysis, etc. However, the basic and most important functionality is: (a) ability to establish **security associations** with either backend service or directly with a backend terminal; (b) enforce **access control** with or without TA being online. Furthermore, an entity that belongs to the system—patient's gateway, backend service, or backend terminal—can access TA when it is online (meaning that there exist a communication channel between accessing node and TA) and either check certificate status or ask for a new certificate.

Next we discuss the requirements we impose on our system. Medical sensor nodes performing long-term health parameters reading will have a **limited processing power** and very **limited battery capacity**. Therefore, such nodes should be stressed with cryptography as little as possible and should not perform any sophisticated tasks with data processing. We thus require that medical sensor nodes perform HIP handshake only once during initial pairing to produce a symmetric keys common to a particular sensor and gateway and store such keys permanently for the entire time of sensor operation.

All monitored patient's data that is transmitted between medical sensor nodes, gateway, backend service or backend terminal should be encrypted to ensure **privacy**. This data should also be labeled with authentication information to ensure **data authenticity** and prevent forgery attacks on patient's data. However, we don't discuss how the data should be stored on a backend server or handled by backend terminals, since it is out of scope of this work.

Finally, we require that strong **access control** mechanisms are implemented and deployed on medical sensor nodes and gateway to prevent unauthorized access to sensitive information.

3 Architecture

Next we present the architecture description which is based on the model specified in Section 2. Specifically, in this section we will describe in detail the following operational phases and components: (i) initial medical sensor to gateway pairing, (ii) gateway to backend service pairing, (iii) backend terminal to gateway pairing, and (iv) access control mechanism. We present general architecture view in Figure 1.

Sensor to Gateway Pairing. When PAN is being deployed for the first time, e.g. when a new patient receives wearable sensors at the hospital, it requires bootstrapping of security associations between all sensors and a gateway. In our application this operational phase is called *initial pairing*.

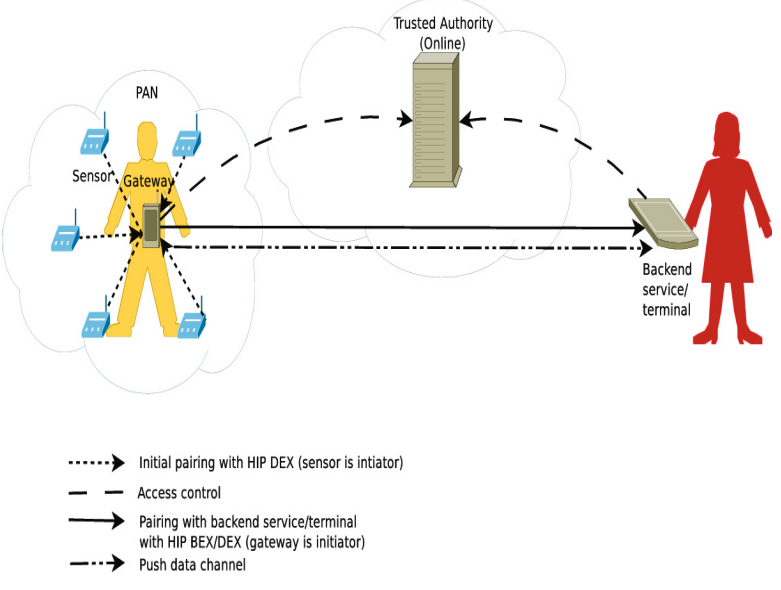

Fig. 1. System architecture

Initial pairing resembles HIP DEX [10]—a HIP handshake protocol which is a variant of HIP BEX [2]—where the public key is fixed and no signature algorithms are used. These two key differences allow HIP DEX to perform better than HIP BEX, and a lot better than SSL or its variants, thus making it a perfect solution for securing communication between low-powered medical sensors. In our architecture HIP DEX between medical sensors and a gateway is running directly on a MAC layer which allows to

save space (indeed this is can be implemented as a variant of 6lowpan to allow header compression and save space). Because HIP DEX does not use signature algorithms, and certificates are not suitable for medical sensors due to limited processing power, and 128 bytes frame size in 802.15.4 radio which is too small to fit a certificate, a two factor authentication process is required to guarantee secure sensor to gateway communication. We suggest several possible ways to achieve this goal.

First, and the most simple approach is to use the link button scheme: prior to initiating HIP DEX a special button should be pressed on a gateway node to allow HIP instance to accept any unknown I1 packets for a short time interval (e.g., of 5-10 seconds). Once the button was pressed medical sensor can be turned on and send its I1 packet. The second approach is considered to be more secure, because it does not leave any opportunity window for an attacker who is in range of patient's 802.15.4 radio. This idea is based on HIP DEX ability to perform mutual authentication with passwords, i.e., HIP DEX allows to perform a challenge-response type authentication. The usage of this feature requires the passwords to be configured externally from HIP. We foresee that the password selection on medical sensor nodes will be implemented in several alternative ways. One way is to implement it as jumpers, or switches, and with a graphical user interface on the gateway. Another way to configure the passwords on sensor and gateway in a secure way is to exchange it via a visual channel [11]. The idea is simple, yet elegant and secure: After boot up the sensor generates a random password of arbitrary length, and conveys the bits to the gateway using series of blinks of a light-emitting diode (LED). Indeed the blinks represent a frequency modulated signal. The gateway in turn captures the blinks using camera and demodulates the signal and reconstructs the password. For the latter two cases above, after the password is stored in the memory (on both, sensor and gateway), the sensor node triggers HIP DEX with gateway (both use the password for mutual authentication).

Irrespectively of what type of authentication is used, the pairing procedure should be repeated for all sensors that will participate in a particular PAN. Moreover, the secret key produced after HIP DEX completion will be stored permanently in hardware on the sensor node and gateway. This will allow to reuse the keys even if the sensor nodes or the gateway reboots, or turn on after battery replacement. However, since the entropy of the secret key is used up every time a new packet is encrypted and sent out, it is preferable that the initial pairing is repeated every now and then, for instance once per month. The advantage of our initial pairing over simple presharing of keys is that it allows to pair nodes from different vendors, which is a necessary feature for commercial products.

Gateway to Backend Service Pairing. The default security rule installed on the gateway node does not allow any communication to be accepted from the Internet, including HIP packets. As such, after completing the initial pairing a gateway will attempt to connect to the backend service by establishing a security association with an instance of HIP BEX protocol. The key difference from the initial pairing is that certificates are mandatory in such pairing. Moreover, both gateway and backend service should exchange their certificates to perform mutual authentication. Detailed description on format and usage of certificates in HIP BEX can be found in [12]. Below we will further discuss how secure access control can be implemented with certificates. Another

difference is that instead of sending I1 packet directly to a backend service the gateway sends it to rendezvous server first (who's location is known to the gateway), which redirects it to a proper backend server. More information on HIP rendezvous mechanism can be found in [13].

Backend Terminal to Gateway Pairing. Another communication pattern can be needed when Internet connection is not available and someone from emergency personnel tries to retrieve critical readings from the patient's sensor nodes. Such situation can occur, for instance, when the patient is transported from home in a rural area to a hospital. As we have mentioned earlier, the security rules on the gateway are configured so that the amount of traffic arriving on UMTS or 802.11 interfaces is limited to avoid denial of service attacks. To make this scenario work flawlessly, the gateway after establishing a connection on a physical layer with a 802.11 access point placed e.g. inside the ambulance, will trigger HIP BEX with certificates similarly to gateway to backend server pairing case. Though the key difference from the previous scenario here is that the gateway will broadcast I1 packet with null value used for destination HIT. This fallback mechanism will allow any backend terminal that receives such an I1 packet to reply with R1 packet. Despite that the destination HIT would be a null value, responder still should include a mandatory certificate in R1 packet which will allow the gateway to enforce access control rules that we discuss next.

Access Control. An important aspect of medical sensor network application is an ability to provide means for nodes to enforce access control by roles, cancel previously granted access rights by revoking issued certificates, and in certain cases to provide anonymous identity to the certificate holder. Due to space limitations we will merely discuss certificate revocation status verification procedure and role-based access control enforcement implemented on a gateway node.

If the certificate was revoked from the system, its further usage should be prohibited. If the nodes, especially gateways, do not have an ability to verify the status of the certificate there is a chance that an intended attacker can receive access to confidential information. Since the TA in our case is not guaranteed to be online all the time, the gateway may not have the ability to verify the status of the received certificate. To combat this, in our system every entity is granted two certificates: (i) *permanent membership certificate (PMC)* which a node receives when it joins the network for the first time (such certificate can for instance be installed on the node by TA) and (ii) *on-demand short term certificates (OSTC)* are granted by TA for a short period of time (e.g., an hour or a day) based on the status of PMC of the node. Consequently, a gateway node will receive HIP BEX packets if and only if such packets contain a valid OSTC certificate. On the other hand, it is responsibility of a particular node to request the next OSTC certificate in a timely manner. For instance, before an ambulance departures to the patient's premises, the backend terminal should be supplied with a valid OSTC certificate based on the PMC certificate permanently installed on the same terminal.

Once the revocation mechanism is in place the gateway can verify OSTC certificate and do a role-based access control to sensor node reading. Each gateway is configured with a set of roles and corresponding access rules for each role. For example, the gateway node may have rules that allow the role "public service" to read only basic

identification information, and rules that allow to read all available information to roles ”physician” and ”paramedic”.

4 Evaluation

In this section we present measurement results for cryptographic primitives that impact the performance of our medical WSN architecture. Table 1 contains key characteristics of one of the most basic operations in our network—HIP handshake. In our experiments we used Imote2 sensor node.

In Table 1 we consider two network types: PAN of the patient, which includes communication between sensors and the gateway, and Internet, when collected data is transmitted from the gateway to a doctor’s machine or a central server. PAN communication should be much lighter than Internet communication due to computational and energy constraints of embedded devices. HIP allows to use DEX instead of BEX mode for this and tune handshake procedure by using a shorter key, disabling signatures, certificates and puzzle, and using a different MAC algorithm. This allows the total size of packets transmitted during DEX handshake to be much smaller than in BEX, also making it considerably faster and less energy demanding.

Table 1. Resource consumption per HIP handshake

Protocol components	**Network types**		
	PAN	Internet	
	ECC HIP DEX	HIP BEX ECC	HIP BEX
Key exchange	Fixed ECDH	ECDH	DH
	160 bit	160 bit	1536 bit
Signatures	None	ECDSA	RSA
Certification method	None	ECDSA	RSA
Puzzle difficulty	0	≥ 10	≥ 10
MAC	CMAC (AES-CBC)	SHA-1	SHA-1
Message sizes (bytes)			
I1	40	40	40
R1	92	916	1544
I2	148	944	1568
R2	102	108	188
	DEX Duration (ms)	**BEX Duration (ms)**	
	72.396	151.26	1115.96
Energy (mj)			
For Initiator (I)	17.0	53.8	471.5
For Responder (R)	17.0	34.1	222.5
Total w/ transmission, I	26.14	73.74	560.1
Total w/ transmission, R	26.14	61.19	443.1

5 Conclusion

In this paper we proposed a secure architecture for medical sensor networks. Our approach is based on the standardized HIP protocol. We considered several use case scenarios of accessing sensor data: when trusted authority used for user authentication is available and when authentication has to be done by the PAN gateway. We achieve this using a 2-tiered certificate infrastructure which involves issuing permanent and short-term certificates. After authentication is complete, the gateway is able to perform

role-based access control to determine what information should the requesting entity be allowed to access. In order to assess feasibility of the proposed architecture we implemented and deployed it on Imote2 sensors, which also allowed us to measure main characteristics of HIP handshake in various scenarios.

References

1. Moskowitz, R., Nikander, P.: Host Identity Protocol architecture. IETF RFC 4423 (May 2006)
2. Moskowitz, R., Nikander, P., Jokela, P., Henderson, T.: Experimental Host Identity Protocol (HIP). IETF RFC 5201 (April 2008)
3. Gurtov, A.: Host Identity Protocol (HIP): Towards the Secure Mobile Internet. Wiley and Sons (2008)
4. Kyriacou, E., Chimonidou, P., Pattichis, C., Lambrinou, E., Barberis, V.I., Georghiou, G.P.: Post Cardiac Surgery Home-Monitoring System. In: Lin, J. (ed.) MobiHealth 2010. LNICST, vol. 55, pp. 61–68. Springer, Heidelberg (2011)
5. Shnayder, V., Chen, B., Lorincz, K., Fulford, J., Welsh, M.: Sensor networks for medical care. In: Proceedings of the 3rd International Conference on Embedded Networked Sensor Systems, SenSys 2005 (November 2005)
6. Shnayder, V., Chen, B., Lorincz, K., Fulford, J., Welsh, M.: Sensor networks for medical care. Harvard University Technical Report TR-08-05 (April 2005)
7. Malasri, K., Wang, L.: Design and implementation of a secure wireless mote-based medical sensor network. In: Proceedings of the 10th International Conference on Ubiquitous Computing, UbiComp 2008, pp. 172–181 (2008)
8. Venkatasubramanian, K., Gupta, S.K.S.: Security solutions for pervasive healthcare. In: Xiao, Y. (ed.) Security in Distributed, Grid, Mobile, and Pervasive Computing, pp. 443–464. Auerbach Publications, CRC Press (April 2007)
9. Garcia-Morchon, O., Flack, T., Heer, T., Wehrle, K.: Security for pervasive medical sensor networks. In: MobiQuitous 2009: Proc. of the 6th Annual International Conference on Mobile and Ubiquitous Systems. ICST/IEEE (July 2009)
10. Moskowitz, R.: HIP Diet EXchange (DEX): draft-moskowitz-hip-rg-dex-05 (March 2011), Expires in September 2011(work in progress)
11. Saxena, N., Ekberg, J.-E., Kostiainen, K., Asokan, N.: Secure device pairing based on a visual channel: Design and usability study. IEEE Transactions on Information Forensics and Security 6, 28–38 (2011)
12. Heer, T., Varjonen, S.: HIP Certificates: draft-ietf-hip-cert-12 (March 2011) (work in progress)
13. Laganier, J., Eggert, L.: Host Identity Protocol (HIP) rendezvous extension. IETF RFC 5204 (March 2008)