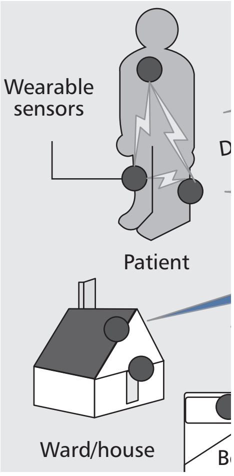
WIRELESS TECHNOLOGIES FOR E-HEALTHCARE

DATA SECURITY AND PRIVACY IN WIRELESS BODY AREA NETWORKS

MING LI AND WENJING LOU, WORCESTER POLYTECHNIC INSTITUTE
KUI REN, ILLINOIS INSTITUTE OF TECHNOLOGY



The authors look into two important data security issues, namely secure and dependable distributed data storage and fine-grained distributed data access control for the sensitive and private patient medical data.

ABSTRACT

The wireless body area network has emerged as a new technology for e-healthcare that allows the data of a patient's vital body parameters and movements to be collected by small wearable or implantable sensors and communicated using short-range wireless communication techniques. WBAN has shown great potential in improving healthcare quality, and thus has found a wide range of applications from ubiquitous health monitoring and computer assisted rehabilitation to emergency medical response systems. The security and privacy protection of the data collected from a WBAN, either while stored inside the WBAN or during their transmission outside of the WBAN, is a major unsolved concern, with challenges coming from stringent resource constraints of WBAN devices, and the high demand for both security/privacy and practicality/usability. In this article we look into two important data security issues: secure and dependable distributed data storage, and fine-grained distributed data access control for sensitive and private patient medical data. We discuss various practical issues that need to be taken into account while fulfilling the security and privacy requirements. Relevant solutions in sensor networks and WBANs are surveyed, and their applicability is analyzed.

INTRODUCTION

Recently, with the rapid development in wearable medical sensors and wireless communication, wireless body area networks (WBANs) have emerged as a promising technique that will revolutionalize the way of seeking healthcare [1–3], which is often termed *e-healthcare*. Instead of being measured face-to-face, with WBANs patients' health-related parameters can be monitored remotely, continuously, and in real time, and then processed and transferred to medical databases. This medical information is shared among and accessed by various users such as healthcare staff, researchers, government agencies, and insurance companies. In this way healthcare processes, such as clinical diagnosis and emergency medical response, will be facilitated and expedited, thereby greatly increase the efficiency of healthcare.

Based on the WBAN, a wide range of novel applications are enabled, such as ubiquitous health monitoring (UHM), computer-assisted rehabilitation, emergency medical response system (EMRS), and even promoting healthy living styles. Specifically, in UHM the WBAN frees people from visiting the hospital frequently, and eases the heavy dependence on a specialized workforce in healthcare. Thus, it is a desirable technique to quickly build cost-effective healthcare systems, especially for countries that are short of medical infrastructure and well trained staff. In addition, in an EMRS temporary WBANs can be rapidly deployed with minimum human effort at a disaster scene so that the vital signs of injured patients can be monitored and reported to the remote health center in time, which is potentially capable of saving the lives of numerous people.

Next, we show the general architecture of a WBAN in Fig. 1. The WBAN mainly consists of tiny wireless sensor nodes that are placed in, on, or around a patient's body. These sensors consistently monitor the patient's vital signs, such as electrocardiogram (ECG), pulse, and blood pressure; or important environmental parameters like temperature and humidity. The sensor monitor readings, patient profile, and so on together are called patient-related data. The sensors collect and transmit the patient-related data to one or more local servers (or gateways), which may perform further data processing, aggregation, or distributed storage. The patient-related data from all WBANs may ultimately be sent to a centralized healthcare database for permanent records. Thus, the users of patient-related data can either remotely access the data from the database or query information locally from the WBAN, depending on the application scenario.

Since the patient-related data stored in the WBAN plays a critical role in medical diagnosis and treatment, it is essential to ensure the security of these data. Failure to obtain authentic and correct medical data will possibly prevent a patient from being treated effectively, or even lead to wrong treatments. In reality, patient-

1536-1284/10/$25.00 © 2010 IEEE

The security and privacy of patient-related data are two indispensable components for the system security of the WBAN. By data security, we mean the data is securely stored and transferred; and data privacy means the data can only be accessed by the people who have authorization to view and use it.

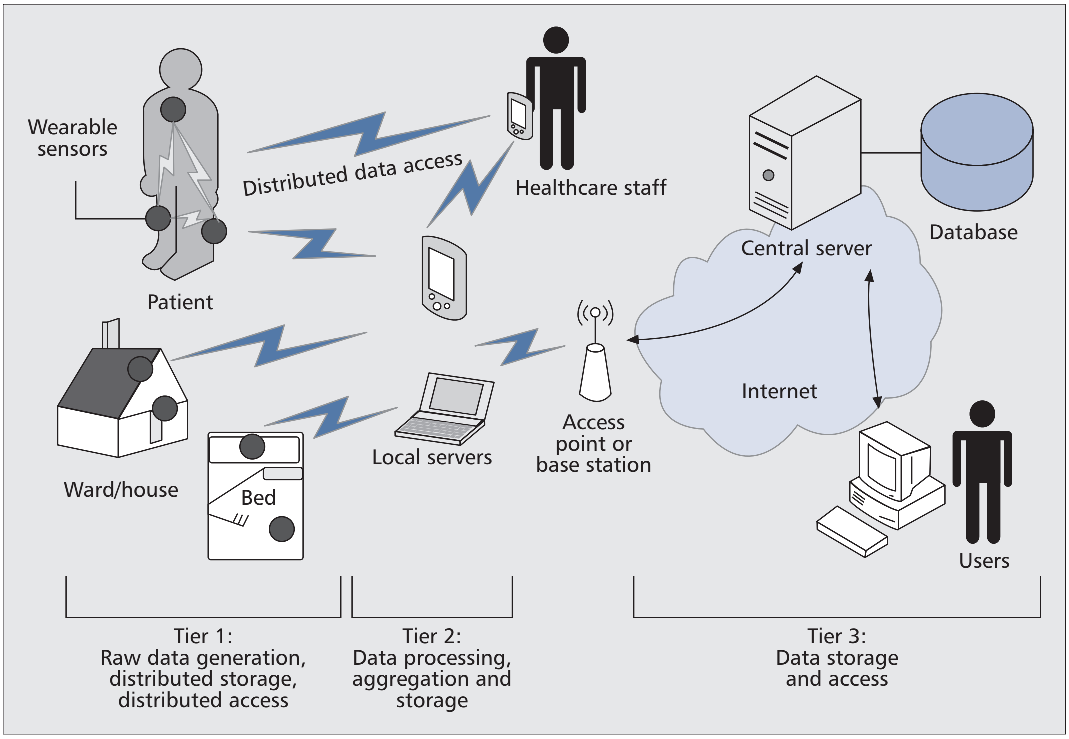

Wearable sensors
Patient
Distributed data access
Healthcare staff
Central server
Database
Ward/house
Bed
Local servers
Access point or base station
Internet
Users
Tier 1: Raw data generation, distributed storage, distributed access
Tier 2: Data processing, aggregation and storage
Tier 3: Data storage and access

Figure 1. *A general architecture of the WBAN, which consists of tier 1 and tier 2. The collected data is either stored in the WBAN for distributed, local access, or transferred from the WBAN to medical databases in tier 3 for centralized, remote access. The users of the patient-related data of the WBAN may include patients, doctors, nurses, support staff, scientists, and insurance companies.*

related data is often stored in a distributive manner; the open and dynamic nature of the WBAN makes the data prone to being lost. Therefore, it is equally important to protect patient-related data against malicious modification and to ensure its dependability (i.e., having it readily retrievable even under node failure).

Meanwhile, we must address various privacy concerns that may hinder wide public acceptance of WBAN technology. Especially access to patient-related data must be strictly limited only to authorized users; otherwise, the patients' privacy could be abused. As a governmental initiative, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) [4] has specified a set of mandatory privacy rules to protect sensitive personal identifiable health information. However, in WBANs distributively stored private data may easily be leaked due to physical compromise of a node. Therefore, data encryption and cryptographically enforced access control is needed to protect the privacy of patients.

To design data security and privacy mechanisms for WBANs, there are a number of challenges one must overcome, including how to make tough balances between security, efficiency, and practicality. Stringent resource constraints on devices within a WBAN, especially the sensor nodes, basically require the security mechanisms to be as lightweight as possible. Practical issues, such as conflicts between security, safety, and usability, also need to be considered carefully. For example, in order to ensure legitimate access to patients' data under time-sensitive scenarios such as emergency care, the access control mechanisms should be context-aware and flexible.

So far, although there are already several prototype implementations of WBANs, studies on data security and privacy issues are few, and existing solutions are far from mature. For example, in the CodeBlue project [3] a medical monitoring sensor network is developed for pre-hospital care and emergency response. To cope with the dynamic environment of emergency response, an elliptic curve cryptography (ECC)-based public key encryption scheme is used for authentication. However, there are no further mechanisms to protect the security of the stored data and control access to it.

In this article we identify the requirements of data security and privacy in WBAN. In particular, we point out the necessity of secure and dependable distributed data storage, and fine-grained distributed data access control. Then we analyze the challenging practical issues underlying these problems. Next, we explore the solution space by surveying related work in both wireless sensor networks and WBANs. We compare these solutions and analyze their suitability for WBANs, and suggest potential future directions.

Requirements for Data Security and Privacy in WBANs

The security and privacy of patient-related data are two indispensable components for the system security of the WBAN. By data security, we mean data is securely stored and transferred;

and data privacy means the data can only be accessed by the people who have authorization to view and use it. In the following we show the security requirements.

APPLICATION SCENARIO

We exemplify the security needs in WBANs by a distributed healthcare application scenario.

Suppose Peter is injured when traveling far away from his hometown. At first, the emergency paramedic reads Peter's implanted RFID tag to obtain his profile and medical records, and a WBAN consisting of wearable medical sensors is established and associated with Peter. Later, various healthcare workers can directly access the vital sign readings from the WBAN in real time, in order to provide better medical care. For instance, a nurse inquires on Peter's health status from his WBAN and uploads an electronic report to the local server in Peter's room.

Peter's PDA has been configured with an initial access policy (AP) that controls who has access to his medical data within his WBAN. The AP automatically adapts to contexts, such as accommodating the reception staff, doctor, and nurse. Peter can also modify the AP at his own will; for example, his sensitive AIDS record is only allowed to be shared with his nurses but not doctors.

Note that medical data is often stored and accessed distributively. Different types of monitoring data may be stored in different sensor nodes; before Peter arrives at a place with wireless Internet coverage, those data can only be stored locally in his WBAN. Direct local access to cached data in Peter's WBAN and local servers allows freshly generated data to be viewed immediately without delay to facilitate in-time diagnosis.

Here, a natural question is how to ensure the security of the distributively stored patient-related data from its storage through transfer to access. Before we discuss the security of distributed data storage and access, we first analyze the threats faced by the distributively stored data in the WBAN.

THREATS FACED BY THE DATA STORED WITHIN WBAN

The WBAN often operates in environments with open access by various people (e.g., hospital staff), which also accommodates attackers. The open wireless channel makes the data prone to being eavesdropped, modified, and injected. These threats have already been extensively analyzed in the literature. Since in this article we mainly focus on data storage and access, we illustrate the threats from the device point of view.

Threats from device compromise: The sensor nodes in a WBAN are subjected to compromise, as they are usually easy to capture and not tamper-proof. If a whole piece of data is directly encrypted and stored in a node along with its encryption key, the compromise of this node will lead to the disclosure of data.

Also, local servers may not be trustworthy, since there are malicious people trying to break into them to obtain patients' privacy information. They can either carry out the attack from the Internet, or simply go to the room where a patient is and wait for the chance to physically compromise a local server.

Threats from network dynamics: The WBAN is highly dynamic in nature. Due to accidental failure or malicious activities, nodes may join or leave the network frequently. Nodes may die out due to lack of power. Attackers may easily place faked sensors in order to masquerade authentic ones, and could take away legitimate nodes deliberately. The patient-related data, if not well kept in more than one node, could be lost easily due to the network dynamics. Also, false data could be injected or treated as legitimate due to lack of authentication.

REQUIREMENTS FOR DISTRIBUTED DATA STORAGE SECURITY

Confidentiality: In order to prevent patient-related data from leaking during storage periods, the data needs to always be kept confidential at a node or local server. Data confidentiality should be resilient to device compromise attacks; that is, compromising one node helps the attacker to gain nothing or little from the data stored at that node or elsewhere.

Dynamic integrity assurance: In WBANs the patient-related data is vital, and modified data would lead to disastrous consequences. Thus, data integrity shall be dynamically protected all the time. In particular, we shall be able to not only detect modification of data at end users, but also check and detect that during storage periods, in order to discover potential malicious modification in advance and alert the user.

Dependability: Dependability is another critical concern in WBANs, because failure to retrieve correct data may become a life-threatening matter. In order to tackle the threats caused by network dynamics, fault tolerance is required, that is, having patient-related data readily retrievable even under Byzantine node failure or malicious modifications.

REQUIREMENTS FOR DISTRIBUTED DATA ACCESS SECURITY

Fine-grained data access control: Access control needs to be enforced for patient-related data in WBANs so that private information will not be obtained by unauthorized parties. In the application scenario we described Peter's medical data may be viewed by doctors, support staff, pharmacies, and other agencies to enhance their services. However, if an insurance company sees Peter's disease report, it might discriminate against Peter by offering health insurance at a high premium. Therefore, a fine-grained access policy must be defined to specify and enforce different access privileges for different users. Fine-grained refers to the small granularity of the data access policy, which distinguishes among each part of the patient-related data and each user role. For example, "doctors are only allowed to view the medical data of those patients they are treating, but not that of other patients," or "personal identifiable information such as

In order to prevent the patient-related data from leaking during storage periods, the data needs to be always kept confidential at a node or local server. The data confidentiality should be resilient to device compromise attacks.

Major security requirements	Description
Data storage security requirements	
Confidentiality	Patient-related data should be kept confidential during storage periods. Especially, its confidentiality should be robust against node compromise and user collusion.
Dynamical integrity assurance	Patient-related data must not be modified illegally during storage periods, which shall be checked and detected by a node dynamically.
Dependability	Patient-related data must be readily retrievable when node failure or data erasure happens.
Data access security requirements	
Access control (privacy)	A fine-grained data access policy shall be enforced to prevent unauthorized access to patient-related data generated by the WBAN.
Accountability	When a user of the WBAN abuses his/her privilege to carry out unauthorized actions on patient-related data, he/she should be identified and held accountable.
Revocability	The privileges of WBAN users or nodes should be deprived in time if they are identified as compromised or behave maliciously.
Non-repudiation	The origin of a piece of patient-related data cannot be denied by the source that generated it.
Other requirements	
Authentication	The sender of the patient-related data must be authenticated, and injection of data from outside the WBAN should be prevented.
Availability	The patient-related data should be accessible even under denial-of-service (DoS) attacks.

Table 1. *Major security requirements for data security and privacy in WBAN.*

patient profile shall not be disclosed to insurance companies."

Scalability: Since there are numerous users of patient-related data, the distributed access control mechanism should be scalable with the number of users in the following aspects:

- Having low management overhead of the access policies, which shall be set up and modified easily
- Having low computation and storage overhead

This will be further illustrated in the next section.

Flexibility: A basic requirement is that the patient himself should have the flexibility to designate APs for his data according to his own will. More important, we shall allow the APs to adapt dynamically to contexts, such as time, location, or certain events related to patients. For example, on-demand authorization to read Peter's monitoring data can be given temporarily to an available doctor who is not on the allowed list when a medical emergency happens. Inability or irresponsiveness in adapting the access rules may threaten a patient's safety.

Accountability, revocability, and non-repudiation: These are additional security requirements and are summarized in Table 1.

The Need for Authentication in Data Security

Authentication is a necessary security service to prevent false data injection and DoS attacks, and is also required to verify a user's identity before data access. Moreover, it is needed to secure data transfer within the WBAN. Since authentication is not the main focus in this article, we only mention it when necessary.

Challenging Practical Issues

To satisfy the above requirements in WBAN, we face several important challenging issues, most of which arise from efficiency and practicality aspects. These issues constrain the solution space, and need to be considered carefully when designing mechanisms for data security and privacy in WBANs.

Conflict between security and efficiency: High efficiency is strongly demanded for data security in WBANs, not only because of the resource constraints, but also for the applications. Wearable sensors are often extremely small and have insufficient power supplies, which render them inferior in computation and storage capabilities. Thus, the cryptographic primitives used by the sensor nodes should be as lightweight as possible, in terms of both fast computation and low storage overhead. Otherwise, the power and storage space of the nodes could be drained quickly. In addition, a DoS attack could easily overwhelm the whole WBAN if the authentication protocol is not fast enough.

Conflict between security and safety: Whether the data can be accessed whenever needed could be a matter of patients' safety [2]. Too strict and inflexible data access control may prevent the medical information being accessed in time by legitimate medical staff, especially in emergency scenarios where the patient may be unconscious and unable to respond. On the other hand, a loose access control scheme opens back doors to malicious attackers. It is hard to ensure strong data security and privacy while allowing flexible access. In CodeBlue [3], when there is network coverage, stronger user authentication is achieved by contacting an authority; when no infrastructure exists such as during disaster response, weaker or no authentication is adopted. Their approach can be regarded as the first step towards addressing the conflict between security and safety.

Conflict between security and usability: The devices should be easy to use and foolproof, since their operators might be non-expert patients. As the setup and control process of the data security mechanisms are patient-related, they shall involve few and intuitive human interactions. For instance, to bootstrap initial secure communication between all the nodes in a WBAN for secure data communication, device pairing techniques can be adopted. However, directly applying device pairing requires $O(N^2)$ human interactions, which is obviously not easy to use. However, increasing usability by omitting some manual steps may not be good for security. As another example, for Peter to give access to his data to an emergency medical staff person who was not originally authorized, it is better to have some second-factor authentication mechanisms.

Requirement for device interoperability: Patients may buy sensor nodes from different manufacturers, among which it is difficult to pre-share any cryptographic materials. It is difficult to establish data security mechanisms that require the least common settings and efforts, and work with a wide range of devices.

Solutions for Data Security and Privacy in WBANs

In this section we investigate the solution space for data storage and access security in WBANs. We organize the section by surveying a few existing related works, discussing whether they can satisfy the previously mentioned requirements and how they address the related practical issues. Meanwhile, we mention some new cryptographic techniques, which may yield better solutions.

Secure and Dependable Distributed Data Storage

Data confidentiality, dependability, and integrity are the three most important requirements for distributed data storage in WBANs. In order to enhance the dependability of the data, error correcting code techniques can be employed to provide redundancy. Chessa *et al*. [5] proposed a secure distributed data storage and sharing scheme for mobile wireless networks, based on the Redundant Residue Number System (RRNS). In RRNS, an integer that could be represented by its residues on a set of h moduli is represented by $h + r$ moduli, where the extra r moduli are redundant. In Chessa's scheme a source node S distributes a file F among n other nodes. S randomly picks $n = h + r$ moduli, computes F's residue vector, and distributes each file share to a different storage node. An authorized node needs to collect enough residues from the storage nodes in order to recover the original file.

Chessa's scheme enhances dependability because the RRNS can tolerate up to $s \le r$ data share erasures and up to

$$\left\lfloor \frac{r-s}{2} \right\rfloor$$

corruptions, and data can be reconstructed using any h of the remaining correct shares. For the same reason, resistance to compromise of up to h nodes is achieved. To provide confidentiality, the data shares are encrypted by the public keys of authorized storage nodes. However, data integrity is not ensured whenever the number of errors is more than the detecting capability. And to distribute public keys to sensor nodes is not a good choice for interoperability. As to efficiency, the length expansion ratio is $(h + r)/h$ for each file. But to maintain a potentially large set of moduli would overwhelm a sensor node's buffer, which is not efficient for WBANs.

In WBANs a node should be able to dynamically check the integrity of the data shares in other nodes before the user retrieves them. Simply using message authentication codes incurs large storage overhead. Recently, Wang *et al*. [6] proposed a secure and dependable distributed data storage scheme. The initial data storage breaks the original encrypted data into n data shares, where each of them consists of a data block generated from (n, k)-erasure coding, and a share of the secret key using (n, k)-secret sharing. Then the data shares are distributed to n neighbor nodes for storage. For a node to do dynamic integrity check, each other storage node computes and broadcasts an *algebraic signature* on one data share, so the checking node can verify the integrity by checking the signature of the other nodes against its own. In this way any data modification will be detected in time.

In Wang's scheme data confidentiality, dependability, and dynamic integrity assurance are achieved simultaneously. It is also shown to be fairly efficient, since only SKC and algebraic signature are used. The signature size is small, and computation and storage overhead are low. A drawback is that it does not allow a third party to carry out integrity checks. This could be inconvenient in WBANs, since we would also want the local server to verify the integrity of the data upon collecting them.

Sometimes, a stronger form of dependability, data survivability, must be achieved, since a more powerful attacker may aim at intentionally destroying/erasing valuable medical data (e.g., vital sign readings) in WBANs. Pietro *et al*. [7] addressed the data survival problem in wireless sensor networks. The attacker is assumed to be aware of the origins of the target data, and can compromise a subset of sensor nodes in each round. The basic defense idea is to move the data from one sensor node to another constantly so that it is harder for the adversary to "catch"

Data confidentiality, dependability, and integrity are three most important requirements for distributed data storage in WBAN. In order to enhance the dependability of the data, error-correcting code techniques can be employed to provide redundancy.

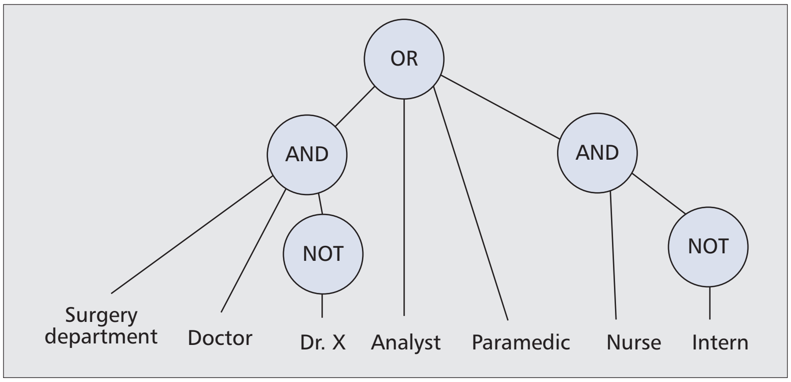


Figure 2. *A sample AP for the vital sign data from a patient's WBAN. The non-leaf nodes stand for the logic gates, while the leaf nodes are user roles or identities.*

the data item. It is shown that constantly moving data around outperforms keeping data in one place or moving only once, in terms of data survival probability. In addition, data replication and encryption are also employed. However, the above techniques incur high communication and storage overhead, which makes it less practical in energy-constrained WBANs.

Although the secure and dependable distributed data storage in WBAN is necessary, it has not gained enough attention up to now. This can be partly ascribed to the conflict between security and efficiency, such as dealing with the small storage space of wearable sensor nodes. However, within most hospital e-health applications where many WBANs and local servers coexist, temporarily storing a window of newly generated medical data in different types of local devices is necessary and possible.

Fine-Grained Distributed Data Access Control

Fine-grained distributed access control is another important security service in e-healthcare, since unauthorized access may compromise patients' privacy. With efficiency, scalability, and flexibility in mind, the variety of users' roles and the potentially complex access rules make fine-grained distributed data access control a complicated problem. Typically, an AP looks like Fig. 2, which interprets as "allow access by a doctor from surgery department but not Dr. X, or an analyst or a paramedic, or a nurse who is not intern."

In a WBAN access rights to patient-related data are often granted to users based on their professional roles. On a high level, this corresponds to the Role-Based Access Control (RBAC) model [8]. It defines the user-role and role-privilege mappings in a decoupled fashion. It is scalable, since a role may encompass a large group of users. Fine-grainedness can be achieved through designating the users' roles appropriately.

In order to achieve flexibility and enhance data accessibility, the context-aware access control model incorporates the system context factor, which dynamically adjusts the access policies across time, space or event. Also, researchers have proposed criticality-aware access control (CAAC) [8] that proactively modifies the access rules to quickly response to medical emergency conditions.

However, the above mentioned access control models do not specify how to achieve cryptographically enforced data access, which is an important component in data privacy. In particular, two requirements shall be satisfied:

- Support complex access policies
- Resistant to user collusion and node compromise attacks

These attacks should not help to obtain any useful information about the keys of other nodes/users or the data stored at those nodes.

SKC-Based Schemes — SKC seems to be an efficient choice for distributed access control in WBANs. A solution is proposed by Morchon *et al*. [9], which utilizes Blundo's key predistribution scheme to support RBAC. By predistributing polynomial key shares, the patient can easily establish a pairwise key with any authorized entity, and encrypt a copy of his/her data using this key for that entity. Although the patient can exert individual control over the entities' access rights, the patient would need to know the exact set of authorized users when distributing a file, and to encrypt one copy for each user in the set, which is impractical.

In general, SKC based approaches suffer from three main disadvantages:

- Fine-grained access control is hard to realize due to the high key management complexity.
- They are vulnerable to user collusion.
- Compromising a node will possibly expose the data, since if a node cannot store encrypted copies for all possible users, it must store the data in plaintext.

It is desirable that the data remain encrypted even when stored in WBAN nodes or servers. In order to achieve both fine-grained access control and efficiency, it is more desirable to encrypt *once and for all* (i.e., encrypt the file once so that all the authorized users can have access).

PKC-Based Schemes — We introduce Attribute-Based Encryption (ABE), an effective primitive to achieve fine-grained access control [10]. ABE is a one-to-many encryption method, where the ciphertext is meant to be readable only by a group of users that satisfy a certain AP. ABE is collusion-resistant; that is, any set of colluding users will not be able to derive any key belonging to other users. Its expressiveness on the AP makes it a good candidate for fine-grained data access control in WBANs.

Ciphertext Policy ABE (CP-ABE) [10] perfectly matches the model of RBAC. Each user is assigned a set of attributes (roles), and a patient can freely choose a set of users/roles that are allowed to gain access to his/her medical data, from which the AP is derived. Whenever a node in the WBAN generates some data, the AP is built into the ciphertext. The key idea of CP-ABE is to split a secret among secret key components belonging to different attributes owned by a user, which are randomized so as to provide collusion resistance. CP-ABE supports a tree-like access policy structure, which is expressive, and it is fairly easy to integrate context related parameters as attributes, such as the time.

Device	Processor/Microcontroller unit	Pairing time (milliseconds)	ECC point multiplication time (milliseconds)
PC	1 GHz Pentium III	20	≈1
PDA	32 bit 624 MHz Intel Bulverde technology based RISC processor	550	85*
Sensor node	8 bit 8 MHz ATMega128L	1551 (with optimized field multiplication)	7450 (optimized)

*: The result is cited from 160 bit TinyECC implemented on Imote2 with a 416 MHz processor, and with no optimizations.

Table 2. *Comparison of time for pairing and point multiplication operations on different hardware platforms [13].*

Accountability and revocability: Accountability is needed for data access in WBAN, especially when a user illegally abuses his/her access privileges, such as gives the key to unauthorized users. Yu *et al*. studied this attack in [11] and proposed a technique to defend against it. The *pirate device* is tricked to decrypt a value that is encrypted under its ID, which will not succeed.

For revocation after identifying a malicious user, the simplest method is to renew every other user's secret key upon revoking one user. However, this may be inefficient when the number of users is large. Yu *et al*. proposed a broadcast-based revocation scheme in wireless sensor networks [12], where key updates are done using only one broadcast message.

The efficiency of ABE: The CP-ABE scheme in [10] requires about 2*m* exponentiations (ECC point multiplications) for encryption, where *m* is the number of attributes included in the AP. For decryption, it uses about 2*l* pairings, where *l* is the number of attributes of the decryptor that match the AP. In order to see its efficiency, we give a rough comparison between computation times on different devices in Table 2.

It is shown that implementing CP-ABE on the sensor nodes may not be a good choice, since one point multiplication and pairing operation takes seconds. The PC is far better than sensor nodes, while the PDA is moderately better. Approximately, when the number of attributes is less than 10, it takes several seconds to do ABE encryption and decryption on a PDA. Considering the architecture of a WBAN, it is feasible to encrypt the data at local servers like PDAs or desktop computers. To do so, the sensor nodes can send their data to the local servers for further encryption for access control, and use symmetric encryption to secure the data transfer between sensors and local servers.

Anonymity in Access Control — Beyond the above PKC-based schemes, patients' privacy information may still be leaked from the access policies, from which patients' or users' identities might be inferred. Therefore, it is desirable to be anonymous. Recently, Nishide *et al*. proposed two constructions of CP-ABE with a partially hidden access policy [14]. They achieve recipient anonymity by hiding which subset of attributes is specified in the AP. However, their complexities are high, which limits the applicability to WBANs.

In another work Zhang *et al*. [15] proposed an anonymous distributed access control scheme, which is suitable for the type of users who obtain valued tokens from the health center before accessing data in the WBAN. Blind signature is used to achieve user anonymity. However, this scheme is not fine-grained, since each anonymous user has the same access rights.

Discussion — Summarizing the above, we can see that the ABE-based access control method is more capable than other techniques of achieving all the security requirements. It is fine-grained, context-aware, revocable, and efficient to implement on local servers.

However, the above mentioned schemes have not satisfactorily addressed the security-safety conflict. Since it is important to allow on-demand access policy adaptations during emergency healthcare, a future direction is to design more flexible, cryptographic enforced, and attribute-based access control schemes for WBANs.

Concluding Remarks

The WBAN is an emerging and promising technology that will change people's healthcare experiences revolutionarily. Data security and privacy in WBANs and WBAN-related e-healthcare systems is an important area, and there still remain a number of considerable challenges to overcome. The research in this area is still in its infancy now, but we believe it will draw an enormous amount of interest in coming years. We hope this article will inspire novel and practical designs of secure, dependable, and privacy-enhanced WBANs.

Acknowledgment

This work was supported in part by the U.S. National Science Foundation under grants CNS-0831628, CNS-0716306, CNS-0746977, and CNS-0831963.

References

[1] E. Jovanov *et al*., "A Wireless Body Area Network of Intelligent Motion Sensors for Computer Assisted Physical Rehabilitation," *J. NeuroEng. Rehab.*, vol. 2, no. 6, Mar. 2005.

[2] D. Halperin *et al*., "Security and Privacy for Implantable Medical Devices," *IEEE Pervasive Comp.*, vol. 7, no. 1, Jan. 2008, pp. 30–39.

[3] K. Lorincz *et al*., "Sensor Networks for Emergency Response: Challenges and Opportunities," *IEEE Pervasive Comp.*, vol. 3, no. 4, Oct.–Dec. 2004, pp. 16–23.

[4] The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule; http://www.hhs.gov/ocr/privacy/

[5] S. Chessa and P. Maestrini, "Dependable and Secure Data Storage and Retrieval in Mobile, Wireless Networks," *Int'l. Conf. Dependable Sys. Net.*, June 2003, pp. 207–16.

[6] Q. Wang *et al.*, "Dependable and Secure Sensor Data Storage with Dynamic Integrity Assurance," *Proc. IEEE INFOCOM '09*, Apr. 2009.

[7] R. Di Pietro *et al.*, "Catch Me (If You Can): Data Survival in Unattended Sensor Networks," *Proc. IEEE PerCom*, Mar. 2008, pp. 185–94.

[8] K. K. Venkatasubramanian and S. K. S. Gupta, "Security Solutions for Pervasive Healthcare," in *Security in Distributed, Grid, Mobile, and Pervasive Computing*, Y. Xiao, Ed., Auerbach, 2007, pp. 443–64.

[9] O. G. Morchon and H. Baldus, "Efficient Distributed Security for Wireless Medical Sensor Networks," *Int'l. Conf. Intelligent Sensors, Sensor Net., Info. Processing*, Dec. 2008, pp. 249–54.

[10] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," *Proc. IEEE Symp. Security and Privacy*, May 2007.

[11] S. Yu *et al.*, "Defending against Key Abuse Attacks in KP-ABE Enabled Broadcast Systems," *SecureComm 2009*, Sept. 2009.

[12] S. Yu, K. Ren, and W. Lou, "FDAC: Toward Fine-grained Distributed Data Access Control in Wireless Sensor Networks," *IEEE INFOCOM '09*, Apr. 2009.

[13] A. Ramachandran, Z. Zhou, and D. Huang, "Computing Cryptographic Algorithms in Portable and Embedded Devices," *IEEE PORTABLE '07*, May 2007, pp.1–7.

[14] T. Nishide, K.Yoneyama and K. Ohta, "Attribute-Based Encryption with Partially Hidden Encryptor-Specified Access Structures," *Proc. LNCS Applied Cryptography Net. Security*, May 2008, pp. 111–29.

[15] R. Zhang, Y. Zhang, and K. Ren, "DP2AC: Distributed Privacy-Preserving Access Control in Sensor Networks," *Proc. IEEE INFOCOM '09*, Apr. 2009.

Biographies

Ming Li (mingli@ece.wpi.edu) received his B.E and M.E degrees from Beihang University, China, in 2005 and 2008, respectively. He is currently a Ph.D. student in the Electrical and Computer Engineering department at Worcester Polytechnic Institute, Massachusetts. His current research interests are in the area of wireless networks and pervasive computing, with emphases on network and system security.

Wenjing Lou (wjlou@ece.wpi.edu) earned a B.E. and an M.E. in computer science and engineering at Xi'an Jiaotong University, China, an M.A.Sc. in computer communications at Nanyang Technological University, Singapore, and a Ph.D. in electrical and computer engineering at the University of Florida. She joined the Electrical and Computer Engineering Department at Worcester Polytechnic Institute as an assistant professor in 2003, where she is now an associate professor. Her current research interests are in the areas of ad hoc, sensor, and mesh networks, with emphases on network security and routing issues. She was a recipient of the U.S. National Science Foundation Faculty Early Career Development (CAREER) award in 2008.

Kui Ren [M] (kren@ece.iit.edu) is an assistant professor in the Electrical and Computer Engineering Department at Illinois Institute of Technology. He obtained his Ph.D. degree in electrical and computer engineering from Worcester Polytechnic Institute in 2007. He received his B.Eng. and M.Eng. from Zhejiang University in 1998 and 2001, respectively. His research interests include network security and privacy and applied cryptography, with the current focus on security and privacy in cloud computing, lower-layer attack and defense mechanisms for wireless networks, e-healthcare, and sensor network security. His research is sponsored by the U.S. National Science Foundation. He is a member of ACM.