Security Issues in Biomedical Wireless Sensor Networks

Tassos Dimitriou, Krontiris Ioannis

Athens Information Technology, 19002 Peania, Athens, Greece

{tdim,ikro}@ait.edu.gr

Abstract—Within the hospital or extended care environment, there is an overwhelming need for constant monitoring of vital body functions and support for patient mobility. Tomorrow's biomedical networks will address these needs by incorporating new technologies like wireless sensor networks into their infrastructure. However, wireless transmission of sensitive patient data presents some obvious security concerns. In this paper we discuss these concerns and how they are addressed by existing systems. We also discuss issues that need further consideration, such as run-time composition of security services depending on the criticality of data transmitted along with a solution for practical sensor systems using TinyOS. Finally, we propose intrusion detection as a future research direction for biomedical sensor networks and we elaborate on the main components of such a system.

I. INTRODUCTION

The pervasive interconnection of autonomous and wireless sensor devices has given birth to a broad class of exciting new applications in several areas of our lives, with health care being one of the most important and rapidly growing one. The emergence of low-power, single-chip radios has allowed the design of small, wearable, truly networked medical sensors. These tiny sensors on each patient can form an ad hoc network, relaying continuous vital sign data to multiple receiving devices, like PDAs carried by physicians, or laptop base stations in ambulances [1].

The benefit of using wireless sensors in health care is twofold: First, they allow monitoring of the patient at home, so that the elderly or patients with chronic diseases can enjoy treatment and medical monitoring in their own environment. Second, they substantially increase the efficiency of treatments inside the hospital environment. Today biomedical sensors are wired, attaching patients to machines, in order to read different values of vital data. The implementation of a more flexible wireless technology can lead to improved data quality, data resolution and increase of patient's mobility outside the surgery room. This results in enhanced decision making for diagnostics, observation and patient treatment.

Despite the increased range of these potential applications, the gap between the security requirements that they pose and the existing WSN security mechanisms remains unresolved. Existing WSN research has focused on monitoring the physical environment. However, a biomedical sensor network has distinct features, like mobility of sensors and sensitive nature of data, which aggravate the security challenges. It is important in such networks that only authorized users can query or monitor the network and that medical data remain protected and uncorrupted.

Security and privacy in biomedical sensor networks has not been investigated in much depth before, and therefore, it provides ample avenues for research. In this paper we make an effort to identify open questions and see whether and how they are addressed by existing proposed systems. The rest of the paper is structured as follows: In Section II, we emphasize the security threats in a biomedical sensor networks while in Section III, we identify the requirements that a security solution has to offer. In Section IV, we review some popular architectures, and in Section V, we discuss the methods that they follow to offer security. Then, in Section VI, we describe how we can make link-layer security flexible enough to allow for different types of security services, depending on the criticality of health data. Finally, in Section VII, we argue that an intrusion detection system is necessary as an automated mechanism to identify possible sources of attack.

II. SECURITY THREATS

The particular threats that a biomedical sensor network has to face can be categorized into outsider and insider attacks. In an *outsider* attack (intruder node attack), the attacker node is not an authorized participant of the sensor network. Authentication and encryption techniques prevent such an attacker to gain any special access to the sensor network. The intruder node can only be used to launch passive attacks, like: (1) passive eavesdropping, where the attacker eavesdrops and records encrypted messages, which may then be analyzed in order to discover secret keys; (2) denial of service attacks, where an adversary attempts to disrupt the networks operation by broadcasting high-energy signals, jamming the communication between legitimate nodes; and (3) replay attacks, where the attacker captures messages exchanged between legitimate nodes and replays them in order to change the aggregation results.

Perhaps more dangerous from a security point of view is an *insider* attack, where an adversary by physically capturing a node and reading its memory, can obtain its key material and forge node messages. Having access to legitimate keys, the attacker can launch several kinds of attacks without easily being detected: (1) unauthorized access to health data; (2) false data injection, where the attacker injects false results, which are significantly different from the true health data determined by the biosensors; (3) selective reporting, where the attacker

stalls the reports of events by dropping legitimate packets that pass through the compromised node; and (4) alteration of health data of a patient, leading to incorrect diagnosis and treatment.

III. SECURITY REQUIREMENTS

Usually in biomedical sensor networks (BSN) there exists one or more base stations operating as data sinks and often as gateways to IP networks. In general, a base station is considered trustworthy, either because it is physically protected or because it has a tamper-resistant hardware. Concerning the rest of the network, we now discuss the standard security requirements (and eventually behavior) we would like to achieve by making the network secure.

- *Confidentiality*: In order to protect sensed data and communication exchanges between sensors nodes it is important to guarantee the secrecy of messages.
- *Integrity and Authentication*: Integrity and authentication is necessary to enable sensor nodes to detect modified, injected, or replayed packets.
- *Availability*: In many sensor network deployments, keeping the network available for its intended use is essential. Thus, attacks like denial-of-service (DoS) that aim at bringing down the network itself may have serious consequences to the health and well being of people.

While designing security mechanisms that address the above requirements, one has to keep in mind specific factors that differentiate BSNs from other types of sensor networks. These factors determine some extra requirements, as indicated below:

- Multiple users in different roles must be supported, each with different privacy interests and decision making power.
- Mobility of the patient must be supported, therefore security mechanisms should adapt quickly to dynamic topologies.
- Any security protocol must add a low communication overhead, since throughput is crucial for such networks. Medical data require high data rates, e.g. ECG data are normally sampled at 250 Hz and blood pressure at 100 Hz [1]. Since these signals are continuously monitored, the traffic in the network is already dense.

Let us emphasize that addressing these security requirements must be balanced against the computational, memory, and power constraints of the individual nodes. This means that computationally expensive algorithms like asymmetric cryptography cannot be applied here (or should be applied with care). Instead, symmetric encryption/decryption algorithms and hash functions constitute the basic tools for securing sensor network communications. However, symmetric key cryptography is not as versatile as public key cryptography, which complicates the design of secure applications.

IV. OVERVIEW OF WSNS IN HEALTH CARE

The architecture and design of biomedical sensor networks depend greatly on the specific application and deployment environment. In this section we review some of the latest developments in such networks, which we will use as examples in the rest of the paper to qualify and compare the security solutions that they offer.

CodeBlue [2] is a sensor network based medical research project being developed at Harvard. It is intended for deployment for pre-hospital and in-hospital emergency care, disaster response and stroke patient rehabilitation. The sensor nodes collect heart rate (HR), oxygen saturation (SpO2), and ECG data, which then is relayed over a short-range wireless network to any number of receiving devices, including PDAs, laptops, or ambulance-based terminals.

ALARM-NET [3] is a wireless sensor network that integrates physiological and environmental sensors in a heterogeneous architecture for pervasive, adaptive health care. A query protocol allows real-time collection and processing of sensor data for authorized care providers and analysis programs.

SNAP [4] is an architecture for medical sensor networks that focuses on security. Taken this approach, it does not address routing, mobility or congestion issues in the network. In the SNAP architecture, one or more wireless sensors are attached to each patient. The transmitted data are forwarded by a number of wireless relay nodes throughout the hospital area. These nodes are categorized into unlimited-powered and limited powered nodes.

Another interesting ongoing project is the biomedical wireless sensor network Nordic project BWSN that was developed, implemented and tested at the Norwegian National Hospital. The hardware platform used is Tmote Sky with integrated sensors, like invasive arterial blood pressure, ECG, epicardial accelerometer and a digital intrapleural drainage system. While the project focuses on wireless communication and data throughput optimization [5], it does not address security.

Finally, the WBAN group [6] is developing wearable health monitoring systems using off-the-shelf ZigBee wireless sensor platforms (Telos platforms from Moteiv), custom signal conditioning boards, and the TinyOS software environment. Sensor nodes are strategically placed on the users body and sample, process, and store information about users physiological signals.

V. SECURITY SOLUTIONS

Several security solutions have been proposed in protecting biomedical sensor network's link layer communication, which constitutes the bottom layer of the sensor network protocol stack. More attention has been given to robust and efficient key management schemes, which serve as the fundamental requirement in encryption and authentication. Here, we describe the main approaches followed by the architectures we mentioned in the previous section (see Table I) and evaluate them on their suitability for biomedical sensor networks.

A. TinySec

TinySec is proposed as a solution to achieve link-layer encryption and authentication of data in biomedical sensor networks [7]. TinySec [8] is a link-layer security architecture

System Architecture	Hardware Platform	Security Scheme
CodeBlue	Mica2	ECC & TinySec
ALARM-NET	Tmote Sky	Hardware Encryption
SNAP	Tmote Sky	TinyECC
BWSN	Tmote Sky	none
WBAN	Tmote Sky	Hardware Encryption

for wireless sensor networks that is part of the official TinyOS release. It generates secure packets by encrypting data packets using a group key shared among sensor nodes and calculating a MAC for the whole packet including the header.

TinySec by default relies on a single key manually programmed into the sensor nodes before deployment. This network-wide shared key provides only a baseline level of security. It cannot protect against node capture attacks. If an adversary compromises a single node or learns the secret key, she can gain access on the information anywhere in the network, as well as inject her own packets. This is probably the weakest point in TinySec, since, node capture has been proved to be a fairly easy process.

B. Hardware encryption

As an alternative to TinySec, one could utilize hardware encryption supported by the ChipCon 2420 ZigBee complaint RF Transceiver, one of the most popular radio chip on wireless sensor nodes. Based on AES encryption using 128-bit keys, the CC2420 can perform IEEE 802.15.4 MAC security operations, including counter (CTR) mode encryption and decryption, CBC-MAC authentication and CCM encryption plus authentication. It can also perform plain stand-alone encryption of 128 bit blocks [9].

The WBAN group, employed this method in their network infrastructure [6], where the personal server shares the encryption key with *all* of the sensors in the WBAN during the session initialization. Hardware encryption is also followed by ALARM-NET [3]. One limitation of the method is that it does not offer AES decryption, so transmitted information cannot be accessed by intermediate nodes if needed (e.g. for aggregation purposes). Any decryption can be performed only at the base station. Another drawback of the method is that it is highly dependent on the specific platform. Other sensor node hardware do not offer hardware encryption support, so a different approach has to be taken in this case.

C. Elliptic Curve Cryptography

Recently, elliptic curve cryptography (ECC) has emerged as a promising alternative to RSA-based algorithms, as the typical size of ECC keys is much sorter for the same level of security. There have been notable advances in ECC implementation for WSNs in recent years. Uhsadel et al. [10] propose an efficient implementation of ECC and Liu et al. developed TinyECC [11], an ECC library that provides elliptic curve arithmetic over prime fields and uses inline assembly code

to speed up critical operations on the ATmega128 processor. Also lately, Szczechowiak et al. presented NanoECC [12], which is relatively fast compared with other existing ECC implementations, although it requires a heavy amount of ROM and RAM sizes.

Even though elliptic curve cryptography is feasible on sensor nodes, its energy requirements are still orders of magnitude higher compared to that of symmetric cryptosystems. Therefore, elliptic curve cryptography would make more sense to be used only for infrequent but security-critical operations, like key establishment during the initial configuration of the sensor network [13], or code updates [14].

D. Biometric Methods

A key establishment method to secure communications in biomedical sensor networks has emerged to be biometrics [15]. It advocates the use of the body itself as a means of managing cryptographic keys for symmetric cryptography. For sensors attached on the same body, if they measure a previously agreed physiological value simultaneously and use this value to generate a pseudo-random number, this number will be the same. Then it can be used to encrypt and decrypt the symmetric key to distribute it securely.

The physiological value to be used should be chosen carefully, as it must exhibit proper time variance and randomness. In different case the whole scheme can be vulnerable to brute force attacks. For example, blood glucose, blood pressure or heart rate are not appropriate. On the other hand, ECG (electrocardiogram) has been shown to be appropriate [16]. However, an important requirement is to have accurate time synchronization, so that sensors take their measurements at the same time and produce the same value. To do that, a time synchronization protocol is needed, using reference broadcasts. Such protocols have been shown to be susceptible to attacks [17] and securing them will require even more of the mote's resources.

Another disadvantage of this method is that only biosensors in and on the body can measure biometrics, so it cannot be applied for securing the communication of other sensor nodes in the general architecture. Moreover, this method assumes that there is a specific pre-defined biometric that all biosensors can measure, which is not necessarily true.

VI. RUN-TIME COMPOSITION OF SECURITY SERVICES

In biomedical sensor networks the criticality of data transmitted varies, in contrast with other applications of sensor networks. For example, the monitoring of the physical activities of patients is less critical than the heart rate monitoring. Even more critical is sending an alarm in case the patient is in an emergency. Consequently, the threats are different in each case, requiring different security levels. The provision of such a service from the link-layer security protocol could lead to a better management of the node's resources and extent their lifetime.

To provide this flexibility on security policy based on message semantics or context, the following two main mechanisms are necessary.
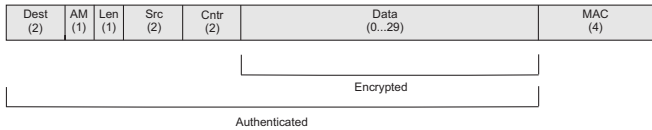
Dest (2)	AM (1)	Len (1)	Src (2)	Cntr (2)	Data (0...29)	MAC (4)

Encrypted

Authenticated

Fig. 1. L^3Sec packet format for full security service.

- A key management scheme that looks into the different ways to establish and distribute cryptographic keys among the different nodes in the sensor network, and
- A mechanism used to encrypt the important data (to provide data confidentiality) and to calculate the MAC (to provide data authenticity and data integrity) using the established cryptographic keys.

For the first part, let's assume the use of a key management scheme based on a post-deployment key derivation, like L^3Sec [18], [19]. Next we describe how it can be used to provide secure services to the higher levels. We propose a flexible scheme by using the most significant *three* bits of the data length field in the packet format as an indicator of the security service(s) to be used. These three bits are never used by TinyOS, as the maximum data length in TinyOS is chosen to be 29 bytes. Consequently, the provision of this feature comes with no overhead.

We can provide run-time composition of security services *without* removing the AM ID or adding extra fields to support integration of services. Each one of the higher three bits of data field of the packet stands for a security service (from higher order bit to the lower: Replay Attack Protection, Access Control and Integrity, Confidentiality) and setting *any* bit means that the related service is provided for that packet. Thus the desired services for different packets can be composed at runtime.

Depending on the desired mode of operation, the TinyOS packets should be modified to support the properties that we mentioned above. Figure 1 shows the fields included in the packet format in the full security mode.

The *Source* field of the packet is used to find the appropriate established pair-wise or broadcast key needed for the security services. Note that TinySec does not use the *Source* field when it is set to authentication only (TinySec-Auth) mode. This is because it assumes that if the attached MAC of a received message is valid then it comes from an authorized source (note that in TinySec the MAC is derived using a specific *global* key shared among all valid nodes, a bad security practice as we explained in Section V-A). However, this assumption is not necessary in other key management protocols, like L^3Sec, which use established keys in order to resist against node capture attacks. As a result, we must include the *Source* field in the packet format.

In other related service modes, such as replay attack protection mode, the packet format contains a counter (*Counter*). Together with the *Source* field, this 2 bytes long counter can be used to avoid *IV* reuse in *CBC* encryption mode. In L^3Sec, similar to TinySec, the *IV* includes the destination address, the

active message (AM) type, the data length, the source address and the counter. The $Source\|Counter$ format guarantees that each node can send 2^{16} messages with the same AM type and the same destination, but with different IV values. As mentioned, another application of the counter value is its role in providing resistance against replay attacks.

Finally, the most significant *three* bits of the data length field indicate the different major security modes that are provided. These include

1) Authentication, Access Control and Integrity (*A*). In this mode the *Counter* field is not required, but obviously the *MAC* field is needed.
2) Confidentiality (*C*). In this mode the *Source* and *Counter* fields are used in the packet format, however receiver nodes do not save the related counter values.
3) Replay Attack Protection (*R*). *Source* and *Counter* fields are also necessary in this mode, but the counter value of each neighbor is kept.

As we mentioned earlier, these modes can be combined in any variation setting the corresponding bits. Table II shows in more detail the different modes, provided services and the corresponding bit values.

TABLE II
OPERATIONAL MODES AND RELATED SETTINGS.

Mode	SetBits	Omitted Fields	Omitted Operations
"RAC"	111	-	-
"RA"	110	-	Encryption
"RC"	101	MAC	MAC
"R"	100	MAC	MAC & Encryption
"AC"	011	-	Counter Saving
"A"	010	Counter	Counter Saving & Encryption
"C"	001	MAC	Counter Saving & MAC
"-"	000	All Security Fields	All Security Operations

VII. INTRUSION DETECTION SYSTEM

Encryption and authentication mechanisms provide reasonable defense for mote-class outsider attacks. However, cryptography is inefficient in preventing against insider attacks. It remains an open problem for additional research and development. The presence of insiders significantly lessens the effectiveness of link layer security mechanisms. This is because an insider is allowed to participate in the network and have complete access to any messages routed through the network and is free to modify, suppress, or eavesdrop on the contents.

The last resort is intrusion detection, which can act as a second line of defense: it can *detect* third party break-in attempts, even if this particular attack has not been experienced before. If the intruder is detected soon enough, one can take appropriate measures before any damage is done or any data is compromised. Other researchers also reference intrusion detection as a solution for biomedical sensor networks [20], [21].

In intrusion detection, we wish to provide an automated mechanism that identifies the source of an attack and generates

an alarm to notify the network or the administrator, so that appropriate preventive actions can take place. However, intrusion detection for sensor networks needs to consider specific constraints imposed by the limited resources of sensor nodes. This along with the fact that any part of the sensor network can be a possible point of intrusion, indicate that an IDS architecture must be decentralized.

In [22], we present such an approach to organizing autonomous but cooperative IDS agents. Our approach organizes the cooperation of the agents according to the distributed nature of the events involved in the attacks, and, as a result, an agent needs to send information to other agents only when this information is necessary to detect the attack. The coordination mechanism arranges the message passing between the agents in such a way so that the distributed detection is equivalent to having all events processed in a central place.

Integrating such an IDS architecture in biomedical sensor networks first requires the identification of methods to characterize traffic routed inside the network. This will allow the IDS agents to raise an alert when an unusual pattern is noticed or certain rules are violated. Determining which methods fit better for health care system applications is an interesting research direction that we plan to explore further in the future.

VIII. CONCLUSIONS

Recent advances in the area of wireless sensor networks have enabled the idea of remote patient monitoring. In this paper we have discussed the security issues that arise when integrating this new technology into health care systems. The viability and long-term success of biomedical wireless sensor networks depends upon addressing these security threats successfully. We explored some of the existing solutions that can be employed and showed how run-time composition of security can be added to offer more flexible and energy efficient services. We also argued that intrusion detection is a necessary mechanism in order to minimize security risks and identify it as a promising future research direction in order to ensure integrity and reliability of the entire system.

REFERENCES

[1] V. Shnayder, B. Chen, K. Lorincz, T. Jones, and M. Welsh, "Sensor networks for medical care," in *SenSys '05: Proceedings of the 3rd International Conference on Embedded Networked Sensor Systems*, 2005.

[2] K. Lorincz, D. J. Malan, T. R. F. Fulford-Jones, A. Nawoj, A. Clavel, V. Shnayder, G. Mainland, M. Welsh, and S. Moulton, "Sensor networks for emergency response: Challenges and opportunities," *IEEE Pervasive Computing*, vol. 3, no. 4, pp. 16–23, 2004.

[3] A. Wood, G. Virone, T. Doan, Q. Cao, L. Selavo, Y. Wu, L. Fang, Z. He, S. Lin, and J. Stankovic, "ALARM-NET: Wireless sensor networks for assisted-living and residential monitoring," Department of Computer Science, University of Virginia, Tech. Rep. CS-2006-1, 2006.

[4] K. Malasri and L. Wang, "Addressing security in medical sensor networks," in *HealthNet '07: Proceedings of the 1st ACM SIGMOBILE international workshop on Systems and networking support for healthcare and assisted living environments*. ACM, 2007, pp. 7–12.

[5] S. Stoa, I. Balasingham, and T. A. Ramstad, "Data throughput optimization in the IEEE 802.15.4 medical sensor networks." in *IEEE International Symposium on Circuits and Systems*, 2007, pp. 1361–1364.

[6] S. Warren, J. Lebak, J. Yao, J. Creekmore, A. Milenkovic, and E. Jovanov, "Interoperability and security in wireless body area network infrastructures," in *Proceedings of the 27th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, 2005, pp. 3837–3840.

[7] S. S. Marci Meingast, Tanya Roosta, "Security and privacy issues with health care information technology," in *EMBS '06: Proceedings of the 28th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, August 2006, pp. 5453–5458.

[8] C. Karlof, N. Sastry, and D. Wagner, "TinySec: A link layer security architecture for wireless sensor networks," in *Second ACM Conference on Embedded Networked Sensor Systems (SenSys 2004)*, November 2004, pp. 162–175.

[9] M. Healy, T. Newe, and E. Lewis, "Efficiently securing data on a wireless sensor network," *Journal of Physics: Conference Series*, vol. 76, 2007.

[10] L. Uhsadel, A. Poschmann, and C. Paar, "Enabling Full-Size Public-Key Algorithms on 8-bit Sensor Nodes," in *Proceedings of European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS 2007)*, ser. LNCS, vol. 4572. Springer-Verlag, 2007, pp. 73–86.

[11] A. Liu and P. Ning, "TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks," *Proceedings of the International Conference on Information Processing in Sensor Networks (IPSN 2008)*, vol. 0, pp. 245–256, 2008.

[12] P. Szczechowiak, L. B. Oliveira, M. Scott, M. Collier, and R. Dahab, "NanoECC: Testing the limits of elliptic curve cryptography in sensor networks," in *Proceedings of the 5th European conference on Wireless Sensor Networks (EWSN)*, ser. Lecture Notes in Computer Science, vol. 4913. Springer, 2008, pp. 305–320.

[13] J. Großschädl, "TinySA: A security architecture for wireless sensor networks (extended abstract)," in *Proceedings of the 2nd International Conference on Emerging Networking Experiments and Technologies (CoNEXT 2006)*. ACM Press, 2006.

[14] I. Krontiris and T. Dimitriou, "Authenticated in-network programming for wireless sensor networks," in *Proceedings of the 5th International Conference on AD-HOC Networks & Wireless (ADHOC-NOW '06)*, 2006, pp. 390–403.

[15] S. Cherukuri, K. K. Venkatasubramanian, and S. K. S. Gupta, "BioSec: A biometric based approach for securing communication in wireless networks of biosensors implanted in the human body," in *Proceedings of the Workshop on Wireless Security and Privacy (WiSPr), International Conference on Parallel Processing Workshops*, 2003, pp. 432–439.

[16] F. M. Bui and D. Hatzinakos, "Biometric methods for secure communications in body sensor networks: resource-efficient key management and signal-level data scrambling," *EURASIP J. Adv. Signal Process*, vol. 8, no. 2, pp. 1–16, 2008.

[17] M. Manzo, T. Roosta, and S. Sastry, "Time synchronization attacks in sensor networks," in *SASN '05: Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*, 2005, pp. 107–116.

[18] H. Soroush, M. Salajegheh, and T. Dimitriou, "Providing transparent security services to sensor networks," in *ICC'07: Proceedings of the IEEE International Conference on Communications*, Glasgow, Scotland, June 2007.

[19] I. Krontiris, T. Dimitriou, H. Soroush, and M. Salajegheh, *Wireless Sensors Networks Security*. IOS Press, 2008, ch. WSN Link-layer Security Frameworks, pp. 142–163.

[20] A. Giani, T. Roosta, and S. Sastry, "Integrity checker for wireless sensor networks in health care applications," in *Proceedings of the 2nd International Conference on Pervasive Computing Technologies for Healthcare*, January 2008.

[21] H. S. Ng, M. L. Sim, and C. M. Tan, "Security issues of wireless sensor networks in healthcare applications," *BT Technology Journal*, vol. 24, no. 2, pp. 138–144, 2006.

[22] I. Krontiris, T. Dimitriou, and T. Giannetsos, "LIDeA: A distributed lightweight intrusion detection architecture for sensor networks," in *Proceeding of the fourth International Conference on Security and Privacy for Communication (SECURECOMM '08)*, September 2008.