Computer Networks 140 (2018) 138–151

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Anonymous hybrid mutual authentication and key agreement scheme for wireless body area network

Aneesh M. Koya*, Deepthi P. P.

Department of Electronics and Communication Engineering, National Institute of Technology, Calicut, Kerala, India

ARTICLE INFO

Article history:
Received 27 November 2017
Revised 19 April 2018
Accepted 12 May 2018

Keywords:
WBAN
Mutual authentication
Anonymity
Key agreement
Biokey
AVISPA

ABSTRACT

Wireless body area networks (WBANs) play a significant role in remote health monitoring as a key application of the Internet of Things (IoT). Mutual authentication and key agreement are vital for the security and privacy of health information involved in the WBAN. Li et al. proposed a lightweight authentication and key agreement scheme for the sensor nodes in WBAN. Their authentication and key agreement scheme protects against various existing attacks. But on detailed analysis, we could find that their scheme is prone to sensor node impersonation attack. Also, security of their scheme relies on the assumption that the hub node is trustworthy, which is practically infeasible. Hence, we propose a hybrid anonymous authentication and key agreement scheme using the physiological signal to overcome the shortcomings in Li et al.'s scheme. The proposed scheme also provides additional security features to resist hub node impersonation attack and key escrow problem. Burrows-Abadi-Needham (BAN) logic is used to prove the correctness of the proposed scheme and the Automated Validation of Internet Security Protocols and Applications (AVISPA) is used to evaluate the security of the proposed scheme.

© 2018 Elsevier B.V. All rights reserved.

1. Introduction

With the fast advancement of Internet of Things (IoT) technology, the impact of wireless body area network (WBAN) in providing improved healthcare service is gaining active attention among the research community. WBAN systems are crucial in driving developments in the field of healthcare, as they provide the basis for information-based diagnosis and treatment of various diseases. However, the vast adoption and deployment of WBANs are hindered due to the concern in security and privacy [1,2] of life-critical medical records and health information. Recent papers [3–5] dealing with the authentication of WSN in IoT environments are propelling the research community to design and implement lightweight authentication and key agreement scheme that can be extended to IoT based WBAN.

The architecture of a typical WBAN system is shown in Fig. 1. WBAN consists of miniature sensor nodes in, on or around the body that facilitate the monitoring of physiological signals such as electrocardiogram (ECG), electroencephalogram (EEG), photoplethysmogram (PPG), electromyogram (EMG), blood pressure, and body temperature. The sensor nodes can be either implanted or wearable. The sensor nodes are connected to the off-body hub via an on-body super node. The super node [6,7] has more computation, communication, sensing, and storage capacity than the other sensor nodes in the network. The hub node/controller node collects the physiological information from the super node and forwards them to the service provider via public networks. The network topology is shown in Fig. 2. The first tier corresponds to the connection between the sensor nodes and the super node. The second tier represents the connection between the super node and the hub node/controller node. In the third tier, the hub node is connected to the medical service provider or the system administrator.

In contrast to the wireless sensor networks (WSN) [8], WBAN has severe resource constraints that pose additional open challenges in designing an efficient scheme for authentication and key agreement [9]. Given the low computational capabilities of a WBAN sensor node, implementation of traditional security solutions for authentication and key agreement is often infeasible. Hence, there is a need to develop lightweight and low-cost techniques for implementing anonymous mutual authentication and efficient key agreement scheme in WBAN.

Most of the key exchange schemes based on hard cryptographic problems in the literature [10,11] are characterized by high processing requirements, high computation costs, and lack of anonymity. In IEEE 802.15.6 standard [12] for WBAN, five elliptic curve (EC) based security association protocols are defined to secure the communication between sensor nodes and the hub

* Corresponding author.
E-mail addresses: aneeshkoya@gmail.com (A.M. Koya), deepthi@nitc.ac.in (D. P. P.).

https://doi.org/10.1016/j.comnet.2018.05.006
1389-1286/© 2018 Elsevier B.V. All rights reserved.

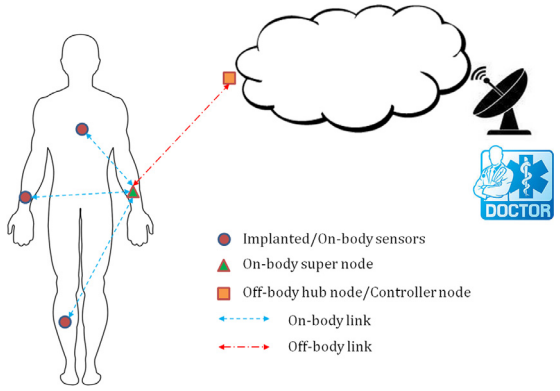

Fig. 1. Architecture of a typical WBAN system.

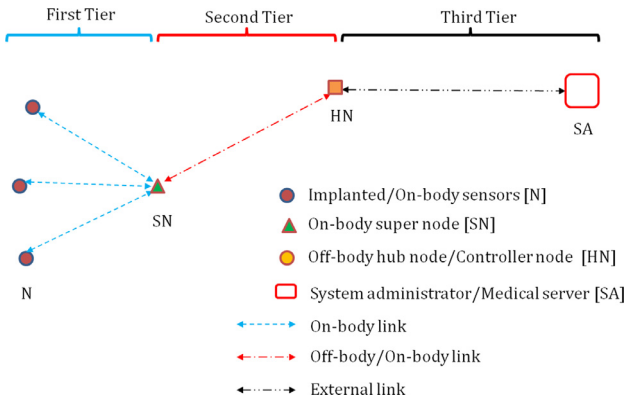

Fig. 2. Network topology.

node. However, Toorani [13] performed a security analysis of IEEE 802.15.6 standard and found that the protocols have severe security problems. Ibrahim et al. [14] put forward an anonymous mutual authentication and key agreement protocol using simple cryptographic primitives such as hash function and XOR operation. However, it is prone to sensor node impersonation attack, key escrow problem, hub node impersonation attack, and jamming attack. The scheme in [7] discusses three protocols for achieving anonymous authentication in inter-WBAN (second tier) communication and beyond WBAN (third tier) communication. The protocol 3 in [7] deals with the authentication between super node and controller node (hub node). Their authentication phase involves only hash invocations and XOR operations giving rise to a computationally low complex scheme as in [14].

Li et al. [6] presented an anonymous mutual authentication and key agreement scheme in WBAN with more security functionalities than the protocol in [14]. The scheme is lightweight and provides anonymity and unlinkable sessions for the sensor nodes. Their authentication and key agreement scheme protects against various existing attacks such as eavesdropping attack, replay attack, hub node spoofing attack, hub node stolen database attack, ephemeral secret key leakage attack, man-in-the-middle attack, and jamming attack. They have shown that their protocol is energy efficient and has lower computational cost than the other existing protocols. However, we found that their protocol is prone to sensor node impersonation attack, key escrow problem and their assumption that the hub node must be trustworthy is unrealistic. In this paper, we propose a hybrid authentication and key agreement scheme using the physiological signal to overcome these shortcomings.

Three factors that are commonly considered in the literature for user authentication are password [15,16] or personal identification number (PIN), smart card [17,18] or hand-held token and biometrics [19–21]. Researchers have also come up with several multi-factor authentication schemes [5,22]. As far as resource constrained WBAN is concerned, biometric is readily accessible to the body sensor nodes, and it cannot be impersonated, lost or forgotten. The generation of a secret key using physiological signal [23,24] was first presented by Poon et al. [25]. The physiological parameters captured by the sensor nodes can be employed to generate entity identifiers (biometrics) for authenticating the nodes and securing the communication links in a WBAN system. The authentication using static biometrics is feasible only if the physiological features used to generate the identifiers exhibit a high permanence. However, it has got two limitations. (i) The static biometric cannot be replaced if it is stolen. (ii) the features may change significantly or become unavailable during physiological data recording. Therefore, the most secure biometric is dynamic biometrics that exhibits low permanence.

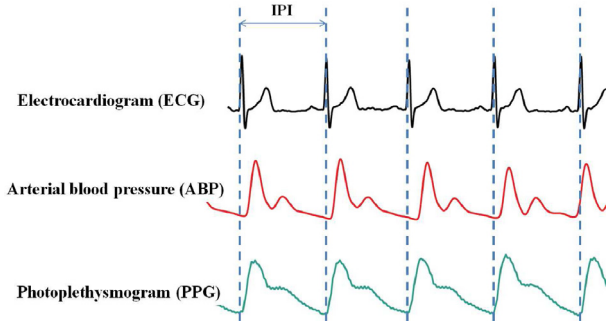

Fig. 3. Interpulse interval (IPI).

In the literature, several dynamic biometrics [26] such as body temperature, blood-glucose, and cardiac signals have been suggested. A promising dynamic biometric candidate for facilitating authentication and key agreement is the cardiac inter-pulse interval (IPI) which is defined as the time interval between consecutive heartbeats. IPI can be measured from various physiological signals related to cardiac system namely, electrocardiogram (ECG), photoplethysmogram (PPG), blood pressure (BP), and heart sounds as shown in Fig. 3.

Related work [27–29] reports that only the in-body and on-body sensors can detect the heartbeats and that the concatenated IPI data may be used to generate a unique and random binary identifier. The randomness of the binary sequence generated using IPIs lie in the least significant bits of adequately quantized individual IPI data. To increase the entropy and security that can be achieved from IPIs, Bao et al. [29] have proposed the multi-interpulse interval (mIPI) for the generation of binary entity identifiers. Seepers et al. [30,31] have confirmed with their experiments that increase in entropy per mIPI will not improve security. In order to enhance the security, they presented two dynamic cardiac biometric (DCB) generators (i) using inter-multipulse interval (ImPI) feature and (ii) using a von Neumann (vN) extractor. They analyzed that the ImPI is more suitable for DCB generation than the vN extractor. ImPI is the time interval between j consecutive heartbeats. IPI can be considered as ImPI with $j = 1$. The time required for binary sequence generation using ImPI is j times compared to that using IPI. Therefore, depending on the session key renewal rate, either IPI or ImPI is used for generating random binary sequences.

The major obstacle in the acceptability of physiological signal based authentication and key agreement scheme is its vulnerability towards denial-of-service attack. This vulnerability is due to the difference in the synchronously measured physiological signal from the same signal source by different sensor nodes. For a 128-bit IPI sequence generated at a particular time instant, the Hamming distance between the IPI sequences derived by the sensor nodes of

Download English Version:

https://daneshyari.com/en/article/6882650

Download Persian Version:

https://daneshyari.com/article/6882650

Daneshyari.com