Future Generation Computer Systems 82 (2018) 727–737

Contents lists available at ScienceDirect

Future Generation Computer Systems

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

A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks

Fan Wu [a], Xiong Li [b],*, Arun Kumar Sangaiah [c], Lili Xu [d], Saru Kumari [e], Liuxi Wu [a], Jian Shen [f]

[a] Department of Computer Science and Engineering, Xiamen Institute of Technology, Xiamen 361021, China
[b] School of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan, 411201, China
[c] School of Computer Science and Engineering, VIT University, Vellore-632014, Tamil Nadu, India
[d] School of Information Science and Technology, Xiamen University, Xiamen 361005, China
[e] Department of Mathematics, Chaudhary Charan Singh University, Meerut, 250005, Uttar Pradesh, India
[f] School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing 210044, China

HIGHLIGHTS

- A lightweight two-factor authentication scheme using WMSNs away from being tracked is presented.
- We use the famous tool Proverif to prove that our scheme is secure against the common attacks.
- The informal analysis and performance comparison with recent schemes show that ours is the best.
- The simulation with NS-3 shows that our scheme is applicable for practice.

ARTICLE INFO

Article history:
Received 31 March 2017
Received in revised form 8 July 2017
Accepted 23 August 2017
Available online 6 September 2017

Keywords:
Wireless medical sensor network
Mutual authentication
Proverif tool
User anonymity
Personalized healthcare system

ABSTRACT

Wireless Sensor Network (WSN) is a very important part of Internet of Things (IoT), especially in e-healthcare applications. Among them, wireless medical sensor networks (WMSNs) have been used in the personalized healthcare systems (PHSs). In recent years, professionals use their mobile devices to access the data collected from sensors which are placed in or on patients' bodies. Due to the danger of wireless transmission circumstance, the security of the data which are collected by the sensors and also transmitted to the doctors faces challenges. In the past decade, many authentication schemes for WMSNs are proposed. However, security disadvantages have been found in such schemes. To overcome the historical security problems, we propose a robust and lightweight authentication scheme for WMSNs, which meets the common security requirements, and keeps away user tracking from attackers. The popular tool Proverif is employed to express that our scheme resists the simulated attacks. Also, the informal security analysis is demonstrated. With the comparison to several very recent schemes and simulation by NS-3, the proposed scheme is suitable for PHSs.

1. Introduction

To meet the requirements of exploring the global circumstance, the notion Internet of Things (IoT) is proposed and applied over the whole world. Such conception means that a system contains computing devices, digital objects, animals, plants and persons. Every entity in the system owns a unique identity and an address, so the data of the concerned targets can be transmitted via the networks. Among the applications, wireless sensor network (WSN) is important. WSN contains a set of technologies which profoundly affect the current industries, agriculture, military, medical care and so forth. With many customized sensors gathering signals from the aimed object, people can obtain the timely situation and make decisions.

Nowadays, social IoT (SIoT) becomes a hot topic among researchers. It means that some objects in IoT build social relationships with other objects, which are about human. These relationships are based on the objects' movements, profile and functions provided for people, such as locating someone in an emergency call, checking the suitable bus and time for going out, etc. Wireless Medical Sensor Network (WMSN) is an important kind of

* Corresponding author.
E-mail address: lixiong@hnust.edu.cn (X. Li).

http://dx.doi.org/10.1016/j.future.2017.08.042
0167-739X/© 2017 Elsevier B.V. All rights reserved.

application of the WSN for personalized healthcare systems (PHSs) in e-healthcare scope. To get various sorts of information from the patient in personalized healthcare systems, heterogeneous sensors in WMSN which can collect different kinds of data show their advantages in many fields. Many bio-sensors of different kinds are placed in or on the patient's body and data like heart and breathing rates, blood pressure and movement are gathered by them. Those data are transferred in the wireless channel, which is known to be very insecure.

The concrete architecture of WMSN in personalized healthcare systems is demonstrated in Fig. 1. There are three kinds of participants in a classic WMSN: the professional, or the user, such as the doctor or the nurse, who needs the data of target patient; the sensors, which gather the special data from the aimed patient and have weak energy and computation ability; the gateway (GW), which has strong calculation power, and much more resource and energy for communication, is a critical and secure intermediary between the user and the sensors. Different patients use different sensor suites. In China, a famous doctor often needs to diagnose patients distributed in different locations. So different WMSNs should be accessed. Generally, if the professional makes a request for data from some sensor, he/she uses his/her mobile device to contact the sensor set via GW first and obtains the data from the special sensor. In recent years, some authentication schemes have employed the way that the sensor contacts with the user directly [1–3]. That way will make the energy in the weak sensor wasted seriously and decrease the life of sensor [4,5]. How to guarantee the security of data transmission between the three entities is an emergent question. To avoid the various attacks from the adversary, information encryption is an important technology to provide the secrecy of entities [6–9]. Moreover, mutual authentication and user anonymity [5,10–19] are two basic required features. However, researchers now consider that a fixed pseudo-identity for user may lead to be tracked by the adversary and try to design schemes where the user employs different pseudo-identities in different sessions. This is stronger than user anonymity. And many researchers proposed their authentication schemes for WMSNs to satisfy the aims [2,19–22].

1.1. Related work

In 2009, Das [23] presented a two-factor authentication scheme for WSNs. In such scheme, the user needs both his/her own password and a mobile device (e.g., a smart card) storing data related to his/her own information, to access the remote server. But soon researchers [24–26] showed that many weaknesses existed in Das' scheme, such as vulnerability to the insider attack and the impersonation attack. Enhanced schemes are proposed in the above three papers. In 2011, Kumar et al. [27] pointed out that weaknesses like lack of mutual authentication and key agreement existed in [25,26]. Also in 2011, Yeh et al. [28] considered that the scheme in [24] had weaknesses containing susceptibility to the insider attack and was devoid of password change. In 2012, Kumar et al. [29] put forward a new two-factor authentication scheme for WMSNs and claimed that it could withstand known attacks. But He et al. [1] showed that the scheme in [29] was vulnerable to the off-line guessing attack and the insider attack. Moreover, the property user anonymity cannot be kept in [29], either. In 2013, Xue et al. [30] showed an authentication scheme for WSNs, with temporal credential including the hash results of user data. But unluckily, Jiang et al. [20] gave the disadvantages of scheme in [30], including vulnerability to the off-line password guessing attack and tracking attack. But papers [21,31] showed that Jiang et al.'s scheme had weaknesses like susceptibility to the de-synchronization attack and user forgery attack. In 2014, Turkanović et al. [32] proposed a new lightweight two-factor authentication scheme for WSNs. In the scheme there are only hash functions and exclusive-or computations. Soon in 2015, Farash et al. [33] and Amin-Biswas [14] considered that the scheme in [32] could not resist the identity guessing attack, the off-line password guessing attack and the user forgery attack. As the illustration in [14], both the schemes in [32,33] employed the style that the user contacted the sensor directly. But the way is not suitable for applications due to sensor energy waste. And they presented a new multi-gateway-based authentication scheme. In 2015, Li et al. [34] and Wu et al. [2] pointed out that the disadvantages like the sensor capture attack, the de-synchronization attack and the off-line guessing attack could be completed on the scheme in [1], respectively. In 2016, Wu et al. [35] claimed that the scheme in [14] could not resist attacks such as sensor capture attack and tracking attack.

In 2016, Amin et al. [4] considered that the schemes in [1,2,29] also had a critical weakness that the user could contact the sensor directly at last in the authentication. And they proposed a novel two-factor authentication scheme for WMSNs. In fact, Amin et al.'s scheme [4] still has weaknesses, such as susceptibility to the off-line guessing attack and the de-synchronization attack. Moreover, Kumari and Om [36] and Amin et al. [4] proposed their two-factor authentication schemes for WSNs, respectively. Both the two schemes are lightweight. And unlike the most of the above schemes, the session key are constructed by all the three entities. Unfortunately, both of them still have weaknesses. The scheme in [36] cannot withstand the off-line guessing attack and the user tracking attack. Also, destitution of proper encryption makes the session key disclosure. In the same year, Kumari et al. [37] showed that the temporal-credential-based authentication schemes proposed by Li et al. [38] and He et al. [17] were both insecure, e.g., vulnerable to off-line password guessing attack. Unfortunately, their scheme is under the off-line guessing attack and has relatively heavy computation burden since chaotic map is employed in all three entities in the session. Furthermore, Gope and Hwang [39] proposed a lightweight authentication scheme for real-time WSN data access. They used a suit of backup mechanism to resist the denial-of-service attack. In 2017, Srinivas et al. [3] deemed that the scheme in [2] has weaknesses such as insider attack and off-line password guessing attack. However, it is unlucky that both the schemes in [3,39] are not secure since off-line guessing attacks could affect them, and they are impractical if running. The latter problem is the most important point.

1.2. Motivation and contributions

From the above demonstration, it is an urgent task to propose a lightweight and secure mutual authentication scheme for WMSNs. Our paper meets this requirement. Moreover, the contributions of our paper are below:

1. A novel and lightweight two-factor authentication scheme for WMSNs resistant from being tracked by the attacker is presented.
2. We use the famous tool Proverif [40] to prove that our scheme is secure against various common attacks.
3. The informal analysis and performance comparison with some very recent schemes of the same sort show that ours is the best.
4. The simulation with NS-3 shows that our scheme is applicable for practice.

1.3. Organization of the paper

The remainder of our paper is constructed as follows. The preliminary knowledge is in Section 2. Our scheme and the relative Proverif code are illustrated in Sections 3 and 4, respectively. After that we give the informal analysis and performance comparison in Section 5. Then the tool NS-3 is used to make a simulation in Section 6. Finally, the conclusion appears in Section 7.