Information Sciences 321 (2015) 263–277

Contents lists available at ScienceDirect

Information Sciences

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

A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks ☆

Debiao He [a], Neeraj Kumar [b,*], Naveen Chilamkurti [c]

[a] State Key Lab of Software Engineering, School of Computer, Wuhan University, Wuhan, China
[b] Department of Computer Science and Engineering, Thapar University, Patiala, India
[c] Department of Computer Science and Computer Engineering, La Trobe University, Australia

ARTICLE INFO

Article history:
Received 13 March 2014
Received in revised form 14 January 2015
Accepted 5 February 2015
Available online 12 March 2015

Keywords:
Temporal credential
Mutual authentication
Key agreement
Wireless sensor network
Smart card

ABSTRACT

With an advancement of wireless communication technology, wireless sensor network (WSN) has emerged as one of the most powerful technologies which can be used in various applications, such as military surveillance, environment monitoring, industrial control, and medical monitoring. WSNs are vulnerable to large collection of attacks than traditional networks because they transmit data using a wireless channel and are deployed in unattended environments. So, in this environment, how to ensure secure communications between different communication parties becomes a challenging issue with respect to the constraints of energy consumption, and large overhead generated during various operations performed. In this direction, the mutual authentication and key agreement (MAAKA) scheme attracts much attention in recent years. In literature, MAAKA schemes were presented in last several years. However, most of these schemes cannot satisfy security requirements in WSNs. Recently, Xue et al. proposed a temporal-credential-based MAAKA scheme for WSNs and proved that it could withstand various types of attacks. However, this paper points out that Xue et al.'s MAAKA scheme is vulnerable to the off-line password guessing attack, the user impersonation attack, the sensor node impersonation attack and the modification attack. Moreover, this paper also points out that Xue et al.'s MAAKA scheme cannot provide user anonymity. To overcome weaknesses in Xue et al.'s MAAKA scheme, this paper proposes a new temporal-credential-based MAAKA scheme for WSNs. Security analysis shows the proposed MAAKA scheme could overcome the weaknesses in Xue et al.'s MAAKA scheme. Performance analysis shows the proposed MAAKA scheme has better performance than the existing benchmarked schemes in literature. Therefore, the proposed MAAKA scheme is more suitable for providing security for various applications in WSNs.

1. Introduction

In the last decade, wireless communication, and sensor technologies have seen tremendous growth. Wireless Sensor Networks (WSN) are widely used in many fields (such as military surveillance, environmental monitoring industrial control,

☆ This paper is the full version of our earlier proposed solution "A secure temporal-credential-based MAAKA scheme with pseudo identity for wireless sensor networks" presented at ISWPC 2014, 20–22 November, 2014, Taiwan.

* Corresponding author.

E-mail addresses: hedebiao@163.com (D. He), neeraj.kumar@thapar.edu (N. Kumar), n.chilamkurti@latrobe.edu.au (N. Chilamkurti).

http://dx.doi.org/10.1016/j.ins.2015.02.010
0020-0255/© 2015 Elsevier Inc. All rights reserved.

medical monitoring). WSN consists of many resource-constrained sensor nodes and is deployed in some unattended environment [7]. WSN can be used for data collection and transmitting the same either in the area where it is deployed or to the remote base station.

For example, considering applications of the WSN in a medical environment, the workflow of various events in the WSN is demonstrated as follows. As shown in Fig. 1, there are three parts in the medical WSN, i.e. the sensor, the gateway node (GWN) and the medical worker (such as doctor, nurse). First, the medical worker and medical sensors register with the gateway and get their private keys. Second, the medical worker places medical sensors on the patient's body or implant them in the patient's body. At last, the medical worker uses his/her private key to generate legal login message and sends it to the GWN and the medical sensor through the Internet. After verifying the legality of the medical worker, the medical sensor sends the patient's vital data (such as temperature, blood pressure and pulse rate) to the medical worker with the help of the GWN. Upon receiving those vital data, the medical worker could analyze the patient's status and give effective treatments. In such an application, all operations are executed remotely and no face-to-face measurement or treatment is needed. The type of application can improve efficiency and can provide convenience to both patients and medical workers.

Compared with traditional networks, WSN is vulnerable to various types of attacks because its communication is done in wireless environment. Therefore, how to ensure secure communication in WSNs has attracted a lot of attention in recent years. The mutual authentication and key agreement (MAAKA) scheme is suitable in such an environment for solving the security problem in WSNs because it could provide mutual authentication among the user, the sensor node and the GWN for generating a session key for future communication. Recently, many MAAKA schemes for WSNs were proposed which are discussed as follows.

1.1. Related work

Benenson et al. [1] discussed security issues of authentication in WSNs and proposed the concept of *n*-authentication. Later, Benenson et al. [2] proposed a MAAKA scheme for WSNs using elliptic curve cryptography (ECC). However, Binod et al. [4] pointed out that Benenson et al.'s MAAKA scheme [2] cannot provide user anonymity as they claimed. Watro et al. [21] use RSA and Diffie–Hellman algorithms to construct another MAAKA scheme for WSNs. Unfortunately, Das [8] demonstrated that Watro et al.'s MAAKA scheme cannot withstand the impersonation attack. To improve performance, Wong et al. [22] proposed a password-based MAAKA scheme for WSNs. Wong et al.'s scheme is more efficient than previous MAAKA schemes because only hash function operations are needed in their scheme. However, Das [8] found that Wong et al.'s scheme is vulnerable to the stolen-verifier attack and the many logged-in user attack. Tseng et al. [20] also pointed out that Wong et al.'s scheme [22] is vulnerable to the replay, and the forgery attacks. Tseng proposed an improved scheme to overcome weaknesses in Wong et al.'s MAAKA scheme. Later, Lee [16] also proposed two security enhanced MAAKA schemes to overcome weaknesses in Wong et al.'s MAAKA scheme. Later, Ko [14] pointed out that Tseng's MAAKA scheme cannot provide mutual authentication. Ko also proposed a security enhanced MAAKA scheme to solve security problems in Tseng's MAAKA scheme. Moreover, Binod et al. [3] found that Tseng' MAAKA scheme is vulnerable to the replay attack and the man-in-the-middle attack. Das [8] proposed a two-factor MAAKA scheme for WSNs using password and smart card.

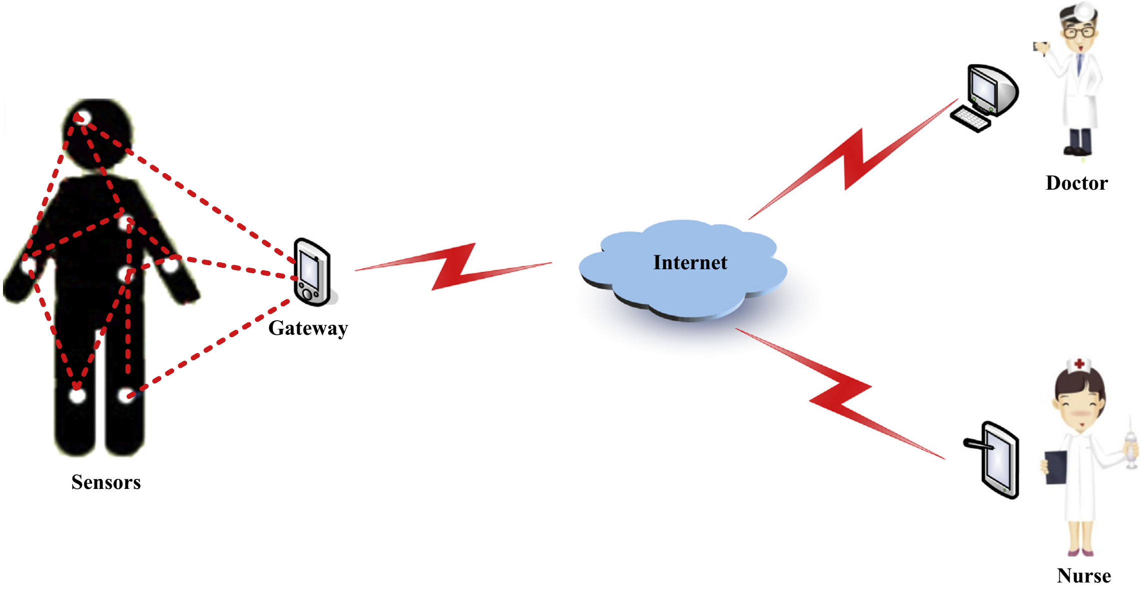

Fig. 1. The application of sensor networks in medical environment.