Future Generation Computer Systems 63 (2016) 56–75

Contents lists available at ScienceDirect

Future Generation Computer Systems

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

A user friendly mutual authentication and key agreement scheme for wireless sensor networks using chaotic maps

Saru Kumari [a,*], Xiong Li [b], Fan Wu [c], Ashok Kumar Das [d], Hamed Arshad [e], Muhammad Khurram Khan [f]

[a] Department of Mathematics, Ch. Charan Singh University, Meerut, Uttar Pradesh, India
[b] School of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan 411201, China
[c] Department of Computer Science and Engineering, Xiamen Institute of Technology, Xiamen 361021, China
[d] Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500 032, India
[e] Department of Computer Engineering, Ferdowsi University of Mashhad, Mashhad, Iran
[f] Center of Excellence in Information Assurance, King Saud University, Riyadh, Saudi Arabia

HIGHLIGHTS

- We examine recently proposed Li et al.'s and He et al.'s schemes for WSN.
- We show security weaknesses in both schemes.
- We propose an improved scheme for WSN using Chebyshev chaotic maps.
- Formal security proof using BAN logic and conventional analysis assure the security of our scheme.
- Comparative evaluation shows the superiority of our scheme over related schemes.

ARTICLE INFO

Article history:
Received 22 July 2015
Received in revised form
8 January 2016
Accepted 23 April 2016
Available online 6 May 2016

Keywords:
User authentication
Wireless sensor networks
User anonymity
Password guessing
Forward secrecy
Chaotic maps

ABSTRACT

Spread of wireless network technology has opened new doors to utilize sensor technology in various areas via Wireless Sensor Networks (WSNs). Many authentication protocols for among the service seeker users, sensing component sensor nodes (*SN*s) and the service provider base-station or gateway node (*GWN*) are available to realize services from WSNs efficiently and without any fear of deceit. Recently, Li et al. and He et al. independently proposed mutual authentication and key agreement schemes for WSNs. We find that both the schemes achieve mutual authentication, establish session key and resist many known attacks but still have security weaknesses. We show the applicability of stolen verifier, user impersonation, password guessing and smart card loss attacks on Li et al.'s scheme. Although their scheme employs the feature of dynamic identity, an attacker can reveal and guess the identity of a registered user. We demonstrate the susceptibility of He et al.'s scheme to password guessing attack. In both the schemes, the security of the session key established between user and *SN*s is imperfect due to lack of forward secrecy and session-specific temporary information leakage attack. In addition both the schemes impose extra computational load on resource scanty sensor-nodes and are not user friendly due to absence of user anonymity and lack of password change facility. To handle these drawbacks, we design a mutual authentication and key agreement scheme for WSN using chaotic maps. To the best of our knowledge, we are the first to propose an authentication scheme for WSN based on chaotic maps. We show the superiority of the proposed scheme over its predecessor schemes by means of detailed security analysis and comparative evaluation. We also formally analyze our scheme using BAN logic.

1. Introduction

Now-a-days, wireless sensor networks (WSNs) are the first choices for remote monitoring in various domains like domestic [1], industry [2–4], military [5], medical [6], scientific research [7], safety [8,9], etc., due to their ease of deployment in harsh/hostile/unattended/unfriendly environment, minimal main-

* Corresponding author.
E-mail addresses: saryusiirohi@gmail.com, saru@ccsuniversity.ac.in (S. Kumari), lixiongzhq@163.com (X. Li), conjurer1981@gmail.com (F. Wu), ashok.das@iiit.ac.in, iitkgp.akdas@gmail.com (A.K. Das), hamedarshad@imamreza.ac.ir, hamedarshad@stu.um.ac.ir (H. Arshad), mkhurram@ksu.edu.sa (M.K. Khan).

http://dx.doi.org/10.1016/j.future.2016.04.016
0167-739X/

tenance and exciting outcomes. In a wireless sensor network (WSN), numerous tiny-sized sensor-nodes (*SN*s) are deployed in the intended field. After deployment, these *SN*s associate themselves in an extemporized manner to communicate with each other and with a resource rich master node called Gateway-node (or base station) *GWN* via wireless links [10]. In this way, the *SN*s wirelessly linked with their neighboring nodes together form a network which is finally linked to the *GWN*, and the network so formed is called the wireless sensor network (WSN). The data sensed by the *SN*s from surroundings is eventually routed to the *GWN* which is then used for decision making and taking necessary action accordingly.

The involvement of WSNs in a wide range of applications requires managing many critical tasks simultaneously. Generally, real applications neglect the security aspect rendering WSNs exposed to various potential threats. Malicious minds can misuse the sensitive (here, sensitive data depends on the domain of WSN, for example, military, healthcare, etc.) data collected by *SN*s for personal reasons, therefore, it is mandatory to regulate authorized access to the WSNs. Therefore, security solutions are essential for proper functioning of the application layer of WSNs, for which user authentication scheme is a prime choice on which other security mechanisms such as Over The Air (OTA) programming and establishment of a secure channel [11] are based on. It provides confidentiality and integrity of data and allows only valid users to access information from the network. However, the design of a user authentication scheme suitable for WSNs is not an easy task due to complicated architecture involving numerous resource-deficient *SN*s as important components. *GWN* is a powerful data processing/storage center with powerful antenna and much more battery power than required to surpass the life-time of all the *SN*s. *GWN* plays a key role in WSN. It acts as registration authority to register willing to be users, serves as a gateway to another network or an access point for human interface [10] and also commands the *SN*s. Contrarily, *SN*s are equipped with limited memory size, low battery power, low data processing capability and short radio transmission range [10]. Hence, a user authentication scheme for WSNs should be characterized with short communication messages, fast algorithm and less power consumption. Data is made available to the user on demand whereby users needs to prove their authenticity before accessing the data. Generally, users transmit their login request to the *GWN* which issues commands to the *SN*s whether to answer or not to the user's query. In scenarios where users directly login the *SN*s, the *SN*s seek the help of the *GWN* to confirm the validity of the user. Therefore, the three involved entities (user, *GWN* and *SN*) should be able to mutually authenticate each other to avoid forgery at any end. Furthermore, user privacy is a focal concern due to the vulnerability of wireless communications.

1.1. Related work

As yet, the design of user authentication schemes for resource-deficient WSNs has been substantially addressed by various researchers [12–33]. However, every scheme is proposed with some merits. Most of these are found to be insecure due to susceptibility to different kinds of security threats.

In 2004, Watro et al. [12] proposed a public-key-based user authentication scheme using Diffie–Hellman [34] and RSA [35] algorithms. In 2006, Wong et al. [13] gave a password-based user authentication scheme for WSN by using only hash function. Nonetheless, Watro et al.'s scheme is identified with an attack in which an adversary can behave as a sensor node to cheat the user [18]. Nevertheless, Wong et al.'s scheme is observed to be flawed with many logged-in-users attack whence many non-registered users possessing the password of a registered user can login to WSN and access data [14,18,20]. Tseng et al. [14] and Das [18] independently pointed out stolen-verifier and replay attacks on Wong et al.'s and Watro et al.'s schemes. In 2007, Tseng et al. [14] proposed a scheme as an enhancement of Wong et al.'s scheme to overcome its weaknesses. They claimed their scheme to be more efficient due to reduced risk of user's password leakage and password changing facility. In 2008, Lee [15] noticed high computational overhead on *SN*s in Wong et al.'s scheme and proposed two improvements. In the first scheme, he focused on reducing the computational overhead of *SN*s without deteriorating the security level. On the other hand, the second scheme is aimed at averting an attacker from masquerading as *GWN* for granting access to illicit persons. In the same year, Ko [16] pointed out that Tseng et al.'s scheme has no provision for mutual authentication between *GWN* & *SN* and between user & *SN*. Ko also presented a new scheme to establish mutual authentication. Vaidya et al. [17,19] analyzed Wong et al.'s, Tseng et al.'s, and Ko's schemes, and devised their improved schemes. Vaidya et al. asserted that their proposed improvements can withstand forgery attack, replay attack, man-in-the-middle attack, and offer user privacy and mutual authentication.

In 2009, Das [18] introduced a two-factor-based user authentication scheme for WSN, his scheme became a center of attraction for many researchers [21–23] working in this field. The scheme is based on the concept of using a password and a smart card as two factors to realize the user authentication. Das claimed his scheme to be free from the security problems such as stolen-verifier, many logged-in-users with the same identity, guessing, impersonation and replay attacks. In 2010, Huang et al. [22] pointed out that Das's scheme does not resist many logged-in-users attack with the same identity and *SN* impersonation attack. As a solution, they proposed a scheme [22] with same performance but possessing additional features of user anonymity and password change feature. In the same year, He et al. [21] demonstrated impersonation attack, privileged insider attack and lack of password changing facility in Das' scheme. Based on their analysis, they built an enhanced scheme [21]. During the same time, Khan and Alghathbar [23] also identified the insider attack, gateway node bypass attack, and the absence of mutual authentication between the *SN* and the *GWN*. Consequently, they proposed [23] an improve method to remove the security loopholes of Das's scheme.

In 2012, Kumar et al. [24] presented an authentication scheme for WMSNs. They used hash function and symmetric cryptographic operation in their scheme to provide security. In 2015, He et al. [25] observed that Kumar et al.'s scheme suffers from some security problems and proposed an authentication scheme for WMSNs to fix these flaws. In the same year, Li et al. [29] found that the authentication processes of He et al.'s scheme [25] is flawful in such a way that the scheme can neither provide proper mutual authentication nor the session key agreement. Hence, Li et al. [29] proposed a new user anonymous authentication scheme for WMSNs. Li et al. [29] also deploy symmetric cryptographic operation in their scheme.

1.1.1. Contribution of Li et al.'s [28] and He et al.'s [29] schemes

In 2013, Xue et al. [30] introduced a temporal-credential-based mutual authentication & key agreement scheme for WSNs. In Xue et al.'s scheme, *GWN* issues a temporal credential to each registered user and *SN* which depends on the identity of the respective entity and *GWN* secret key. The temporal credential of the user is stored in her/his smart card and for *SN* it is stored in its memory. The authors asserted that their scheme was lightweight and fulfilled the security requirements of WSNs. In 2013, Li et al. [31] examined Xue et al.'s scheme and found it vulnerable to many logged-in-users attack with same identity, stolen verifier attack, privileged insider attack, smart card loss problem and password disclosure problem. To preclude the security risks of Xue et al.'s scheme, they suggested an advanced scheme. They utilized