Journal of Network and Computer Applications 36 (2013) 316–323

Contents lists available at SciVerse ScienceDirect

Journal of Network and Computer Applications

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

A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks

Kaiping Xue *, Changsha Ma, Peilin Hong, Rong Ding

The Information Network Lab of EEIS Department, USTC, Hefei 230027, China

ARTICLE INFO

Article history:
Received 21 November 2011
Received in revised form
30 April 2012
Accepted 25 May 2012
Available online 7 June 2012

Keywords:
Temporal credential
Mutual authentication
Key agreement
Wireless sensor network
Gateway node

ABSTRACT

Wireless sensor network (WSN) can be deployed in any unattended environment. With the new developed IoT (Internet of Things) technology, remote authorized users are allowed to access reliable sensor nodes to obtain data and even are allowed to send commands to the nodes in the WSN. Because of the resource constrained nature of sensor nodes, it is important to design a secure, effective and lightweight authentication and key agreement scheme. The gateway node (GWN) plays a crucial role in the WSN as all data transmitted to the outside network must pass through it. We propose a temporal-credential-based mutual authentication scheme among the user, GWN and the sensor node. With the help of the password-based authentication, GWN can issue a temporal credential to each user and sensor node. For a user, his/her temporal credential can be securely protected and stored openly in a smart card. For a sensor node, its temporal credential is related to its identity and must privately stored in its storage medium. Furthermore, with the help of GWN, a lightweight key agreement scheme is proposed to embed into our protocol. The protocol only needs hash and XOR computations. The results of security and performance analysis demonstrate that the proposed scheme provides relatively more security features and high security level without increasing too much overhead of communication, computation and storage. It is realistic and well adapted for resource-constrained wireless sensor networks.

© 2012 Elsevier Ltd. All rights reserved.

1. Introduction

Wireless sensor networks (WSNs) composing of a large number of sensor nodes can be deployed in any unattended environment, such as field observation, military battlefield and so on. In the past decade, WSNs have gained great achievements both in the academic circle and the industrial field. With the new developed IoT (Internet of Things) technology, remote authorized users are allowed to access reliable sensor nodes to obtain data and even are allowed to send commands to the nodes in WSN. Two aspects of this scene should be considered: On the one hand, only legitimate users can access specific sensor nodes to obtain data. On the other hand, the sensor node for access is required to be verified as a legitimate one. In order to ensure the above two points, mutual authentication between the user and the sensor node is required in the protocol design. Although existing schemes could provide perfect security transmission protocols in the link and network layers, how to design an efficient mutual authentication and key agreement scheme has not been well addressed. Because of the resource-constrained feature of sensor nodes in WSN, the mutual authentication and key agreement protocol requires to be lightweight on the premise of secure. Lightweight features can be reflected in the overhead of computation, communication and storage.

There are three main disadvantages of the traditional certificate-based authentication schemes in WSNs. Firstly, they all need a third party public key infrastructure, which is inconvenient to be deployed in WSN. Secondly, mutual authentication is based on asymmetric encryption, resulting in high computation cost of sensor nodes. Thirdly, the certificate validation operation is online. Although some improved schemes based on elliptic curve algorithm are proposed to reduce computational complexity, additional security infrastructures are still required. Online access to the CRL (Certificate Revocation List) for the certificate validity verification also brings a single point problem. Meanwhile, it is hard for the sensor node and the external infrastructure to set up an end-to-end communication path. Improved schemes based on offline CRL require each node to maintain a CRL list which is updated based on CRL broadcasting by a trusted third party. This is unrealistic for sensor nodes with limited storage and communication capacity. A large number of secret key sharing based schemes have difficulties in distributing and updating keys. To conclude, in order to achieve data accessing with authorization and security, designing mutual authentication and key agreement schemes is an important and difficult issue in WSNs.

Currently, some gateway node (GWN)-aid based authentication schemes are proposed, which make possible that the mutual authentication and key agreement protocol has both features of

* Corresponding author. Tel./fax: +86 551 360 1334.
E-mail address: kpxue@ustc.edu.cn (K. Xue).

1084-8045/$ - see front matter © 2012 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.jnca.2012.05.010

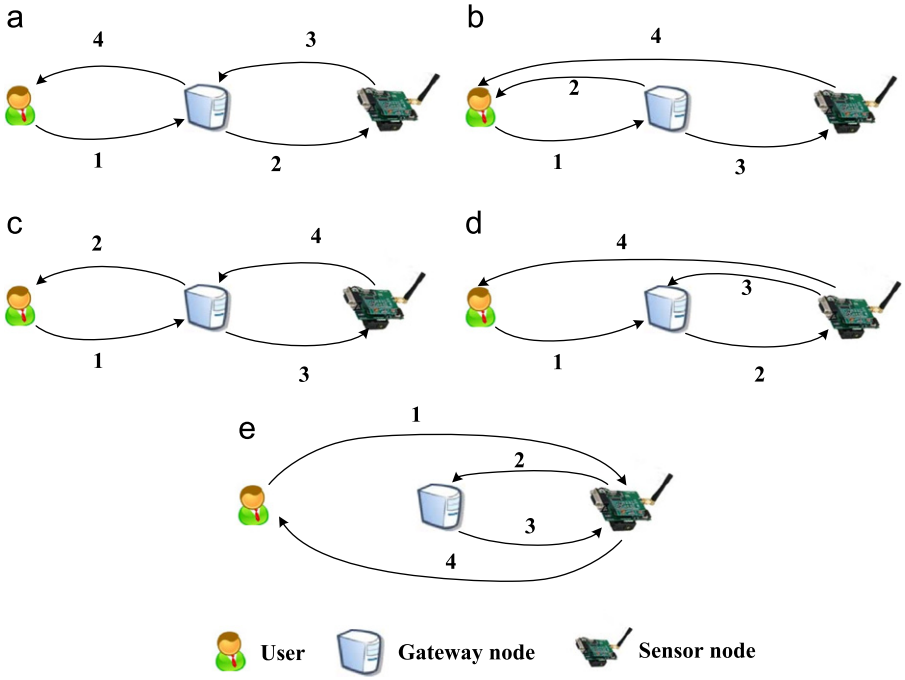

Fig. 1. Five basic authentication models for WSNs.

security and lightweight. GWN plays an important role in the network. In order to further reach the specific sensor node, remote users is required to reach GWN through Internet at first. Contrary, sensing data from the sensor nodes firstly gets to GWN, then further reaches the user end. If the data in the network is made available to the remote user on demand, mutual authentication between them must be ensured before allowing the remote user to access. With the aid of GWN, impenetrability of lightweight mutual authentication is going to be possible. Because of being usually deployed in harsh environments, authentication of the gateway node is also necessary for the user and the sensor. As in Fig. 1, there are five basic authentication models among the user, GWN, and the sensor node.

All of them need four messages to implement mutual authentication. Among them, Fig. 1(d) uses the recursive style to achieve mutual authentication among the user, GWN and the sensor node, in which Steps 3 and 4 can be processed in parallel. Most existing GWN-aid schemes are based on these five models. However, we find that most of these schemes have more or less security flaws. Because of unrealistic assumptions, some of them are not suitable for the resource-constrained wireless sensor networks. Wong et al. (2007) firstly proposed a hash based user authentication scheme, which is less complex, lightweight and dynamic. But some researchers found that it is vulnerable to stolen-verifier, replay, and forgery attacks. Das proposed a two factor method of user authentication (Das, 2009), which has become a frequently cited literature in this area of password based authentication (He et al., 2010; Khan and Alghathbar, 2010; Chen and Shih, 2010; Yeh et al., 2011; Xu et al., 2009; Song, 2010). Das's scheme, which implements password based authentication with the aid of GWN, is suitable for resource-constrained WSNs. In the beginning of Das's scheme, the user provides his/her user identity and password. Then after the verification, GWN issues a temporal credential for the user. When authenticating a user again, the GWN has no need to search the password with the key of its identity from the database. Meanwhile, GWN has no need to store any security information. Protocol processing only needs hash and XOR computations, with no additional symmetric encryption and asymmetric encryption. Das's scheme reduces the computational complexity, which applies to resource-constrained sensor nodes and user equipments. Unfortunately, this scheme has some security flaws and does not provide mutual authentication and key agreement. A series of schemes are subsequently put forward to improve it. He et al. (2010) proposed a similar protocol as in Das (2009). Although this scheme enhances password security, it did not essentially make up for the security flaws. In Khan and Alghathbar (2010), the authors presented several improvements. The first improvement is using hash value of the password instead of directly using the password. The improvement is reasonable, because in most password-based authentication systems, the hash value of the user password, rather than the plain password, is stored in the server. The second improvement is giving a password updating method. But in Khan and Alghathbar (2010), this improvement does not have practical significance, because the password has no specific signification in the initial verification process. The third one is providing mutual authentication among GWN and the sensor node based on the assumption of having a pre-shared key between GWN and each sensor node, which brings storage and lookup overhead to GWN. GWN needs to share a unique security key with each user and sensor node in Khan and Alghathbar (2010). Chen and Shih (2010) provides mutual authentications among the user, GWN, and the sensor node, but it is still vulnerable to replay, forgery and Bypassing attacks. Yeh et al. (2011) proposes an ECC-based user authentication and key agreement protocol. Xu et al. (2009) and Song (2010) both provide Deffie–Hellman key agreement (Diffie and Hellman, 1976) based mutual authentications between the user and the sensor node. Besides increasing computational complexity, Yeh et al. (2011), Xu et al. (2009), and Song (2010) also require additional storage overhead of public keys of other sensor nodes or users.

In this paper we propose an temporal-credential-based mutual authentication and key agreement scheme for WSNs. With the help of password-based authentication, GWN can issue a temporal credential to each user and sensor node. For a user, his/her temporal credential can be securely protected and stored openly in a smart card. For a sensor node, its temporal credential is related to its identity and must privately stored in its storage medium. Furthermore, based on using temporal credentials, the proposed protocol provides mutual authentication among the user, GWN, and the

Download English Version:

https://daneshyari.com/en/article/460024

Download Persian Version:

https://daneshyari.com/article/460024

Daneshyari.com