Journal of Zhejiang University-SCIENCE C (Computers & Electronics)
ISSN 1869-1951 (Print); ISSN 1869-196X (Online)
www.zju.edu.cn/jzus; www.springerlink.com
E-mail: jzus@zju.edu.cn

An efficient and DoS-resistant user authentication scheme for two-tiered wireless sensor networks

Rong FAN[†], Dao-jing HE[†‡], Xue-zeng PAN, Ling-di PING

(*School of Computer Science and Technology, Zhejiang University, Hangzhou 310027, China*)

[†]E-mail: {allanrong, hedaojinghit}@gmail.com

Received Oct. 27, 2010; Revision accepted Feb. 23, 2011; Crosschecked May 30, 2011

Abstract: Wireless sensor networks (WSNs) are vulnerable to security attacks due to their deployment and resource constraints. Considering that most large-scale WSNs follow a two-tiered architecture, we propose an efficient and denial-of-service (DoS)-resistant user authentication scheme for two-tiered WSNs. The proposed approach reduces the computational load, since it performs only simple operations, such as exclusive-OR and a one-way hash function. This feature is more suitable for the resource-limited sensor nodes and mobile devices. And it is unnecessary for master nodes to forward login request messages to the base station, or maintain a long user list. In addition, pseudonym identity is introduced to preserve user anonymity. Through clever design, our proposed scheme can prevent smart card breaches. Finally, security and performance analysis demonstrates the effectiveness and robustness of the proposed scheme.

Key words: User authentication, User anonymity, Smart card, Two-tiered, Wireless sensor network (WSN)
doi:10.1631/jzus.C1000377 **Document code:** A **CLC number:** TP393

1 Introduction

Recently, there have been many studies of wireless sensor networks (WSNs) due to the critical need for applications, e.g., environmental monitoring, precision agriculture, health-care, and factory automation. Most large-scale WSNs follow a two-tiered architecture (Desnoyers *et al.*, 2005; Gnawali *et al.*, 2006; Diao *et al.*, 2007): a lower tier and an upper tier (Fig. 1). A great number of resource-constrained sensor nodes are included in the lower tier, while the upper tier contains only a few master nodes (i.e., gateway nodes) that act as cluster heads. Note that sensor nodes are in charge of sensing tasks, while master nodes, which have more resources than sensor nodes, are responsible for processing the raw sensed data and forwarding the processed data to the base station or legitimate users. Furthermore, master nodes constitute a multi-hop wireless mesh network to communicate with each other. As is well known, this two-tiered sensor network architecture is indispensable for increasing network capacity and scalability, reducing the complexity of system management, and prolonging the lifetime of the network (Desnoyers *et al.*, 2005; Gnawali *et al.*, 2006; Diao *et al.*, 2007).

Although most data queries are issued by a base station in WSN applications, there has been a great demand for authorized users to be able to send real-time data queries to sensor nodes. This may be inefficient, unscalable, and vulnerable to many potential attacks along the long communication path between the base station and each sensor node. Thus, the authorized users should have the ability to enter the sensor field to directly access data on sensor nodes without involving a base station. And it is essential for each sensor node to authenticate the data queries from users.

Due to typical features of two-tiered WSNs, providing user authentication for this architecture

‡ Corresponding author

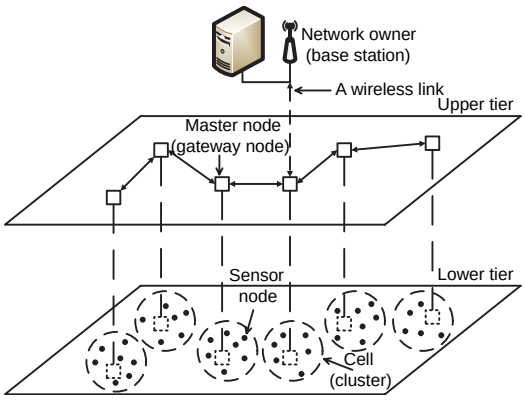

Fig. 1 Architecture of an abstract two-tiered sensor network

brings challenges. On the one hand, sensor nodes in WSNs are limited in computation, storage, and energy resources. Thus, asymmetric cryptography (e.g., the signature schemes based on RSA or ECC) is often too expensive for many applications. Therefore, symmetric cryptographic (e.g., DES and AES) and one-way hash (e.g., MD5, SHA-1, and SHA-2) operations are more suitable for WSNs. On the other hand, the sensor nodes can be easily captured by the intruder, since WSNs are deployed in a hostile environment. Thus, all the secret information stored in sensor nodes is exposed to the intruder.

In practice, a large-scale WSN may have tens of thousands of users. To reduce the communication load between the base station and master nodes, each master node may have to maintain a long user list. Although the master nodes can provide stable network services through this method, it is too expensive in terms of storage and management. Meanwhile, there is a growing requirement of protecting users' anonymity. If the users' personal information is stored in the master nodes, the intruder can obtain this from compromised master nodes. Although anonymity is widely considered to be an important right in the literature, it is difficult to preserve user anonymity due to the open wireless communication environment.

A smart card is any pocket-sized card with embedded integrated circuits that can process and store data, and communicate with a terminal via radio waves (http://en.wikipedia.org/wiki/Smart_card). Das (2009) applied smart cards to store registration information, validate the user's identity and password, and issue the login message to the gateway node that the user wants to login. Note that malicious parties may obtain the sensitive information stored in the smart card. One example is that an intruder successfully cracks the smart card that was lost by the user, and obtains security information via an illegal card reader or device. With the information stored in the smart card and the messages intercepted during the previous login transactions, the intruder can repeatedly guess the user's password via an offline hacking program. If an intruder acquires the correct user password by decrypting the information stored in the smart card, he/she can pass the authentication process and obtain this user's privilege (Fan *et al.*, 2005). Recently, a set of user authentication protocols has been proposed for sensor networks (Benenson *et al.*, 2005; Wong *et al.*, 2006; Das, 2009; He *et al.*, 2010). However, these user authentication protocols are not suitable for two-tiered WSNs. More details of these schemes will be provided in Section 2. In addition, relevant studies have been carried out by Shi *et al.* (2009) and Zhang *et al.* (2009), which focused mainly on ensuring secure range queries in event-driven two-tiered sensor networks, offering data confidentiality, and allowing the network owner to verify whether a query result is authentic and complete (Shi *et al.*, 2009). However, these two studies did not address the problems of user authentication in two-tiered WSNs.

In this paper, we propose a new user authentication protocol, which employs only exclusive-OR operations and a one-way hash function. This feature makes our proposal more suitable for large-scale resource-limited sensor networks. The proposed scheme uses data tables of warrants to achieve user anonymity, and is secure against replay attacks, impersonation attacks, denial-of-service (DoS) attacks, and other network attacks. To ensure that our proposal is secure, the model checking tool AVISPA (automated validation of Internet security protocols and applications) (http://www.avispa-project.org) is applied. By examining all possible execution traces of our proposal in the presence of a Dolev-Yao intruder (Dolev and Yao, 1983), it is shown that the scheme is trustworthy to enforce its security guarantees.

2 Related work

As far as we know, the design of an efficient user authentication for WSNs has not been addressed adequately, owing to the open nature of wireless com-

munication and the limited resources of sensor nodes. In particular, to the best of our knowledge, there has been no user authentication scheme for two-tiered WSNs. Moreover, with the disclosure of a user's real identity, unauthorized entities are permitted to track his/her moving history and current location. Therefore, user anonymity has captured more and more attention from researchers in wireless communication protocols. We review the user authentication schemes for wireless communication below.

2.1 User authentication schemes for the global mobility network

In the literature, there have been some studies on smart card based user authentication schemes for wireless communication (Lee *et al.*, 2006; Tsai, 2008; Wu *et al.*, 2008; Hsiang and Shih, 2009; Liao and Wang, 2009; He *et al.*, 2011). A light-weight and efficient authentication scheme was presented in Lee *et al.* (2006). There are some security weaknesses in Lee *et al.* (2006), however, and a modified version was proposed in Wu *et al.* (2008) to overcome them. Compared with other authentication schemes, there are mainly three advantages in these two schemes (Lee *et al.*, 2006; Wu *et al.*, 2008). Firstly, they require simple operations on a mobile user's smart card, such as symmetric encryption/decryption and hash function operation. Secondly, they take only one round of login message exchange between a mobile user and a visited network, as well as between the visited network and home network. Thus, these protocols totally require only four message exchanges. Thirdly, these protocols implement the one-time key between the mobile user and the visited network. Thus, their realizations are simple and reliable for wireless communication. However, three recent studies (Lee *et al.*, 2009; Xu and Feng, 2009; Zeng *et al.*, 2009) reported that the schemes of Lee *et al.* (2006) and Wu *et al.* (2008) cannot provide user anonymity. In particular, an intruder who has registered as a user of a home agent can obtain the identities of other users as long as they have registered at the same home agent. Later, Hsiang and Shih (2009) proposed an improved version to overcome the shortcomings of Liao and Wang (2009). He *et al.* (2011) showed that the protocol of Hsiang and Shih (2009), however, is still vulnerable to the masquerade attacks when the secrets stored in the smart card are used by the intruder. On the basis of above studies, we have proposed a strong user authentication scheme with a smart card for a wireless communication network (He *et al.*, 2011). The protocol is the first user authentication scheme for the global mobility network that can prevent a smart card security breach.

2.2 User authentication schemes for wireless sensor networks

In the literature, there have been many studies on user authentication schemes for WSNs. Solutions for user authentication with smart cards were firstly proposed in Chang and Wu (1991). The base station or authentication server issues a smart card to a user who registers in the system. Later, each user possesses the smart card for login to any foreign network. Due to tamper-resistance and convenience in managing passwords, smart card based authentication is one of the most effective methods for user authentication and secret session key establishment (He *et al.*, 2011). A number of user authentication schemes using smart cards can be found (Hwang and Li, 2000; Awasthi, 2004; Awasthi and Lal, 2004; Das *et al.*, 2004; Lee *et al.*, 2005). The scheme of Hwang and Li (2000) adopts El-Gamal encryption, which uses a pair of asymmetric keys for encryption and decryption. However, the scheme can be broken by creating a valid pair of the user's identity and password without knowing the secret key of the system (Wong *et al.*, 2006). A malicious user can impersonate another legitimate user by means of the shortcoming. Further, this protocol is not suitable for resource-limited devices in WSNs. To address these problems, Benenson *et al.* (2005) implemented a user authentication based on elliptic curve cryptography (ECC) with the redundancy to withstand the node capture. ECC signature is implemented on sensor nodes, and thus it is not applicable to the large-scale sensor network, since ECC needs more resources than the symmetric key scheme. Das (2009) proposed a two-factor user authentication protocol using only hash function operations. He *et al.* (2010) have shown that this protocol is insecure, however, for insider attacks and impersonation attacks, and proposed an improved version to remedy these security weaknesses.

On the other hand, dynamic ID-based user authentication schemes are also widely used for WSNs. Das *et al.* (2004) proposed a dynamic ID-based scheme based on the strong-password authentication

approach. The network users can change their identities and passwords freely in their scheme, and it is unnecessary to assign a password for a certain user. This feature has been incorporated into subsequent user authentication schemes for WSNs as well. The scheme of Das *et al.* (2004) was claimed to be secure against ID-theft, and able to resist replay attacks, forgery attacks, and insider attacks. However, it was later found to have loopholes in the process of password verification (Awasthi, 2004). These flaws are already enough to make the whole system insecure, as an intruder can use any random password to log into the system. Later, Wong *et al.* (2006) proposed a light-weight user authentication just based on exclusive-OR operations and a one-way hash function. However, He *et al.* (2010) found that the user identity is exposed to everyone, and anyone can trace the user's activity in login and authentication phases.

To the best of our knowledge, no user authentication scheme has been proposed for two-tiered WSNs. Moreover, none of the protocols mentioned above are suitable for two-tiered WSNs.

3 Network and intruder models

3.1 Network model

We assume that a large-scale two-tiered WSN is deployed over a region, which contains thousands of resource-poor sensor nodes and relatively few resource-rich master nodes. As shown in Fig. 1, the network region is partitioned into several physical cells, each consisting of one master node and many sensor nodes. We follow the conventional assumption that all the nodes know which cell they belong to. And the sensor nodes in each cluster need only to transfer data to the corresponding cluster head (i.e., master node) through one-hop.

Compared to normal sensor nodes, master nodes are assumed to have abundant resources in storage, energy, and computation, and they form a multi-hop wireless mesh network via relatively long-range, high-rate radios, such as 802.11b and 802.11g. On the contrary, sensor nodes are constrained in resources, and they communicate with neighbor nodes via low-power, low-rate, and short-distance radios such as 802.15.4. Moreover, considering that WSNs are deployed in the hostile environment, before sending the data queries, network users have to register to the network owner.

3.2 Intruder model

We assume that an intruder can launch outsider and insider attacks. In outsider attacks, an intruder may launch arbitrary attacks such as physical-layer jamming, passive eavesdropping, and bogus-message injection to disturb sensor network operations, for which we resort to existing elegant defenses (Eschenauer and Gligor, 2002; Du *et al.*, 2003; Liu and Ning, 2003; Lazos and Poovendran, 2004; Zhang *et al.*, 2006; Zhou and Fang, 2007; Zhou *et al.*, 2007; Ren *et al.*, 2008; He *et al.*, 2009). In insider attacks, an intruder can compromise a number of master nodes and sensor nodes. Once compromising a master/sensor node, the intruder can access all secret information stored there; afterward, the compromised master/sensor nodes can be used to inject the forged data packets, or return juggled and/or incomplete data in response to user queries. In this study, we focus mainly on user authentication on the sensor nodes side. That is, we deal with how to authenticate a registered user for all sensor nodes.

4 The proposed user authentication scheme

In this section, we propose an efficient and denial-of-service (DoS)-resistant user authentication scheme for two-tiered WSNs. Under the network model mentioned in Section 3, the WSN can be divided into a number of cells (i.e., clusters) to enhance its flexibility and energy conservation. Each cluster is administered by a master node (i.e., gateway node). Legitimate users can access a cell in the WSN by their access devices (e.g., PDA, mobile phone, laptop). The devices are assumed to have the ability to perform computational operations and communicate with sensor or master nodes. Considering that WSNs are deployed in the hostile environment, before sending the data queries to nodes, the network users have to register with the network owner. Our main idea is that each user will receive a warrants data table in the registration process. The table includes the certificates of each cell that the network user can access. Then, with the help of a smart card, the user can log into the master node and access data from the cell or a sensor node directly. The proposed scheme is divided into three phases: registration, login, and

authentication. The notations used throughout this paper are shown in Table 1.

Table 1 Notations used in the protocol

Notation	Description
U_i	The ith user of WSN
MN_j	The jth master node of WSN
BS	The network owner (base station) of WSN
ID_i	The identity of U_i
PW_i	The password of U_i
X	The symmetric key of BS
Y_j	The secret number shared between BS and MN
S_k	The secret number shared between MN and its sensor nodes
N_{ij}	The ith user's warrant for the jth master node
$h(\cdot)$	One-way hash function
$h^n(m)$	Operating n-times hash function on message m

4.1 Registration phase

We assume each master node, say MN_j, has already been deployed in the designated area and shares the secret number Y_j with the base station, say BS; meanwhile, each sensor node in a cell shares the secret number S_k with the master node. Suppose a new user U_i wants to register with the BS for accessing services. The registration phase is as shown in Fig. 2. The details are presented as follows.

Step R1: U_i sends his/her identity ID_i and password PW_i through a secure channel to the base station BS. An example is that U_i encrypts $\{\mathrm{ID}_i, \mathrm{PW}_i\}$ using BS's public key and issues it to BS.

Step R2: To conceal the real identity, we introduce a pseudonym identity RID_i for each user U_i, which has already been applied in Jiang *et al.* (2006). BS selects a random sufficiently large number R_i (e.g., 256 bits) and computes $\mathrm{RID}_i = h(R_i \| \mathrm{ID}_{\mathrm{BS}}) \oplus \mathrm{ID}_i \oplus \mathrm{ID}_{\mathrm{BS}}$, where $\mathrm{ID}_{\mathrm{BS}}$ represents the identity of BS. Then BS calculates the following equations:

$$A_i = h(X) \oplus h^2(\mathrm{ID}_i \| \mathrm{PW}_i),$$
$$V_i = h^3(\mathrm{ID}_i \| \mathrm{PW}_i).$$

Meanwhile, BS generates a data table including user U_i's warrant N_{ij} (e.g., the network user's permissions, the period of validity, and the master node's identity) for relative master nodes and the value of $B_{ij} = h(N_{ij} \| Y_j) \oplus h(\mathrm{ID}_i \| \mathrm{PW}_i)$ (Table 2). Note that U_i may not need to access all of the cells in the WSN, and the warrant table can restrict users as to which cell they can login. In this way, it is unnecessary for each master node to maintain a long user list.

Step R3: The information of $\{\mathrm{RID}_i,\ R_i\}$ is added into the registration database in the BS, and BS does not record any information about U_i's password. With this approach we can conceal the real identity ID_i and provide identity anonymity for users without increasing the computation complexity. Then BS personalizes a smart card with the parameters $h(\cdot)$, RID_i, V_i, A_i, and the data table of warrants $\{N_{ij}, B_{ij}\}$. Note that the argument N_{ij} is fixed-size in our scheme (e.g., 88 bits including 8 bits of the network user's permissions, 64 bits of the period of validity, and 16 bits of the master node's identity). The size of B_{ij} is also fixed since it is a hash value (e.g., 256 bits). Thus, the total size of each warrant is 344 bits, and the whole table will not exceed 42 KB if there are 1000 master nodes. Considering the small size of the warrant table, most mobile devices (e.g., smart card and PDA) have sufficient space to store it. Finally, the BS sends the personalized smart card to U_i in a secure manner.

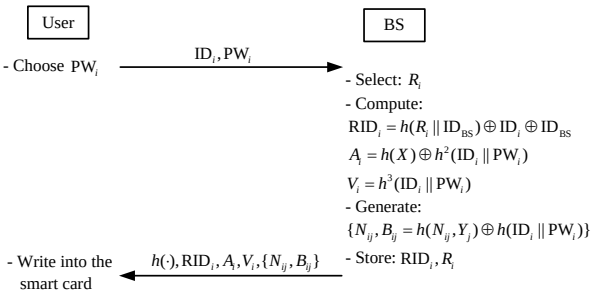

Fig. 2 The registration phase of the proposed scheme

Table 2 An example of the data table of user U_i

N_{ij}	B_{ij}
N_{11}	$B_{11} = h(N_{11} \| Y_1) \oplus h(\mathrm{ID}_1 \| \mathrm{PW}_1)$
N_{12}	$B_{12} = h(N_{12} \| Y_2) \oplus h(\mathrm{ID}_1 \| \mathrm{PW}_1)$
N_{13}	$B_{13} = h(N_{13} \| Y_3) \oplus h(\mathrm{ID}_1 \| \mathrm{PW}_1)$
N_{14}	$B_{14} = h(N_{14} \| Y_4) \oplus h(\mathrm{ID}_1 \| \mathrm{PW}_1)$
N_{15}	$B_{15} = h(N_{15} \| Y_5) \oplus h(\mathrm{ID}_1 \| \mathrm{PW}_1)$
...	...

4.2 Login phase

When user U_i wants to acquire sensed data, he/she needs to insert the smart card into a terminal, and input ID_i and PW_i. The smart card computes

the value of $h^3(\mathrm{ID}_i\|\mathrm{PW}_i)$, and compares the result with the stored V_i. The steps to be performed in this phase are detailed as follows.

Step L1: U_i keys ID_i^* and PW_i^*. Note that the smart card issued by BS has been inserted into the user's mobile devices.

Step L2: The smart card computes $V_i^* = h^3(\mathrm{ID}_i^*\|\mathrm{PW}_i^*)$, and checks whether V_i^* and V_i are equal or not. If yes, the legitimacy of the user can be assured and the phase proceeds to the next step. Otherwise, end this phase.

Step L3: U_i chooses which master node to login, and the smart card reads corresponding values of the master node: $\{N_{ij}, B_{ij}\}$. Then it computes the following equations:

$$\begin{aligned}\mathrm{TK}_i &= h((B_{ij}\oplus h(\mathrm{ID}_i\|\mathrm{PW}_i))\|T)\\ &= h(h(N_{ij}\|Y_j)\|T),\\ \mathrm{SID}_i &= \mathrm{RID}_i\oplus h((A_i\oplus h^2(\mathrm{ID}_i\|\mathrm{PW}_i))\|T)\\ &= \mathrm{RID}_i\oplus h(h(X)\|T),\end{aligned}$$

where T is the time-stamp of U_i generating the login message.

Step L4: The smart card computes $C_1 = \mathrm{SID}_i\oplus\mathrm{TK}_i$ and $C_2 = h(\mathrm{TK}_i\|\mathrm{SID}_i\|N_{ij}\|T)$, and sends the message $\{N_{ij}, C_1, C_2, T\}$ to the master node. Meanwhile, the smart card erases ID_i, PW_i, SID_i, $h(N_{ij}\|Y_j)$, $h(\mathrm{ID}_i\|\mathrm{PW}_i)$, and $h^2(\mathrm{ID}_i\|\mathrm{PW}_i)$ from its memory, and records the last login time-stamp T in the mobile device's cache.

4.3 Authentication phase

Upon receiving the message $\{N_{ij}, C_1, C_2, T\}$ at time T^*, the master node authenticates U_i by the following steps.

Step A1: Validate T. If $T^* - T \le \Delta T$ holds, the master node proceeds to the next step, where T^* indicates the time-stamp when the master node MN_j receives the login message.

Step A2: Compute $\mathrm{TK}_i^* = h(h(N_{ij}^*\|Y_j)\|T)$, where Y_j is the pre-shared key between MN_j and BS. Furthermore, the master node computes the shadow identity $\mathrm{SID}_i^* = C_1\oplus\mathrm{TK}_i^*$ and $C_2^* = h(\mathrm{TK}_i^*\|\mathrm{SID}_i^*\|N_{ij}\|T)$. If $C_2^* = C_2$, the master node accepts the login request. Otherwise, the master node simply rejects the login request.

Step A3: After accepting the login request, the master node stores $\{\mathrm{SID}_i, T\}$ for the subsequent operation. Note that MN_j can report U_i's abnormal behaviors to BS; meanwhile, BS can collect the data of U_i's usage information in each MN_j for pricing. If BS receives the message $\{\mathrm{SID}_i, T\}$ sent by a master node, it can calculate $\mathrm{RID}_i^* = \mathrm{SID}_i\oplus h(h(X)\|T)$ and reveal the real identity of the network user U_i (i.e., ID_i) by computing $\mathrm{ID}_i = \mathrm{RID}_i\oplus\mathrm{ID}_{\mathrm{BS}}\oplus h(R_i\|\mathrm{ID}_{\mathrm{BS}})$.

Step A4: The master node computes the temporary authentication key $\mathrm{TKM}_j = h(h(N_{ij}\|Y_j)\|\mathrm{SID}_i\|T_{\mathrm{MN}})$ for the network user U_i, where T_{MN} is the time-stamp of the master node MN_j generating the message, and selects the random number K to generate session key $\mathrm{Key} = h(S_k\|K)$. Afterwards, the master node calculates the following equations:

$$\begin{aligned}D_1 &= \mathrm{Key}\oplus\mathrm{TKM}_j,\\ D_2 &= h(\mathrm{Key}\|\mathrm{TKM}_j\|T_{\mathrm{MN}}),\end{aligned}$$

and sends the message $\{D_1, D_2, T_{\mathrm{MN}}\}$ back to user U_i. Meanwhile, MN_j issues a random number K to its sensor nodes, which is included in $\{K, T_{\mathrm{MN}}, h(K\|T_{\mathrm{MN}}\|S_k)\}$. Then the sensor node computes the hash value of $\{K\|T_{\mathrm{MN}}\|S_k^*\}$, where S_k^* is the secret number shared between MN and its sensor nodes. If the hash value is equal to the one included in the message, the sensor node can obtain the session key by computing $\mathrm{Key} = h(S_k\|K)$. Thus, an authenticated user can send queries to either master nodes or sensor nodes.

Step A5: Upon receiving the message issued by the master node MN_j, the smart card checks the time-stamp as in Step A1. Then the smart card requires the network user to re-enter his/her identity and password for verification. If it is correct, the smart card will recalculate $h(N_{ij}\|Y_j)$ and SID_i as in Step L3. As the last login time-stamp T has recorded in the cache, $h(N_{ij}\|Y_j)$ and SID_i are easily calculated. Finally, the smart card calculates $\mathrm{TKM}_j^* = h(h(N_{ij}\|Y_j)\|\mathrm{SID}_i\|T_{\mathrm{MN}})$ and $\mathrm{Key}^* = D_1\oplus\mathrm{TKM}_j^*$. If D_2^* $(= h(\mathrm{Key}^*\|\mathrm{TKM}_j^*\|T_{\mathrm{MN}}))$ is equal to D_2 which is included in the message, the network user U_i accepts the session key Key and after that, U_i can send queries and receive sensed data encrypted by Key. Note that all the temporary variables will be removed after the network user logs out the master node.

Fig. 3 shows the login and authentication phases, where MN and SN represent a master node and its sensor nodes, respectively.

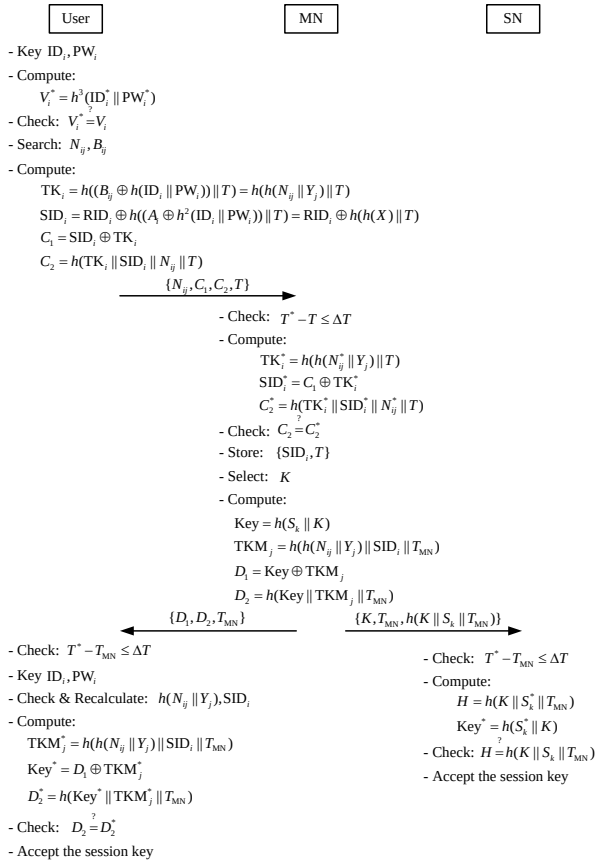

Fig. 3 The login and authentication phases of the proposed scheme

5 Analytical evaluation

In this section, we present the analysis of security features of the proposed protocol and a comparison of the costs.

5.1 Security analysis

In the following, we analyze the security of the proposed scheme.

5.1.1 User anonymity

As shown in Fig. 2, the real identity ID_i of U_i is replaced with his/her pseudonym identity $\mathrm{RID}_i = h(R_i \| \mathrm{ID_{BS}}) \oplus \mathrm{ID}_i \oplus \mathrm{ID_{BS}}$, and the random number R_i is not stored in user's own smart card or master nodes. Thus, only BS knows the relationship between RID_i and the user's identity ID_i, and nobody except BS can trace the network user U_i. On the other hand, as shown in Fig. 3, C_1 included in the login message contains $\mathrm{SID}_i = \mathrm{RID}_i \oplus h(h(X) \| T)$; its value varies with the time-stamp T and is concealed by $\mathrm{TK}_i = h(h(N_{ij} \| Y_j) \| T)$. Anybody who wants to obtain the RID_i from C_1 must generate $h(X)$ and $h(N_{ij} \| Y_j)$. Clearly, the value of $h(N_{ij} \| Y_j)$ concealed by the hash value of the user's identity and password is installed only in the user's smart card, and anyone who wants to obtain the value of $h(N_{ij} \| Y_j)$ must crack the user's smart card and own the user's identity and password. Therefore, there is no feasible way for the intruder to extract the pseudonym identity RID_i from C_1 and trace the location of a targeted mobile user. Given all this, the proposed scheme can preserve user anonymity.

5.1.2 Preventing the smart card breach

Although it is generally assumed that the smart card is safe and cannot be cracked, there is a risk of a smart card crack. Here, it is demonstrated that our proposed scheme can prevent the smart card breach. The details are as follows: Firstly, if the intruder attains a smart card and cracks it, he/she can obtain $h(\cdot)$, RID_i, $V_i = h^3(\mathrm{ID}_i \| \mathrm{PW}_i)$, $A_i = h(X) \oplus h^2(\mathrm{ID}_i \| \mathrm{PW}_i)$ and $\{N_{ij}, B_{ij} = h(N_{ij} \| Y_j) \oplus h(\mathrm{ID}_i \| \mathrm{PW}_i)\}$. The intruder has no feasible way to generate $h(X)$ and $h(N_{ij} \| Y_j)$ without knowing U_i's identity ID_i and password PW_i. As the smart card does not record any procedure variable, such as SID_i and $h(N_{ij} || Y_j)$, the intruder cannot obtain the user's permissions. Secondly, a malicious user can crack his/her own smart card to obtain the secret value $h(X)$. When the malicious user steals another network user U_n's smart card and obtains the value $h^2(\mathrm{ID}_n \| \mathrm{PW}_n)$ from A_n, he/she has no feasible way to obtain the value of $h(N_{nj} \| Y_j)$ from B_{nj}, since he/she does not know the user's $\{\mathrm{ID}_n, \mathrm{PW}_n\}$. The malicious user cannot generate $h(\mathrm{ID}_n \| \mathrm{PW}_n)$ based on $h^2(\mathrm{ID}_n \| \mathrm{PW}_n)$. Hence, he/she cannot obtain the authentication of user U_n. Furthermore, if the malicious user forges SID_i to prevent from being tracked by BS, the license included in N_{ij} will be terminated through broadcasting the 'termination' message by BS, and the user is no longer permitted to log into the related master node. Given this, the proposed scheme can prevent a smart card breach.

5.1.3 Resisting the password guessing attack

The hash value of user's password PW_i is stored only in the user's smart card, which is concealed in $V_i = h^3(\mathrm{ID}_i \| \mathrm{PW}_i)$, $A_i = h(X) \oplus h^2(\mathrm{ID}_i \| \mathrm{PW}_i)$, and

$B_{ij} = h(N_{ij}\|Y_j) \oplus h(\mathrm{ID}_i\|\mathrm{PW}_i)$. Assume an intruder steals the smart card of a network user and cracks it. It is infeasible to guess the user's password without knowing $h(X)$, Y_j, and ID_i. Thus, the intruder has no convenient way to ascertain the password. Therefore, the proposed scheme can resist a password guessing attack.

5.1.4 Resisting the replay attack

A replay attack (replaying an intercepted message) cannot work in our protocol. Suppose the intruder intercepts a valid login request $\{N_{ij}, C_1, C_2, T\}$ and tries to login to the master node by replaying the same. The verification of this login request fails because of the interval $T^* - T > \Delta T$, where T^* is the master node's system time while receiving the replayed message. Therefore, the proposed scheme can resist a replay attack.

5.1.5 Resisting the impersonation attack

In our protocol, if the intruder wants to impersonate a user to pass the verification of the master node, he/she must calculate a valid $\{C_1, C_2\}$, where $C_1 = \mathrm{SID}_i \oplus \mathrm{TK}_i$ and $C_2 = h(\mathrm{TK}_i\|\mathrm{SID}_i\|N_{ij}\|T)$. Because the intruder does not obtain $h(X)$ and $h(N_{ij}\|Y_j)$ which are stored in the user's smart card, the intruder cannot forge a valid message $\{N_{ij}, C_1, C_2, T\}$. As the above provides, even if the smart card is cracked, the intruder cannot extract $h(X)$ or $h(N_{ij}\|Y_j)$ without knowing the user's ID_i and PW_i. Therefore, the intruder has no chance to log in by launching the impersonation attack.

5.1.6 Resisting the stolen-verifier attack

Assume that an intruder has stolen verifier $V_i = h^3(\mathrm{ID}_i\|\mathrm{PW}_i)$. To pass the verification of a master node, the intruder must have $h(\mathrm{ID}_i\|\mathrm{PW}_i)$ to generate TK_i, and $h^2(\mathrm{ID}_i\|\mathrm{PW}_i)$ to generate SID_i. The intruder cannot calculate $h(\mathrm{ID}_i\|\mathrm{PW}_i)$ since he/she does not know the user's ID_i or PW_i. Therefore, the proposed scheme can resist a stolen-verifier attack.

5.1.7 Resisting the denial-of-service attack

As shown in Fig. 3, the whole process of user authentication requires only two hash operations for each sensor node. Thus, the authentication of each message will not occupy too much energy, memory, or computational resources on the sensor node. Therefore, the proposed scheme can resist the DoS attack.

5.2 Formal proof

5.2.1 AVISPA

Formal proof is not an easy task due to the complicated procedure. Any intruders who are called the Dolev-Yao intruder (Dolev and Yao, 1983) can overhear, intercept messages, inject new messages, or modify messages in transit. AVISPA (automated validation of Internet security protocols and applications) (http://www.avispa-project.org) is a tool which provides a modular and expressive formal language, called the high level protocol specification language (HLPSL), for specifying intended protocols and formally validating them. The current version of the tool integrates the following four back-ends: on-the-fly model-checker (OFMC), constraint-logic-based attack searcher (CL-AtSe), SAT-based model-checker (SATMC), and tree automata based on automatic approximations for the analysis of security protocols (TA4SP). The Dolev-Yao intruder is implemented in AVISPA, which is appropriate to the analysis of wireless security protocols.

5.2.2 Verifying the proposed protocol

Since the user's identity ID_i, password PW_i, and the smart card are encrypted in the transfer channel, the intruder cannot crack the network user or the BS's secret messages through a secure channel. Thus, the formal proof is focused mainly on the login and authentication phases. The whole process is as follows. Firstly, the network user calculates related parameters and then sends the login message to the master node. Secondly, the master node verifies the login message. If the message can pass the verification, the master node selects a random number, and generates a session key for the user and sensor nodes in its cell. Finally, the master node issues the session key to the user, which is concealed by a temporary key. Meanwhile, it issues the random number to the sensor nodes. Fig. 4 presents the diagram transitions for the whole process mentioned above, which can be easily translated to HLPSL.

The test results are detailed as follows: (1) OFMC reports that the protocol is safe; (2) CL-AtSe reports that the protocol is safe; (3) SATMC reports that it does not support the protocol owing

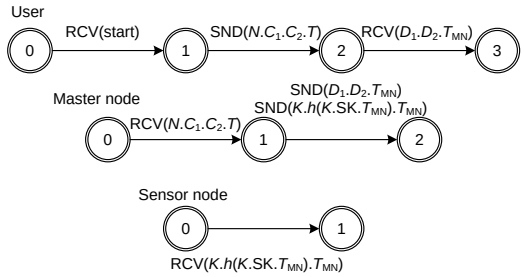

Fig. 4 The diagram transitions for the login and authentication phases

to the requirement of the algebraic equation on the XOR operator; (4) TA4SP also reports that it does not support the XOR operator currently.

5.3 Cost overhead evaluation

In this section, we analyze the proposed scheme in terms of computation and communication costs. Some notations are further defined as: (1) T_h, the time of performing a one-way hash function $h(\cdot)$; (2) $T_{\rm XOR}$, the time for performing an XOR operation; (3) $C_{\rm ub}$, the delay time for the communication between a user and the base station; (4) $C_{\rm um}$, the delay time for the communication between a user and the master node (i.e., gateway node); (5) $C_{\rm ms}$, the delay time for the communication between the master node and a sensor node.

Assume that there are n master nodes in the network scopes. Table 3 shows the overall cost of the proposed efficient and DoS-resistant user authentication scheme for two-tiered WSNs.

As shown in Table 3, the total cost, which is the sum of computation and communication costs for all the three phases, is $(25+n)T_h + (11+n)T_{\rm XOR} + 2C_{\rm ub} + 2C_{\rm um} + C_{\rm ms}$. In order to suit to the two-tiered architecture of WSN, the network model of our proposed scheme assumes fewer resource-rich master nodes (i.e., gateway nodes) in the WSN.

5.3.1 Computation cost

Considering the constrained resource in the sensor node, we use only a one-way hash function and exclusive-OR operation. As shown in Table 3, even though the BS needs to operate n times hash function operations for the network user to generate the warrant table, the computational cost of our scheme in the registration phase is well-suited to the assumed network model. Especially, if there is only one master node, the total computational cost in the registration phase is $6T_h + 4T_{\rm XOR}$. Furthermore, the master node needs no computation and stores the users' registration information. As the sensor node requires only two hash operations, the computational cost of our protocol in the authentication phase is fit for the resource-limited sensor node. Therefore, our scheme is practical for real world applications in enhancing the security over wireless communications.

5.3.2 Communication cost

In our proposed scheme, the user login and authentication phases require three messages be exchanged among the user, the master node, and sensor nodes. Obviously, the message size is under control owing to the length of the hash value, such as C_1, D_1, and $h(K\|S_k\|T_{\rm MN})$. Thus, the consumption of communication is low and restricted.

To sum up, according to the above analysis, the proposed scheme is simple and efficient for two-tiered WSNs.

6 Conclusions

In this paper, an efficient and DoS-resistant user authentication scheme has been proposed for two-tiered wireless sensor networks. The proposed scheme does not request master nodes to forward login request messages or to maintain a long user list. Further, the proposed approach can preserve user anonymity and prevent a smart card security breach. According to security analysis, the scheme can withstand replay attacks, impersonation attacks, DoS attacks, and various other network attacks. Since the proposed approach applies only the one-

Table 3 Cost of the proposed protocol in all the three phases

Phase	Overhead cost			
	U_i	Base station	Master node (gateway node)	Sensor node
Registration	$C_{\rm ub}$	$(5+n)T_h + (3+n)T_{\rm XOR} + C_{\rm ub}$		
Login	$6T_h + 3T_{\rm XOR} + C_{\rm um}$			
Authentication	$6T_h + 3T_{\rm XOR}$		$6T_h + 2T_{\rm XOR} + C_{\rm um} + C_{\rm ms}$	$2T_h$

way hash function and exclusive-OR operations, it is suitable for the resource constrained sensor nodes. To the best of our knowledge, there has to date been no user authentication scheme for two-tiered WSNs. In conclusion, our proposed authentication scheme for two-tiered WSNs is efficient and secure enough to be applied in the real world.

References

Awasthi, A., 2004. Comment on a dynamic ID-based remote user authentication scheme. *Trans. Cryptol.*, **1**(2):15-17.

Awasthi, A., Lal, S., 2004. An enhanced remote user authentication scheme using smart cards. *IEEE Trans. Consum. Electron.*, **50**(2):583-586. [doi:10.1109/TCE.2004.1309430]

Benenson, Z., Gedicke, N., Raivio, O., 2005. Realizing Robust User Authentication in Sensor Networks. Proc. Workshop on Real-World Wireless Sensor Networks, p.1-5.

Chang, C.C., Wu, T.C., 1991. Remote password authentication with smart cards. *IEE Proc. E Comput. Digit. Tech.*, **138**(3):165-168. [doi:10.1049/ip-e.1991.0022]

Das, M.L., 2009. Two-factor user authentication in wireless sensor networks. *IEEE Trans. Wirel. Commun.*, **8**(3):1086-1090. [doi:10.1109/TWC.2008.080128]

Das, M.L., Saxena, A., Gulati, V.P., 2004. A dynamic ID-based remote user authentication scheme. *IEEE Trans. Consum. Electron.*, **50**(2):629-631. [doi:10.1109/TCE.2004.1309441]

Desnoyers, P., Ganesan, D., Shenoy, P., 2005. TSAR: a Two Tier Sensor Storage Architecture Using Interval Skip Graphs. Proc. 3rd Int. Conf. on Embedded Networked Sensor Systems, p.39-50. [doi:10.1145/1098918.1098923]

Diao, Y., Ganesan, D., Mathur, G., Shenoy, P.J., 2007. Rethinking Data Management for Storage-Centric Sensor Networks. Proc. Conf. on Innovative Data Systems Research, p.22-31.

Dolev, D., Yao, A., 1983. On the security of public key protocols. *IEEE Trans. Inform. Theory*, **29**(2):198-208. [doi:10.1109/TIT.1983.1056650]

Du, W., Deng, J., Han, Y., Varshney, P., 2003. A Pairwise Key Predistribution Scheme for Wireless Sensor Networks. ACM Conf. on Computer and Communications Security, p.42-51.

Eschenauer, L., Gligor, V.D., 2002. A Key-Management Scheme for Distributed Sensor Networks. Proc. 9th ACM Conf. on Computer and Communications Security, p.41-47. [doi:10.1145/586110.586117]

Fan, C.I., Chan, Y.C., Zhang, Z.K., 2005. Robust remote authentication scheme with smart cards. *Comput. & Secur.*, **24**(8):619-628. [doi:10.1016/j.cose.2005.03.006]

Gnawali, O., Jang, K.Y., Paek, J., Vieira, M., Govindan, R., Greenstein, B., Joki, A., Estrin, D., Kohler, E., 2006. The Tenet Architecture for Tiered Sensor Networks. Proc. 4th Int. Conf. on Embedded Networked Sensor Systems, p.153-166. [doi:10.1145/1182807.1182823]

He, D.J., Cui, L., Huang, H., Ma, M., 2009. Design and verification of enhanced secure localization scheme in wireless sensor networks. *IEEE Trans. Parall. Distr. Syst.*, **20**(7):1050-1058. [doi:10.1109/TPDS.2008.166]

He, D.J., Gao, Y., Chan, S., Chen, C., Bu, J.J., 2010. An enhanced two-factor user authentication scheme in wireless sensor networks. *Int. J. Ad Hoc Sensor Wirel. Networks*, **10**(4):361-371.

He, D.J., Ma, M., Zhang, Y., Chen, C., Bu, J.J., 2011. A strong user authentication scheme with smart cards for wireless communications. *Comput. Commun.*, **34**(3):367-374. [doi:10.1016/j.comcom.2010.02.031]

Hsiang, H.C., Shih, W.K., 2009. Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment. *Comput. Stand. Interfaces*, **31**(6):1118-1123. [doi:10.1016/j.csi.2008.11.002]

Hwang, M.S., Li, L.H., 2000. A new remote user authentication scheme using smart cards. *IEEE Trans. Consum. Electron.*, **46**(1):28-30. [doi:10.1109/30.826377]

Jiang, Y., Lin, C., Shen, X., Shi, M., 2006. Mutual authentication and key exchange protocols for roaming services in wireless mobile networks. *IEEE Trans. Wirel. Commun.*, **5**(9):2569-2577. [doi:10.1109/TWC.2006.05063]

Lazos, L., Poovendran, R., 2004. SeRLoc: Secure Range-Independent Localization for Wireless Sensor Networks. Proc. 3rd ACM Workshop on Wireless Security, p.21-30. [doi:10.1145/1023646.1023650]

Lee, C.C., Hwang, M.S., Liao, I.E., 2006. Security enhancement on a new authentication scheme with anonymity for wireless environments. *IEEE Trans. Ind. Electron.*, **53**(5):1683-1687. [doi:10.1109/TIE.2006.881998]

Lee, C.Y., Lin, C.H., Chang, C.C., 2005. An Improved Low Communication Cost User Authentication Scheme for Mobile Communication. 19th Int. Conf. on Advanced Information Networking and Applications, p.249-252. [doi:10.1109/AINA.2005.106]

Lee, J.S., Chang, J.H., Lee, D.H., 2009. Security flaw of authentication scheme with anonymity for wireless communications. *IEEE Commun. Lett.*, **13**(5):292-293. [doi:10.1109/LCOMM.2009.090074]

Liao, Y.P., Wang, S.S., 2009. A secure dynamic ID based remote user authentication scheme for multi-server environment. *Comput. Stand. Interfaces*, **31**(1):24-29. [doi:10.1016/j.csi.2007.10.007]

Liu, D., Ning, P., 2003. Establishing Pairwise Keys in Distributed Sensor Networks. ACM Conf. on Computer and Communications Security, p.52-61.

Ren, K., Lou, W., Zhang, Y., 2008. LEDS: providing location-aware end-to-end data security in wireless sensor networks. *IEEE Trans. Mob. Comput.*, **7**(5):585-598. [doi:10.1109/TMC.2007.70753]

Shi, J., Zhang, R., Zhang, Y., 2009. Secure Range Queries in Tiered Sensor Networks. IEEE INFOCOM, p.945-953. [doi:10.1109/INFCOM.2009.5062005]

Tsai, J.L., 2008. Efficient multi-server authentication scheme based on one-way hash function without verification table. *Comput. & Secur.*, **27**(3-4):115-121. [doi:10.1016/j.cose.2008.04.001]

Wong, K.H.M., Zheng, Y., Cao, J.N., Wang, S.W., 2006. A Dynamic User Authentication Scheme for Wireless Sensor Networks. IEEE Int. Conf. on Sensor Networks, Ubiquitous, and Trustworthy Computing, **1**:244-251. [doi:10.1109/SUTC.2006.1636182]

Wu, C.C., Lee, W.B., Tsaur, W.J., 2008. A secure authentication scheme with anonymity for wireless communications. *IEEE Commun. Lett.*, **12**(10):722-723. [doi:10.1109/LCOMM.2008.080283]

Xu, J., Feng, D., 2009. Security flaws in authentication protocols with anonymity for wireless environments. *ETRI J.*, **31**(4):460-462. [doi:10.4218/etrij.09.0209.0026]

Zeng, P., Cao, Z., Choo, K.K., Wang, S., 2009. On the anonymity of some authentication schemes for wireless communications. *IEEE Commun. Lett.*, **13**(3):170-171. [doi:10.1109/LCOMM.2009.081821]

Zhang, R., Shi, J., Zhang, Y., 2009. Secure Multidimensional Range Queries in Sensor Networks. Proc. 10th ACM Int. Symp. on Mobile Ad Hoc Networking and Computing, p.197-206. [doi:10.1145/1530748.1530777]

Zhang, Y., Liu, W., Fang, Y., Wu, D., 2006. Secure localization and authentication in ultra-wideband sensor networks. *IEEE J. Sel. Areas Commun.*, **24**(4):829-835. [doi:10.1109/JSAC.2005.863855]

Zhou, Y., Fang, Y., 2007. A two-layer key establishment scheme for wireless sensor networks. *IEEE Trans. Mob. Comput.*, **6**(9):1009-1020. [doi:10.1109/TMC.2007.1008]

Zhou, Y., Zhang, Y., Fang, Y., 2007. Access control in wireless sensor networks. *Ad Hoc Networks*, **5**(1):3-13. [doi:10.1016/j.adhoc.2006.05.014]