User authentication schemes with pseudonymity for ubiquitous sensor network in NGN

Binod Vaidya1, Joel J. Rodrigues2 and Jong Hyuk Park3,∗,†

1Instituto de Telecomunicações, Covilhã, Portugal
2Instituto de Telecomunicações, University of Beira Interior, Covilhã, Portugal
3Department of Computer Science and Engineering, Seoul National University of Technology, Seoul, Korea

SUMMARY

Owing to the ubiquitous nature, ease of deployment, and wide range of potential applications, wireless sensor networks (WSNs) have received a lot of attention recently. WSNs can be deployed in unattended environments; however, they have many challenges. It should be guaranteed that not only illegitimate users cannot login and access data in the network but also user privacy should be maintained. Since sensor nodes have limited computation power, storage, and energy, it is desirable for the authentication protocol to be simple and secure. In this paper, we propose two user authentication protocols that are variations of a recent strong-password-based solution. It uses one-way hash functions and XOR operations to achieve lower computational and communication overheads. We have analyzed the performance of both the proposed authentication schemes in terms of various metrics. We have also provided security evaluation of the proposed protocols. Comparing with the previous schemes, our proposed schemes are more robust and provide better security. Copyright © 2009 John Wiley & Sons, Ltd.

Received 30 March 2009; Revised 9 September 2009; Accepted 3 October 2009

KEY WORDS: wireless sensor network; user authentication; pseudonymity; next generation network

1. INTRODUCTION

Wireless sensor networks (WSNs) have received a lot of attention recently due to the ubiquitous nature, ease of deployment, and wide range of potential applications [1]. They usually consist of a large number of low-cost, battery-powered sensor nodes that are of limited computation and communication capability and communicate over an ad hoc wireless network. In fact, the WSNs are the key players in the next-generation network (NGN) for moving toward a ubiquitous world. Nowadays applications using the WSNs are considered such as collection and management...
of environment data, emergency medical system, smart buildings, target tracking, monitoring of
critical infrastructures, etc., and it is expected to expand rapidly to various fields around our world.
In many applications, integrity and confidentiality of collected data as well as user privacy will
be a critical concern. Therefore, it is important not only to authenticate users who access the data
directly from sensor node but also to provide privacy to the user.
Furthermore, the IEEE 802.15.4 [2] is the most appropriate communication protocol for low-
power sensor networks, which will be one of the key components for the NGN. It is believed
that next-generation low-power sensor networks will be mainly based on solar-power. Hence, the
next-generation solar-powered sensor devices require very light-weight authentication protocol.
In past years, many user authentication schemes [3–9] have been proposed. Some user authen-
tication protocols are suitable for wireless mobile devices [10, 11] and some for low-power
devices [12].
However, deploying low-power sensor nodes in an unattended environment makes the networks
vulnerable to a variety of potential attacks, the inherent power and memory limitations of sensor
nodes make conventional security solutions infeasible. Only in recent years, a number of research
works [13–18] have focussed on the user authentication schemes suited for WSNs.
In the paper [13], n-authentication protocol is introduced, in which the whole authentication
succeeds if the user can successfully authenticate with any subset of sensors out of a set of n
sensors. Benenson et al. [14] proposed a public key-based user authentication protocol using Elliptic
Curve Cryptography (ECC) as in [19]. This user authentication protocol is more feasible for WSNs
than TinyPK [20]. In 2006, Wong et al. [16] proposed a strong-password-based dynamic user
authentication scheme, which imposes very light computational load as it requires only one-way
hash function and exclusive-OR operations. More improved dynamic user authentication schemes
are presented in [17, 18].
However, most of the above-mentioned schemes cannot preserve user anonymity. In order to
protect the real identity of the user, pseudonym can be used in WSNs. Random dynamic pseudonym,
such as hashing-based ID random pseudonym, can be the ideal solution for hiding real identity of
the user. Hence, some researchers have proposed user authentication protocols with user anonymity
for distributed computing environments [21–23] as well as for wireless environments [24, 25].
However, only few research works have focussed on user authentication scheme with privacy
protection [26].
In this paper, we propose two dynamic user authentication protocols with user privacy that are
variations of the strong-password-based schemes. It uses one-way hash functions and XOR oper-
ations to achieve lower computational and communication overheads. Furthermore, our schemes
have not only user privacy but also mutual authentication.
The rest of this paper is organized as follows. In Section 2, we present the related work whereas
in Section 3, we provide cryptoanalysis of the previous schemes. Section 4 describes our proposed
user authentication protocols whereas Section 5 discusses the security analysis as well as efficiency
analysis of the proposed protocols. Section 6 describes about the performance evaluation of the
proposed schemes and finally, Section 7 concludes the paper and points out future works.

2. RELATED WORKS

This section describes the existing works related to our proposed schemes. Wong et al. proposed
a light-weight strong-password-based dynamic user authentication protocol for WSNs [16].
It consists of three phases: Registration, Login, and Authentication. Figure 1 shows the registration process whereas Figure 2 depicts login and authentication processes.

The communication flows for the three phases are summarized in Figure 3. They have claimed in [16] that, if Registration phase is carried out in a secure mode, the above protocol is resistant to attacks such as valid userID, fake PW; invalid userID, valid/fake PW; and replay login request with or without modifying the login message.

Later, Tseng et al. [17] pointed out several weaknesses in Wong et al.’s scheme, and proposed an improved scheme to overcome the weaknesses and allow legitimate users to change their password freely. Thus, it consists of four phases: Registration, Login, Authentication, and Password changing. The communication flows for Tseng et al.’s scheme are summarized in Figure 4. Tseng et al. [17] claimed that their scheme not only retains all advantages in Wong et al.’s scheme but also possesses many advantages, including resistance to the replay and forgery attacks, reduction of users password leakage risk, capability of changeable password, and better efficiency.
Furthermore, Ko [18] showed that Tseng et al.’s scheme still comes with several drawbacks that might cause authentication mechanism insecure; thus proposed a novel scheme, which not only inherits all the advantages of Tseng et al.’s scheme but also achieves mutual authentication and enhances its security strength. The communication flows for Ko’s scheme are summarized in Figure 5.

3. CRYPTANALYSIS OF REPRESENTATIVE SCHEMES

In this section, we provide cryptanalysis of three existing representative user authentication schemes that are suitable for WSNs. Although Wong et al. proposed a dynamic user authentication scheme that allows legitimate users to query at any of the sensor nodes and imposes very light computational load, there still remains several security weaknesses in their scheme. Tseng et al. showed some of the security weaknesses in Wong et al.’s scheme. In the paper [18], Ko showed some of the security weaknesses in Tseng et al.’s scheme as well.
At this point, we show some of the security weaknesses for three existing schemes, namely, Wong et al.’s scheme [16], Tseng et al.’s scheme [17] and Ko’s scheme [18].

3.1. Wong et al.’s scheme

3.1.1. Forgery attacks with node capture attacks

1. Capture node LN to obtain $UID$, $A$, $TS$.
2. Eavesdrop login message $UID$, $PW$.
3. Compute $B_e = H(A \| H(PW))$; $C_{1e} = H(T' \oplus B_e)$; $C_{2e} = B_e \oplus A$.
4. Send $UID$, $C_{1e}$, $C_{2e}$, $T'$ to GW.
5. As long as $(T - T') < \Delta T$ then the attack will be successful.
3.1.2. Replay attacks on Acc_login. The replay attacks on Acc_login can occur in two ways:

First way

1. Suppose a malicious intermediate node has intercepted and stored Acc_login from GW before forwarding it to LN.
2. In the next session, when this malicious node receives message to GW from legitimate LN, it just drops that message and replays the stored Acc_login to LN as pretending legal GW.
3. Since LN does not check the correctness, it will forward Acc_login to UD.
4. UD will accept Acc_login as it also does not check the correctness.

Second way
1. While transmitting Acc_login from LN to UD, an adversary node can eavesdrop it.
2. Next time the login message from UD can be blocked by the adversary node.
3. The captured Acc_login message is replayed to UD as pretending legal LN.
4. As UD does not check the correctness, it will be counterfeited.

3.1.3. Stolen verifier attack with node capture attack
1. Steal PW for UID from GW.
2. Break node LN to get UID, A, TS.
3. Send UID, PW as login message to LN as pretending legal UD.
4. The attack will be successful.

3.1.4. Secret key forward secrecy
1. Suppose secret key x is revealed to an adversary node.
2. Login message UID, PW is eavesdropped by this adversary node.
3. It computes $A_e = H(UID||x)$; $B_e = H(A||H(PW))$.
4. Then it computes $C_{1e} = H(T' \oplus B_e)$; $C_{2e} = B_e \oplus A$.
5. It sends $UID, C_{1e}, C_{2e}, T'$ to GW.
6. If $(T - T') < \Delta T$ is true, it cannot provide forward secrecy.

3.2. Tseng et al.'s scheme

3.2.1. Replay attacks on Acc_login. The replay attacks on Acc_login can occur in two ways as similar to Wong et al.'s scheme.

First way
1. While transmitting Acc_login from GW to LN, the malicious intermediate node can intercept it before forwarding it.
2. Next time when this malicious node receives message to GW from legitimate LN, it just drops that message and replays the captured Acc_login to LN as pretending legal GW.
3. LN does not check the correctness, so it will also send Acc_login to UD.
4. UD will accept Acc_login as it also does not check the correctness.

Second way
1. While transmitting Acc_login from LN to UD, adversary node can eavesdrop it.
2. Next time the login message from UD can be blocked by adversary node.
3. The captured Acc_login message is replayed to UD as pretending legal LN.
4. As UD does not check the correctness, it will be counterfeited.

3.2.2. Man-in-the-middle attacks
1. UID, A, t is intercepted or eavesdropped.
2. UID, C, T, t is also intercepted.
3. $C^* = H(A \oplus T^*)$ is then computed.
4. $UID, C^*, T^*, t$ is forwarded to GW.
5. For verification, $A$ and $C'^* = H(A \oplus T^*)$ will be computed by GW.
6. As long as $(T - T^*) < \Delta T$ is valid, $C^*$ will be same as $C'^*$.

### 3.2.3. Stolen verifier attack with node capture attack

1. Steal $H(PW)$ for UID from GW.
2. During password changing phase, $H(PW)$ is changed $H(PW_1)$ for $UID$.
3. Again steal $H(PW_1)$ from GW.
4. Trace the changes of $H(PW)$ for $UID$ for sometime.
5. Then break LN to get $UID, T_{S_1}$ and learn the timestamp for that $UID$.
6. Then the adversary computes $A_{ie} = H(H(PW_1) \oplus t_{ie})$.
7. Send $UID, A_{ie}, t_{ie}$ as login message to LN.
8. As long as validity of message is within allowed time interval, this kind of attack will be successful.

### 3.3. Ko’s scheme

#### 3.3.1. Stolen verifier attack with node capture attacks

1. Break LN to get $UID, N, TS$.
2. Steal $H(PW)$ for $UID$ from GW.
3. Compute $h(x \oplus UID) = N \oplus H(PW)$.
4. Password is changed $H(PW_1)$ for $UID$.
5. Break LN to get $UID, N_1, T_{S_1}$.
6. Compute $H(PW_1) = N_1 \oplus h(x \oplus UID)$.
7. Knowing legitimate $UID$, it can generate $A_e = (H(PW_1) \oplus t_{ie})$.
8. Send login message $(UID, A_e, t_{ie})$ to LN.
9. As long as validity of message is within allowed time interval, this kind of attack will be successful.

### 4. PROPOSED USER AUTHENTICATION SCHEMES

In this section, we propose two user authentication schemes to overcome the above-stated weaknesses and improve security. In our first proposed scheme, it is assumed that as one-hop communication between UD and LN occurs, it is less likely to have malicious action. Hence, we have only considered mutual authentication between GW and LN. Our second proposed scheme considers mutual authentication between not only GW and LN but also GW and UD. Compared with the first scheme, the second scheme has advantage of being resistant to the attack of an intruder impersonating the GW to grant access right to illegitimate users. The tradeoff is a slight increase in the computational load and the communication cost.

Our design goal is to reduce potential problems caused by illegitimate users and compromised sensor nodes; thus protecting honest sensor nodes from DOS attacks and user privacy from all the sensor nodes. In addition, we will propose user authentication schemes to satisfy the following...
Table I. Notations used in the proposed schemes.

<table>
<thead>
<tr>
<th>Notation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UD</td>
<td>User’s device such as PDA, PC</td>
</tr>
<tr>
<td>GW</td>
<td>Registration Sensor Gateway</td>
</tr>
<tr>
<td>LN</td>
<td>Sensor Login node</td>
</tr>
<tr>
<td>$N_0, N_1$</td>
<td>Random nonces</td>
</tr>
<tr>
<td>$\oplus$</td>
<td>Exclusive-OR (XOR) operation</td>
</tr>
<tr>
<td>$\parallel$</td>
<td>Concentration</td>
</tr>
<tr>
<td>Succ_Reg</td>
<td>Successful Registration message</td>
</tr>
<tr>
<td>Acc_login</td>
<td>Accept login message</td>
</tr>
<tr>
<td>Succ_Chang</td>
<td>Successful Changes message</td>
</tr>
<tr>
<td>$x$</td>
<td>Secret key known to the GW</td>
</tr>
<tr>
<td>UID</td>
<td>User’s identity</td>
</tr>
<tr>
<td>TID</td>
<td>Temporary User ID</td>
</tr>
<tr>
<td>PW</td>
<td>Password chosen by user</td>
</tr>
<tr>
<td>TS</td>
<td>Timestamp for particular user</td>
</tr>
<tr>
<td>$t, T, T_i$</td>
<td>Current time recorded by one of the nodes</td>
</tr>
<tr>
<td>$\Delta T$</td>
<td>Allowed time interval for transmission delay</td>
</tr>
</tbody>
</table>

requirements:

- **Mutual authentication**: Mutual authentication between GW and LN as well as between GW and UD are desired to prevent forgery attacks.

- **User pseudonymity**: If the ID of a user is revealed during user authentication process, it will violate user privacy because every sensor node (GW or LN) is vulnerable to ‘node capture attack’ by which an attacker can easily track the movement of the user.

- **Lightweight**: Typical sensor nodes, such as Telosb or MicaZ, have very limited resources and limited energy. Therefore, the scheme must be efficient in terms of communication and computation in order to reduce the energy consumption of sensor node.

Both schemes are composed of four phases: the registration phase, the login phase, the authentication phase, and the ID/password change phase. Table I shows notations used in the proposed schemes.

4.1. **First proposed scheme**

In Registration phase (Figure 6), the UD randomly chooses a password $PW$ and calculates $vpw = H(PW)$. Afterwards, the UD submits its identity $UID$ and $vpw$ to the GW in a secure way. The GW computes $TID = g \oplus N_0$ and $A = X = H(TID \parallel x)$. Then the GW replies to the user for successful registration with $N_0$, stores $(TID, vpw, X, TS)$, and distributes $(TID, X, TS)$ to those sensor nodes that are able to provide a login interface to users. On receiving $N_0$ from GW, UD obtains $TID = g \oplus N_0$.

The message flow for Registration phase is as follows:

*Step R1. UD*: Compute $vpw = H(PW)$

*Step R2. UD $\Rightarrow$ GW*: $UID$, $vpw$

*Step R3. GW*: Compute $g = H(UID)$;

*Generate $N_0$;*
Figure 6. Communication flows for the first proposed scheme.

Compute $TID = g \oplus N_0$ and $X = H(TID\|x)$;

Store $TID$, $vpw$, $X$, $TS$.

**Step R4.** $GW \Rightarrow UD$: $Succ\_Reg(N_0)$

**Step R5.**

$UD$: Compute $g = H(UID)$;

Get $TID = g \oplus N_0$;

Store $TID$. 
Step R6. GW $\Rightarrow$ LNs: TID, X, TS

Step R7. LN: Store TID, X, TS

In Login phase, a user submits $(TID, A, t)$ to a login node. Upon receiving the login request at time $T_0$, the login node checks its lookup table to see if $TID$ is a valid user and checks $T_0 - t \geq \Delta T$. If it is not true, the login request will be rejected. Otherwise, the login node retrieves the corresponding $A$ and computes $C_K = (X \oplus A \oplus T_0)$. It then sends $(TID, C_K, T_0, t)$ to the GW.

Step L1. UD: Compute $A = H(vpw\|t)$
Step L2. UD $\Rightarrow$ LN: TID, A, t
Step L3.

LN: Check TID

Check $T_0 - t \geq \Delta T$
Compute $C_K = (X \oplus A \oplus T_0)$

Step L4. LN $\Rightarrow$ GW: TID, $C_K$, $T_0$, $t$

In Authentication phase, the GW checks whether or not TID is a valid user and $t$. The login request is rejected if it is not. Otherwise, the GW verifies if $T_1 - T_0 \geq \Delta T; T_0 - t \geq \Delta T$. If the condition is satisfied, then the login request is considered as a replay message and thus is rejected. On the other hand, the GW retrieves the corresponding $vpw$ and $A$ and computes $A' = H(vpw\|t)$ and $C'_K = (X \oplus A' \oplus T_0)$. A reject message is sent to the login node if $C_K \neq C'_K$. Otherwise, computes $V_M = H(X||A'||T_1)$ and sends accept message $(Acc_{login}, V_M, T_1)$ to the login node which, in turn, is forwarded to the user.

Step A1.

GW: Check TID, $t$

Check $T_1 - T_0 \geq \Delta T; T_0 - t \geq \Delta T$
Compute $A' = H(vpw\|t)$
Compute $C'_K = (X \oplus A' \oplus T_0)$
Verify $C_K = C'_K$
Compute $V_M = H(X\|A'||T_1)$
Store $t$

Step A2. GW $\Rightarrow$ LN: Acc_{login}, $V_M$, $T_1$

Step A3.

LN: Check $T_2 - T_1 \geq \Delta T$

Compute $V'_M = H(X\|A\|T_1)$
Verify $V_M = V'_M$

Step A4. LN $\Rightarrow$ UD: Acc_{login}
In the Password-changing phase, UD changes his password \( PW \) to \( PW_1 \). Then it computes \( vpw_1 = H(PW_1) \) and sends the triple \((TID, vpw, vpw_1)\) to the GW in the secure channel. The GW computes \( TID, X_1, TID'_1 \), and sends success change \( Succ\_Change(N_1) \) to the UD. At the same time, the GW distributes updated information to all the LNs. Upon receiving updates, LNs obtain \( TID'_1 \) and update their databases.

**Step P1. UD**: Compute \( vpw_1 = H(PW_1) \)

**Step P2. UD \( \Rightarrow \) GW**: \( TID, vpw, vpw_1 \)

**Step P3. GW**: Generate \( N_1 \)

\[
\text{Compute } TID_1 = g \oplus N_1 \\
\text{Compute } X_1 = H(TID_1 \parallel x) \\
\text{Compute } TID'_1 = TID_1 \oplus X \\
\text{Update } TID, vpw, X, TS
\]

**Step P4. GW \( \Rightarrow \) UD**: \( Succ\_Change(N_1) \)

**Step P5. UD**: Obtain \( TID_1 = g \oplus N_1 \)

**Step P6. GW \( \Rightarrow \) LNs**: \( TID, TID'_1, X_1, TS_1 \)

**Step P7. LN**: Obtain \( TID_1 = TID'_1 \oplus X \)

\[
\text{Update } TID, X, TS
\]

The communication flow of the first proposed scheme is shown in Figure 6.

### 4.2. Second proposed scheme

The second proposed scheme differs from the first scheme with slight changes in Registration and Password changing phases whereas major changes in Authentication phase.

In the Registration phase, while sending \( Succ\_Reg \) message it also includes \( X \). Upon receiving this message, UD will store \( X \) for future use. Here, S1(Step R4) is same as Step R4 of the first proposed scheme, while S2(Step R5) represents Step R5.

**S1 (Step R4.) GW \( \Rightarrow \) UD**: \( Succ\_Reg(X, N_0) \)

**S2 (Step R5.) UD**: \( Store \ TID, X \)

In the Application phase, after verification of \( V_M = V_M' \), it computes \( Y_K = H(V_M' \parallel T_2) \). The LN sends \((Acc\_login, Y_K, T_1, T_2)\) to the UD. Upon receiving the message at time \( T_3 \), the UD checks if \( T_1 - T_0 \geq \Delta T; T_0 - t \geq \Delta T \). If the conditions are true, then the login request is rejected. Otherwise, the login node retrieves the corresponding \( A \), performs \( V_M'' = H(X \parallel A \parallel T_1) \) and \( Y_K' = H(V_M'' \parallel T_2) \), and checks if \( Y_K = Y_K' \). If it is true, then the UD starts obtaining data if the condition holds. Otherwise, accept login message is rejected. Similarly, here, S1(Step A3) is same as Step A3 of the first proposed scheme, and so on.
S1 (Step A3.)

**LN:**  \( \text{Check } T_2 - T_1 \geq \Delta T \)

Compute \( V_M' = H(X \| A \| T_1) \)

Verify \( V_M = V_M' \)

Compute \( Y_K = H(V_M' \| T_2) \)

S2 (Step A4.) **LN \Rightarrow UD:** Acc_login, \( Y_K, T_1, T_2 \)

S3 (Step A5.)

**UD:**  \( \text{Check } T_1 - T_0 \geq \Delta T; T_0 - t \geq \Delta T \)

Compute \( V_M'' = H(X \| A \| T_1) \)

Compute \( Y_K' = H(V_M'' \| T_2) \)

Verify \( Y_K = Y_K' \)

In the Password-changing phase, as in registration phase, \( X_1 \) is send along Succ_Change(\( N_1 \)) by the GW to UD. Likewise, here, S1(Step P4) represents Step P4 of the first proposed scheme, and so on.

S1 (Step P4.) **GW \Rightarrow UD:** Succ_Change(\( X_1, N_0 \))

S2 (Step P5.) **UD:** Update \( X \)

Communication flows for the second proposed scheme is depicted in Figure 7.

5. ANALYSIS OF THE PROPOSED SCHEMES

In this section, we analyze the performance evaluation and security of our proposed schemes. The Access Control List (ACL) and security modes of IEEE 802.15.4 specification can be incorporated into our proposed protocols to provide data confidentiality on frame level at the MAC sub-layer in all three phases.

The security property that one-way hash function is computationally infeasible to inverse [27] is employed.

5.1. Security analysis

Proclaim 1

The proposed schemes can resist a replay attack of login message.

Proof

Assume an adversary eavesdrops the login message sent by \( UD_i \) and uses it to impersonate \( UD_i \) when logging into the LN in a later session. However, the replay of \( UD_i \)'s previous login message will be detected by the GW since the user has already bound the current timestamp \( t \) into the login message according to Step L1, and the GW will check the user's TID and the timestamp \( t \) used by \( UD_i \). Therefore, the adversary cannot replay the login message. \( \square \)
Proclaim 2
The proposed schemes can resist a replay attack on accept login message.

Proof
As every message received at every node is checked whether it is within the allowed time interval $\Delta T$, replaying any messages can be easily noticed and discarded. For this purpose, time synchronization mechanism [28–31] for WSNs is required.

The proposed schemes can resist replay attack of Acc_login message in two ways.
1. While transmitting $Acc_{login}$ from GW to LN, the malicious intermediate node can intercept it before forwarding it.
2. Next session when this malicious node receives message to GW from legitimate LN, it just drops that message and the captured $Acc_{login}$ is replayed to LN as pretending legal GW.
3. LN verifies by equation; it will reject if the condition does not meet.

or

1. While transmitting $Acc_{login}$ from LN to UD, adversary node can eavesdrop it.
2. Next session the login message from UD can be blocked by adversary node.
3. The captured $Acc_{login}$ message is replayed to UD as pretending legal LN.
4. As UD check the correctness, it will reject if the condition does not meet.

$Proclaim 3$

The proposed schemes can resist a forgery attack with node capture attack.

$Proof$

The proposed schemes can resist a forgery attack in two ways.

1. Eavesdrops or intercepts login message $(TID, C_K, T_0, t)$.
2. Captures LN to get $TID, X, TS$.
3. Adversary cannot compute $C_K$ since it does not know $A$.

or

1. Captures LN to get $TID, X, TS$.
2. Eavesdrop login message $TID, A, t$.
3. Computes $C_{Ke} = H(X \oplus A \oplus T_e)$ with timestamp $T_e$.
4. Sends $TID, C_{Ke}, T_e, t$ to GW.
5. Failed as $t$ is already in the database.

$Proclaim 4$

The proposed schemes can resist an MITM attack.

$Proof$

The proposed schemes can resist a MITM attack in the following way:

1. $TID, A, t$ is intercepted or eavesdropped.
2. Intercepts $TID, C_K, T_0, t$.
3. Adversary cannot compute $C_K$ since it does not know $X$.

$Proclaim 5$

The proposed schemes can resist a stolen verifier attack even if the node is compromised.

$Proof$

The proposed schemes can resist a stolen verifier attack in the following way:

1. Steal $vpw$ for $TID$ from GW.
2. During password changing phase, $vpw$ is changed $vpw_1$ along with change of $TID$. 
3. As \( TID_1 \) is not disclosed during password changing phase, the adversary will not be able to identify \( vpw_1 \) for \( TID_1 \) from GW.

4. The adversary can break LN to get \( TID_1, X_1, TS_1 \) to learn the timestamp for that \( TID_1 \).

5. Although the adversary computes \( A_{ie} = H(vpw_i \oplus t_{ie}) \), it will be rejected by the GW.

\[ \square \]

**Proclaim 6**

The proposed schemes can provide secret key forward secrecy.

**Proof**

Suppose secret key \( x \) of the GW is revealed to an adversary. Although the adversary eavesdrops the login message \( TID, A, t \), it would not be able to compute \( C_K \) without knowing \( X \).

\[ \square \]

**Proclaim 7**

The proposed schemes can provide user pseudonymity.

**Proof**

If an adversary eavesdrops the login message, it cannot extract the user’s identity from the \( TID \) since user’s identity (\( UID \)) is hashed and is XORed with \( N_0 \), during the registration phase. In addition, due to the use of the nonce, every time the user changes his password, it also changes his \( TID \). Hence, it is difficult for the adversary to discover a user’s identity. Clearly, the proposed schemes can provide user pseudonymity.

\[ \square \]

**Proclaim 8**

The proposed schemes can provide mutual authentication.

**Proof**

Both the proposed schemes can provide mutual authentication between GW and LN. In those schemes, the LN gives \( C_K \) and the GW gives \( X \) during login phase and during registration phase, respectively. Therefore, LN and the GW can use \( X \) and \( C_K \), respectively, to realize mutual authentication between the GW and the LN.

Furthermore, the second proposed scheme can provide mutual authentication between GW and UD. In case of the second proposed scheme, the UD gives \( vpw \) and the GW gives \( X \) (securely exchange) during registration phase. Therefore, UD and the GW can use \( X \) and \( vpw \), respectively, to realize mutual authentication between the GW and the UD.

\[ \square \]

5.2. Efficiency analysis

We examine the performance of our proposed schemes. We use overheads cost as a metric to evaluate the performance of the proposed schemes with the existing representative schemes such as Wong et al.’s scheme [16], Tseng et al.’s scheme [17], and Ko’s scheme [18]. The evaluation parameters used are shown in Table II.

The number of elements contained in transmitted messages is not considered in the comparison. Table III summarizes the comparisons of the three representative schemes and our two proposed schemes in terms of overheads cost.

From Table III, it can be seen that the overheads cost for the first proposed scheme is only slightly higher than those of Wong et al.’s scheme and Tseng et al.’s scheme, and the second proposed scheme has quite higher overheads cost than the two formal existing schemes. It is
Table II. Evaluation parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$K$</td>
<td>The number of sensor nodes that are able to provide a login interface to users</td>
</tr>
<tr>
<td>$T_H$</td>
<td>The time for performing a one-way hash function</td>
</tr>
<tr>
<td>$T_{XOR}$</td>
<td>The time for performing an XOR operation</td>
</tr>
<tr>
<td>$C_{MH}$</td>
<td>The delay time for the communication taken place between the LN and the GW in multi-hops</td>
</tr>
</tbody>
</table>

Table III. Comparison among representative schemes and the proposed schemes in terms of overheads cost.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Registration</th>
<th>Login</th>
<th>Authentication</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wong et al.’s</td>
<td>$3T_H + KC_{MH}$</td>
<td>$3T_H + 2T_{XOR} + 1C_{MH}$</td>
<td>$1T_H + 2T_{XOR} + 1C_{MH}$</td>
<td>$7T_H + 4T_{XOR} + (K + 2)C_{MH}$</td>
</tr>
<tr>
<td>scheme [16]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tseng et al.’s</td>
<td>$1T_H + KC_{MH}$</td>
<td>$2T_H + 2T_{XOR} + 1C_{MH}$</td>
<td>$2T_H + 2T_{XOR} + 1C_{MH}$</td>
<td>$5T_H + 4T_{XOR} + (K + 2)C_{MH}$</td>
</tr>
<tr>
<td>scheme [17]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ko’s scheme [18]</td>
<td>$2T_H + 2T_{XOR} + KC_{MH}$</td>
<td>$3T_H + 3T_{XOR} + 1C_{MH}$</td>
<td>$11T_H + 13T_{XOR} + 1C_{MH}$</td>
<td>$16T_H + 18T_{XOR} + (K + 2)C_{MH}$</td>
</tr>
<tr>
<td>First proposed</td>
<td>$4T_H + 2T_{XOR} + KC_{MH}$</td>
<td>$2T_H + 2T_{XOR} + 1C_{MH}$</td>
<td>$4T_H + 2T_{XOR} + 1C_{MH}$</td>
<td>$10T_H + 6T_{XOR} + (K + 2)C_{MH}$</td>
</tr>
<tr>
<td>scheme</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Second proposed</td>
<td>$4T_H + 2T_{XOR} + KC_{MH}$</td>
<td>$2T_H + 2T_{XOR} + 1C_{MH}$</td>
<td>$7T_H + 2T_{XOR} + 1C_{MH}$</td>
<td>$13T_H + 6T_{XOR} + (K + 2)C_{MH}$</td>
</tr>
<tr>
<td>scheme</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table IV. Comparison among representative schemes and the proposed schemes in terms of functional requirements.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Password changing</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Mutual authentication between GW and LN</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Mutual authentication between GW and UD</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>User pseudonymity</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

due to fact that in order to provide full mutual authentication between GW and LN as well as GW and UD, more computational overheads are incorporated. However, while comparing with Ko’s scheme, both our proposed schemes have much lesser overheads cost than it. It should be noticed that both our schemes can provide user privacy with negligible increase in computational overhead.

We also summarize the functional requirements of our proposed schemes in this subsection. The criteria in the user authentication scheme are secure password change, mutual authentication and user anonymity. Table IV summarizes the comparison of the representative three schemes and our two proposed schemes in terms of various functional requirements.
It can be seen that all three existing representative schemes do not preserve user privacy, and Wong et al.’s scheme and Tseng et al.’s scheme do not provide any mutual authentication. Furthermore, Wong et al.’s scheme does not have provision to change the user’s password. Thus, the Wong et al.’s scheme is the most vulnerable dynamic user authentication protocol among the five above-mentioned schemes.

Our first proposed scheme can only provide mutual authentication between GW and LN; however, it cannot provide mutual authentication between GW and UD. In case of second proposed scheme, it can provide mutual authentication between GW and LN as well as mutual authentication between GW and UD.

6. PERFORMANCE EVALUATIONS

In this section, we show the performance of the proposed schemes under different simulation settings. We study the effect of different parameters on the performance. In particular, we study the effect of the number of users and the number of hops on computational overheads for authentication and authentication latency time, respectively. We have conducted experiments on both first and second proposed schemes. Simulations were conducted using OPNET Modeler [32].

In simulations, a network of 25 WSN nodes is located in $100\times100$ m area. These nodes were randomly deployed (uniform distribution). The transmission range was set to 20 m. For each node, a free-space propagation channel model was assumed with a transmission speed of 250 kbps. All simulation results were obtained by averaging from 90 runs.

We have considered and evaluated following performance metrics: computational overheads for authentication and authentication latency time. The effects of two parameters on these metrics are studied. These parameters are the number of users accessing the network simultaneously, and the number of hops between LN and GW.

Figure 8 shows the effect of number of users accessing the networks simultaneously on the computational overheads for authentication. In the case of the second proposed scheme, the computational overhead for authentication is higher than that in the first proposed scheme when the number of users is high. It can be seen that the computational overhead increases almost linearly with the increase in the number of the users for both the proposed schemes. This is due to the fact that with the increase in number of users to login the network, more LN nodes get engaged and GW node has more computational loads.

Figure 9 shows the effect of number of hops between LN and GW on the authentication latency time. It can be seen that the authentication latency time increases slowly with the increasing number of the hops for both the proposed schemes. The authentication latency time in the first proposed scheme is lower than that in the second proposed scheme.

7. CONCLUSION AND FUTURE WORKS

In this paper, we have proposed two strong-password-based dynamic user authentication protocols with user pseudonymity for WSNs. We have provided not only security analysis but also efficiency analysis for both the proposed schemes. Comparing with the existing representative schemes, our
proposed protocols are robust against many security attacks and have better security properties in terms of user privacy and mutual authentication. We have analyzed the proposed schemes using simulations and the results show that both are quite efficient.

Figure 8. Computational overheads for authentication.

Figure 9. Authentication latency time.
An interesting further research topic, which is currently under investigation, is to enhance or modify the proposed schemes so that the authentication process is resistant to attacks caused by compromised sensor nodes. Furthermore, we will conduct thorough performance analysis of both the proposed schemes.

ACKNOWLEDGEMENTS

This research is supported by the Ubiquitous Computing and Network (UCN) Project, Knowledge and Economy Frontier R&D Program of the Ministry of Knowledge Economy (MKE) in Korea and a result of subproject UCN 09C1-T2-10M.

REFERENCES


**AUTHORS’ BIOGRAPHIES**

**Dr Binod Vaidya** received the MS degree in Radio Communication Engineering from Odessa Electro-technical Institute of Communications, Ukraine in 1997 and the PhD degree in Information and Communication Engineering from Chosun University, Korea in 2007. Since 1997, he has been working as a Lecturer in the Institute of Engineering, Tribhuvan University, Nepal, though he is on academic leave since 2004. During the period 1997–2004, he served in various positions in the Institute of Engineering, Tribhuvan University, Nepal. He was a Post-doctoral Researcher in Chosun University from September 2007 to August 2008, and a Research Associate in Gwangju Institute of Science and Technology (GIST) Korea from September 2008 to February 2009. Currently he is affiliated with Instituto de Telecomunicações, Portugal since March 2009. He has served as chairs for several International conferences and workshops and also as TPC member for various conferences and workshops. He not only serves as an Editorial Board Member for IJEHMC, IGI Publisher and JCIT, AICIT but also is a guest editor for several International Journals. His research interests are ubiquitous computing, wireless ad-hoc and sensor networks, resilience, security, and delay tolerant networks.
Joel J. Rodrigues is a Professor in the Department of Informatics of the University of Beira Interior, Covilhã, Portugal, and researcher at the Instituto de Telecomunicações, Portugal. He received a PhD degree in Informatics Engineering, an MSc degree from the University of Beira Interior, Portugal, and a 5-year BS degree (licentiate) in Informatics Engineering from the University of Coimbra, Portugal. His main research interests include sensor networks, vehicular delay-tolerant networks, high-speed networks, and mobile and ubiquitous computing. He is the Editor-in-Chief of the International Journal on E-Health and Medical Communications. He is or was the general Chair of the MAN 2009 and 2010 (with IEEE ICC), N&G 2010 (with IEEE AINA), Chair of eHealth Track from Selected Areas on Communications Symposium at IEEE ICC 2011, co-Chair of the Communications Software, Services and Multimedia Applications Symposium at IEEE Globecom 2010, Chair of the Symposium on Ad-Hoc and Sensor Networks of the SoftCom Conference and chaired many other technical committees. He is or was member of many international program committees and several editorial review boards (IEEE Communications Magazine, Journal of Communications Software and Systems, International Journal of Communications Systems, International Journal of Business Data Communications and Networking, etc.), and he has served as a guest editor for a number of journals including the Journal of Communications Software and System. He chaired many technical sessions and gave tutorials at major international conferences. He has authored or co-authored over 100 papers in refereed international journals and conferences, a book and a patent pending. He is a licensed Professional Engineer and a member of the ACM SIGCOMM, a member of the Internet Society, IARIA Fellow, and a Senior Member of the IEEE Computer Society, IEEE Communications Society and IEEE Education Society, and a member of several IEEE Technical Committees related to his research areas.

Dr Jong Hyuk Park received his PhD degree in Graduate School of Information Security from Korea University, Korea. From December, 2002 to July, 2007, Dr Park had been a research scientist of R&D Institute, Hanwha S&C Co., Ltd., Korea. From September, 2007 to August, 2009, he had been a professor in the Department of Computer Science and Engineering, Kyungnam University, Korea. He is now a professor in the Department of Computer Science and Engineering, Seoul National University of Technology, Korea. Dr Park has published about 100 research papers in international journals and conferences. He has been serving as the chair, program committee, or organizing committee chair for many international conferences and workshops. He is the editor-in-chief (EiC) of International Journal of Information Technology, Communications and Convergence (IJITCC), InderScience. He was EiCs of the International Journal of Multimedia and Ubiquitous Engineering (IJMUE) and the International Journal of Smart Home (IJSH). He is Associate Editor/Editor of 14 international journals including 8 journals indexed by SCI(E). In addition, he has been serving as a Guest Editor for international journals by some publishers: Springer, Elsevier, John Wiley, Oxford Univ. press, Hindawi, Emerald, Inderscience. His research interests include security and digital forensics, ubiquitous and pervasive computing, context awareness, multimedia services, etc. He got the best paper award in ISA-08 conference, April, 2008, and he got the outstanding leadership awards from IEEE HPCC-09 and ISA-09, June, 2009.