A Secure and efficient elliptic curve based authentication and key agreement protocol suitable for WSN

Majid Bayat

bayat@khu.ac.ir

Department of Mathematical Sciences and Computer, University of Kharazmi, Tehran ,Iran.

MohammadReza Aref

aref@sharif.edu

ISSL, Department of Electrical Engineering, Sharif University of Technology, Tehran, Iran.

Abstract

Authentication and key agreement protocols play an important role in wireless sensor communication networks. Recently Xue et al'. suggested a key agreement protocols for WSN which in this paper we show that the protocol has some security flaws. Also we introduce an enhanced authentication and key agreement protocol for WSN satisfying all the security requirements.

Keywords: Autehntication, Privacy, Wireless sensor networks, key agreement protocol.

1. Introduction

Wireless Sensor network (WSN) is composed of many low-cost and small wireless sensor nodes distributed in a designated region. Their positions need not be engineered or pre-determined so that they can be randomly deployed in inaccessible terrains and adverse area. For example the sensor nodes can be dropped into a forest by the helicopter to monitor the temperature and issue fire breakout warnings. WSN research grew out of the distributed sensor networks project at the Defense Advanced Projects Research Agency (DARPA)[1], although the technology of the 1970s limited processing and communications and restricted the nodes to large form factors. With the exponential progress and cost reduction in microprocessing during the 1990s and 2000s, many new applications for WSN deployment transpired. Since then deployment of wireless sensor networks has been considered for diverse spectrum domains, including logistics, medicine, environmental monitoring, military monitoring and etc. Surveys of WSN concepts and technology illustrate the directions descripted in [2]. Authentication and privacy are fundamental requirement in WSN such that the lack of authenticated messaging makes WSN vulnerable to potential attacks. WSN deployed for tracking targets provide valuable applications layer notifications about the location of the target. Without authentication, the attacker can perpetrate attacks such as spoofing, dropping or forcing the entire network to in to a continual state of reorganization. Until now, many authentication schemes have been suggested for WSN. Das et al [3] in 2009 proposed a password based scheme suitable for WSN but does not provide mutual authentication and key agreement. Later He et al [4] declared that the Das's protocol is vulnerable to insider attack and impersonation attack and they proposed an enhanced protocol without mutual authentication and key agreement. Khan et al [5] proposed an authentication scheme for WSN with mutual authentication between Gateway node(GWN) and the sensor nodes. The authentication scheme is based on pre-shared key between GWN and each sensor node which causes a huge load on the GWN. Chen an Shih [6] suggested an authentication scheme with mutual authentication between the user, GWN and the sensor node that has some security flaws such as impersonation attack, insider attack and synchronization problem[7]. Some of the authentication schemes for WSN are public key based schemes that high computation cost and additional storage overhead of public keys of other sensor nodes or users main disadvantages of these schemes[8, 9, 10]. Recently Xue et al.[11] proposed an temporal-credential-based authentication and key agreement protocol that GWN can issue a temporal credential to each user and sensor node using a password based authentication scheme. In this paper we show that the Xue et al.'s scheme is vulnerable to dictionary attack and stolen smart card attack and the key agreement protocol can not satisfy the forward secrecy property. Next, we design a secure temporal-credential-based authentication and key agreement scheme for WSN which passes all the security requirements. The proposed scheme uses the password based authentication between the GWN, user and sensor node and the computations are based the elliptic curve which is suitable for WSN.

The rest of this paper is organized as follows: In Section 2 we bring some preliminaries and Section 3 reviews the Xue et al's protocol for WSN. In Section 4 we introduce our authentication and key agreement scheme for WSN and the security analysis is discussed in Section 5. The conclusion is stated in Section 6.

1.1. Related Works

- Key agreement protocols: These protocols enable two or more users to establish a shared secret key in an insecure and public channel which is not computable by other users. The key agreement protocols play an essential role in cryptographic systems and each weaknesses of which results in a destructive attack. Hence, there are several security requirements mentioned for the key agreement protocols which are listed in the following [12, 13]:

  - Known Session Key Security: This property emphasises that if an adversary obtains a session key, the session keys of the coming sessions remain secure.
  - Forward Secrecy: This security notifies that by revealing the long term private keys of the two users (perfect forward secrecy) or one of the users (weak forward secrecy), the adversary cannot obtain the previous session keys. Strong security is a kind of forward secrecy which states that if the short term private keys of the two users, or one user's long term private key and the short term private key of the other are revealed, the previous session keys can not be computed by the adversary.
  - Key Compromise Impersonation (KCI): Let A and B be two users. If the adversary has the long term private key of A, it can obviously forge A. KCI states that the adversary can not forge B by obtaining the long term private key of A.
  - Unknown Key Security: Let A and B be two users of a key agreement protocol. This property states that an active adversary C cannot interfere in the protocol execution such that A believes that it makes a session key with B, while B knows C as his participant in the protocol.

- Password based authenticated key exchange(PAKE)protocols: PKAE protocols are kind of key agreement protocols which two parties agree on a high-entropy cryptographic key using a pre-shared low entropy password. These protocols are suitable for many applications such as Internet, remote login and data base management systems. Bellovin and Merrit [14] proposed the first PAKE protocol and until now many PAKE protocols have been proposed[15, 16, 17, 18, 19, 20, 21, 22]. PAKE protocol are very suitable for client-server based applications, but in large scale environments they are inefficient and costly, because a large number of weak passwords should be shared among all the users. So many tripartite password based authenticated key exchange (3PAKE) protocols[23, 24, 25, 26, 27, 28, 29] have been proposed to solve the problem of PAKE protocols. In 3PAKE protocols each pair of users can agree on a secure cryptography key with help of a trusted server while each user only remember a weak password shared with the server. This makes 3PAKE protocols more practical than two-party PAKE protocols in the real world. However, the server has to participate in the protocol run as a online party to help the users. Since each user remembers a weak password for authentication and key agreement protocols, PAKE protocol are vulnerable to password guessing attacks[23, 30].

2. Preliminaries

Elliptic curve group:

Suppose that E/F_p denotes an elliptic curve E over a prime finite field F_p. The curve E is defined as follows:

$$y^2 = x^3 + ax + b$$

Such that $a, b \in F_q$ and $\Delta = 4a^3 + 27b^2 \neq 0$ is the discriminant. The points on E/F_p with an extra point at infinity O construct a cyclic additive elliptic curve group:

$$G = \{(x, y) : x, y \in F_p, E\,(x, y) = 0\} \cup \{O\}\,.$$

G is a cyclic group under the point "+" defined as follows: Let $P, Q \in G$, l be the line containing P and Q(tangent line to E/F_p if $P = Q$), and R be the third point of intersection of l with E/F_p. Let l' be the line connecting

R and O. Then $P+Q$ is the point such that l' intersects E/F_q at R and O. A scalar multiplication over E/F_p can be computed as follows:

$$tP = P + P + ... + P(t \ times)$$

in which $t \in Z_p^*$ and $P \in G$.

Computational Diffie-Hellman(CDH) Problem:

Assume a generator P of G and two points (aP, bP) for unknown $a, b \in Z_p^*$ be given . The CDH problem is to compute abP.

Bilinear Pairing:

Let G is a cyclic additive elliptic curve group with generator P and a cyclic multiplicative group G_1 of order of a prime number p and the generator g. $e : G \times G \to G_1$ is a bilinear paring if the following conditions are hold:

- Bilinearity: For all $X, Y \in G$ and $a, b \in Z_p^*$, $e\left(aX, bY\right) = e\left(X, Y\right)^{ab}$.
- Non-degeneracy: $e\left(P, P\right) \neq 1$.
- Computability: For all $X, Y \in G$, there is an efficient algorithm to compute $e\left(X, Y\right)$.

Bilinear Diffie Hellman Problem(BDH):

Let $e : G \times G \to G_1$ and aP, bP and cP, be the given values of G. The problem is to find the value $e\left(P, P\right)^{abc}$, where $a, b, c \in Z_p^*$.

3. Review on Xue's key agreement protocol for WSN

In this section we review the key agreement protocol for WSN introduced by Xue's et al. The protocol has three phases registration phase, login phase and authentication and key agreement phase as follows:

- **Registration phase:** In this phase the users and the sensor nodes register to the gateway node of the wireless sensor network , GWN. Let each user has a common and secure password with GWN and the identities and the hashed password of each user are stored in GWN. Also each sensor node is pre-configured a password, hash of which is stored in GWN's side. The registration phase for the users is as follows:

- Let a hash function $h : \{0,1\}^* \to \{0,1\}^p$. The user U_i obtains the current time stamp value TS_1 and computes

$$VI_i = h(TS_1 \| h(PW_i)) \tag{1}$$

  Then U_i submits TS_1, V_i and ID_i to GWN in an open and public environment.

- After receiving the message, GWN checks TS_1. Assume that T^*_{GWN} is the current time and ΔT is a predefined time value for an authorized delay. If $T^*_{GWN} - TS_1 > \Delta T$, GWN rejects the incoming message and sends REJ message back to U_i. Otherwise; GWN obtains $h(PW_i)$ corresponded to ID_i and computes $VI^*_i = h\left(TS_1 \left\| h\left(PW_i\right)\right.\right)$ and verifies whether $VI^*_i = VI_i$. If not, GWN stops here; otherwise, GWN computes P_i, TC_i and PTC_i as follows:

$$\begin{aligned} P_i &= h\left(ID_i \left\| TE_i\right.\right) \\ TC_i &= h\left(K_{GWN-U} \left\| P_i \right\| TE_i\right) \\ PTC_i &= TC_i \oplus h\left(PW_i\right) \end{aligned} \tag{2}$$

  where TE_i is the expiration time of the temporal credential set by GWN and K_{GWN-U} is the GWN's private key. Finally GWN issues a smart card containing $\{h(.), ID_i, h(h(PW_i)), TE_i, PTC_i\}$ for U_i.

The details of the registration phase for sensor nodes are as follows:

- Let SID_j be the identity of the sensor node. The sensor node S_j obtains its current timestamp TS_2 and computes

$$VI_j = h\left(TS_2 \left\| h\left(PW_j\right)\right.\right) \tag{3}$$

  Then S_j sends SID_j, TS_2 and VI_j to GWN in a open and public channel.

- Let T^*_{GWN} is the current time of GWN. After the receiving the message, GWN sends REJ to S_j if $T^*_{GWN} - TS_2 > \Delta T$; otherwise it gets its own copy of $h(PW_j)$ by using the SID_j and computes

$VI_j^* = h\,(TS2\,\|h\,(PW_j\,)\,)$. If $VI_j^* \neq VI_j$ GWN rejects; otherwise it computes

$$\begin{aligned} TC_j &= h\,(K_{GWN-S}\,\|SID_j\,) \\ REG_j &= h\,(h\,(PW_j)\,\|TS_3\,) \oplus TC_j \end{aligned} \tag{4}$$

where $TS3$ is the timestamp value, K_{GWN-S} is the GWN's private key, TC_j is the temporal credential for S_j issued by GWN. Then TS_3 and REG_i are sent to the sensor node S_j.

- Let T_j^* is the current time of the sensor S_j. if $T_j^* - TS_3 > \Delta T$, S_j rejects; otherwise computes and stores $TC_j = h\,(h\,(PW_j)\,\|TS_3\,) \oplus REG_j$ as its temporal credential.

- Login phase: The user U_i inserts his/her smart card to a terminal and enters his/her ID_i and PW_i. The terminal validates ID_i and PW_i with the stored ID_i and $h(h(PW_i))$ in the smart card. If they are not matching the terminal rejects the request; otherwise U_i passes the verification and can read the information stored in the smart card. Finally U_i computes

$$TC_i = PTC_i \oplus h(PW_i) \tag{5}$$

.

- Authentication and key agreement phase: This phase is executed between the user U_i, the sensor node S_j and GWN as follows:
  - The user node U_i obtains its current timestamp TS_4 and randomly selects a key sharing K_i. Then it computes the following values:

$$\begin{aligned} &DID_i = ID_i \oplus h\,(TC_i\,\|TS_4\,) \\ &C_i = h\,(h\,(ID_i\,\|TS_4\,) \oplus TC_i) \\ &PKS_i = K_i \oplus h\,(TC_i\,\|TS_4\,\|''000''\,) \end{aligned} \tag{6}$$

  The user U_i sends $DID_i, C_i, PKS_i, TS_4, TE_i$ and P_i to GWN.

  - Upon receiving the message, GWN verifies whether the transmission delay is authorized. Let T_{GWN}^* be the current time of GWN.

If $T^*_{GWN} - TS_4 > \Delta T$, GWN rejects U_i; otherwise it computes as follows:

$$\begin{aligned} &ID_i = DID_i \oplus h\,(h\,(K_{GWN-U}\,\|P_i\,\|TE_i\,)\,\|TS_4\,) \\ &P^*_i = h\,(ID_i\,\|TE_i) \\ &TC_i = h\,(K_{GWN-U}\,\|P^*_i\,\|TE_i\,) \\ &C^*_i = h\,(h\,(ID^*_i\,\|TS_4) \oplus TC^*_i) \end{aligned} \tag{7}$$

If $C^*_i \neq C_i$ or $P^*_i \neq P_i$, GWN rejects, else it accepts U_i's login request and computes:

$$K_i = PKS_i \oplus h\,(TC_i\,\|TS_4\,\|'000'\,) \tag{8}$$

The GWN computes $TC_j = h\,(K_{GWN-s}\,\|SID_j)$ as the S_j's temporal credential and the following values:

$$\begin{aligned} &DID_{GWN} = ID_i \oplus h\,(DID_i\,\|TC_j\,\|TS_5\,) \\ &C_{GWN} = h\,(ID_i\,\|TC_j\,\|TS_5\,) \\ &PKS_{GWN} = K_i \oplus h\,(TC_j\,\|TS_5) \end{aligned} \tag{9}$$

where TS_5 is a timestamp. Finally, GWN sends $TS_5, DID_i, DID_{GWN}, C_{GWN}$ and PKS_{GWN} to S_j.

– After receiving the message at the current time T^*_j, S_j checks TS_5. If $T^*_j - TS_5 > \Delta T$, it rejects the message; otherwise S_j computes as follows:

$$\begin{aligned} &ID_i = DID_{GWN} \oplus h\,(DID_i\,\|TC_j\,\|TS_5\,) \\ &C^*_{GWN} = h\,(ID_i\,\|TC_j\,\|TS_5\,) \end{aligned} \tag{10}$$

If $C^*_{GWN} = C_{GWN}$, S_j accepts GWN and computes

$$K_i = PKS_{GWN} \oplus h\,(TC_j\,\|TS_5) \tag{11}$$

Them S_j generates a timestamp TS_6 , selects a random key sharing K_j and computes the following values:

$$\begin{aligned} &C_j = h\,(K_j\,\|ID_i\,\|SID_j\,\|TS_6\,) \\ &PKS_j = K_j \oplus h\,(K_i\,\|TS_6) \end{aligned} \tag{12}$$

Finally S_j sends SID_j, TS_6, C_j and PKS_j to U_i and GWN.

– After receiving the message, U_i and GWN checks TS_6 and separately compute K_j and C_j^* as follows:

$$
\begin{aligned}
K_j &= PKS_j \oplus h\left(K_i \| TS_6\right) \\
C_j^* &= h\left(K_j \| ID_i \| SID_j \| TS_6\right)
\end{aligned}
\tag{13}
$$

If $C_j^* = C_j$, GWN accepts S_j and also U_i accepts S_j and GWN.

Finally U_i and S_j compute the session key as follows:

$$KEY_{ij} = h(K_i \oplus K_j) \tag{14}$$

3.1. Security analysis of Xue's protocol

In this section we analysis the Xue's protocol and describe its security vulnerability.

- In the registration phase, U_i sends VI_i, TS_1 and ID_i to GWN. The adversary guesses a password PW_i' and according to the Equation 1 computes $VI_i' = h(TS_1 \parallel h(PW_i'))$. If $VI_i = VI_i'$, the adversary obtains the correct password PW_i; otherwise the adversary selects another password and checks the Equation 1. This is a practical attack, because the password has a low entropy and the adversary can search all passwords in a polynomial time. So the registration phase of the protocol is not secure against dictionary attack.

- The registration phase for the sensor node is vulnerable to dictionary attack and the adversary can guess the password using the Equation 3. Details of the attack is same as the dictionary attack on the registration phase for the user.

- The smart card contains $\{h(.), ID_i, h(h(PW_i)), TE_i, TC_i\}$. So an adversary who has stolen the smart card can extract the stored data in the card and as we described above, the password is revealed by the dictionary attack on the $h(h(PW_i))$. So if an adversary has the smart card, it can obtain the corresponding password of the user.

- The protocol does not satisfy forward secrecy property. Assume that an adversary obtains the secret key K_{GWN-U} of GWN and he/she saved

Table 1: The used notations at the proposed protocol

Notations	Description
P	The generator of the elliptic curve group G
s	The secret key of GWN
$P_0 = sP$	The public key of GWN
h	A hash function: $\{0,1\}^* \to \{0,1\}^p$
H	A map to point hash function: $\{0,1\}^* \to G$
TS	Timestamp
ID_i	The identity of a user U_i
SID_j	The identity of the sensor S_j
PW_i	The password of the user U_i
PW_j	The password of the sensor U_i

$\{DID_i, C_i, PKS_i, TS_4, TE_i, P_i\}$ and $\{SID_J, TS_6, C_j, PKS_j\}$ of a session. So the session key $h(K_i \oplus K_j)$ is computed as follows:

$$\begin{aligned} &ID_i = DID_i \oplus h\left(h\left(K_{GWN-U} \| P_i \| TE_i\right) \| TS_4\right) \\ &TC_i = h\left(K_{GWN-U} \| ID_i\right) \\ &K_i = PKS_i \oplus h\left(TC_i \| TS_4 \| '000'\right) \\ &K_j = PKS_j \oplus h\left(K_i \| TS_6\right) \\ &KEY = h(K_i \oplus K_j) \end{aligned} \tag{15}$$

4. The proposed key agreement protocol for WSN with mutual authentication

In this section we introduce our key agreement protocol for wireless sensor networks. The protocol contains registration phase, login phase and authentication and key agreement phase as follows. The used notations are listed in table 1.

- Registration phase: In this phase the sensor nods and the users register to GWN . Assume that each user has a common password with GWN and the identity and the hashed password of each user are stored in GWN's side. Also assume that each sensor has a common password with GWN and the identity and the hashed password of each sensor are stored in GWN's side. In the following we describe this phase for the users and the sensor nodes separately.

Registration phase for the users:

- The user U_i selects a random number $y_i \in Z_p^*$ and obtains a time stamp TS_1. Then he/she computes

$$R_i = y_i P_0 + H(h(PW_i), TS_1, ID_i) \tag{16}$$

  and sends $\{R_i, y_i P, TS_1, ID_i\}$ to GWN.

- After receiving the message, GWN verifies TS_1 and if the delay is authorized, it searches ID_i and obtains $h(PW_i)$. GWN computes $H(h(PW_i), TS_1, ID_i)$ and checks that $R_i - H(h(PW_i), TS_1, ID_i) = sy_i P$. If it holds, GWN computes $G_i = sH(s, TE_i) + H(h(PW_i))$, $P_i = H(ID_i, TE_i)$ and delivers a smart card containing $\{G_i, P_i, TE_i, ID_i, H, h\}$ to U_i.

The details of the registration phase is described in Figure 1.

Registration phase for the sensor nodes

- The sensor S_j selects a random number $y_j \in Z_p^*$ and obtains a time stamp TS_2. Then it computes

$$R_j = y_j P_0 + H(h(PW_j), TS_2, SID_j) \tag{17}$$

  and sends $\{R_j, y_j P, TS_2, SID_j\}$ to GWN.

- GWN verifies TS_2 and if the delay is acceptable, GWN finds $h(PW_j)$ corresponding to SID_j in the database. Then it computes $H(h(PW_j), TS_2, SID_j)$ and verifies the equation $y_j P_0 = R_j - H(h(PW_j), TS_2, SID_j)$. If the equation holds, GWN computes $G_j = sH(SID_j, s) + H(TS_3) + H(h(PW_j))$ and $H(SID_j, TS_3)$. Then $\{G_j, TS_3, H(SID_j, TS_3)\}$ are sent to the sensor node.

- If the sensor node accepts TS_3 and $H(SID_j, TS_3)$, it computes $sH(s, SID_j) = G_j - H(TS_3) - H(h(PW_j))$ and stores $sH(s, SID_j)$.

The details of the registration phase for the sensor node are described in the Figure 2.

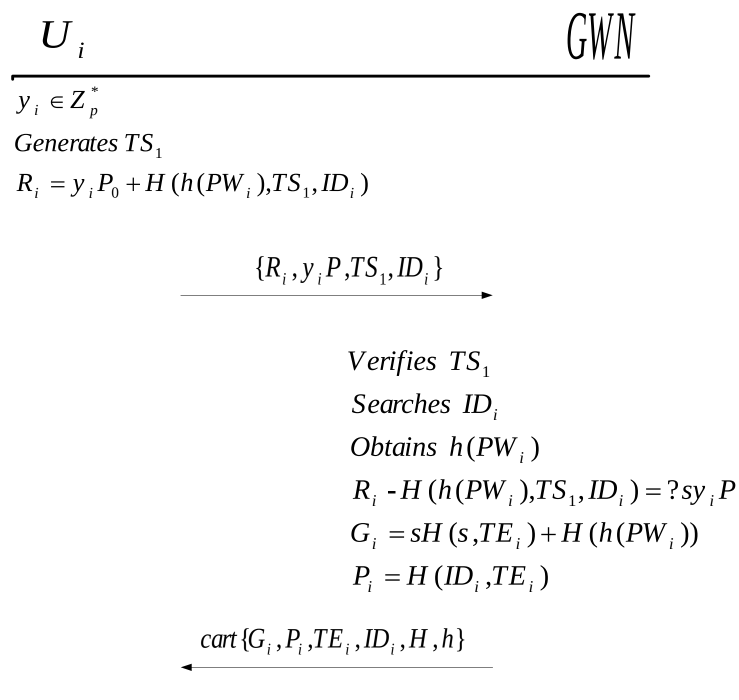

Figure 1: Details of the registration phase for the user U_i

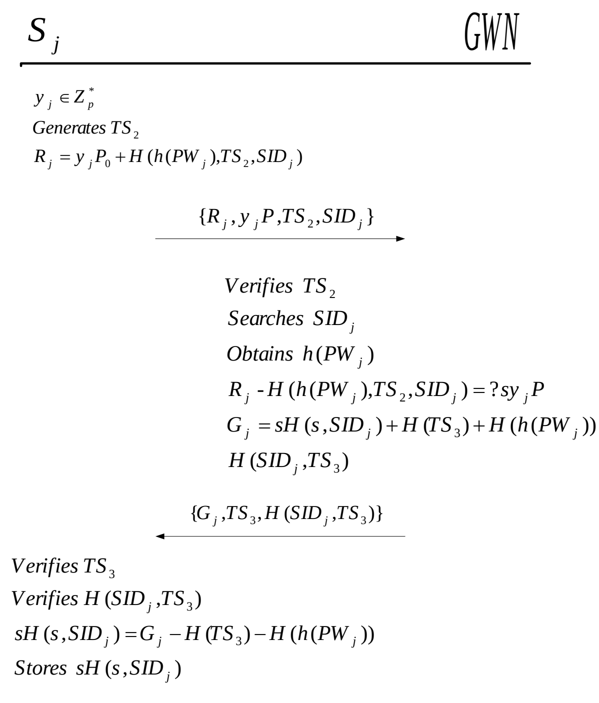

Figure 2: Details of the registration phase for the sensor S_j

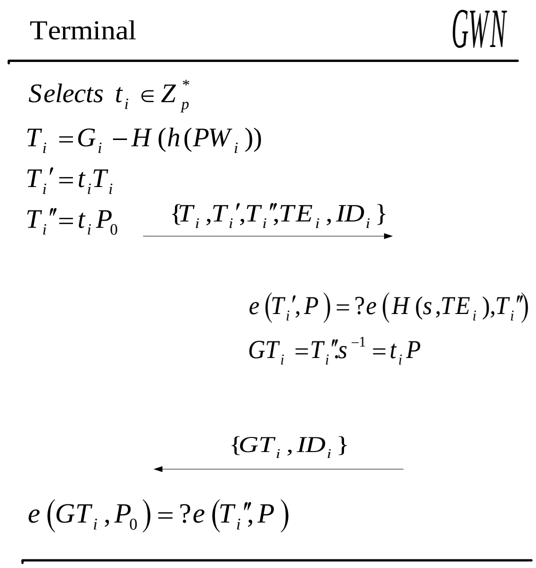

Figure 3: Details of the login phase

- Login phase: In this phase a terminal interacts with GWN to verify the smart card. The details are as follows and are described in Figure 3.
  - User U_i inserts the the smart card in a terminal and enters his/her password PW_i and identity ID_i. Then the terminal selects a random number $t_i \in Z_p^*$ and computes $T_i = G_i - H(h(PW_i)), T_i' = t_i T_i, T_i'' = t_i P_0$, and sends $\{T_i, T_i', T_i'', TE_i, ID_i\}$ to GWN in an open public channel.
  - After receiving the message, GWN checks whether $e(T'_i, P) = e(H(s, TE_i), T''_i)$ holds. If GWN accepts the equation, it computes $GT_i = T_i''.s^{-1} = t_i P$ and sends $\{GT_i, ID_i\}$ to the terminal.
  - If the equation $e(GT_i, P_0) = e(T_i'', P)$ holds, the terminal accepts GWN and the smart card.
- Key agreement phase: In this phase, the user U_i, the sensor node S_j and GWN establish a common and secure key. The details of the key agreement phase are described in the Figure 4.

– The user U_i obtains a time stamp TS_4 and selects a random number $a \in Z_p^*$. Then he/she computes

$$sH(s,TE_i) = G_i - H(h(PW_i)) \tag{18}$$
$$P_i = H(ID_i, TE_i, TS_4, \{aP\}_x)$$
$$DID_i = sH(s,TE_i) + H(ID_i) + H(TS_4)$$
$$PKS_i = aP + sH(s,TE_i) + H(ID_i, TS_4)$$

and sends $\{DID_i, PKS_i, TE_i, P_i, TS_4\}$ to GWN. $\{aP\}_x$ is the x-coordinate of the point aP.

– After receiving the messages, GWN checks TS_4 and if the delay is acceptive, GWN computes

$$H(ID_i) = DID_i - sH(s,TE_i) - H(TS_4) \tag{19}$$

and finds ID_i corresponding to $H(ID_i)$. Then GWN computes

$$aP = PKS_i - sH(s,TE_i) - H(ID_i, TS_4) \tag{20}$$

and checks that $P_i = H(ID_i, TE_i, TS_4, \{aP\}_x)$. If it holds, GWN gets a time stamp TS_5 and computes

$$DID_j = sH(s,SID_j) + H(ID_i) + H(TS_5) \tag{21}$$
$$P_j = H(SID_j, TS_5, \{aP\}_x)$$
$$PKS_{GWN} = aP + sH(s,SID_j) + H(SID_j, TS_5, '000')$$

and sends $\{PKS_{GWN}, TS_5, DID_j, P_j\}$ to the sensor S_j.

– The sensor checks TS_5 and computes

$$aP = PKS_{GNW} - sH(s,SID_j) - H(SID_j, TS_5, '000') \tag{22}$$
$$H(ID_i) = DID_j - sH(s,SID_j) - TS_5$$

Then S_j checks the equality $P_j = H(SID_j, TS_5, \{aP\}_x)$ and if it holds, S_j selects a random number $b \in Z_p^*$, obtains a time stamp TS_6 and computes

$$PKS_j = bP + aP + H(TS_6) \tag{23}$$
$$C_j = H(h(SID_j), TS_6, \{aP\}_x, \{bP\}_x)$$

Finally $\{PKS_j, C_j, TS_6, h(SID_j)\}$ are sent to GWN.

U_i	GWN	S_j
Obtains TS_4 Selects $a \in Z_p^*$ $sH(s, TE_i) = G_i - H(h(PW_i))$ $P_i = H(ID_i, TE_i, TS_4, \{aP\}_x)$ $DID_i = sH(s, TE_i) + H(ID_i) + H(TS_4)$ $PKS_i = aP + sH(s, TE_i) + H(ID_i, TS_4)$		
$\xrightarrow{\{DID_i, PKS_i, TE_i, P_i, TS_4\}}$		
	Checks TS_4 $H(ID_i) = DID_i - sH(s, TE_i) - H(TS_4)$ Finds ID_i $aP = PKS_i - sH(s, TE_i) - H(ID_i, TS_4)$ $P_i = ?H(ID_i, TE_i, TS_4, \{aP\}_x)$ Obtains TS_5 $DID_j = sH(s, SID_j) + H(ID_i) + H(TS_5)$ $P_j = H(SID_j, TS_5, \{aP\}_x)$ $PKS_{GWN} = aP + sH(s, SID_j) + H(SID_j, TS_5, \text{'000'})$	
	$\xrightarrow{\{PKS_{GWN}, TS_5, DID_j, P_j\}}$	
		Chechs TS_5 $aP = PKS_{GWN} - sH(s, SID_j) - H(SID_j, TS_5, \text{'000'})$ $H(ID_i) = DID_j - sH(s, SID_j) - TS_5$ $P_j = ?H(SID_j, TS_5, \{aP\}_x)$ Selects $b \in Z_p$ Obtains TS_6 $PKS_j = bP + aP + H(TS_6)$ $C_j = H(h(SID_j), TS_6, \{aP\}_x, \{bP\}_x)$
	$\xleftarrow{\{PKS_j, C_j, TS_6, h(SID_j)\}}$	
	Checks TS_6 $bP = PKS_j - aP - H(TS_6)$ $C_j = ?H(h(SID_j), TS_6, \{aP\}_x, \{bP\}_x)$	
$\xleftarrow{\{PKS_j, C_j, TS_6, h(SID_j)\}}$		
Checks TS_6 $bP = PKS_j - aP - H(TS_6)$ $C_j = ?H(h(SID_j), TS_6, \{aP\}_x, \{bP\}_x)$		

Figure 4: Details of the key agreement phase

– After receiving the message GWN Checks TS_6. If the delay is authorized, it computes

$$bP = PKS_j - aP - H(TS_6) \tag{24}$$

and checks whether $C_j = H(h(SID_j), TS_6, \{aP\}_x, \{bP\}_x)$ holds. If all tests are passed, GWN delivers $\{PKS_j, C_j, TS_6, h(SID_j)\}$ to the user U_i.

– After receiving the message, U_i checks TS_6 and if the time stamp is acceptable the user computes

$$bP = PKS_j - aP - H(TS_6) \tag{25}$$

If $C_j = H(h(SID_j), TS_6, \{aP\}_x, \{bP\}_x)$, U_i accepts GWN and S_j as legitimate participants in the protocol.

Finally GWN, U_i and S_j compute $K = h(\{aP\}_x, \{bP\}_x), \{sP\}_x))$ as the session key.

5. Security Analysis

In this section we analyze the security of the proposed protocol and we show that our protocol satisfy all necessary security requirements.

- Mutual authentication: The proposed protocol satisfy the mutual authentication properties. The sensor node S_j authenticates GWN by checking the value P_j and GWN verifies the sensor node by evaluating the value C_j. GWN and U_i authenticate each other by checking the values P_i and C_j respectively.

- Password Protection: The registration phase for the user U_i and the sensor S_j is secure against dictionary attack. According to the relations (16) and (17), the random numbers y_i and y_j are unknown values for the adversary, so the adversary can not establish the dictionary attack on the values R_i or R_j. In the login phase and the key agreement phase all transmitted message are password free, so the adversary can not guess the password by eavesdropping the channel.

- Password changing/updating: The user can easily change the password. In the login phase, he/she sends the changing password request and

Table 2: Security comparison of the proposed scheme and the related schemes

Security requirements	Das[3]	Khan et al.[5]	Chen et al.[6]	Yeh et al[9]	Xue et al[11]	Ours
Mutual authentication	N	Y	Y	Y	Y	Y
Password protection	N	Y	N	Y	N	Y
Password changing	N	Y	N	N	Y	Y
Identity protection	Y	Y	Y	N	Y	Y
Secure key agreement	N	N	N	Y	N	Y
Resiliency to stolen smart cart attack	N	N	N	N	N	Y
Reply attack	Y	Y	Y	N	Y	Y

enters the old password PW_i and the new password PW_i'. The terminal after verifying the smart card and GWN computes the new value G_i' as follows:

$$G_i' = G_i - H(h(PW_i)) + H(h(PW_i'))$$

Then the terminal replaces G_i with G_i' in the smart card.

- Identity protection: In our protocol the value DID_i causes that only GWN knows the identity of the user and from the DID_j the sensor node obtains the hashed identity of the user U_i. So the proposed protocol protects the anonymity of the user.

- Key agreement: In our protocol, GWN, the sensor node and the user agree on a secure and common session key to protect their communications. In contradiction to the Xue's protocol, the proposed protocol satisfies forward secrecy. Let the adversary obtains the long term private key of the server, s. Since the adversary does not know ID_i, it can not compute aP from the value PKS_i (Equation (20)). Also aP can not be computed of the value PKS_{GWN}, because SID_j is a unknown identity for the adversary(Equation 21). Therefore the adversary can not compute aP, bP and the session key K.

- Resiliency to stolen smart cart attack: Let an adversary has stolen a smart card containing$\{G_i, P_i, TE_i, ID_i, H, h\}$. Since $sH(s, TE_i)$ is a unknown value for the adversary, obtaining the embedded password from the value G_i in the cart, is impossible. So the proposed scheme is secure against stolen smart cart attack.

- Reply attack: Using the time stamp makes the proposed scheme to be immune against reply attack.

Table 3: Computation cost comparison of the proposed scheme and the related schemes

	User	GWN	Sensor node
Das[3]	$3T_H$	$4T_H$	T_H
Khan et al.[5]	$3T_H$	$5T_H$	$2T_H$
Chen et al.[6]	$4T_H$	$5T_H$	$2T_H$
Yeh et al[9]	$T_H + 2T_{ECC}$	$4T_H + 4T_{ECC}$	$3T_H + 2T_{ECC}$
Xue et al[11]	$7T_H$	$10T_H$	$5T_H$
Ours	$8T_H + 1T_S$	$10T_H + 2T_S$	$5T_H + 1T_S$

T_H:denotes the time for the hash operation, T_{ECC} denotes the time for the encryption/decryption operation in ECC-160 algorithm, T_S denotes the time for scalar multiplication operation in ECC-160 algorithm.

6. Conclusion

In this paper we analysed a recently proposed key agreement protocol for WSN suggested by Xue et al. and we showed that the protocol is insecure against dictionary attack and stolen smart card attack. Also we stated the proposed protocol does not satisfy forward secrecy property. Consequently we designed a secure and efficient key agreement protocol for WSN. Table 2 compares the security of our protocol with some related protocols and it shows that the proposed protocol passes all the security requirements. The computation cos of the proposed protocol is compared with the related protocols in Table 3 and it expresses that the computation cost of our protocol is near the Xue et al protocol.

References

[1] Defense Advanced Research Projects Agency (13 Oct 2006) Defense Advanced Research Projects Agency Home [online], available: http://www.darpa.mil/index.html [accessed 26 July 2007].

[2] J. Yick, B. Mukherjee and D. Ghosal, Wireless sensor network survey, Computer Networks, vol. 52, (2008), pp. 22922330.

[3] M.L. Das , Two-factor user authentication in wireless sensor networks.IEEE Transactions on Wireless Communications 2009;8(3):108690.

[4] D. He ,Y. Gao,S. Chan,C. Chen,J. Bu, An enhanced two-factor user authentication scheme in wireless sensor networks, Ad Hoc and Sensor Wireless Network 2010;10(4):36171.

[5] M.K. Khan ,K. Alghathbar, Cryptanalysis and security improvements of two-factor user authentication in wireless sensor networks, Sensors 2010(10) : 24509.

[6] T.H. Chen ,WK. Shih, A robust mutual authentication protocol for wireless sensor networks, ETRI Journal 2010 ; 32(5) : 70412.

[7] E. J . Yoon , K. Y. Yoo, Cryptanalysis of robust mutual authentication protocol for wireless sensor networks , 10th IEEE International Conference on Cognitive Informatics and Cognitive Computing (ICCI*CC), 2011 .

[8] J. Xu ,W. Zhu,D. Feng, An improved smart card based password authentication scheme with provable security, Computer Standards and Interfaces 2009;31(4):7238.

[9] H.L. Yeh , T.H. Chen, P.C. Liu, T.H. Kim, H.W. Wei, A secured authentication protocol for wireless sensor networks using elliptic curves cryptography, Sensors 2011(11):476779.

[10] R. Song , Advanced smart card based password authentication protocol, Computer Standards and Interfaces 2010 (32) : 3215.

[11] K. Xue, C. Ma, P. Hong, R. Ding, A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks, Journal of Network and Computer Applications 36 (2013) 316323.

[12] S. Blake-Wilson, A. Menezes, Authenticated Diffie-Hellman Key Agreement Protocols, In Selected Areas in Cryptography - SAC 1998, pages 339361. Springer- Verlag, 1998. Vol. 1556/1998 of LNCS.

[13] B. LaMacchia, K. Lauter and A. Mityagin, Stronger Security of Authenticated Key Exchange, In: Susilo, W., Liu, J.K., Mu, Y. (eds.) ProvSec 2007. LNCS, vol. 4784, pp. 1-16. Springer, Heidelberg (2007)

[14] S.M. Bellovin ,M. Merritt, Encrypted key exchange: password-based protocols secure against dictionary attacks, In: Proc. 1992 IEEE Symposium on Research in Security and Privacy. Lecture Notes in Computer Science, 1992; 7284.

[15] Y. Lee, S. Kim, D. Won, Enhancement of two-factor authenticated key exchange protocols in public wireless LANs, Computers and Electrical Engineering 36 (2010) 213223

[16] M. Abdalla, O. Chevassut, D. Pointcheval, One-time verifier-based encrypted key exchange, in: Proceedings of the 8th International Workshop on Theory and Practice in Public Key (PKC 05), LNCS 3386, 2005, pp. 4764.

[17] M. Abdalla, D. Pointcheval, Simple Password-Based Encrypted Key Exchange Protocols, in: Proceedings of Topics in Cryptology CT-RSA05, LNCS 3376, 2005, pp. 191208.

[18] P.D. MacKenzie, S. Patel, R. Swaminathan, Password-authenticated key exchange based on RSA, in: Proceedings of Advances in Cryptology ASIACRYPT00, LNCS 1976, 2000, pp. 599613.

[19] M. Abdalla, E. Bresson, O. Chevassut, B. Mller, D. Pointcheval, Provably secure password-based authentication in TLS, in: Proceedings of AsiaCCS06, 2006, pp. 3545.

[20] E. Bresson, O. Chevassut, D. Pointcheval, New security results on encrypted key exchange, in: Proceedings of PKC04: 7th International Workshop on Theory and Practice in Public Key Cryptography, LNCS 2947, 2004, pp. 145158.

[21] R. Gennaro, Y. Lindell, A framework for password-based authenticated key exchange, in: Proceedings of Advances in Cryptology EUROCRYPT03, LNCS 2656, 2003, pp. 524543.

[22] C. Boyd, P. Montague, K. Nguyen, Elliptic Curve Based Password Authenticated Key Exchange Protocols, in: Proceedings of 28th Australasian Conference on Information Security and Privacy ACISP01, LNCS 2119, 2001, pp. 487501.

[23] H. S. Kim, J. Y. Choi, Enhanced password-based simple three-party key exchange protocol, Computers and Electrical Engineering, Volume 35, Issue 1, January 2009, Pages 107114.

[24] R. Lu, Z. Cao, Simple three-party key exchange protocol, Computers and Security 26 (1) (2007) 9497.

[25] M. Abdalla, P.A. Fouque, D. Pointcheval, Password-based authenticated key exchange in the three-party setting, in: Proceedings of PKC05, LNCS 3386, 2005, pp. 6584. (Full version appeared in IEE Information Security 153(1) (2006) 2739).

[26] H.M. Sun, B.C. Chen, T. Hwang, Secure key agreement protocols for three-party against guessing attacks, Journal of Systems and Software 75 (12) (2005) 6368.

[27] H.F. Huang, A simple three-party password-based key exchange protocol. International Journal Of Communication Systems. 2009; 22:857862.

[28] J. Zhao, G. Dawu, Provably secure three-party password-based authenticated key exchange protocol, Information Sciences 184 (1) (2012) 310323.

[29] S. Wu, Q. Pu, S. Wang, D. He, Cryptanalysis of a communication-efficient three-party password authenticated key exchange protocol, Information Sciences 215 (2012) 8396.

[30] Y. Ding , P.Horster, Undetectable on-line password guessing attacks. ACM Operating Systems Review. 1995; 29(4):7786.