Weakness of a Secured Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography

Weiwei Han

School of Mathematics & Computer Science, Guangdong University of Business Studies, Guangzhou, China

Email: hww_2006@163.com

Abstract*:* Authenticating remote users in wireless sensor networks (WSN) is an important security issue due to their un-attended and hostile deployments. Usually, sensor nodes are equipped with limited computing power, storage, and communication module, thus authenticating remote users in such resource constrained environment is a critical security concern. Recently, Yeh et al. proposed a two-factor user authentication scheme in WSN and claimed that his scheme is secure against different kind of attacks. However, in this paper, we prove that Yeh et al. scheme has some critical security pitfalls and is not recommended for real application. We point out that have the following weakness: 1) no mutual authentication between the user and the sensor node, 2) no perfect forward secrecy, 3)no key agreement between the user and the sensor node.

Key words*: authentication; security; elliptic curve cryptosystem; wireless sensor network*

1. Introduction

Recently, wireless sensor networks (WSN) have emerged as a very active research avenue of communication technologies. WSNs have many common features with wireless ad hoc network and in several cases, they are considered as a special case of them [1]. Wireless sensor network usually consists of a large number of autonomous sensor nodes, which are generally deployed in unattended environments. Each sensor node has some level of computing power, limited storage, and a small communication module to communicate with the outside world over an ad hoc wireless network [2]. Wireless sensor networks are widely used in many areas, such as military, battlefield, homeland security, health care, environment monitoring, agriculture and cropping, manufacturing, and so on.

Very recently, Yeh et al. [3] proposed a user authentication protocol using the elliptic curve cryptography (ECC). Unfortunately, we point out that have the following weakness: 1) no mutual authentication between the user and the sensor node, 2) no perfect forward secrecy, 3)no key agreement between the user and the sensor node.

The remainder of this paper is organized as follows. Section 2 reviews the concept of Yeh et al.'s protocol, and section 3 discusses its weakness analysis. Conclusions are given in Section 4.

2. Review of Yeh et al.'s protocol

The notations used throughout this paper are summarized as follows:

- p, n : two large prime numbers;
- F_p : a finite field;
- E : an elliptic curve defined on finite field F_p with large order;
- G : the group of elliptic curve points on E ;
- P : a point on elliptic curve E with order n ;
- U : a user;
- ID_U : the user U 's identity;
- pw_U : the user U 's password;
- $GW-node$: the Gateway node of WSN;
- S_n : the nearest sensor node of WSN;
- (q_s, Q_s): the $GW-node$'s private/public key pair, where $Q_s = q_s \times P$;
- $H_1(\cdot)$: a secure one-way hash function, where $H_1 : \{0,1\}^* \to G$;
- $h(\cdot)$: a secure one-way hash function;
- ||: a string concatenation operation
- $\oplus$: a string XOR operation

When setting the system, the $GW-node$ selects a base point P with the order P over E . Then, the $GW-node$ derives its private/public key pair (q_s, Q_s) by computing $Q_s = q_s \times P$.

There are four phases in Yeh et al.'s protocol: registration, login, verification and password-changing. A description of each follows.

Registration phase. In this phase, user U has to submit an identity, ID_U, and a password, pw_U, to the $GW-node$ in a secured way. Then, the $GW-node$ issues a license to U. The detailed steps are depicted as follows:

1) U choose his identity ID_U and password pw_U, generates a random number b_U, and computes $\overline{pw_U} = h(pw_U \oplus b_U)$. Then, U sends ID_U and $\overline{pw_U}$ to the $GW-node$.

2) Upon receiving the registration request, the $GW-node$ computes $K_U = q_s \times H_1(ID_U)$, $B_U = h(ID_U \oplus \overline{pw_U})$ and $W_U = h(ID_U \| \overline{pw_U}) \oplus K_U$. Then the $GW-node$ stores $\{B_U, W_U, h(\cdot), H_1(\cdot), H_2(\cdot), H_3(\cdot)\}$ into a smart card and sends it to the user U.

3) After receiving the smart card, the user U inputs b_U into it and finishes the registration.

Login phase. When U enters an ID_U and a pw_U in order to deliver some query to or access data from the WSN, the smart card must perform the following steps to validate the legitimacy of U:

1) U enters his ID_U and pw_U to login to obtain the message for $GW-node$ request.

2) The smartcard computes $\overline{pw_U} = h(pw_U \oplus b_U)$ and $B'_U = h(ID_U \oplus \overline{pw_U})$ and checks whether $B'_U = B_U$. If it does hold, the smartcard stops the request. Otherwise, the smartcard generates a random point $R_U = (x_U, y_U)$, $t_U = H_2(T_U)$, $M_U = R_U + t_U \times K_U$ computes $K_U = h(ID_U \| \overline{pw_U}) \oplus W_U$ and $R^*_U = x_U \times P$, where T_U is the current timestamp. At last, the smart card sends $Msg(T_U, ID_U, M_U, R^*_U)$ to the $GW-node$ through .

Verification Phase. After receiving the login request message $Msg(T_U, ID_U, M_U, R^*_U)$ at time T' from the nearest sensor node S_n, the $GW-node$ executes the following steps to verify the user U.

1) The $GW-node$ checks whether $T' - T_U \le \Delta T$ holds, where ΔT is the legal time interval for transmission delay. If the answer is yes, the validity of T_U can be assured, and the $GW-node$ proceeds to the next step. If no, the $GW-node$ rejects the request.

2) The $GW-node$ computes $Q_U = H_1(ID_U) = (x_{Q_U}, y_{Q_U})$, $t_U = H_2(T_U)$, and $R'_U = M_U - q_s \times t_1 \times Q_U = (x'_U, y'_U)$. $GW-node$ checks whether the equation $R^*_U = x'_U \times P$ holds. If the equation does not hold, $GW-node$ stops the session.

3) The $GW-node$ generates a random point $R_{GW} = (x_{GW}, y_{GW})$, $t_{GW} = H_2(T_{GW})$, $M_{GW} = R_{GW} + q_s \times t_{GW} \times Q_U$, session key $k = H_3(x_{Q_U}, x_U, x_{GW})$ and $M_k = (k + x_s) \times P$, where T_{GW} is the current timestamp. At last, $GW-node$ sends $Msg(T_{GW}, M_{GW}, M_k)$ to S_n.

Mutual Verification Phase. After receiving the login request message $Msg(T_{GW}, M_{GW}, M_k)$ at time T'' from $GW-node$ S_n, the S_n executes the following steps to verify the $GW-node$.

1) The S_n checks whether $T'' - T_{GW} \le \Delta T$ holds, where ΔT is the legal time interval for transmission delay. If the answer is yes, the validity of T_{GW} can be assured, and the S_n proceeds to the next step. If no, the S_n rejects the request.

2) The S_n computes $Q_U = H_1(ID_U) = (x_{Q_U}, y_{Q_U})$, $t_{GW} = H_2(T_{GW})$, and $R'_{GW} = M_{GW} - t_{GW} \times K_{ID_U} = (x'_{GW}, y'_{GW})$.

3) The S_n computes the session key $k' = H_3(x_{Q_U}, x_U, x'_{GW})$ and $M'_k = (k' + x'_s) \times P$ to verify whether $M_k = M'_k$. If the equation does not hold, S_n stops the session. Otherwise, S_n sends $Msg(ACC-LOGIN)$ to the user U.

3. Weaknesses of Yeh et al.'s protocol

In this section, we will show weaknesses of Yeh et al.'s protocol.

3.1 No mutual authentication between the user and the sensor node

Assume that a malicious user, U' , wants to attack a WSN. He can accomplish his purpose by eavesdropping and masquerading. A more detailed description of the attack can be stated as follows.

When U sends the message $Msg(T_U, ID_U, M_U, R^*_U)$ to the GW-node to access the WSN, the GW-node sends the message $Msg(T_{GW}, M_{GW}, M_k)$ to S_n

asking for the service for U. At this point, U' can provide an S_M (which was not arranged by the GW-node) to impersonate the S_n and get U's request data or hold back the request. Since S_M co-works with U continuously, U will fail the accessing request continuously as well.

3.2 No perfect forward secrecy

A protocol is called perfect forward secrecy, if compromise of the private keys of the participating entities does not affect the security of the previous session keys. We will show that Yeh et al.'s protocol can not provide the perfect forward secrecy.

In Yeh et al.'s protocol, the $GW-node$ and S_n can compute the session key $k = H_3(x_{Q_U}, x_U, x_{GW})$. Once the private key q_s of $GW-node$ is gotten by some adversary A, then A could compute the session from the message $Msg(T_U, ID_U, M_U, R_U^*)$ and $Msg(T_{GW}, M_{GW}, M_k)$ though the following steps.

1) A computes $Q_U = H_1(ID_U) = (x_{Q_U}, y_{Q_U})$, $t_U = H_2(T_U)$, and $R_U = M_U - q_s \times t_1 \times Q_U = (x_U, y_U)$.

2) A computes $t_{GW} = H_2(T_{GW})$ and $R_{GW} = M_{GW} - q_s \times t_{GW} \times Q_U = (x_{GW}, y_{GW})$.

3) A computes the session key $k = H_3(x_{Q_U}, x_U, x_{GW})$.

Then Yeh et al.'s protocol can not provide the perfect forward secrecy. Moreover, there is no session key between the user U and the sensor node S_n, since U just receives $Msg(ACC-LOGIN)$ from the sensor node S_n.

3.3 No key agreement between the user and the sensor node

From the description of Yeh et al.'s scheme in Section 3, we know that the gate node and the sensor node can compute the session key $k = H_3(x_{Q_U}, x_U, x_{GW})$ and $k' = H_3(x_{Q_U}, x_U, x'_{GW})$ separately. However, the user does not compute any session key for future communication. Then Yeh et al.'s scheme is not suitable for WSNs.

4. Conclusions

In this paper, we have shown that the recently proposed two-factor user authentication scheme in wireless sensor network environment is insecure against different kind of attacks and should not be implemented in the real-applications. We have demonstrated that in Yeh et al.'s scheme, there is 1) no mutual authentication between the user and the sensor node, 2) no perfect forward secrecy, 3)no key agreement between the user and the sensor node.

Reference

[1]. Chiara, B., Andrea, C., Davide, D., Roberto, V.: An Overview on Wireless Sensor Networks Technology and Evolution. Sensors 9, 6869–6896 (2009)

[2]. Callaway, E.H.: Wireless Sensor Networks, Architectures and Protocols. Auerbach Publications, Taylor & Francis Group, USA (2003)

[3]. Yeh H.-L., Chen T.-H., Liu P.-C., Kim T.-H., Wei H.-W., A Secured Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography, Sensors 2011, 11, 4767-4779.