Article

An Improved Protocol for the Password Authenticated Association of IEEE 802.15.6 Standard that Alleviates Computational Burden on the Node

Jie Zhang 1,2,‡, Xin Huang 1,‡*, Paul Craig 1, Alan Marshall 2 and Dawei Liu 1

1 Department of Computer Science and Software Engineering, Xi’an Jiaotong-Liverpool University
2 School of Electrical Engineering and Electronics and Computer Science, University of Liverpool;
Jie.Zhang3@liverpool.ac.uk
* Correspondence: xin.huang@xjtlu.edu.cn; Tel.: +86-0512-8816-1511
‡ These authors contributed equally to this work.

Abstract: The IEEE Std 802.15.6 is an international standard for wireless body area networks (WBANs). It contains many aspects of communications, and also provides security services since some communications in WBANs can carry sensitive information. In this standard, the password authenticated association is a protocol for two participants to identify each other and establish a new master key based on a pre-shared short password. However, recent researches show that this protocol is vulnerable to several attacks. In this paper, we propose an improved protocol which can resist all of these attacks. Moreover, the improved protocol alleviates computational burden on one side of the two participants, the node, which is usually less powerful compared with the other side, the hub.

Keywords: body area networks; password authenticated association; security; key establishment; IEEE 802.15.6

0. Introduction

A wireless body area network (WBAN) is a wireless network of wearable computing devices including implanted devices embedded inside the body or attached on the skin, and accompanied devices which humans can carry by hand, in clothes pockets or in bags[1–4]. WBANs applications[5,6] are growing and becoming more indispensable in people’s life due to the increasing accessibility of network service and computing devices. Despite the great progress in networking and computing technology, security is one significant factor that influences users’ choice of WBANs applications since such applications involve a lot of personal information and therefore are vulnerable to security issues.

IEEE Std 802.15.6[7] is an international standard for wireless communication between nodes and hubs in WBANs. It provides strong security for communications which carry sensitive information. In the security services of this standard, security association procedure activates a pre-shared or generates a new shared master key (MK) between a node and a hub. Several security association protocols suitable for a variety of use cases are provided in this standard. Among these protocols, password authenticated association[8,9] is a protocol for a node and a hub to generate a new shared MK from a pre-shared secret, i.e. the password. However, recent researches show that this protocol is vulnerable to several attacks, such as man-in-the-middle and impersonation attacks illustrated in [10], and the off-line dictionary attack and being lack of forward secrecy which are discussed in [11,12]. To eliminate these attacks, [10] also proposes a modified version to this protocol.
In this paper, an improved password authenticated association protocol is proposed. In the rest of this paper, we denote this protocol by the improved protocol, protocol in [10] by the modified protocol and protocol in the IEEE 802.15.6 standard by the standard protocol. Compared with the modified protocol and the standard protocol, the improved protocol eliminates all the above attacks on one hand. Moreover, it alleviates computational burden on the node. Since the node usually has limited computational power compared with the hub, the improved protocol is meaningful in practice.

The rest parts of this paper is organized as follows. Section 1 contains preliminaries and symbols that are useful in this paper. In Section 2, we reviews the standard protocol and available attacks in literatures. In Section 3, the improved protocol is proposed and its security and performance are analyzed in Section 4 and 5 respectively. Section 6 shows a use case of this improved protocol. Related works are provided in Section 7. At last, Section 8 concludes this paper.

1. Preliminaries and Symbols

1.1. Elliptic Curve Public Key Cryptography

Elliptic Curve.

The IEEE 802.15.6 password authenticated association protocol is based on the Diffie-Hellman key exchange[13] employing the elliptic curve public key cryptography (ECC). An elliptic curve $E$ can be characterized by the following equation[14,15]:

$$y^2 \equiv x^3 + ax + b \mod p$$

with $a, b \in GF(p), 4a^3 + 27b^2 \neq 0$ (1)

where $(x, y)$ is a point on the curve; $a$ and $b$ are coefficients; $p$ is an odd prime; and $GF(p)$ is a prime finite field. For the choices of a suitable elliptic curve, the IEEE Std 802.15.6 suggests to use Curve p-256 in FIPS Pub 186-3. Values of $a, b, p$, the base point $G = (G_x, G_y)$ and the order $r$ of $G$ are given in the standard.

Elliptic Curve Diffie-Hellman.

Elliptic curve Diffie-Hellman (ECDH) is an anonymous key agreement protocol that allows two parties, each having an elliptic curve public-private key pair, to establish a shared secret over an insecure channel [16]. Suppose $SK_A$ and $SK_B$ are private keys of two communicating parties A and B respectively. $SK_A$ and $SK_B$ are random integers from the set $\{1, ..., r - 1\}$. The corresponding public keys $PK_A$ and $PK_B$ are computed as follows

$$PK_A = SK_A \times G, PK_B = SK_B \times G$$

(2)

where $\times$ denotes scalar multiplication of $G$ by an integer. In the ECDH protocol, A and B exchange their public keys and compute $(x_k, y_k) = SK_A \times PK_B$ and $(x_k, y_k) = SK_B \times PK_A$ respectively. The shares key is $x_k$, i.e. the $X$ coordinate of the point.

1.2. Password Authenticated Key Exchange

The password authenticated association protocol in IEEE 802.15.6 standard is a variation of password authenticated key exchange (PAKE)[17]. A PAKE protocol uses a pre-shared password for an authenticated key establishment. The password is usually short and easy for human to remember, and is not stored directly in the memory of physical devices for security purpose, instead, it is input by the users at the beginning of each run of the PAKE protocol.
Table 1. Symbols and definitions

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>identity of the initiator (i.e. the node)</td>
</tr>
<tr>
<td>R</td>
<td>identity of the responder (i.e. the hub)</td>
</tr>
<tr>
<td>A</td>
<td>identity of an adversary</td>
</tr>
<tr>
<td>PW</td>
<td>the pre-shared password</td>
</tr>
<tr>
<td>K</td>
<td>the temple Diffie-Hellman key used for computing CMAC</td>
</tr>
<tr>
<td>MK</td>
<td>the master key to be generated</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>SK_I, PK_I</td>
<td>private and public keys of the initiator</td>
</tr>
<tr>
<td>SK_R, PK_R</td>
<td>private and public keys of the responder</td>
</tr>
<tr>
<td>SK_A, PK_A</td>
<td>private and public keys of the adversary</td>
</tr>
<tr>
<td>N_I</td>
<td>a nonce generated by the initiator</td>
</tr>
<tr>
<td>N_R</td>
<td>a nonce generated by the responder</td>
</tr>
<tr>
<td>N_A</td>
<td>a nonce generated by the adversary</td>
</tr>
<tr>
<td>Q(x)</td>
<td>a function that maps a positive integer x to a point on the elliptic curve</td>
</tr>
<tr>
<td>G</td>
<td>base point in the elliptic curve</td>
</tr>
<tr>
<td>×</td>
<td>scalar multiplication</td>
</tr>
<tr>
<td>RMB_n(x)</td>
<td>the n rightmost bits of x</td>
</tr>
<tr>
<td>LMB_n(x)</td>
<td>the n leftmost bits of x</td>
</tr>
</tbody>
</table>

1.3. Symbols

The association protocol is initiated by the node to generate a shared master key with the hub from a pre-shared password between them. We denote the node as the initiator and the hub as the responder. Some other symbols used in this paper are summarized in Table 1.

2. IEEE 802.15.6 Password Authenticated Association Protocol

We review the IEEE 802.15.6 password authenticated association protocol, i.e. the standard protocol, and discuss its vulnerabilities in this section.

2.1. Description of The Standard Protocol

Setup

The initiator and the responder set up their private and public key as follows.

1. Initiator chooses a random SK_I and computes the public key PK_I = SK_I × G.
2. Responder selects its private key SK_R and computes PK_R = SK_R × G.

Master Key Generation

The initiator and the responder execute the following steps to generate a shared master key.

1. The initiator computes a password-scrambled public key

   \[ PK'_I = PK_I - Q(PW) \]  (3)

   and sends it to the responder along with a nonce N_I and the identities I and R:

   \[ M_1 = \{ R, I, N_I, PK'_I \} \]

2. After receiving M_1, the responder sends the identities, a nonce and its public key back to the initiator:

   \[ M_2 = \{ I, R, N_R, PK_R \} \]
3. The responder recovers $PK_I$ as follows

$$PK_I = PK'_I + Q(PW)$$  (4)

The initiator and the responder compute the Diffie-Hellman key respectively through

$$K = SK_I \times PK_R = SK_R \times PK_I$$  (5)

The responder computes a message authentication code

$$MAC_3 = \text{CMAC}_{64}(RMB_{128}(K), I\|R\|N_I\|N_R)$$  (6)

and then sends the initiator

$$M_3 = \{I, R, N_R, PK_R, MAC_3\}$$

4. The initiator verifies the received $MAC_3$. If the verification succeeds, the initiator computes a message authentication code

$$MAC_4 = \text{CMAC}_{64}(RMB_{128}(K), R\|I\|N_R\|N_I)$$  (7)

and sends the responder

$$M_4 = \{R, I, N_I, PK_I, MAC_4\}$$

5. The responder verifies $MAC_4$. If the verification succeed, both parties compute and activate their new master key as follows:

$$MK = \text{CMAC}_{128}(LMB_{128}(K), N_I\|N_R)$$  (8)

2.2. Security Problems

The standard protocol uses the password to hide the public key of the initiator through $PK'_I = PK_I - Q(PW)$ in the first step, so that only the responder can recover $PK_I$ from $PK_I = PK'_I + Q(PW)$. However, the protocol reveals $PK_I$ in $M_4$ of step 4, which means an eavesdropper who intercepts $M_4$ can acquire $Q(PW)$. In this case, the password is no longer secret in following runs of the protocol. This is the reason for the vulnerabilities of the standard protocol. Security problems and attacks to this standard protocol in literatures are summarized as follows:

- Impersonation attack. [10] illustrates an initiator impersonation attack and a responder impersonation attack to the standard protocol. At the end of these attacks, the attackers successfully establish a master key with one side of the communicating parties, while the other side thinks it has the shared master key with the true participant.

- Man-in-the-middle attack. In [10] the authors show that an attacker breaks into the communication between the initiator and the responder and modifies the messages at his/her will. At last, the attacker shares two master keys with the initiator and the responder respectively, while the initiator and the responder think they have a shared master key. Figure 1 is a time-sequence diagram that illustrates the procedure of man-in-the-middle attack against the protocol.

- Off-line dictionary attack. [11,12] show that a dictionary attacker who eavesdrops messages between the initiator and the responder in a protocol run can obtain $PK'_I$ and $PK_I$ and compute $Q(PW)$ from $Q(PW) = PK_I - PK'_I$. Then $Q(PW)$ can be used as a verifier and the attacker can try probable $PW$s from a dictionary of most probable passwords and check them using $Q(PW)$.

- Lack of forward secrecy. The author in [11,12] illustrates that if $SK_I$ has been compromised by an attacker, the attacker can acquire the Diffie-Hellman key $K$ through computing $K = SK_I \times PK_R$ and $MK$ from $MK = \text{CMAC}_{128}(LMB_{128}(K), N_I\|N_R)$ since $PK_R$, $N_I$ and $N_R$ are sent in clear.
2.3. The Modified Protocol

The authors in [10] propose a modified protocol to the standard protocol. Specifically, the modified protocol is similar with the standard one except that it does not send $PK_I$ in clear in $M_4$. This modification solves most security problems as we mentioned in Section 2.2, but it still fails to provide forward secrecy. We will compare security and performance of the two protocols with those of our new proposed protocol later in this paper.

3. The Improved Protocol

The improved protocol assumes that $PK$ and $SK$ can be reused in each round of protocol. This assumption is reasonable since in the improved protocol the temporary Diffie-Hellman key $K$ is derived from two random values chosen by the initiator and the responder respectively, rather than the public and private keys of them. The improved protocol is described in detail as follows.

1. The initiator chooses a random value $R_I$ and computes

$$U_I = R_I + SK_I$$

and

$$PK'_I = PK_I - Q(PW).$$

Then the initiator sends message $M_1$ to the responder.

$$M_1 = \{ I, R, U_I, PK'_I, N_I \}$$

2. The responder chooses a random value $R_R$ and computes

$$U_R = R_R + SK_R$$
and
\[ T_R = U_R \times G. \]  
(12)

Then the responder sends message \( M_2 \) to the initiator
\[ M_2 = \{ R, I, T_R, PK_R, N_R \}. \]
3. The responder recovers \( PK_I \) as follows
\[ PK_I = PK'_I + Q(PW). \]  
(13)

The initiator computes the Diffie-Hellman key through
\[ K = (T_R - PK_R) \times R_I = G \times R_R \times R_I. \]  
(14)

The responder computes \( K \) as follows
\[ K = (U_I \times G - PK_I) \times R_R = G \times R_R \times R_I \]  
(15)

With the \( K \) the responder computes a message authentication code
\[ MAC_3 = CMAC_{64}(RMB_{128}(K), I || R || N_I || N_R) \]  
(16)

and then sends the initiator
\[ M_3 = \{ I, R, N_R, PK_R, MAC_3 \} \]
4. The initiator verifies the received \( MAC_3 \). If the verification succeeds, the initiator computes a message authentication code
\[ MAC_4 = CMAC_{64}(RMB_{128}(K), R || I || N_R || N_I) \]  
(17)

and sends the responder
\[ M_4 = \{ R, I, N_I, MAC_4 \} \]
5. The responder verifies \( MAC_4 \). If the verification succeeds, both parties compute and activate their new master key as follows:
\[ MK = CMAC_{128}(LMB_{128}(K), N_I || N_R) \]  
(18)

4. Security Analysis

In Section 2.2 we listed all the attacks to the standard protocol, and in this section, we will prove the security of the improved protocol under all of these attack.

4.1. Impersonation Attack.

Proposition 1. Suppose the initiator and the responder have shared a password \( PW \) secretly, an attacker is not able to impersonate the initiator to establish the master key \( MK \) with the responder.

Proof. Assume \( A_I \) is an attacker who attempts to impersonate the initiator and establish \( MK \) with the responder. \( A_I \) attacks the protocol as follows:
1. \( A_I \) initializes the protocol with the responder by sending the first message \( M_{A1} \) as follows:
\[ M_{A1} = \{ I, R, U_A, PK'_I, N_A \}. \]

where \( U_A = R_A + SK_A \) and \( R_A \) and \( N_A \) are random values generated by \( A_I \).
2. After receiving \( M_{A1} \), the responder chooses a random value \( R_R \) and computes \( U_R = R_R + SK_R \) and \( T_R = U_R \times G \). Then the responder replies \( A_1 \) with \( M_2 \):

\[
M_2 = \{ R, I, T_R, PK_R, N_R \}.
\]

3. The responder recovers \( PK_I \) and computes \( K = (U_A \times G - PK_I) \times R_R \). Then the responder computes \( MAC_3 = CMAC_{64}(RMB_{128}(K), I || R || N_A || N_R) \) and sends the following message \( M_3 \) to \( A_1 \):

\[
M_3 = \{ I, R, N_R, PK_R, MAC_3 \}.
\]

4. At this step, \( A_1 \) needs to send the responder with \( MAC_{A4} \) which should be equivalent with \( CMAC_{64}(RMB_{128}(K), R || I || N_R || N_A) \) so that it can pass the verification at the beginning of the next step.

In step 4, in order to compute a valid \( MAC_{A4} \), \( A_1 \) has to calculate \( K \) equals to \( K = (U_A \times G - PK_I) \times R_R = (R_A \times G + PK_A - PK_I) \times R_R \). However, without any of \( PK_I \) and \( R_R \), \( A_1 \) has no choice but to guess such a \( MAC_{A4} \). The probability of guessing a valid \( MAC_{A4} \) is \( \frac{1}{2^{64}} \).

Alternatively, in the first piece of message \( M_{A1} \), the adversary \( A_1 \) can send a \( U_I \) intercepted in previous protocol runs instead of \( U_A \). In this case, \( K \) computed by the responder in step 3 equals to \( (U_I \times G - PK_I) \times R_R = G \times R_I \times R_R \) and \( (T_R - PK_R) \times R_I \). It is still infeasible for \( A_1 \) to compute the \( K \) since \( R_R \) and \( R_I \) are unknown to \( A_I \).

From the above analysis, now we can draw the conclusion that the probability for \( A_1 \) successfully impersonating the initiator and establishing a master key with the responder is \( \frac{1}{2^{64}} \), which is a minor value in a life circle of a normal node in WBANs applications. □

**Proposition 2.** Suppose the initiator and the responder have shared a password \( PW \) secretly, an attacker is not able to impersonate the responder to establish the master key \( MK \) with the initiator.

**Proof.** Assume \( A_R \) is an attacker who intends to impersonate the responder and establish \( MK \) with the initiator. \( A_R \) attacks the protocol as follows:

1. The initiator sends \( A_R \) with \( M_1 \) which is the same with the step 1 in the improved protocol:

\[
M_1 = \{ I, R, U_I, PK'_I, N_I \}.
\]

2. After receiving \( M_1 \), \( A_R \) replies the initiator with \( M_{A2} \):

\[
M_{A2} = \{ R, I, T_A, PK_A, N_A \}
\]

with \( T_A = U_A \times G \) and \( U_A = R_A + SK_A \) where \( SK_A \) is the private key of \( A_R \) and \( R_A \) and \( N_A \) are random values generated by \( A_R \).

3. At this step, \( A_R \) needs to send the initiator with \( MAC_{A3} \) involved in \( M_{A3} \) so that it can pass the verification at the beginning of the next step.

The \( MAC_{A3} \) is checked to be valid only if it equals to \( CMAC_{64}(RMB_{128}(K), I || R || N_I || N_A) \). In order to generate a valid \( MAC_{A3} \), \( A_R \) can compute the CMAC output by inputting \( K, I, R, N_I, N_A \) or guess the 64-bit result. To compute the CMAC output, \( A_R \) has to calculate \( K \) that equals the \( K \) calculated by the initiator through \( K = (T_A - PK_A) \times R_I = G \times R_A \times R_I \). However, since \( R_I \) is unknown to \( A_R \), it is infeasible for \( A_R \) to acquire a valid \( K \). Therefore, the adversary can only guess a valid \( MAC_{A3} \) with a successful probability at \( \frac{1}{2^{64}} \), otherwise, the protocol will stop at the beginning of step 4 and the attack will fail.

□

From Proposition 1 and 2 we can see impersonation attacks fail no matter the attacker impersonate the initiator or the responder.
4.2. Man-in-the-middle Attack

Proposition 3. Suppose the initiator and the responder have successfully shared a password $PW$, a man-in-the-middle attacker is not able to complete the improved protocol between the initiator and the responder without being detected.

Proof. Suppose $A$ is a man-in-the-middle attacker between the initiator and the responder. $A$ participates in the improved protocol as follows:

1. The initiator sends $A$ with $M_1$ which is the same with $M_1$ in the improved protocol:
   
   $$M_1 = \{ I, R, U_I, PK'_I, N_I \}. $$

   1$_A$. $A$ replaces $M_1$ with $M_{1A}$ and sends it to the responder:

   $$M_{A1} = \{ I, R, U_A, PK'_I, N_A \}. $$

2. The responder replies $A$ with $M_2$ which is the same with $M_2$ in the improved protocol:

   $$M_2 = \{ R, I, T_R, PK_R, N_R \}. $$

   2$_A$. $A$ sends $M_{A2}$ to the initiator:

   $$M_{A2} = \{ R, I, T_A, PK_A, N_A \} .$$

3. At this step, the Diffie-Hellman key $K_{IA}$ between $A$ and the initiator and $K_{RA}$ between $A$ and the responder are determined. Specifically, the initiator calculates $K_{IA} = (T_A - PK_A) \times R_I = G \times R_A \times R_I$ and the responder calculates $K_{RA} = (U_A \times G - PK_I) \times R_R = (R_A \times G + PK_A - PK_I) \times R_R$.

   The responder computes $MAC_3 = CMAC_{64}(RMB_{128}(K_{RA}), I || R || N_A || N_R)$ and sends $A$ with $M_3$:

   $$M_3 = \{ I, R, N_R, PK_R, MAC_3 \}.$$  

3$_A$. $A$ should send the initiator with

   $$M_{A3} = \{ I, R, N_A, PK_A, MAC_{A3} \} .$$

   where $MAC_{A3} = CMAC_{64}(RMB_{128}(K_{IA}), I || R || N_I || N_A)$

4. The initiator verifies $MAC_{A3}$.

4$_A$. $A$ should send the responder with

   $$M_{A4} = \{ R, I, N_A, MAC_{A4} \}. $$

   where $MAC_{A4} = CMAC_{64}(RMB_{128}(K_{RA}), I || R || N_A || N_R)$

5. The responder verifies $MAC_{A4}$

Since $A$ does not have any of $R_I$, $R_R$, $PK'_I$, it is infeasible for $A$ to compute $K_{IA}$ and $K_{RA}$, and therefore $A$ can not compute correct $MAC_{A3}$ in step 3$_A$ and $MAC_{A4}$ in step 4$_A$. Without valid $MAC_{A3}$ and $MAC_{A4}$, the initiator will stop the protocol at the beginning of step 4 and the responder will stop at the beginning of step 5, which means $A$ fails to establish a $MK$ either with the initiator or the responder. □

4.3. Off-line Dictionary Attack

Proposition 4. Suppose the initiator and the responder have successfully shared a password $PW$, a passive eavesdropper who records the one or more sessions of the improved protocol cannot eliminate a significant number of possible passwords.
Proof. In the improved protocol, values that are sent in clear include $I, R, UI_{I}, PK_{I}, NI_{I}, TR, PK_{R}, NR,$ $MAC_{3}$ and $MAC_{4}$. In order to carry out an off-line dictionary attack, the adversary needs to acquire information that can help him to check possible passwords from a dictionary. Among all of these values sent in clear, $PW$ has relationship only with $PK_{I}$ through the equation $PK_{I} = PK_{I} - Q(PW)$. $PK_{I}$ is kept secretly in the protocol, and $PK_{I} = SK_{I} \times G$ where $SK_{I}$ is a random integer. Therefore, $PK_{I}$ is a random value and is unknown to the adversary. The equation of $PK_{I} = PK_{I} - Q(PW)$ and the value of $PK_{I}$ do not give more information of $PW$ to the attacker. Based on these acquired knowledge, the attacker is unable to eliminate possible passwords. □

According to Proposition 4, an off-line dictionary attack to the improved protocol is infeasible.

4.4. Forward Secrecy

Proposition 5. Suppose the initiator and the responder have successfully shared a password $PW$, compromise of the long-term secret keys of a set of principals does not compromise the MKs established in previous runs of the improved protocol involving those principals.

Proof. The principals of this protocols are the initiator and the responder, and the long-term secret keys of these principals are the private keys $SK_{I}$ and $SK_{R}$, the password $PW$ and the public key $PK_{I}$ that is masked during transmission. Assume the adversary $A$ compromises these long-term secrets of the initiator and the responder, then (s)he has $SK_{I}, SK_{R}, PW$ and $PK_{I}$. In order to calculate a $MK$ established in a previous run, $A$ needs to compute $MK$ from the formula $MK = CMAC_{128}(LMB_{128}(K), NI_{I} || NR)$ where $K$ is a necessary input in that run. Note that $A$ can not use these values to run the protocol with the principles, since in this case the $MK$ is not belong to previous run, but is established in the current run. Therefore, $A$ has to compute $K$ through $K = (TR - PK_{R}) \times RI_{I}$, $K = (UI_{I} \times G - PK_{I}) \times R_{R}$ or $K = G \times R_{R} \times RI_{I}$. All of the three formulas require at least one of $RI_{I}$ and $R_{R}$. However, $RI_{I}$ and $R_{R}$ are random values chosen by the initiator and the responder respectively in each run of the protocol, which means these values change in every protocol run and are kept unknown to $A$. Without any of $RI_{I}$ and $R_{R}$, $A$ fails to compromise the $MK$, although (s)he compromises all the long-term secret keys and values. □

From Proposition 5 we can see the improved protocol provides forward secrecy.

5. Performance

In order to observe the performance of the improved protocol, we evaluate the computation and communication cost theoretically. In addition, we also test the performance through a set of experiments.

5.1. Evaluation

The overall burden of the protocol contains three parts: communication cost, computation cost on the node and computation cost on the hub. For the communication cost, we count the whole pieces of messages transmitted between the node and the hub within a run of the protocol. In order to evaluate the computation cost, we count the number of cryptographic algorithm CMAC and scalar multiplication of an element from the elliptic curve by an integer, since other operations such as addition and subtraction require minor computation cost.

Denote the cost of transmitting a piece of message by $M$, the cost of executing one CMAC algorithm by $H$, and the cost of executing the operation of scalar multiplication for one time by $S$, we compare the evaluated cost of the improved protocol with the modified protocol and the standard protocol in Table 2.

From Table 2 we can see that the improved protocol reduces computation cost on the node, while overall computation and communication cost does not increase. One time-consuming operation $S$ is
Table 2. Evaluation of Performance

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Computation cost on node</th>
<th>Computation cost the hub</th>
<th>Total computation cost</th>
<th>Communication cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>improved protocol</td>
<td>( S + 2H )</td>
<td>( 3S + 2H )</td>
<td>( 4S + 4H )</td>
<td>( 4M )</td>
</tr>
<tr>
<td>modified protocol</td>
<td>( 2S + 2H )</td>
<td>( 2S + 2H )</td>
<td>( 4S + 4H )</td>
<td>( 4M )</td>
</tr>
<tr>
<td>standard protocol</td>
<td>( 2S + 2H )</td>
<td>( 2S + 2H )</td>
<td>( 4S + 4H )</td>
<td>( 4M )</td>
</tr>
</tbody>
</table>

Table 3. Details of the node (implemented on Arduino Uno)

<table>
<thead>
<tr>
<th></th>
<th>Micro controller 16MHz, 8bit (ATmega328)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SRAM 2KB</td>
</tr>
<tr>
<td></td>
<td>EEPROM 1KB</td>
</tr>
<tr>
<td></td>
<td>Flash memory 32KB (bootloader 0.5K)</td>
</tr>
</tbody>
</table>

5.2. Experiments

The improved protocol contains the algorithm of CMAC and ECC key-generation (generating a private key and using scalar multiplication to compute the public key). We test the runtime of these algorithms on the node through a set of experiments. In the experiments, we use Arduino Uno as the node, SHA-256 as the CMAC algorithms and the ATECC108A crypto chip from Atmel to execute the ECC key-generation. The elliptic curve is Curve p-256 in FIPS Pub 186-3. Description of the node is listed in Table 3 and the results are summarized in Table 4.

From Table 4 we can see the runtime of executing these algorithms is affordable for the node, which means the improved protocol is suitable for WBANs applications.

6. Use Case

As described before, our improved protocol reduced the computational burden on one side of communication. This is a significant strength for some applications in wireless sensor networks. Here we describe a smart lock system that uses our improved protocol to generate a master key. The specific system and the usage of the improved protocol is described as follows.

Smart Lock System

As is shown in Figure 2, the smart lock system is consist of a lock which is a physical host embedded with a computational device, and a phone which has installed a smart lock application. The aim of this system is using this phone application to securely lock or unlock the lock. Obviously, the computationally limited lock is the initiator and the relatively powerful phone is the responder. The smart lock system includes the following three phases, and our protocol is involved in the first phase.

1. **Master Key Generation.** The lock and the phone secretly input the short password, and then execute our improved protocol. After this stage, a relatively long master key is shared by the lock and the phone.

Table 4. Runtime of involved cryptographic algorithms on the node

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Length of keys (bits)</th>
<th>Runtime (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECC key generation</td>
<td>–</td>
<td>48</td>
</tr>
<tr>
<td>SHA-256</td>
<td>512</td>
<td>3</td>
</tr>
</tbody>
</table>
2. Session Key Generation. With the master key, the lock and the phone execute the session key
   generation protocol (such protocols are available in literatures) to generate their session key for
   this round of communication.

3. Secure Communication. The newly generated session key is used for this round of
   communication between the phone and the lock. We describe the steps of as
   (1) The phone computes
   \[
   MAC = \text{HMAC}(\text{sessionkey}, P \| L \| \text{Request} \| \text{Counter})
   \]
   and sends the request (LOCK / UNLOCK) with the MAC to the lock. Here \( P \) and \( L \) denote
   the identity of the phone and the lock, and \( \text{Counter} \) denotes the value of counter.
   (2) The lock verifies the MAC. If the verification succeeds, the lock executes the request to
   lock or unlock; else it does not execute the request or responds a failure message.

Analysis

The smart lock system is secure since the session key is kept secretly by the two participants.
An adversary can not request the system to lock or unlock, because they can not compute the correct
MAC without the session key. Therefore, the security of the session key is significant for the security
of the whole system. Our improved protocol provides secure generation for the master key which in
turn guarantees the security of the session key.

Additionally, the device embedded in the lock is a less powerful device compared with a normal
cell phone. Our password-based authenticated association protocol in the first phase reduces the
computational cost of the lock, which makes the smart lock system more practicable.

7. Related Works

7.1. Comparison

In Section 5.1 we compared the cost of the improved protocol with other related protocols in
Table 2. The comparison in terms of security of these protocols is listed in Table 5, where √ means
being secure under the corresponding attacks or providing the corresponding security feature, while
× means being insecure or not providing.

7.2. Password-based Two-party Key Exchange

Several password-based authenticated key exchange protocols have been proposed. In this
subsection, we compare our improved protocol with three kinds of two-party key exchange protocols
which are based on password.
Table 5. Comparison of security (“√” denotes the protocol resist the attack or possess the security feature, and “×” denotes the the protocol does not resist the attack or does not possess the security feature)

<table>
<thead>
<tr>
<th>Attacks / Security feature</th>
<th>improved protocol</th>
<th>modified protocol</th>
<th>standard protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Impersonation attack</td>
<td>√</td>
<td>√</td>
<td>×</td>
</tr>
<tr>
<td>Man-in-the-middle attack</td>
<td>√</td>
<td>√</td>
<td>×</td>
</tr>
<tr>
<td>Off-line dictionary attack</td>
<td>√</td>
<td>√</td>
<td>×</td>
</tr>
<tr>
<td>Forward secrecy</td>
<td>√</td>
<td>×</td>
<td>×</td>
</tr>
</tbody>
</table>

Encrypted Key Exchange Using Diffie-Hellman

Diffie-Hellman-based Encrypted Key Exchange (EKE) protocols transmit the public keys encrypted using the password. The original protocol is proposed by Bellovin and Merritt in [21]. Variants and extensions of this protocol have been proposed. Such protocols are proved to be secure in random-oracle model, however, in practice attacks against these protocols exist since the two parties are not able to verify the integrity of the received messages. If an attacker maliciously modifies the message, the two participants will generate different keys while they are not aware.

The IEEE std password authenticate association protocol and our improved protocol are developed from these kind of protocols. As in the IEEE std protocol and our improved protocol HMAC is used for verifying the integrity of messages transmitted between the two parties, the above attacks against the original Diffie-Hellman-based EKE protocols are eliminated.

RSA-Based Protocols

RSA-Based Protocols use the RSA algorithm as the basis of the password authentication key exchange scheme. In [22] MacKenzie proposed a variant of RSA based open key exchange protocol called SNAPI (Secure Network Authentication with Password Information). Verification for the integrity of transmitted messages is involved in this protocol. However, this protocol is not suitable for wireless sensor networks since sensors are usually not powerful enough to run the RSA algorithm.

Protocols Using a Server Public Key

Some password-based authenticated key exchange protocols use a server public key in addition to the pre-shared password. Such protocols include the GLNS compact protocol proposed by Gong et al. in [23], Gong’s Optimal GLNS nonce-based protocol in [24], Kwon-Song Protocol in [25] and Halevi-Krawczyk Protocol in [26]. However, all of the four protocols used public key encryption, which is too high in computational cost for sensor devices. Moreover, the former two protocols need the participation of a server.

8. Conclusion

In low-power, low-complexity wireless sensor network applications such as WBANs, the communications security requirements mainly include authentication between participants, as well as confidentiality and integrity of transmitted messages. Mechanisms that aim to satisfy these requirements usually need a secret key to be held by participants. Therefore, key establishment and management are significant for security service in communications networks. The password authenticated association protocol is a scheme for the participants to generate a master key from a pre-shared password.

Considering the asymmetric power of the two participants in WBANs, we propose an improved password authenticated association protocol that reduces the computational cost on the less powerful participant of communication. The improved protocol can resist both impersonation attacks and man-in-the-middle attacks. A master key between the node and the hub will be established securely and efficiently through this protocol, and afterwards this is used for pairwise temporal key (PTK)
creation, and the PTK is the key used in encryption and decryption process to provide authentication, confidentiality and integrity for communication.

The improved protocol requires one scalar multiplication and two HMAC computations on the nodes (i.e. the initiator). Since the computational costs of these algorithms are acceptable to devices with limited power in WBANs, the improved protocol is suitable for applications in WBANs.

**Acknowledgments:** This work has been supported by the XJTLU research development fund projects RDF140243 and RDF150246, as well as by the Suzhou Science and Technology Development Plan under grant SYC201516, Jiangsu Province National Science Foundation under grant BK20150376, and the Natural Science Foundation of Jiangsu Province under Grant BK20140404.

**Author Contributions:** Jie.Zhang and Xin.Huang. attacked the standard protocol, conceived and designed the improved protocol; Paul.Craig. and Alan.Marshall. analyzed the result; Jie.Zhang wrote the paper; Paul.Craig. and Alan.Marshall. modified the English language of the manuscript. Duwei.Liu and Xin.Huang contributed analysis tools.

**Conflicts of Interest:** The authors declare no conflict of interest.

**Abbreviations**

The following abbreviations are used in this manuscript:

- **WBAN:** wireless body area network
- **PTK:** pairwise temporal key
- **MAC:** message authentication code
- **EKE:** encrypted key exchange
- **SNAPI:** secure network authentication with password information

**References**


© 2016 by the authors. Submitted to *Symmetry* for possible open access publication under the terms and conditions of the Creative Commons Attribution license (http://creativecommons.org/licenses/by/4.0/).