<table>
<thead>
<tr>
<th>Title</th>
<th>An Efficient EAP-Based Pre-Authentication for Inter-WRAN Handover in TV White Space</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Wang, Cong; Ma, Maode; Zhang, Lei</td>
</tr>
<tr>
<td>Citation</td>
<td>Wang, C., Ma, M., &amp; Zhang, L. (2017). An Efficient EAP-Based Pre-Authentication for Inter-WRAN Handover in TV White Space. IEEE Access, 5, 9785-9796.</td>
</tr>
<tr>
<td>Date</td>
<td>2017</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/10220/44222">http://hdl.handle.net/10220/44222</a></td>
</tr>
<tr>
<td>Rights</td>
<td>2017 IEEE. Translations and content mining are permitted for academic research only. Personal use is also permitted, but republication/redistribution requires IEEE permission. See <a href="http://www.ieee.org/publications_standards/publications/rights/index.html">http://www.ieee.org/publications_standards/publications/rights/index.html</a> for more information.</td>
</tr>
</tbody>
</table>
An Efficient EAP-Based Pre-Authentication for Inter-WRAN Handover in TV White Space

CONG WANG¹, MAODE MA², (Senior Member, IEEE), AND LEI ZHANG¹,³

¹School of Computer Science and Technology, Tianjin University, Tianjin 300072, China
²School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore
³Tianjin Key Laboratory of Advanced Network Technology and Application, Tianjin 300072, China

Corresponding author: Lei Zhang (lzhang@tju.edu.cn)

This work was supported by the National Instrumentation Program of China under Grant 2013YQ030915.

ABSTRACT The IEEE 802.22 standard regulates wireless regional area network (WRAN) operating at the very high frequency and ultrahigh frequency television white space (TVWS) bands. WRAN supports extensible authentication protocol (EAP)-based authentication schemes. However, due to its public key cryptography operations, a full EAP-based authentication scheme is time-consuming, which is unacceptable for the WRAN handover process. In this paper, an efficient EAP-based pre-authentication scheme for inter-WRAN handovers (EPW) in TVWS is proposed. By applying the proposed pre-authentication scheme, the customer premises equipment and the target secondary user base station can accomplish a seamless handover using symmetric key. Through logic derivation by Burrows, Abadi, and Needham logic and formal verification by automated validation of Internet security protocols and applications, we conclude that the proposed EPW scheme can obtain mutual authentication and maintain key secrecy with a high resistance to attack. Additionally, the performance of the EPW scheme has been investigated by simulation experiments. The results show that the EPW scheme provides a lower computation delay than that mandated by the security scheme regulation of the IEEE 802.22 standard.

INDEX TERMS Pre-authentication, TV white space, WRAN, handover, EAP, key secrecy.

I. INTRODUCTION

In modern wireless communication networks, a common problem is spectrum resource scarcity. However, many frequency bands are underutilized, such as TV broadcast bands. The United States Federal Communications Commission (FCC) [1] has permitted the use of TV broadcast white space (TVWS) [2] by secondary users (SUs), including customer premises equipment (CPE) and secondary user base stations (SUBS), on the condition that this use does not disturb primary users (PUs). Proper development of TVWS can alleviate the shortage of available wireless spectrum caused by the underutilization of these bands. There are approximately 300 MHz of bandwidth made available from the TV spectrum. This large TV broadcast band with good propagation characteristics and favorable path loss features can be developed for unlicensed usage as specified by the IEEE 802.22 standard [3]. According to this standard, to avoid disturbing the PUs, the SUs must sense a spectrum temporally and spatially to determine whether it is occupied by PUs and must vacate any spectrum once it is reclaimed by PUs.

One of the primary problems in configuring the wireless regional area network (WRAN) in TVWS regulated as the IEEE 802.22 standard, as in other wireless communication networks, is the security issue. Additionally, the WRAN faces ot merely the conventional security menaces but also new challenges inherent to cognitive functions Security concerns are also critical to the handover process for WRAN. Due to the mobility and the cognitive function of CPEs, it is extraordinarily practical for a CPE to set up a security association with another SUBS once the CPE leaves the service region of its current SUBS. An authentication scheme that permits authorized secondary users to join in the service provided by the target SUBS in WRAN and that refuses any unauthorized users is required to accomplish the security association in the handover process.

The IEEE 802.22 standard supports an extensible authentication protocol (EAP)-based authentication scheme [4] with the participation of a back-end authentication server (AS). The EAP has been devised by the Internet Engineering Task Force (IETF) for Point-to-Point Protocol (PPP) for an
optional authentication phase after the PPP link has been established. The EAP framework supports more than one authentication scheme and can be used in a particular scheme, such as EAP-based transport layer security protocol (EAP-TLS), to achieve mutual authentication [5]. The flexibility of the EAP-TLS authentication protocol makes it a good choice for WRAN. An inter-WRAN handover is a CPE handover from one SUBS to another SUBS in the same WRAN cell. Before the handover, the CPE completes a full EAP-TLS authentication with the SUBS through the AS, in which the CPE performs a security association’s traffic encryption key (SA-TEK) 3-way handshake with the SUBS. The handover procedure in WRAN must be very efficient and fast to effectively maintain a security association. A full EAP-TLS authentication requires roughly 50 ms due to time-consuming public key cryptography operations and the latency of information exchange over the several round-trips between the CPE and the AS.

For the sake of reducing handover delay, WRAN may support the optimization of the handover procedure by recycling key information from previous authentication processes [3], which, however, results in successful man-in-the-middle (MITM) attacks and replay attacks due to its lack of a secure entity authentication protocol. Alternative solutions [6]–[9] focus on decreasing the latency of the EAP-based authentication scheme without considering security functions. The currently popular schemes proposed for handover optimization generally include a pre-authentication scheme by which the AS distributes a new secret CPE handover key for the next handover before the handover occurs. Thus, the handover latency can be decreased to the amount of time required by a 3-way handshake protocol, resulting in the shortest possible authentication latency [10]–[14].

The pre-authentication scheme does not reuse the cryptographic key materials directly, which achieves greater security. An EAP-based pre-authentication scheme has been proposed by the Handover Keying working group in [9]. The scheme, known as the handover early authentication (HOEA) protocol, is applied to the mobile IPv6 network [11]. The HOEA protocol completes a full EAP authentication process before the Mobile Station (MS) handover occurs, then uses proactive signaling to find a potential access network for the MS handover. The HOEA protocol, however, only operates when the link layer supports proactive signaling. Worse, the pre-authentication process may not be complete before the handover process is triggered, which leads to a failure of pre-authentication. Sun et al. [12] propose an EAP-based pre-authentication scheme (EPA) in WiMax to decrease the authentication latency for inter-base station (BS) handovers by which an MS is authenticated with neighboring BSs for handover. The EPA does not require proactive signaling, which is an advantage over the HOEA protocol. The EPA, however, is susceptible to replay attacks and Denial of Service (DoS) attacks [13], which will degrade its level of security. The EPA also wastes effort on superfluous key exchanges between the MS and those BSs that the MS never roams to, which is not efficient. Junbeom et al. [14] apply public key cryptography in the pre-authentication scheme. Public key cryptography consumes massive computational resources, which is undesirable. Nguyen and Ma [13] propose an enhanced EAP-based pre-authentication scheme (EEP) to improve the security level and the efficiency of the EPA. The EEP scheme can defend against replay attacks and DoS attacks, but the MS and AS cannot obtain key agreement in the pre-authentication process.

Normally, a security mechanism consists of an authentication mechanism and a key management mechanism. The EAP-TLS authentication scheme could be used in WRAN defined by the IEEE 802.22 standard. However, a full EAP-TLS authentication process needs 50 ms [15] to complete, which is unacceptable for WRAN. The EAP-based authentication protocol is inefficient in the WRAN handover process. In addition, CPEs must vacate a spectrum needed by PUs. CPEs are more mobile in WRAN, and their handovers are consequently more frequent, than in other wireless networks. The IEEE 802.22 standard also presents a public key certificate based authentication scheme that is vulnerable to interleaving attacks [16]. The certificate based authentication scheme requires the participation of a third party, which is not efficient for WRAN. To the best of our knowledge, there are few works focusing on handover optimization for WRAN in TVWS.

To design an efficient and secure handover protocol for WRAN in TVWS with less latency and strong security functionality, we propose an efficient EAP-based pre-authentication for inter-WRAN handovers (EPW) in TVWS in this paper. The outstanding contribution of our proposal is the distribution, before the handover, of the pre-master secret (PMS) by the AS to the CPE using a pre-authentication scheme, resulting in the AS and the CPE having PMS agreement. When a handover occurs, the target SUBS requests the master session key for authenticating the CPE from the AS. Then the target SUBS and the CPE can proceed directly with the 3-way handshake protocol and key agreement. Using Burrows, Abadi, and Needham (BAN) logic and formal verification by Automated Validation of Internet Security Protocols and Applications (AVISPA), we can conclude that the EPW scheme can provide mutual authentication and key secrecy with strong attack resistance via pre-authentication. Additionally, the performance of the EPW scheme in terms of authentication delay has been evaluated by simulation experiments, with the results demonstrating that the EPW scheme is much more efficient, requiring less computation and fewer communication resources.

The rest of the paper is organized as follows. We briefly describe the background of the WRAN system in Section II. Then, we present the proposed EPW scheme in Section III. In Section IV, we validate the EPW scheme using BAN logic and AVISPA, followed by performance evaluation in Section V. Section VI presents the conclusion of the paper.
II. SYSTEM BACKGROUND
A. SYSTEM ARCHITECTURE
The overall architecture of the system under study consists of a primary network and some secondary networks. The primary network, which has a higher priority when using the spectrum, includes TV translators, TV receivers, TV boosters and wireless microphones. The secondary networks, namely, WRAN, include a SUBS and the related CPEs, as shown in Fig. 1. The SUBS controls itself and all the related CPEs in its service area, and also regulates the medium access and the communications between the CPEs and the SUBS. Unlike conventional licensed-band fixed wireless networks, a WRAN needs a cognitive mechanism for monitoring PU activity. The SUs need to sense the spectrum holes to avoid disturbing the operation of the PUs. The SUBS can offer high-speed Internet communication service within its coverage area for more than 512 portable or fixed CPEs with cognitive modules and still satisfy the FCC’s rules for protecting the PUs.

B. SECURITY MECHANISM IN THE IEEE 802.22 STANDARD
The security mechanism offers protection for IEEE 802.22 users, service providers and most importantly, PUs with spectrum priority. Therefore, the security mechanism in the IEEE 802.22 is actualized by 2 security sub-layers. Sub-layer 1, called a non-cognitive security mechanism, provides the same security functions as traditional wireless networks, while sub-layer 2, called a cognitive security mechanism, has cognitive functions to protect the PUs. Sub-layer 2 is not investigated in this paper.

The non-cognitive security mechanism offers SUs authentication or confidentiality for user data and MAC management messages transmitted across the WRAN in TVWS, as illustrated in Fig. 2. The security functions are implemented using cryptographic transforms to MAC protocol data units (PDUs) carried across connections between the CPEs and SUBS. The security sub-layer 1 specified by IEEE 802.22, newly named the security control management (SCM) protocol, is evolved from the privacy key management versions 1 and 2 (PKMv1 and PKMv2) specified in the IEEE 802.16-2009 standard [17]. The SCM protocol offers secure key distribution from the SUBS to the CPEs. According to the SCM, once a SUBS and CPE accomplish mutual authentication, they establish an authorization key, which is then used for later secure SCM information exchanges. The SCM scheme manages all aspects of security by deriving and producing different keys. The Traffic Data Processing scheme decrypts or encrypts the messages and performs the authentication process for the messages. Control Message Processing precedes different related SCM MAC messages and offers either encryption or authentication of such MAC messages.

C. OVERVIEW OF EAP-TLS
The EAP-TLS [18] uses the transport layer security protocol, in which a server and a client set up a connection by a handshake process. To establish a security function, some quantities are determined during the handshake process. The handshake starts when a client requests a safe connection to a TLS server using a set of keys and the hash functions supported by the client. The server selects the most robust keys and hash function from the current supported list. Then the server sends its certificate to the client. The certificate consists of the server’s certificate authority, server name, public key and validation time. Once the server’s certificate is confirmed, the client generates a nonce under the encryption of the server’s public key. This message, which may only be decrypted by the user with the corresponding private key, is sent to the server. By using a nonce, the server and the client can generate a session key containing the handshake process and the generated PMK to allow further safe communication. The session key can be used for encrypting and decrypting the information exchanged in the rest of the session. The authentication process and message exchange of the EAP-TLS scheme is illustrated in Fig. 3.

The EAP-TLS scheme is able to achieve mutual authentication. A hostile server cannot masquerade as the authentic server without user knowledge. Furthermore, the EAP-TLS scheme offers a strong forward and backward security...
function, meaning the attacker cannot get the session keys from either the backward or forward sessions with acquired session keys. The EAP-TLS scheme provides a very high level of security. The attacker cannot break the EAP-TLS even if he possesses the user’s password, because the attacker does not have the private key. However, the EAP-TLS scheme requires both the server’s and the client’s certificates. The issuance of public key certificates demands much additional administrative work as well as overhead, and the validation of the certificates is also time-consuming. In addition, a full EAP-TLS authentication process requires many rounds of information exchange between the server and the client, consuming approximately 50 ms, which is unacceptable for WRAN in TVWS.

III. PROPOSED PRE-AUTHENTICATION SCHEME

To reduce the overall latency produced by the full EAP-TLS authentication process and, further, to support secure handover in the WRAN, we want to design and propose a novel, efficient, EAP-based pre-authentication for inter-WRAN handover in TVWS. According to the proposed solution, if a CPE is entering a cell of the WRAN for the first time, the EAP-TLS authentication protocol is applied to perform a full authentication. Otherwise, the EAP-based pre-authentication scheme will be invoked to perform a simple and quick pre-authentication.

The EPW scheme comprises the pre-authentication phase shown in Fig. 4 and the handover phase illustrated in Fig. 5. When a CPE and some SUBS, hSUBS, complete the full EAP-TLS authentication process via the AS, the CPE and hSUBS will share the symmetric key $K_{hSUBS\rightarrow CPE}$, and hSUBS and the AS will share the symmetric key $K_{hSUBS\rightarrow AS}$. The symmetric key is not revealed to any other entity. The procedure of the proposed pre-authentication phase, illustrated in Fig. 4, is as follows.

1) PRE-AUTHENTICATION INITIALIZATION

hSUBS transmits the PREAUTH_INT message, including a 64 bit session identifier (SID), to the CPE under encryption with the symmetric key $K_{hSUBS\rightarrow CPE}$. Whenever hSUBS starts a fresh pre-authentication with the same CPE, the SID will be incremented.

2) PRE-AUTHENTICATION REQUEST

The CPE decrypts the PREAUTH_INT message using the symmetric key $K_{hSUBS\rightarrow CPE}$, then verifies the SID, finds a decrease of signal intensity at hSUBS and decides to handover to another SUBS, tSUBS, the CPE may initialize the handover phase. Table 1 describes the principal notations used to describe the EPW scheme.

A. PRE-AUTHENTICATION PHASE

After the CPE completes a full EAP-TLS authentication process with hSUBS via the AS, the CPE and hSUBS will share the symmetric key $K_{hSUBS\rightarrow CPE}$, and hSUBS and the AS will share the symmetric key $K_{hSUBS\rightarrow AS}$. The symmetric key is not revealed to any other entity. The procedure of the proposed pre-authentication phase, illustrated in Fig. 4, is as follows.

1) PRE-AUTHENTICATION INITIALIZATION

hSUBS transmits the PREAUTH_INT message, including a 64 bit session identifier (SID), to the CPE under encryption with the symmetric key $K_{hSUBS\rightarrow CPE}$. Whenever hSUBS starts a fresh pre-authentication with the same CPE, the SID will be incremented.

2) PRE-AUTHENTICATION REQUEST

The CPE decrypts the PREAUTH_INT message using the symmetric key $K_{hSUBS\rightarrow CPE}$, then verifies the SID,
by checking whether the last SID received from hSUBS is less than the current SID received, to guarantee that it is not a replayed message. Then, the CPE randomly produces 64 bit nonce \(N_{CPE}\). The PREAUTH_REQ message contains the SID, \(N_{CPE}\) and the CPE’s identifier, \(ID_{CPE}\). The CPE then sends the PREAUTH_REQ message encrypted with the symmetric key \(K_{hSUBS-CPE}\) to hSUBS. After hSUBS receives the message, hSUBS decrypts it with \(K_{hSUBS-CPE}\), then compares the received SID with the SID sent in the PREAUTH_INT message. If they are the same, hSUBS can confirm this message comes from the CPE, encrypt the PREAUTH_REQ message with the symmetric key \(K_{hSUBS-AS}\), and transmit it to the AS.

3) PRE-AUTHENTICATION RESPONSE

After the AS receives the encrypted PREAUTH_REQ message, the AS will repeat the verification done by hSUBS at the second step. Then, the AS randomly generates 64 bit nonce \(N_{AS}\) and produces a PMS key supported by the CPE. The PREAUTH_RSP message contains SID, the new nonce \(N_{CPE}\), the received \(N_{CPE}\), \(ID_{CPE}\) and the PMS. The AS encrypts the PREAUTH_RSP message with the symmetric key \(K_{hSUBS-AS}\) and then sends it to hSUBS. hSUBS decrypts the received message from the AS and does verification, as in the second step, by comparing the SIDs. Then, hSUBS decrypts the PREAUTH_RSP message with the symmetric key \(K_{hSUBS-AS}\) and transmits it to the CPE. After the CPE gets the encrypted PREAUTH_RSP message, the CPE decrypts it with \(K_{hSUBS-CPE}\), then compares the SID and \(N_{CPE}\) received in the PREAUTH_RSP message with the SID received in the PREAUTH_INT message and \(N_{CPE}\) sent in the PREAUTH_RSP message, respectively. If they are the same, the CPE can confirm this message is from hSUBS.

4) PRE-AUTHENTICATION ACKNOWLEDGMENT

The CPE can get the PMS from the PREAUTH_RSP message. Then, the CPE constructs the PREAUTH_ACK message including SID and \(N_{AS}\), encrypts it with the PMS, and sends \(\{SID, N_{AS}\}_{PMS}\) to hSUBS. hSUBS also receives the PMS in the PREAUTH_RSP message, decrypts the PREAUTH_ACK messages with the PMS, and does verification as in the third step with SID and \(N_{AS}\). Then, hSUBS relays the PREAUTH_ACK message to the AS.

The messages exchanged between the CPE and the AS through hSUBS in the pre-authentication process are shown in Table 2.


<table>
<thead>
<tr>
<th>Message Type</th>
<th>Message Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>PREAUTH _INT</td>
<td>(hSUBS \rightarrow CPE: {SID}<em>{K</em>{PME,hSUBS}})</td>
</tr>
<tr>
<td>PREAUTH _REQ</td>
<td>(CPE \rightarrow hSUBS: {SID, N_{CPE}, ID_{CPE}}<em>{K</em>{PME,hSUBS}})</td>
</tr>
<tr>
<td></td>
<td>(hSUBS \rightarrow AS: {SID, N_{CPE}, ID_{CPE}}<em>{K</em>{PME,AS}})</td>
</tr>
<tr>
<td>PREAUTH _RSP</td>
<td>(AS \rightarrow hSUBS: {SID, N_{AS}, N_{CPE}, ID_{CPE}, PMS}<em>{K</em>{hSUBS,AS}})</td>
</tr>
<tr>
<td></td>
<td>(hSUBS \rightarrow CPE: {SID, N_{AS}, N_{CPE}, ID_{CPE}, PMS}<em>{K</em>{hSUBS,AS}})</td>
</tr>
<tr>
<td>PREAUTH _ACK</td>
<td>(CPE \rightarrow hSUBS: {SID, N_{AS}}_{PMS})</td>
</tr>
<tr>
<td></td>
<td>(hSUBS \rightarrow AS: {SID, N_{AS}}_{PMS})</td>
</tr>
</tbody>
</table>

### B. HANDOVER PHASE

Whenever the CPE finds a decrease of signal intensity in hSUBS and decides to handover to tSUBS, the CPE may initialize the handover phase. The decision may originate either at the CPE or hSUBS, using the handover message. Before the handover is triggered, hSUBS signals the possible tSUBS about the CPE’s intention to handover via a handover notification message (HO_REQ) including \(ID_{CPE}\) and \(ID_{AS}\). If tSUBS allows the CPE handover, tSUBS replies with a handover notification response (HO_RSP) to hSUBS. Then, hSUBS relays the HO_RSP to the CPE and releases the connection to the CPE. Note that the tSUBS will ask the AS for the MSK by transmitting a KEY_REQ message to the AS, including \(ID_{CPE}\) and \(ID_{SUBS}\) encrypted with the symmetric key \(K_{SUBS,AS}\). The AS derives the MSK using (1), in a manner similar to that of EAP-TLS key derivation in [3]:

\[
\begin{align*}
\text{Master}\_\text{secret} &= TLS - PRF \\
&= 48 \text{ (PMŠ, "master sec ret"}, ID_{CPE}||ID_{SUBS})
\end{align*}
\]

\[
\begin{align*}
\text{Key}\_\text{Material} &= TLS - PRF - 128(Master\_\text{secret}, \\
&\text{"EAP encryption"}, ID_{CPE}||ID_{SUBS})
\end{align*}
\]

\[
\text{MSK} = \text{Key}\_\text{Material} (0, 63)
\]

More information on the TLS-PRF-X function can be found in [17]. The AS sends the MSK with the encryption of the symmetric key \(K_{SUBS,AS}\) to tSUBS by the KEY_RSP message. Meanwhile, the CPE can derive the MSK in the same manner. The CPE and tSUBS obtain the same MSK, then derive the authorization key (AK) and continue with the SA-TEK 3-way handshake protocol as regulated by the IEEE 802.22 standard [3]. The handover phase is depicted in Fig. 5.

C. USE CASE STUDY

In order to better understand the proposed EPW for inter-WRAN handover, we describe a use case study showing how EPW works and how anonymity user is stopped. Fig. 6 illustrates the network topology in the WRAN scenario used as the use case study. Apart from the CPE subscribed to, there are two SUBS namely hSUBS and tSUBS within the same
WRAN domain which deploys an authentication server AS managing the access control tasks such as authentication, authorization and accounting.

We analyze how our proposed EPW operates to offer privacy to the authentication.

1) BOOTSTRAPPING PHASE
When a CPE is the first time for connecting to his hSUBS, a bootstrapping process is performed. After the CPE and hSUBS complete a full EAP-TLS authentication via the bootstrapping process, the AS and the CPE are mutually authenticated to share a fresh PMS for handover and that the AS and the CPE share the belief that each of them holds the PMS. When using BAN logic to analyze a particular protocol, all protocol messages must be converted into specified BAN logic formulas, in accordance with the knowledge of the facts, to complete the idealized protocol and advance reasonable assumptions through logic rules. The idealized protocol and the assumptions are used to derive a specific agreement as to whether the particular protocol can achieve the desired objective.

The logic postulates applied in the proof of the EPW’s validity are presented here.

1) The message-meaning rule presents the messages’ interpretation, according to (2). The rule interprets how to derive beliefs from the original messages.

2) The nonce-verification rule checks whether a message is recent, and hence that the sender still believes in it, according to (3):

3) The jurisdiction rule, as presented in (4), provides that P will believe that Q has said X, that is, P believes in Q if P believes that X is recent, and Q once said X.

4) The freshness rule, (5), states that if one part of a formula is known to be fresh, then the whole formula must also be fresh.

IV. EVALUATION OF EPW
A. LOGIC CORRECTNESS PROOF BY BAN LOGIC
In this subsection, employing the BAN logic proposed by Burrows et al. [19], we will prove the logical correctness of the EPW scheme. BAN logic can be applied to check whether a protocol’s execution achieves its desired objectives and to detect any defects in the design of the protocol. The objective of the proposed EPW scheme is to guarantee that, after execution of the pre-authentication phase, the AS and the CPE are mutually authenticated to share a fresh PMS for handover.

FIGURE 6. Use Case Scenario.
By using $N_A$ with the freshness rule, we infer (15)

$$A| \equiv \#(N_A)$$

Using the nonce-verification rule, we can infer (16)

$$A| \equiv \#(A \leftrightarrow S), A| \equiv S| \sim A \leftrightarrow S$$

Using the jurisdiction rule, we can also derive (17)

$$A| \equiv (S| \Rightarrow (A \leftrightarrow S)), A| \equiv (A \leftrightarrow S)$$

$$A| \equiv \#(A \leftrightarrow S)$$

From the PREAUTH_ACK message, via the message-meaning rule, we can obtain (18)

$$S| \equiv (S| \Rightarrow (A \leftrightarrow S)), A| \equiv (A \leftrightarrow S)$$

We have obtained two results, $A| \equiv \#(A \leftrightarrow S)$ and $S| \equiv \#(A \leftrightarrow S)$, indicating that $A$ and $S$ have mutual authentication and PMS key agreement, which are also the goals of EPW.

### B. SECURITY ANALYSIS

In this subsection, the security properties of the proposed EPW scheme, including mutual authentication, session key agreement and the ability to resist replay attacks and MITM attacks, are analyzed.

1) **MUTUAL AUTHENTICATION AND SESSION KEY AGREEMENT**

The messages exchanged in the pre-authentication phase are all encrypted with a symmetric key, which guarantees that only one who has the corresponding symmetric key can view the message. The symmetric key $K_{\text{SUBS.CPE}}$ is only shared by the CPE and hSUBS; $K_{\text{SUBS.AS}}$ is only shared by hSUBS and the AS. In response to the PREAUTH_REQ message, the AS sends a randomly generated nonce $N_A$ and the PMS encrypted with $K_{\text{SUBS.AS}}$, which can only be read by hSUBS, hSUBS relays the $N_A$ and the PMS encrypted with $K_{\text{SUBS.CPE}}$, which can only be read by the CPE. When the AS receives the nonce $N_A$ encrypted with the PMS, then the AS can verify this message has been sent by the CPE, authenticating the CPE and confirming that the CPE has gotten the PMS for further handover. The CPE authenticates
the AS in the same way using the nonce $N_{CPE}$. In the handover phase, tSUBS can ask the AS for the MSK for communication with the CPE. The CPE can derive the MSK, using the same formula as the AS, from the PMS. Then, the CPE and tSUBS similarly compute the AK from the MSK. Finally, the CPE and tSUBS get mutual authentication and key agreement using the SA-TEK 3-way handshake protocol as regulated by the IEEE 802.22 standard [3], where messages are encrypted using the AK. Even though the CPE must initiate a new handover with another tSUBS when the previous handover fails, the CPE can utilize the same PMS to construct a new MSK with the new tSUBS, because the identity of the new tSUBS, $ID_{tSUBS}$, is used as the input of the key derivation function and each tSUBS has a single identity. The new MSK that the CPE shares with the new tSUBS is different from that shared with the former tSUBS. Therefore, our proposed EPW can guarantee mutual authentication and session key agreement.

2) RESISTANCE TO MALICIOUS ATTACKS

Using a replay attack, a legal message exchange could be fraudulently or maliciously repeated or delayed by an attacker. The replay attack can be launched by an attacker who holds the message and retransmits it. The EPW scheme employs the SID to guarantee the messages to be fresh. The attacker cannot replay the message, as the SID is incremented whenever a SUBS initiates a new request, by which an SID can be used only once. In the pre-authentication phase, using the nonce-challenge mechanism, both the CPE and the AS can confirm the message to be fresh. For example, when the AS gets the PREAUTH_ACK message, the AS can decrypt the nonce $N_{AS}$ with the PMS. By comparing whether the nonce $N_{AS}$ and the $N_{AS}$ sent in the PREAUTH_RSP message are same, the AS can determine whether this message is fresh. In this manner, our proposed EPW scheme is able to resist replay attacks.

Using MITM attacks, an adversary can make independent connections with the victims and then retransmit the messages between them, duping the victims into thinking they are communicating directly with one another over a private connection. The adversary can hold all the messages transmitted between the two victims and control the entire conversation. The attacker can intercept all the messages exchanged between them. In the EPW scheme, all the messages are encrypted with symmetric keys, and only one who has the corresponding symmetric keys can understand the message. An adversary cannot modify the messages, as it does not have the corresponding symmetric keys. For example, in the pre-authentication phase, the AS issues the PMS encrypted with the symmetric key, and an adversary cannot decrypt the PMS without. In the handover phase, the CPE and tSUBS derive the AK using the PMS. Without the PMS, the adversary cannot obtain the AK. Therefore, the EPW scheme is safe against MITM attacks.

C. FORMAL VERIFICATION BY AVISPA

AVISPA is a modern tool that can be used for automatic protocol validation and falsification [20]. Protocol verification and falsification differ in the sense that in verification, AVISPA attempts to validate the tested protocols’ correctness, whereas in falsification, AVISPA attempts to discover vulnerabilities in the tested protocols under various attacks. To express specifications for tested protocols, AVISPA applies a special modeling language, called High Level Protocol Specification Language (HLPSL), which is compiled into a low level intermediate format (IF) by applying an hlpsl2if translator. Then, one of the four supported back-ends simulates IF code to discover any possible security vulnerabilities in the protocols being analyzed.

The AVISPA architecture is illustrated in Fig. 7. Presently, AVISPA supports 4 back-ends: the On-the-Fly Model Checker (OFMC), Constraint-Logic-based Attack Searcher (CL-AtSe), SAT-based Model Checker (SATMC), and Tree Automata based on automatic approximations for the analysis of security protocols (TA4SP). The OFMC executes bounded verification and protocol falsification on protocol models applying the lazy intruder technique to create valid limitless state space in a demand-driven way. The CL-AtSe completes bounded verification and protocol falsification by incorporating different optimizing methodologies to lessen uselessness and redundancies in the protocol models being tested. The SATMC is used to reduce security vulnerabilities of the protocol being tested by building a propositional formula encoding all the possible attacks on the protocol and feeding the results to a state-of-the-art SAT solver. Finally, the TA4SP performs the unbounded verification of security properties of the protocol using regular tree languages and rewriting to generate under- and over-approximations.

We have used the four back-ends of the AVISPA framework to test our proposed EPW scheme. The results show that the EPW scheme is secure according to all four back-ends, as illustrated in Fig. 8, indicating that the EPW scheme, as specified by the HLPSL, satisfies the desired objectives of mutual authentication and secrecy of the shared keys under replay attacks and MITM attacks. Namely, the particular security objectives we specified for the EPW scheme can be satisfied for a bounded number of sessions, and the SATMC and TA4SP find that no attack can break the EPW scheme. Therefore, we can assert that our proposed EPW scheme can
achieve mutual authentication and preserve the secrecy of sensitive data from a passive intruder.

V. PERFORMANCE EVALUATION

In this section, we will compare the EPW scheme with the EAP-TLS authentication scheme suggested in the IEEE 802.22 standard [3] and the EEP scheme [12] proposed in the IEEE 802.16 standard in terms of the number of cryptographic operations and the authentication delay. This comparison reveals that the EPW scheme can not only provide security functionality but also efficiently decrease computational costs and delay.

A. NUMBER OF CRYPTOGRAPHIC OPERATIONS

We compare the number of cryptographic operations executed by the CPE and the SUBS in the pre-authentication process in the EAP-TLS scheme (TLS) regulated by the IEEE 802.22 standard, the EEP scheme and the EPW scheme. To improve comparison accuracy, we classify the required cryptographic operations into five basic types. The basic cryptographic operation types are 1) Cert verification (CEV), 2) Rivest, Shamir and Adleman (RSA) public key encryption (RPE), 3) RSA public key decryption (RPD), 4) symmetric encryption/decryption (SED), and 5) bilinear pairing (PAR). Table 3 shows the results of the cryptographic operation comparisons among the TLS scheme, the EEP scheme and the EPW scheme. Table 3 clearly shows that the EPW scheme needs far fewer basic cryptographic operations than does the TLS scheme, except in the number of symmetric encryption/decryption operations performed in the pre-authentication phase. It is important to note that symmetric encryption/decryption can significantly reduce the authentication delay. The EEP scheme uses fewer RSA public key encryption and decryption operations than those of the TLS.
scheme and zero bilinear pairing operations. The EEP scheme uses more RSA public key encryption and decryption operations than the EPW scheme does because the EEP scheme requires verification on the certificate and the public key signature. Only the TLS scheme requires a bilinear pairing operation, which takes much more time than other operations.

### B. PRE-AUTHENTICATION DELAY

The pre-authentication delay incurred is defined as the total time cost of all cryptographic operations in the pre-authentication process. To evaluate the latency applied by the cryptographic operations, we use the information offered in [21], where the cryptographic algorithms are coded in C++, compiled with Microsoft Visual C++ 2005 SP1, and executed over an Intel Core 2 1.83 GHz processor under Windows Vista in 32-bit mode. Among these cryptographic operations, the bilinear pairing operations are the most time-consuming. Additionally, the time cost of an RSA public key encryption operation is similar to the time cost of a symmetric encryption/decryption operation.

We first compare the TLS scheme, the EEP scheme and the proposed EPW scheme in the case that there is no attack on the WRAN in TVWS. In this case, the total authentication delay caused by the 3 schemes can be calculated using equations (20), (21), and (22) and the basic cryptographic operation costs provided in Table 4:

\[
\begin{align*}
T_{TLS} &= t_{CEV,CPE} + t_{CEV,BS} + t_{CEV,AS} + t_{RPE,CPE} + 2*t_{RPE,BS} + t_{RPE,AS} + t_{RPD,CPE} + t_{RPD,BS} + 2*t_{RPD,AS} + t_{SED,CPE} + t_{SED,BS} + t_{PAR,CPE} + t_{PAR,BS} = 55.427(\text{ms}) \\
T_{EEP} &= t_{CEV,CPE} + 2*t_{RPE,CPE} + 2*t_{RPD,BS} + 2*t_{RPD,AS} + t_{SED,CPE} + t_{SED,BS} = 11.38(\text{ms}) \\
T_{EPW} &= 4*t_{SED,CPE} + 7*t_{SED,BS} + 3*t_{SED,AS} = 12.687(\text{ms})
\end{align*}
\]

From the simulation results in Fig. 10, we can see that the average pre-authentication delays of the 3 schemes increase when the ratio of unknown attacks rises from 0 to 0.7. This increase occurs because the CPEs consume a

![FIGURE 9. Total Pre-authentication Delay under Different Number of Handovers.](image)

\[
T_{EPW} = 4*t_{SED,CPE} + 7*t_{SED,BS} + 3*t_{SED,AS} = 12.687(\text{ms})
\]
random period of pre-authentication time for an unsuccessful pre-authentication process, which makes the average successful pre-authentication delay larger. Although the average pre-authentication delays of the 3 schemes increase rapidly, it is clear that the average pre-authentication delay of the EPW scheme is only 1/50 of that of the TLS-EAP scheme and approximately 1/10 of that of the EEP scheme.

VI. CONCLUSION

We have proposed an EAP-based pre-authentication scheme for inter-WRAN handover in TVWS. The EPW scheme obtains not only mutual authentication but also secret key agreement. The EPW scheme has been proven to be logically correct by BAN logic and formally verified to have resistance to common malicious attacks by AVISPA. A corresponding performance evaluation has been performed to show that the EPW scheme can significantly reduce the authentication delay by the use of fewer cryptographic operations when compared with the EAP-TLS scheme and the EEP scheme.

REFERENCES


CONG WANG was born in Hunan, China, in 1988. She received the B.E. degree majoring in wireless network from the School of Computer Science and Technology, Tianjin University, in 2012, where she is currently pursuing the Ph.D. degree with the Computer Science and Technology, on Design and Enhancement of Security Functionality in TVWS Network. Her research interest includes TVWS security and authentication protocol design.
MAODE MA (SM’09) received the B.E. degree from Tsinghua University, Beijing, China, in 1982, the M.E. degree from Tianjin University, Tianjin, China, in 1991, and the Ph.D. degree from The Hong Kong University of Science and Technology, Hong Kong, in 1999.
He is currently an Associate Professor with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore. He has authored or co-authored about 200 international academic publications, including over 80 journal papers, over 140 conference papers and/or book chapters, and three academic books. His research interests are wireless networking and wireless network security.
Dr. Ma is a member of a few technical committees in the IEEE Communication Society. He has been a member of the technical program committees for over 100 international conferences. He has been a General Chair, Technical Symposium Chair, Tutorial Chair, Publication Chair, Publicity Chair, and Session Chair for over 50 international conferences. He serves as an Editor-in-Chief/Associate Editor for six international journals.

LEI ZHANG received the Ph.D. degree in computer science from Auburn University, Auburn, AL, USA, in 2008. She was an Assistant Professor with the Computer Science Department, Frostburg State University, Frostburg, MD, USA, from 2008 to 2011. She is currently an Associate Professor with the School of Computer Science and Technology, Tianjin University, Tianjin, China. Her current research interests include computer networks, wireless communications, distributed algorithms, and network security.