IEICE TRANS. INF. & SYST., VOL.E93–D, NO.3 MARCH 2010

PAPER Special Section on Trust, Security and Privacy for Pervasive Applications

An Efficient Authentication Protocol for WLAN Mesh Networks in Trusted Environment

Zhuo MA[†a)], **Jianfeng MA**[††], ***Nonmembers***, **SangJae MOON**[†††b)], ***Member***, ***and*** **Xinghua LI**[†], ***Nonmember***

SUMMARY Trusted Network Connect provides the functionality of the platform authentication and integrity verification which is crucial for enhancing the security of authentication protocols. However, applying this functionality directly to concrete authentications is susceptible to unknown attacks and efficiency degradation. In this paper, we propose TWMAP, a novel authentication protocol for WLAN Mesh networks in a trusted environment which completed the platform authentication and integrity verification during the user authentication. And, the Schnorr asymmetric signature scheme is utilized to reduce the overhead of the client. The security properties of the new protocol are examined using the Universally Composable Security model. The analytic comparisons and simulation results show that the new protocol is very efficient in both computing and communication costs.

key words: *WLAN mesh, trusted network connect, universally composable security*

1. Introduction

The traditional Wireless Local Area Networks (WLANs) have encountered several problems, such as limited transmission power, narrow coverage ranges, and relatively low bandwidth, etc. Consequently, a new networking technology, WLAN Mesh [1], emerges as the times require. In this context, we have witnessed an evolution of WLAN architecture. Unfortunately, such evolution brings efficiency and security problems during the security access [2]. Therefore, the Efficient Mesh Security and Link Establishment (EMSA) [3] was proposed by the task group IEEE 802.11s.

However, there are not any efficient solutions to the source security of wireless terminals in WLAN Mesh networks. To ensure the authentication security, the connections must be established from the integrity of the terminals, which comes into being the original idea of the Trusted Network Connect (TNC) [4].

In the TNC architecture, a TPM chip, which plays a key role in the trusted access, is installed. And the additional platform authentication and platform integrity verification are performed [4], making current authentication protocols inapplicable to this environment. Meanwhile, available TNC protocols [5]–[7] are designed under traditional WLANs. The mobility of the Mesh Access Points (MAPs) and their mutual authentications should be considered in WLAN Mesh networks. Therefore, current TNC protocols can not be used in WLAN Mesh networks without any modifications. This paper is proposed for such goals.

CONTRIBUTIONS: We present an authentication protocol TWMAP for WLAN Mesh networks that is suitable for the trusted environment. As far as we know, this is the first protocol in this field. The protocol is provably secure with respect to the active and concurrent attacks. It is achieved by utilizing the Universally Composable security (UC-security) model [8].

A novelty of our protocol (and perhaps an explanation why the protocol can be used in the trusted environment) is that we integrate the platform authentication and platform integrity verification with the user authentication. In addition, we take advantage of the DH key exchang to realize the explicit key agreement. Furthermore, an asymmetric scheme of distributing computations [9] is utilized in the proposed protocol.

The main achievement of the new protocol is its efficiency: For utilizing the DH key exchange instead of mutual 4 way handshake, the protocol rounds are reduced. Meanwhile, the integrity of the platform authentication, the platform integrity verification, and the user authentication enhances the efficiency of the protocol. Once an user with untrusted platform tries to access the network, the server will terminate the authentication in the fourth protocol round. Finally, Schnorr signature scheme is used by the client side. This improves on the computing complexity of the client side. In contrast to both the protocols of [10] and [3], our protocol is low in communication and computing costs.

The remainder of this paper is structured as follows. In Sect. 2 we introduce TNC architecture and the UC-security model. Then the new protocol is described in Sect. 3. The security proof of the protocol is presented in Sect. 4. The performance of such protocol is comparison analyzed and simulated with OPNET in Sect. 5. Finally, the conclusions are summarized and the future works are given in Sect. 6.

2. Related Works

802.11s started as a Study Group of IEEE 802.11 in September 2003, and it became a Task Group in July 2004. The main work of it is to standardize the corresponding tech-

Manuscript received June 25, 2009.
Manuscript revised October 4, 2009.

[†]The authors are with the School of Computer Science, Xidian University, Xi'an 710071, China.
[††]The author is with Key Laboratory of Computer Networks and Information Security (Ministry of Education), Xidian University, Xi'an 710071, China.
[†††]The author is with Mobile Network Security Technology Research Center Kyungpook National University Sankyuk-dong Bukku, Daeyu 702–701, Korea.
a) E-mail: mazhuo@mail.xidian.edu.cn
b) E-mail: sjmoon@ee.knu.ac.kr

DOI: 10.1587/transinf.E93.D.430

nologies of the WLAN Mesh. The draft evolved through informal comment resolution until it was submitted for a Letter Ballot in November 2006 as Draft D1.00 [10]. As of April 2008 the draft is at D2.00. In order to maintain the compatibility with the series standard of IEEE 802.11, the authentication scheme of IEEE 802.11i standards [11] is still used in Draft 802.11s. The task group 802.11s also proposed EMSA (Efficient Mesh Security and Link Establishment), on the basis of 802.11i, to achieve the authentication.

Trusted Network Connect Group (TNC-SG), a Sub Group of Trusted Computing Group (TCG), has developed TNC architecture in 2006. Recently, a substantial body of work on authentication protocols in trusted environment has appeared in the literature of security. An integrity reporting protocol was proposed by Stumpf, Tafreschi, Patrick Röder, and Eckert [12] for preventing masquerading attacks in remote attestation. A novel system that establish trust upon the client policy enforcement before allowing clients (remote) access to corporate Internet services was designed by Sailer, Jaeger, Zhang, and Doorn [6]. However, these protocols and systems cannot satisfy the requirements of WLAN Mesh networks.

3. Preliminaries

Trusted Network Connect (TNC) [4]: The Trusted Network Connect Sub Group (TNC-SG) is working to define and promote an open solution architecture TNC that enables network operators to enforce policies regarding the security state of endpoints in order to determine whether to grant access to a requested network infrastructure. The Entities within the architecture are the Access Requestor (AR), the Policy Enforcement Point (PEP) and the Policy Decision Point (PDP). Three abstract layers of the architecture are identified, grouping entities possessing similar functions or roles: the network access layer, the integrity evaluation layer, and the integrity measurement layer.

Universally Composable Secure Model [8]: Universally composable security is a framework for defining the security of cryptographic protocols. In this framework, an uncorruptable ideal functionality F which can provide a certain service, a set of dummy parties $\tilde{P}$ and an ideal adversary S are defined. On the other hand, an actual protocol π that can achieve the special service, a set of real parties P, and a real-world adversary A are correspondingly defined. Three major theorems, including the universally composable security, composition theorem, and hybrid model, are proven.

4. An Efficient Authentication Protocol for WLAN Mesh Networks in the Trusted Environment

Communication environment: WLAN Mesh networks in the trusted environment differs a lot from that in the traditional environment. In the trusted environment, the nodes seeking access to the WLAN Mesh networks are called ARs. An AR is a mesh point (MP) or an IEEE 802.11 station with the trusted platform modular (TPM) installed. MPs with additional access point functionality are called PEP. Once an AR with such functionality successfully access the WLAN Mesh network, it should become a PEP. The authentication server plays the role of PDP in this environment. It can perform the decision-making regarding the access request of AR. All the messages exchanged between AR and PDP must be forwarded by PEP.

Hypothesis: To simplify the description of the protocol, the following assumptions are given: 1) The authentication information of the users were stored in PDP. Meanwhile, the certificate of PDP was pre-allocated to each user. This is a reasonable assumption, which shorten the exchanged messages between AR and PDP. 2) According to the general assumptions of the wireless network security, PEP communicates with PDP under the protection of a secure channel. 3) PDP, the services provider, controls the whole networks. 4) PDP is a credible entity which responds to the access request honestly. 5) AR has accessed to the Privacy-CA for an AIK certificate.

The idea of protocol design: The security and performance are what we need to be considered in the protocol design. Firstly, different DH key exchange between AR and PEP as well as AR and PDP should be performed, respectively. The purpose of it is to ensure that privacy requirements are taken into account during the process of communication between AR and PEP. In addition, mutual authentication between AR and PEP as well as AR and PDP should be achieved. Secondly, the platform authentication and platform integrity verification between AR and PDP should be realized together with the user authentication in the fourth protocol round, which will enhance the efficiency of the protocol. When an AR with an untrusted platform tries to access the network, PDP will refuse it in the fourth round without executing the whole protocol. Thirdly, the computing costs of the client side are greatly increased with the addition of platform verification. However, the wireless clients are low in computing capability. Therefore, how to reduce the computing cost in the client side should be considered. To achieve this objective, an especial signature scheme, called Schnorr Signature Scheme [9], using asymmetric distribution of computations is utilized.

The protocol is shown in Fig. 1. The notations that are frequently used in the protocol description are summarized

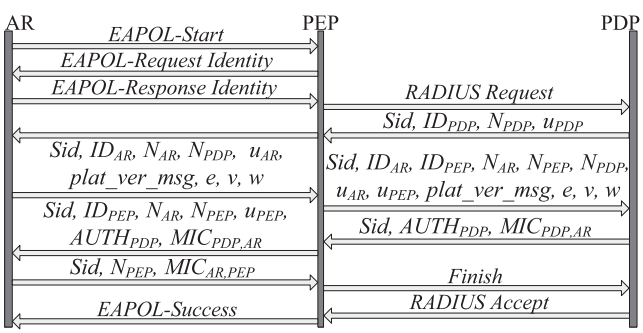

Fig. 1 Authentication protocol for WLAN mesh networks in trusted environment.

Table 1 Notations of TWMAP.

Sid	session identification
ID_i	identity of participant i
AIK	attestation identity key
SML	stored measurement log
$prf()$	pseudo-random function
$h()$	hash function
$HMAC(k, M)$	message authentication code of M generated with authentication key k
$AUTH$	authentication information

in Table 1.

The detailed description of protocol is as follows.

Step 1. When an access request is received, PDP
Generates: $z \in Z_q^*$, $N_{PDP} \in Z_q^*$.
calculates: $u_{PDP} = g^z$.
records: z.
PDP→AR: $(Sid, ID_{PDP}, N_{PDP}, u_{PDP})$.

Step 2. After receiving the message sent by PDP, AR
Generates: $x = TPM\_RNG()$,
$N_{AR} = TPM\_RNG()$,
$(k, v = g^{-k})$(according [13]).
Loads AIK from TPM by using SRK.
Computes:
$Quote = sig\{N_{AR}|N_{PDP}|PCRs|ID_{AR}|u_{AR}\}_{AIK_{priv_{AR}}}$,
$plat\_ver\_msg = SML|Quote|Cert(AIK_{pub})$
$u_{AR} = g^x$,
$MK = prf(u_{PDP}^x, Sid|ID_{AR}|ID_{PDP}|N_{AR}|N_{PDP})$,
$e = h(MK, Sid|ID_{AR}|ID_{PDP}|N_{AR}|N_{PDP}|u_{AR}|plat\_ver\_msg)$,
$w = x + ke$.
records: x.
AR→PEP: $(Sid, ID_{AR}, N_{AR}, N_{PDP}, u_{AR}, plat\_ver\_msg, e, v, w)$

Step 3. After receiving the message sent by AR, PEP
Verifies: Sid.
Generates: $y \in Z_q^*$, $N_{PEP} \in Z_q^*$.
Computes: $u_{PEP} = g^y$.
Records: y.
PEP→PDP: $(Sid, ID_{AR}, ID_{PEP}, N_{AR}, N_{PEP}, N_{PDP}, u_{AR}, u_{PEP}, plat\_ver\_msg, e, v, w)$
And then, PEP Computes:
$PMK = prf(u_{AR}^y, Sid|ID_{AR}|ID_{PEP}|N_{AR}|N_{PEP})$.
securely erases: y.
calculates: $PTK = prf(PMK)^*$.

Step 4. After receiving the message sent by PEP, PDP
Verifies: Sid and N_{PDP}.
Computes: $\overline{u_{AR}} = g^w v^e$,
$\overline{MK} = prf(\overline{u_{AR}}^z, Sid|ID_{AR}|ID_{PDP}|N_{AR}|N_{PDP})$.
Securely Erases: z.
Checks: $\overline{MK} = MK$, and
$e = h(\overline{MK}, Sid|ID_{AR}|ID_{PDP}|N_{AR}|N_{PDP}|u_{AR}|plat\_ver\_msg)$.
If both the results are TRUE, PDP authenticates the identity of AR.
And then, checks: $plat\_ver\_msg$ (platform authentication and platform integrity verification).
Computes: $AUTH_{PDP} = SIG\{msg1\}_{Priv_{PDP}}$,
$MIC_{PDP,AR} = HMAC(MK, Sid|ID_{AR}|ID_{PEP}|ID_{PDP}|N_{AR}|N_{PEP}|u_{PEP}|u_{PDP}|AUTH_{PDP})$.
PDP→PEP: $(Sid, AUTH_{PDP}, MIC_{PDP,AR})$

Step 5. Upon receipt of the message sent by PDP,
PEP→AR: $(Sid, ID_{PEP}, N_{AR}, N_{PEP}, u_{PEP}, AUTH_{PDP}, MIC_{PDP,AR})$

Step 6. Upon receipt of the message sent by PEP, AR
Verifies: Sid, N_{AR}, and $AUTH_{PDP}$.
Computes: PMK and PTK (as what PEP does).
Securely Erases: x.
Checks: $MIC_{PDP,AR}$.
And then, computes
$MIC_{AR,PEP} = HMAC(PTK, Sid|ID_{AR}|ID_{PEP}|N_{AR}|N_{PEP}|u_{AR}|u_{PEP})$.
AR→PEP: $(Sid, N_{PEP}, MIC_{AR,PEP})$

Step 7. Upon receipt of the message from AR, PEP
Verifies: Sid, N_{PEP}, and $MIC_{AR,PEP}$.
If all the results are $TRUE$, PEP notifies PDP that the session key is negotiated.
PEP→PDP: $Finish$.

5. Security Analysis

The security of the proposed protocol is analyzed with the UC-security model. If the message $plat\_ver\_msg$ is not tampered before it has transmitted to PDP, PDP could assure that the correctness of the platform authentication and the platform integrity verification. In our protocol, such properties are guaranteed by the messages e, v and w. In following descriptions, ID_R, ID_{I_1}, and ID_{I_2} denote the identity of AR, PEP, and PDP, respectively. $M1 = Sid|ID_R|\ ID_{I_2}|N_R|N_{I_2}|g^x$, $M2 = Sid|ID_R|ID_{I_1}|ID_{I_2}|N_R|N_{I_1}|g^y|g^z|$, $M3 = Sid|ID_R|ID_{I_1}|N_R|N_{I_1}|g^x|g^y$.

To simplify the security analysis of the protocol, TWMAP is abstracted as π described in Table 2, with only necessary messages. PEP and PDP are considered as a whole because of the secure channels between them. Therefore, let the protocol π interact between two entities I and R.

The idea of protocol proof: The protocol π is divided into two sub-protocols π_1 and π_2, where π_1 for AR and PDP, and π_2 for AR and PEP. The description of these two sub-protocols are shown in Table 3. We firstly prove π_1 and π_2 are UC-security protocols, respectively. And then, we claim that the composition of π_1 and π_2 is UC-secure. Finally, we prove that the composed protocol is equivalent to the abstract protocol π. That is to say the protocol π is a UC-security protocol, namely the protocol TWMAP is UC-secure. The proof process has been shortened due to space limitations. The full version is available on request. Next,

Table 2 The abstract description of trusted access protocol for WLAN Mesh networks.

1. I generates a random number N_{I_2} and a pair of public key (z, g^z), records z, and sends (N_{I_2}, g^z) to R.
2. Upon receipt of the message (N_{I_2}, g^z), R generates a random number N_R, two public/private key pairs (x, g^x) and $(k, v = g^{-k})$, records x, and computes $K1 = H_{KD}((g^z)^x, Sid|ID_R|ID_{I_2}|N_R|N_{I_2})$. And then, R computes $e = h(K1, M1|plat\_ver\_msg)$, $w = x + ke$, and securely erases k. Thereafter, R sends the message $(Sid, N_R, N_{I_2}, g^x, plat\_ver\_msg, e, v, w)$ to I.
3. Upon receipt of the message that are sent by R in step 2:
   3.1 I computes $g^{x'} = g^w v^e$ and $K1' = H_{KD}((g^x)^z, Sid|ID_R|ID_{I_2}|N_R|N_{I_2})$, securely erases z, and checks $K1' = K1$ and $e = h(K1, M1|plat\_ver\_msg)$. If both the results are $TRUE$, it verifies the validity of $plat\_ver\_msg$.
   3.2 I generates a random number N_{I_1} and a public/private key pair (y, g^y), computes $K2 = H_{KD}((g^x)^y, Sid|ID_R|ID_{I_1}|N_R|N_{I_1})$ and securely erases y.
   3.3 And then, I computes $AUTH_{I_2} = SIG\{M2\}_{Priv_{I_2}}$ and $MIC_{I_2,R} = HMAC(K1, M2|AUTH_{I_2})$, and sends $(N_R, N_{I_1}, g^y, AUTH_{I_2}, MIC_{I_2,R})$ to R.
4. Upon receipt of message that are sent by I in step 3:
   4.1 R verifies the validity of the $AUTH_{I_2}, MIC_{I_2,R}$. And then, it computes $K2 = H_{KD}((g^y)^x, Sid|ID_R|ID_{I_1}|N_R|N_{I_1})$, and securely erases x.
   4.2 Thereafter, R computes $MIC_{R,I_1} = HMAC(PTK, M3)$, and sends (N_{I_1}, MIC_{R,I_1}) to I.

Table 3 Sub-protocols π_1 and π_2.

Sub-protocol π_1	
$I \rightarrow R$	N_{I_2}, g^z
$R \rightarrow I$	$N_R, N_{I_2}, g^x, plat\_ver\_msg, e, v, w$
$I \rightarrow R$	$N_R, AUTH_{I_2}, MIC_{I_2,R}$
Sub-protocol π_2	
$R \rightarrow I$	N_R, g^x
$I \rightarrow R$	$N_R, N_{I_1}, g^y, MIC_{I_2,R}$
$R \rightarrow I$	N_{I_1}, MIC_{R,I_1}

Table 4 The protocol ρ_s in ideal environment.

The protocol ρ_s that based on the signature algorithm $Sig = (gen, sig, ver)$ is executive between the participant p_i and p_j.

1. Upon reception of (signer, id), P_i runs algorithm gen, records sign key s and sends Verification Key v to P_j.
2. When P_j wants to sign a message m, it sends $(sign, id, m)$ to P_i. P_i sets $\sigma = sig(s, m)$ and sends $(signature, id, m, \sigma)$ to P_j.
3. When P_j wants to verify a signature σ, it sends $(verify, id, m, \sigma)$ to P_i. P_i outputs $(verified, id, m, ver(v, m, \sigma))$ to P_j

the proof process of sub-protocol π_1 is given, and the proof of π_2 is the same.

The idea of proof of π_1*:* We start by presenting a simple protocol ρ_s that securely realizes the ideal functionality F_{sig}. Next we construct a protocol π_1' and prove that the protocol securely realizes the ideal functionality F_{KE} with the aid of F_{sig}. And then, we compose the protocol ρ_s and π_1'. At last we prove that the composed protocol is equivalent to the protocol π_1, and it realizes the ideal functionality F_{KE} in real environment according to the Composition theorem [8].

Let $Sig = (gen, sig, ver)$ be a signature algorithm that described in [8]. Then the protocol ρ_s, as shown in Table 4, securely realizes F_{sig} in real environment, iff the signature is secure against existential forgery in chosen message attack [14].

Lemma 1: If the DDH assumption [15] is hold and the MAC is secure, the protocol π_1' realizes F_{KE} with the aid of ideal functionality F_{sig}.

PROOF: Firstly, we construct π_1' that based on the key exchange ideal functionality F_{KE} as shown in Table 5.

Let π_1' be a key-exchange protocol in F_{sig}-*hybrid* model, and let H be a PPT adversary. We construct an ideal-process adversary S, such that the view of any environment Z of an interaction with H and π_1' in F_{sig}-*hybrid* model is distributed identically to its view of an interaction with S and F_{KE} in the ideal-life. That is, for any environment Z we have:

$$F_{sig} - hybrid_{\pi_1',H,Z} \approx IDEAL_{F,S,Z} \tag{1}$$

For space limitions, the construction and the validity of the simulator S, and a distinguisher D which is used to validate the S are not given.

Let π_1' be a F_{sig}-*hybrid* protocol and ρ_s be a protocol securely realizes F_{sig}. Then for any PPT adversary A there exists a PPT adversary H such that for any PPT environment Z we have:

$$REAL_{\pi_1'^{\rho_s},A,Z} \approx F_{sig} - hybrid_{\pi_1',H,Z} \tag{2}$$

That is the protocol π_1' in F_{sig}-*hybrid* model is securely realized by the composed protocol $\pi_1'^{\rho_s}$ [8].

Theorem 1: Protocol π_1 securely realizes the ideal functionality F_{KE} in real environment. That is, for any environment Z we have:

$$REAL_{\pi_1,A,Z} \approx IDEAL_{F_{KE},S,Z} \tag{3}$$

PROOF: Since the composed protocol $\pi_1'^{\rho_s}$ is identical to the protocol π_1 in real environment. And according to Eqs. (1), (2), and the Composition Theorem [8], Eq. (3) as required.

Similar to the proof of Theorem 1, we can get that the protocol π_2 securely realizes the ideal functionality F_{KE} in real environment. That is, for any environment Z we have:

$$REAL_{\pi_2,A,Z} \approx IDEAL_{F_{KE},S,Z} \tag{4}$$

Theorem 2: Since the protocol π securely realizes the

Table 5 The protocol π_1' in ideal environment.

The protocol π_1' that based on the key exchange ideal functionality F_{KE}
1. Let p and q be two primes such that $q/(p-1)$ and the length of q is k bits. Let g be a subgroup of Z_p^* of order q. The protocol π_1' that based on the ideal functionality F_{sig} is executive between the participant P_i and P_j.
2. Upon receipt of (P_i, P_j, Sid), the initiator P_i sends initial message $(signer, 0, Sid)$ to F_{sig}. Upon receipt of (P_j, P_i, Sid), the responder P_j sends message $(signer, 1, Sid)$ to F_{sig}.
3. P_i randomly chooses $N_{I_2} \leftarrow Z_p$ and computes $\gamma = g^z$, and then sends $(P_i, Sid, \text{“}Star\text{''}, N_{I_2}, \gamma)$ to P_j.
4. Upon receipt of initial message, P_j randomly chooses $N_R \leftarrow Z_p$ and computes $\alpha = g^x$ and K_1. Then P_j sends $(sign, 1, Sid, N_R, N_{I_2}, PCRs, P_j, \alpha)$ to F_{sig}. When F_{sig} returns the signature σ_j, it computes e, w and sends $(Sid, N_R, N_{I_2}, \alpha, \sigma_j, e, v, w)$ to P_i.
5. Upon receipt of $(Sid, N_R, N_{I_2}, \alpha, \sigma_j, e, v, w)$, P_i sends $(verify, 1, Sid, P_j, N_R, N_{I_2}, P_j, \alpha, \sigma_j)$ to F_{sig}. If F_{sig} successfully verifies the message, P_i computes K_1 and verifies e. If e is successfully verified, P_i computes $\beta = g^y$ and K_2, and sends $(sign, 0, Sid, M_2)$ to F_{sig}. Upon receipt of signature σ_i from F_{sig}, P_i computes $\varphi_i = MIC_{I_2}$ with K_1. Then P_i sends $(Sid, N_R, N_{I_1}, \beta, \sigma_i, \varphi_i)$ to P_j.
6. Upon receipt of $(Sid, N_R, N_{I_1}, \beta, \sigma_i, \varphi_i)$, P_j sends $(verify, 0, Sid, P_i, M_2, \sigma_i)$ to F_{sig}. If F_{sig} successfully verifies the message, P_j computes K_1 and verifies φ_i. And if φ_j is successfully verified, P_j computes K_2. And then, P_j computes $\varphi_j = MIC_{R,1}$ with K_2 and sends $(Sid, N_{I_1}, \varphi_j)$ to P_i. Finally, P_j erase x and locally outputs $(Sid, P_i, P_j, K_1, K_2)$.
7. Upon receipt of $(Sid, N_{I_1}, \varphi_j)$, P_i verifies φ_j. If the result is TRUS, P_i erase y, z and locally outputs $(Sid, P_j, P_i, K_1, K_2)$.

ideal functionality F_{KE} in real environment, for any environment Z we have:

$$REAL_{\pi,A,Z} \approx IDEAL_{F_{KE},S,Z} \quad (5)$$

That is the protocol TWMAP is a UC-secure protocol.

PROOF: The protocol π_1 and π_2 are divided from the protocol π, so the composed protocol of π_1 and π_2 is indistinguishable from the protocol π. According to Eqs. (3), (4), and the Composition Theorem [8], we can get that the composed protocol of π_1 and π_2 is a UC-secure protocol. From above analysis, Theorem 2 as required.

6. Performance Analysis

We present both analytic comparisons and simulation results to demonstrate the efficiency of TWMAP.

6.1 Analytic Comparisons

In order to compare the performance of TWMAP with that of the existing protocols, a protocol round is added to the protocol presented in [10] and [3], and an additional signature operation is performed on the client side, which are used to achieve the platform authentication and integrity verification according to the TNC specifications. We denote these two protocols as $M-EAP-4way^{T+}$ and $EMSA^{T+}$.

Table 6 compares the performance among the protocols when AR firstly trusted access to the WLAN Mesh networks. It is shown that TWMAP has the same computing cost in the client side with that of $EMSA^{T+}$, and reduces one signature operation to $M-EAP-4way^{T+}$ and $EMSA^{T+}$. For the server side, the computing costs of TWMAP and $EMSA^{T+}$ are one half of those of $M-EAP-4way^{T+}$. Compared with the other two protocols, TWMAP only need 7 protocol rounds to achieve the same work, which greatly enhances the communication efficiency.

The resource and energy costs of each operation are given, so as to make the analytic comparison more intuitively. Processor cycles spend in execution of RSA 1024 Signature, Modular exponentiation, and HMAC (SHA-1) are about 2.71, 0.82, and 0.0015 megacycles [16], respectively. And the energy cost in execution of these operations are about 875.96, 546.5, and 0.148 millijoule [17], respectively.

Table 6 Comparison of the computing and communication costs.

	Protocol rounds	Costs of AR	Costs of PEP	Costs of PDP
$M-EAP-4way^{T+}$	7+7+1	2E+2F +4M	2E+1F +4M	4E+2F +2M
$EMSA^{T+}$	5+4+1	2E+2F +3M	2M	2E+1F +1M
TWMAP	7	2E+1F +2M	2E	2E+1F +1M

E: Modular exponentiation; F: Signature; M: MAC

Table 7 Comparison of the processor cycles.

	AR (Megacycles)	PEP (Megacycles)	PDP (Megacycles)
$M-EAP-4way^{T+}$	7.066	4.356	8.703
$EMSA^{T+}$	7.0045	0.0015	4.3515
TWMAP	4.353	1.64	4.3515

Table 8 Comparison of the energy cost.

	AR (mj)	PEP (mj)	PDP (mj)
$M-EAP-4way^{T+}$	2845.512	2299.012	4597.136
$EMSA^{T+}$	2845.068	0.296	2298.568
TWMAP	2298.716	1751.92	2298.568

Table 7 and Table 8 show the the comparison of the processor cycles and energy cost among the three protocols when AR firstly trusted access to the WLAN Mesh networks. The analysis shows TWMAP has the least resource and energy costs in the client and server side, which will greatly improve the efficiency when AR moves and accesses to different PEPs (i.e., handoff).

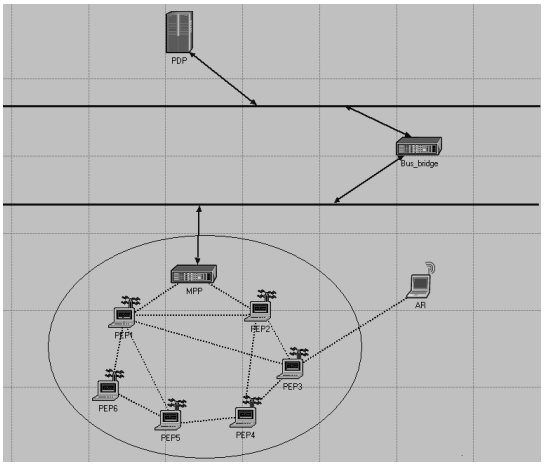

Fig. 2 Simulation environment.

Table 9 Simulation parameters.

Simulation parameter	Values
Network coverage	10 km*10 km
Physical layer	IEEE802.11b
Data rate	11 Mbps
MAC layer	DCF
HMAC (MD5)	100.7MB/sec
RSA signature (512 bits)	4.92 ms
RSA signature verification (512 bits)	0.43 ms
modular exponentiation	5 ms

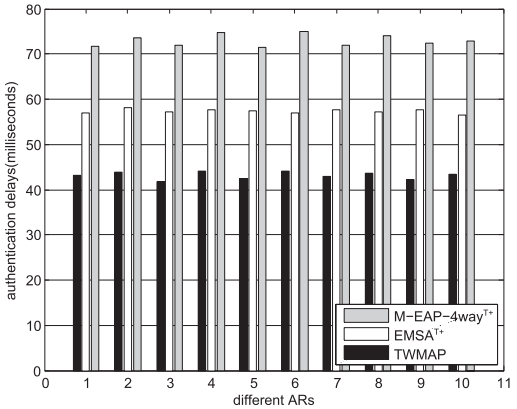

Fig. 3 The comparison of authentication delays when ARs successfully access the network.

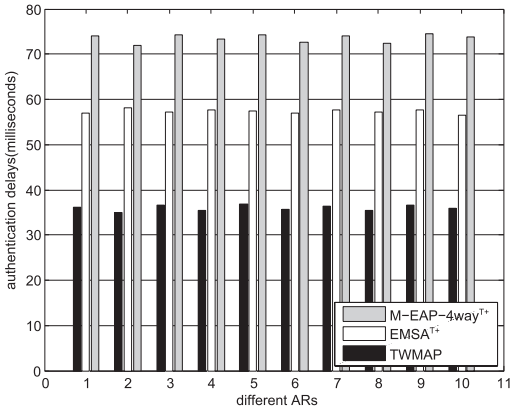

Fig. 4 The comparison of authentication delays when ARs fail to access the network.

6.2 Simulations

In this section we present simulation results on how the protocols ($M-EAP-4way^{T+}$, $EMSA^{T+}$, and $TWMAP$) perform while the integrity of the platform and the computing capability of client varies. The OPNET 10.0.A [18] is used for the simulation.

Simulation Objectives:

1) To observe the authentication delays.

2) To observe the computation delays of ARs with different computation power.

3) To observe the received and transmitted data packets of protocol

Simulation Environment: Each simulation starts with an AR connected to a WLAN Mesh network. It is assumed without loss of generality that the WLAN Mesh network is composed of 6 PEPs, an MPP, a bus_bridge, and a PDP in the trusted environment. The simulation environment is shown in Fig. 2. The simulation parameters are summarized in Table 9. The simulation runs on a PC (CPU: Intel Core 2 Duo E8300 2.83 GHz, RAM: 2 GB, OS: Windows XP SP3 5.1.2600). The physical layer of this environment are based on IEEE 802.11b, the Direct Series Spread Spectrum (DSSS) technology is ultilized, and the maximum raw data rate is 11 Mbps. The MAC layer used for this simulation is the distributed coordination function (DCF).

Simulation Results:

1) *Authentication Delays*: It is configured that 10 ARs with different computation power try to access the network in the simulation. For each AR, we run the simulation 10 times and evaluate the average value. In this scenario, two cases are considered. The first one, shown in Fig. 3, is the comparison of authentication delays among the three protocols when ARs successfully access the network. In the second case, shown in Fig. 4, the access request of ARs with un-trusted platform was rejected. For both two cases, the authentication delays was measured. Figure 3 shows that the average authentication delay of TWMAP is about 43.05 ms which is much lower than 72.939 ms of $M-EAP-4way^{T+}$ and 57.618 ms of $EMSA^{T+}$. Figure 4 shows the authentication delays of TWMAP is only about 50% that of $M-EAP-4way^{T+}$ and 60% that of $EMSA^{T+}$. The platform authentication and integrity verification are realized together with the user authentication in the fourth protocol round, which is speculated to be the reason of the reduction in authentication delays.

2) *Computation Delays of ARs*: Fig. 5 shows the com-

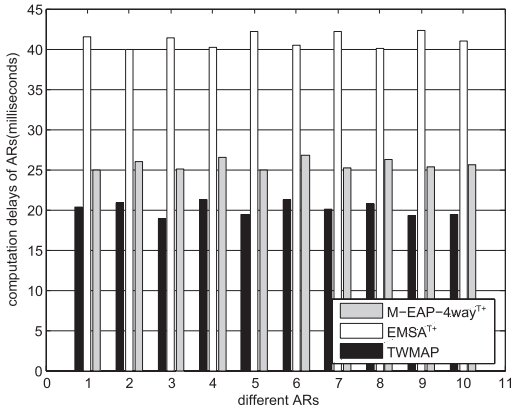

Fig. 5 The comparison of the computation delays of ARs.

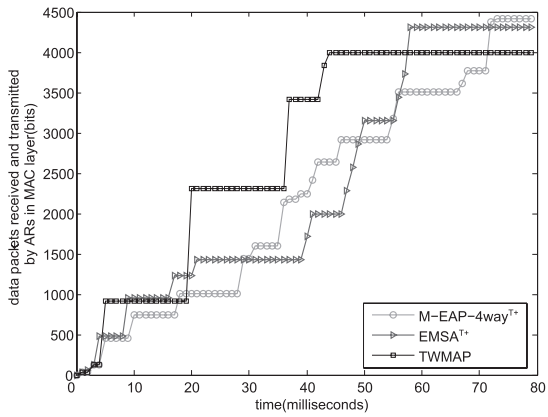

Fig. 6 The comparison of data packets received and transmitted by ARs in MAC layer.

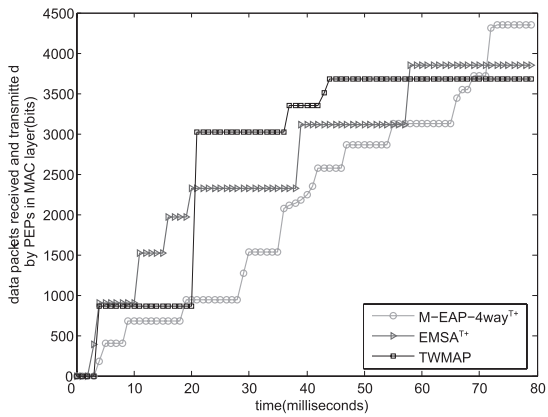

Fig. 7 The comparison of data packets received and transmitted by PEPs in MAC layer.

putation delays of ARs. As expected, TWMAP has the minimum time consumption. Clearly, this has a direct impact on the power saving in ARs.

3) *Data Packets Received and Transmitted by Protocol Participants*: Fig. 6, Fig. 7, and Fig. 8 show the total numbers of data packets transmitted and received by the participants in MAC layer for the whole duration of

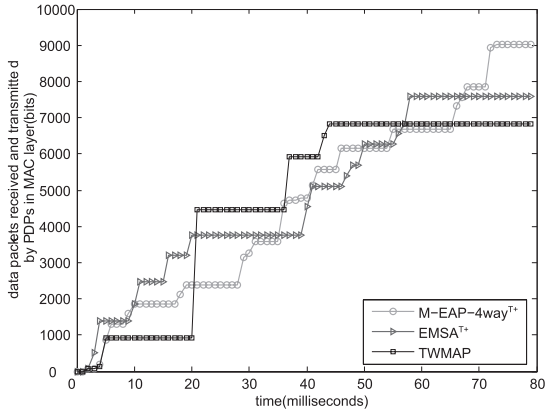

Fig. 8 The comparison of data packets received and transmitted by PDPs in MAC layer.

protocols simulation. Figure 6 shows the received and transmitted data packets of AR in TWMAP is the lowest one. Meanwhile, the figure shows the transmission delay of TWMAP is about 7 ms which is much lower than the 18 ms of $M-EAP-4way^{T+}$ and 13 ms of $EMSA^{T+}$. Figure 7 and Fig. 8 show that TWMAP also has great advantages over $M-EAP-4way^{T+}$ and $EMSA^{T+}$ in terms of the throughput and transmission delay of PEPs and PDPs, respectively.

7. Conclusion and Future Work

In this paper, an authentication protocol TWMAP is proposed for WLAN Mesh networks in the trusted environment. For utilizing the DH key exchange instead of mutual 4 way handshake, the protocol rounds are reduced. Meanwhile, the key exchange and confirmation are achieved between AR and PEP as well as AR and PDP, respectively. In addition, the integrity of the platform authentication, the platform integrity verification, and the user authentication enhances the efficiency of the protocol. Furthermore, Schnorr signature scheme is used by the client side, which reduces the computing cost of it.

The UC security model is utilized to ensure the security of our scheme in the complicated and concurrent environment. Both analytic comparison and simulation results have confirmed that the effectiveness and efficiency of TWMAP in computing and communication costs.

Considering the motion of AR in WLAN Mesh networks and the QoS services, the fast handoff protocols in the trusted environment are what we need to study. Therefore, our future work is to design a new fast handoff protocol for WLAN Mesh networks which is suitable for the trusted environment. This protocol must satisfy some security and performance requirements, such as UC-security, handoff delay must less than 50 ms, etc.

Acknowledgment

This paper was supported in part by the Major Program of National Natural Science Foundation of China

(60633020), the National Natural Science Foundation of China (60573036, 60702059, 60503012), the National High Technology Research and Development Program of China (2007AA01Z429), the Korea Research Foundation Grant funded by the Korean Government (KRF-2008-521-D00449), and the opening foundation of key lab of cryptologic Technology and Information Security (MoE, Shandong University).

References

[1] P. Whitehead, "Mesh networks: A new architecture for broadband wireless access systems," Proc. IEEE RAWCON2000, pp.43–46, 2000.
[2] I.F. Akyildiz, X.D. Wang, and W.L. Wang, "Wireless mesh networks: A survey," IEEE Commun. Mag., vol.43, no.9, pp.23–30, 2006.
[3] T. Braskich, W.S. Conner, J. Kruys, S. Emeott, J. Walker, M. Zhao, and R. Falk, "Efficient mesh security and link establishment," doc.: IEEE 802.11-06/1470r3, Nov. 2006, https://mentor.ieee.org/802.11/public/06/11-06-1470-03-000s-efficient-mesh-security-and-link-establishment.doc
[4] Trusted Computing Group, "TCG Trusted Network Connect TNC Architecture for Interoperability," May 2007, https: //www.trustedcomputinggroup.org/
[5] R. Sailer, T. Jaeger, X. Zhang, and L. van Doorn, "Attestation-based policy enforcement for remote access," CCS '04: Proc. 11th ACM Conference on Computer and Communications Security, pp.308–317, New York, NY, USA, 2004.
[6] R. Sailer, X. Zhang, T. Jaeger, and L. van Doorn, "Design and implementation of a tcg-based integrity measurement architecture," SSYM '04: Proc. 13th Conference on USENIX Security Symposium, p.16, Berkeley, CA, USA, 2004.
[7] K. Goldman, R. Perez, and R. Sailer, "Linking remote attestation to secure tunnel endpoints," STC '06: Proc. 1st ACM Workshop on Scalable Trusted Computing, pp.21–24, New York, NY, USA, 2006.
[8] R. Canetti, "Universally composable security: A new paradigm for cryptographic protocols," FOCS '01: Proc. 42nd IEEE Symposium on Foundations of Computer Science, pp.136–145, Washington, D.C., USA, 2001.
[9] C.P. Schnorr, "Efficient identification and signatures for smart cards," CRYPTO '89: Proc. Advances in Cryptology, pp.239–252, Santa Barbara, California, United States, 1989.
[10] IEEE 802.11 Task Group S, "IEEE Draft Amendment to Standard for Information Technology - Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Amendment: ESS Mesh Networking, IEEE P802.11s/D1.0," March 2007. http://grouper.ieee.org/
[11] IEEE 802.11 Task Group i, "IEEE Standard, Supplement to Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Specification for Enhanced Security, IEEE 802.11i," July 2004. http://grouper.ieee.org/
[12] F. Stumpf, O. Tafreschi, and P. Röder, and C. Eckert, "A robust integrity reporting protocol for remote attestation," WATC '06: Proc. Workshop on Advances in Trusted Computing, Tokyo, Japan, 2006.
[13] Trusted Computing Group, Trusted Platform Module Main Specification, May 2007. https: //www.trustedcomputinggroup.org/
[14] S. Goldwasser, S. Micali, and R. Rivest, "A digital signature scheme secure against adaptive chosen-message attacks," SIAM J. Comput., pp.281–308, Philadelphia, PA, USA, 1988.
[15] M. Abdalla, M. Bellare, and P. Rogaway, "The oracle Diffie-Hellman assumptions and an analysis of DHIES," CT-RSA 2001: Proc. 2001 Conference on Topics in Cryptology, pp.143–158, London, UK, 2001.
[16] W. Dai, Crypto++ 5.6.0 Benchmarks, http://www.cryptopp.com/benchmarks.html
[17] N.R. Potlapally, S. Ravi, A. Raghunathan, and N.K. Jha, "A study of the energy consumption characteristics of cryptographic algorithms and security protocols," IEEE Trans. Mobile Computing, vol.5, no.2, pp.128–143, Feb. 2006.
[18] OPNET, https://www.opnet.com

Zhuo Ma is a PH.D. candidate in the School of Computer Science, Xidian University, China. He received his B.S. degree in computer science technology and M.S. degree in computer architecture from Xidian University in 2003 and 2006, respectively. His current research interests include wireless networks, trusted computing, and information and network security. He has published 3 refereed articles in these areas and coauthored one books.

Jianfeng Ma received his B.S. degree in mathematics from Shaanxi Normal University, China in 1985, and obtained his M.E. and Ph.D. degrees in computer software and communications engineering from Xidian University, China in 1988 and 1995, respectively. From 1999 to 2001, he was with Nanyang Technological University of Singapore as a research fellow. He is an IEEE member and a senior member of Chinese Institute of Electronics (CIE). Now he is a Professor and Ph.D. supervisor in the School of Computer Science at Xidian University, Xi'an, China, and the director of the Key Laboratory of Computer Networks and Information Security of Ministry of Education (China). His current research interests include distributed systems, wireless and mobile computing systems, computer networks, and information and network security. He has published over 150 refereed articles in these areas and coauthored ten books.

SangJae Moon is a Professor in the School of Electrical Engineering and Computer Science, Kyungpook National University, Korea. Professor Moon received his B.S. and M.S. degrees from Seoul National University in 1972 and 1974, respectively, all in Electronic Engineering, and Ph.D. degree from UCLA (USA). He is now the President of Korea Institute of Information Security & Cryptology. His research areas are wireless networks, network security, and mobile computing. He has published more than 200 papers in major journals, referred conference proceedings, book chapters related to these research areas.

Xinghua Li is an associate professor in the School of Computer Science, Xidian University, China. He received his M.S. degree and PH.D. degree in computer application from Xidian University in 2004 and 2007, respectively. His current research interests include network and information security, trusted computing.