Hindawi
Mobile Information Systems
Volume 2017, Article ID 4078521, 11 pages
https://doi.org/10.1155/2017/4078521

Research Article

An Anonymous Access Authentication Scheme Based on Proxy Ring Signature for CPS-WMNs

Tianhan Gao,[1] Quanqi Wang,[1] Xiaojie Wang,[2] and Xiaoxue Gong[3]

[1]*Software College, Northeastern University, Shenyang 110819, China*
[2]*School of Software, Dalian University of Technology, Dalian 116024, China*
[3]*School of Computer Science and Engineering, Northeastern University, Shenyang 110819, China*

Correspondence should be addressed to Xiaojie Wang; wangxj1988@mail.dlut.edu.cn
and Xiaoxue Gong; gongxiaoxue@stumail.neu.edu.cn

Received 27 January 2017; Accepted 12 April 2017; Published 4 June 2017

Academic Editor: Jun Cheng

Copyright © 2017 Tianhan Gao et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Access security and privacy have become a bottleneck for the popularization of future Cyber-Physical System (CPS) networks. Furthermore, users' need for privacy-preserved access during movement procedure is more urgent. To address the anonymous access authentication issue for CPS Wireless Mesh Network (CPS-WMN), a novel anonymous access authentication scheme based on proxy ring signature is proposed. A hierarchical authentication architecture is presented first. The scheme is then achieved from the aspect of intergroup and intragroup anonymous mutual authentication through proxy ring signature mechanism and certificateless signature mechanism, respectively. We present a formal security proof of the proposed protocol with SVO logic. The simulation and performance analysis demonstrate that the proposed scheme owns higher efficiency and adaptability than the typical one.

1. Introduction

With the prosperous development of mobile communication and versatile mobile devices [1, 2] and the diversification of the network environment [3–5], the requirement of accessing ubiquitous network becomes more and more imperative for Cyber-Physical Systems (CPS) [6]. Owing to the advantages of low cost, expansible, self-healing, fine mobility support, and high efficiency, Wireless Mesh Network (WMN) is regarded as a critical accessing technology of the next generation CPS network [7, 8]. As for the open nature of transmission medium free users' movement, as well as the multihop transmission method, WMN suffers from security issues in both wired and wireless environment. Efficient and secure access authentication technology forms the baseline of CPS-WMN's security. Moreover, user's privacy should also be preserved during the access authentication process. Thus, the security and privacy in CPS-WMNs become the research focus recently [9].

In the past few years, a lot of researches have been carried out for WMN's access authentication. The authors in [10] present an efficient identity-based authentication scheme for WMN using tickets, which avoids multihop wireless communications in order to minimize the authentication delay, while in a complex network environment, with the increasing number of MRs, handover authentication efficiency decreases. The authors of [11] propose an authentication scheme for WMN based on EAP-TLS, although the scheme offers mutual authentication and robustness against malicious attacks. But the asymmetric cryptography mechanisms result in high computation cost. The author [12] improves the access control function of IEEE 802.1X by the port operation so that user may acquire message through the dynamic channel under current or previous access point. However, the requirement of keeping the channel alive during the authentication procedure limits the adaptability of the scheme. Some distributed authentication schemes to reduce the authentication delay have been discussed in [13], while the scheme performs poorly when handling multiple mobile users. A symmetric key generation scheme based on hierarchical multivariable function for WMN is presented in [14], which achieves efficient mutual authentication and key generation for entities, whereas the scheme is not suitable for the scenario when the network users grow rapidly. The identity information of

mobile users is divided into critical information and noncritical information that the critical information is only visible to the mobile user and his/her group manager in [15]. With the help of improved short ring signature mechanism and special binding policy, the scheme is able to provide anonymity during authentication. However, the key escrow problem is inevitable since the private key is generated by the group manager. In general, the literature WMN access authentication schemes suffer from security, privacy, efficiency, and adaptability issues. The needs of an efficient and anonymous authentication scheme for CPS-WMNs are impending.

In terms of the security issues shown above, an anonymous authentication scheme based on proxy ring signature is proposed in this paper. The scheme utilizes a high-efficient proxy ring signature mechanism to achieve proxy-authorization and anonymous authentication which are able to preserve mobile users' privacy. In addition, certificateless signature mechanism is incorporated into our intragroup authentication to obtain high handover efficiency. The formal security proof based on SVO logic and other security analyses show that the proposed scheme possesses such advantages as reliability, anonymity, unforgeability, and reliability. Through the simulation and performance analysis, we demonstrate the efficiency and adaptability of our scheme.

The rest of this paper is organized as follows. Section 2 briefly describes the related preliminaries. Section 3 elaborates the proposed anonymous mutual authentication scheme. Sections 4 and 5 present the security and performance analysis of the scheme, respectively. Finally, we make a conclusion of the scheme and discuss the future research work in Section 6.

2. Preliminaries

2.1. Bilinear Pairing. Let G be an additive group and let G_T be a multiplicative group of the same prime order q and I_{GT} is the generator of G_T. Assume that the discrete logarithm problem is hard on both G and G_T [16]. A mapping e: $G \times G \to G_T$ which satisfies the following properties is called bilinear pairing:

(1) Bilinearity: for all $P, Q \in G$ and , $b \in Z_q^*$, $e(aP, bQ) = e(bP, aQ) = e(P, Q)^{ab}$.

(2) Nondegeneracy: there exists $P, Q \in G$, so that $e(P, Q) \neq I_{GT}$.

(3) Computability: for all $P, Q \in G$, there is an efficient algorithm to compute $e(P, Q) \in G_T$.

2.2. BB1 Encryption. BB1 [17], nonadaptive selective-ID encryption, was presented by Boneh and Franklin in 2003. The BB1 works as follows.

(1) BB1-Setup. Given a security parameter $k \in Z_q^*$, the algorithm works as the following steps.

Step 1. Run G on input k to generate a prime q, two cycle groups $(G_1, +)$, $(G_2, \times)$ of order q, and an admissible bilinear pairing $e : G_1 \times G_1 \to G_2$. Choose a random generator $\in G_1$.

Step 2. Pick a random $s \in Z_q^*$ and set $P_{\text{pub}} = sP$.

Step 3. Choose a cryptographic hash function $H_1 : \{0,1\}^* \to G_1$. Choose a cryptographic hash function $H_2 : G_2 \to \{0,1\}^n$ for some n. The message space is $M = \{0,1\}^n$. The ciphertext space is $C = G_1 \times \{0,1\}^n$. The system parameters are $\{H_1, H_2, G_1, G_2, q, e, P, P_{\text{pub}}\}$. The master key is $s \in Z_q^*$.

(2) BB1-Extract. For a given string ID $\in \{0,1\}^*$, compute $Q_{\text{ID}} = H_1(\text{ID}) \in G_1$ and set the private key d_{ID} to be $d_{\text{ID}} = sQ_{\text{ID}}$.

(3) BB1-Encrypt. To encrypt $m \in M$ under the public key ID, compute $Q_{\text{ID}} = H_1(\text{ID}) \in G_1$, choose a random $r \in Z_q^*$, and set the ciphertext to be $C = \langle rP, m \oplus H_2(g_{\text{ID}}^r)\rangle$, where $g_{\text{ID}} = e(Q_{\text{ID}}, P_{\text{pub}})$.

(4) BB1-Decrypt. Let $c = \langle U, V\rangle \in C$ be a ciphertext encrypted using the public key ID. To decrypt c using the private key $d_{\text{ID}} \in G_1$, compute $m = V \oplus H_2(e(d_{\text{ID}}, U))$.

2.3. Certificateless Signature. Certificateless signature (CLS) [18] allows that users' private key is comprised by the key issued by system and the secret generated by user. In addition, users' public key is conducted by their own secret which avoids key escrow problem. The CLS scheme is mainly used in the Intra-WMN authentication in this paper. The algorithms of CLS [18] are shown as follows.

(1) CLS-Setup. Given security parameter l, prime $q \geq 2^l$, $(G_1, +)$, and $(G_2, \times)$ are cycle groups of order q. Three hash functions are as follows: $H_1 : \{0,1\}^* \to G_1$, $H_2 : \{0,1\}^* \times G_1 \to G_1$, and $H_3 : \{0,1\}^* \times G_1 \times G_2 \to Z_q^*$. Private key generator (PKG) chooses $s \in Z_q^*$ as private key and generates system public key $P_0 = sP$, where P is the generator of G_1. Let $g = e(P, P)$; system public parameters Param = $(G_1, G_2, e, q, P, P_0, g, H_1, H_2, H_3)$.

(2) CLS-Extract-sk. User A sends identity $\text{ID}_\text{A} \in \{0,1\}^*$ to PKG. After authenticating ID_A, PKG generates partial private key of A : $D_\text{A} = sH_1(\text{ID}_\text{A})$.

(3) CLS-Gen-sk. A chooses $x_\text{A} \in Z_q^*$ as secret. A's private key is (x_A, D_A).

(4) CLS-Gen-pk. A computes $P_\text{A} = x_\text{A}P$ as A's public key.

(5) CLS-Sign. A signs message $m \in \{0,1\}^*$, and outputs $\sigma = \{U, \delta\}$ through following steps:

(a) Choose $r \in Z_q^*$ and calculate $U = g^r$.

(b) $V = H_2(\text{ID}_\text{A} \parallel P_\text{A})$.

(c) $h = H_3(m \parallel U \parallel \text{ID}_\text{A} \parallel P_\text{A})$.

(d) $\delta = rP - h(D_\text{A} + x_\text{A}V)$.

(6) CLS-Verify. Verifier B uses $P_0, P_\text{A}, \text{ID}_\text{A}$ to verify the signature $\sigma = \{U, \delta\}$.

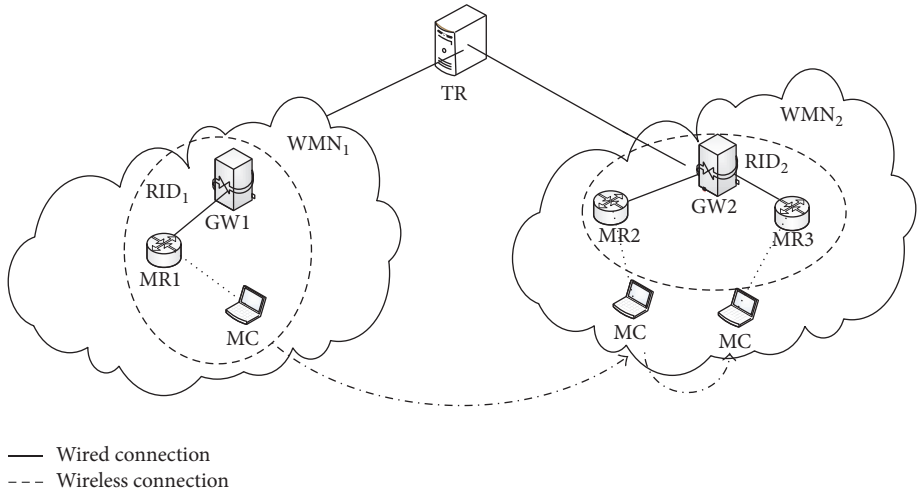


Figure 1: Hierarchical mobile network architecture for CPS-WMNs.

(a) Compute $V = H_2(\mathrm{ID_A} \parallel P_A)$ and $h = H_3(m \parallel U \parallel \mathrm{ID_A} \parallel P_A)$.

(b) Check if the equation $U = e(\delta, P)(e(H_1(\mathrm{ID_A}), P_0)e(P_A V))^h$ is hold. If yes, σ is valid; otherwise, σ is invalid.

2.4. Proxy Ring Signature. Proxy ring signature (PRS) [19] allows an original signer delegate authorization to a group of signers in which every member in the group can represent the original signer to sign the message and is able to keep anonymous. In this paper, we incorporate proxy ring signature into the access authentication process of WMN, which not only achieves mutual authentication between mobile user and accessed network but also solves the problem of privacy preserving for mobile user. The algorithms of PRS are as follows.

(1) PRS-Setup. Given secure parameter K as system input and the output is (G_1, G_2, q, e, P). G_1 is a cyclic additive group generated by the generator P, whose order is prime q, and G_2 is a cyclic multiplicative group of the same prime order of q. $e : G_1 \times G_1 \to G_2$ is a bilinear pairing map. In addition, there are two hash functions: $H_0 : \{0,1\}^* \times G_1 \to Z_q^*$ and $H_1 : \{0,1\}^* \to G_1$.

(2) PRS-Generation. Original signer O chooses $x_0 \in Z_q^*$ as the private key and calculates the public key $Y_o = x_o P$. u_i belonging to proxy signer group U randomly chooses private key $x_i \in Z_q^*$ and calculates the public key $Y_i = x_i P$.

(3) PRS-Delegation. O generates a warrant m_ω which includes the descriptions of the relationship between O and proxy signer. O chooses a random number $r \in Z_q^*$, calculates $R = rp$, $s = r + x_o H_o(m_\omega, R) \bmod q$, and then sends (m_ω, R, s) to the group $U = \{u_1, \ldots, u_n\}$ of proxy signers.

(4) PRS-Verify-Auth. After receiving (m_ω, R, s), each proxy signer μ_i checks $sP \stackrel{?}{=} R + Y_o H_o(m_\omega, R) \bmod q$. If the verification fails, the authorization will be rejected. Otherwise, u_i calculates his own proxy signing key $\mathrm{psk}_i = s + x_i H_o(m_\omega, R) \bmod q$.

(5) PRS-Sign. The proxy signer u_s signs message $m \in \{0,1\}^*$ as follows:

(a) For all $i \in \{1, 2, \ldots, n\}$ and $i \neq s$, choose a random number $r_i \in Z_q^*$ and calculate $\delta_i = r_i P$.

(b) Calculate $\delta_s = (1/\mathrm{psk}_s)(H_1(m \parallel m_\omega) - \sum_{i \neq s} r_i (R + H_o(m_\omega, R)(Y_o + Y_i))$.

(c) Send $\delta = (\delta_1, \delta_2, \ldots, \delta_n, m, m_\omega, R)$ to the verifier.

(6) PRS-Verify-Sign. After receiving δ from the proxy signer, the verifier checks if the following equation holds with the public key $Y_0, Y_1, \ldots, Y_n$:

$$\prod_{i=1}^{n} e\left(R + H_0\left(m_\omega, R\right)\left(Y_o + Y_i\right), \delta_i\right) \stackrel{?}{=} e\left(P, H_1\left(m \parallel m_\omega\right)\right). \quad (1)$$

If yes, δ is valid. Otherwise, δ is invalid.

3. Anonymous Mutual Authentication Scheme

3.1. Hierarchical Mobile Network Architecture. As shown in Figure 1, a hierarchical mobile network architecture is designed for CPS-WMNs. In the first level, Trusted Root (TR), as original signer who can delegate signing right to proxy signers, is creditable to all of the network entities. In the second level, there are many WMNs that each one can be regarded as a group of proxy signers including Gateway (GW), Mesh Routers (MRs), and mobile Mesh Clients (MCs). MC is able to handover across different WMNs or between different MRs in the same WMN. To achieve mutual authentication between MC and visiting network based on PRS, we build the group of proxy rings for network entities in terms of the hierarchical mobile network architecture shown above. Assuming that a group of the proxy ring (abbreviated as a

Table 1: Symbols and descriptions.

Symbols	Descriptions
RID_i	Ring i's identification
PK_X/SK_X	The public/private key of entity X
Param	System parameters
W_{ri}	The warrant for the members in ring i
$Auth_X$	The authorization of proxy signature for X
$K_{X\text{-}Y}$	The session key between X and Y
Enc_$K\{M\}$	Using symmetric key K to encrypt message M
ENCR_ALG_$PK_X\{M\}$	Using algorithm ALG and Xs public key PK_X to encrypt message M
SIGN_ALG_$SK_X\{M\}$	Using algorithm ALG to sign message M with X's signing key SK_X
TS_i	The current timestamp
$M_1 \parallel M_2$	Concatenation of messages M_1 and M_2

ring) is composed of GW, MRs (connected with the GW), and MCs (connected with the MRs). We denote ring ID as RID_i in Figure 1 (RID_1 means ring 1 and RID_2 means ring 2). GW takes the role of a manager of the ring and is responsible for managing and maintaining the members in the ring.

The symbols used sections are shown in Table 1.

3.2. Trust Model. As shown in Figure 2, the trust model is presented according to the mobile network architecture. TR is trusted by all the entities. GW in different CPS-WMNs does not trust each other. Moreover, different MR belonging to the same GW does not own trust relationship, the same as the MRs in different CPS-WMNs. In addition, we assume that GW is trusted by the MR which is connected to itself. MC only trusts the MR in its home CPS-WMN. The main objective of our proposed scheme is to set up the trust relationship between MC and the accessed MR during MC's roaming.

3.3. System Initialization. As the trusted root, TR generates Param and broadcasts it to all entities. Param = $\{G_1, G_2, e : G_1 \times G_1 \to G_2, P \in G_1, PK_{TR} = sP, H_1 : \{0,1\}^* \to G_1, H_2 : \{0,1\}^* \times G_1 \to Z_q^*, g = (P, P)\}$, where q is the order of G_1 and G_2 and s is the master key of TR. All entities' public key in the ring should be delivered to TR. In addition, GW generates the ring's public and private keys through random choosing of $SK\_R_i \in Z_q^*$ as the private key; the corresponding public key is $PK\_R_i = SK\_R_i \cdot P$. PK_R_i is shared by all the members in the ring, while SK_R_i is only allocated to the legitimate members who are authenticated by TR in system initialization phrase.

3.4. Inter-WMN Authentication Protocol. When MC wants to leave the WMN it belonged to and accesses another WMN, the MC needs to achieve mutual Inter-WMN authentication with the visiting WMN. As shown in Figure 1, when the MC in WMN_1 wants to access WMN_2 and connect to MR_2, MC triggers mutual authentication with MR_2. The mutual authentication details are shown in Figure 3.

(1) $MR_2 \to MC : PK_{GW_2}, PK_{MR_2}$. MR_2 broadcasts PK_{MR_2} and PK_{GW_2} to MC. MC executes PRS-Verify-auth to verify PK_{GW_2}.

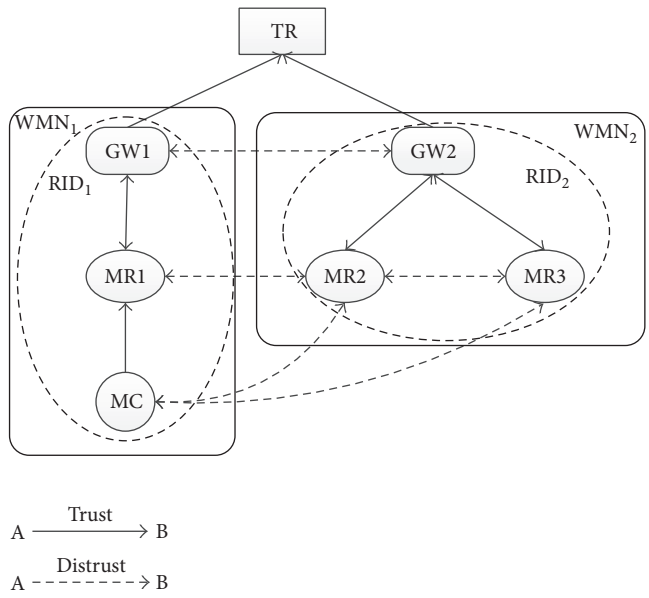


Figure 2: Trust model.

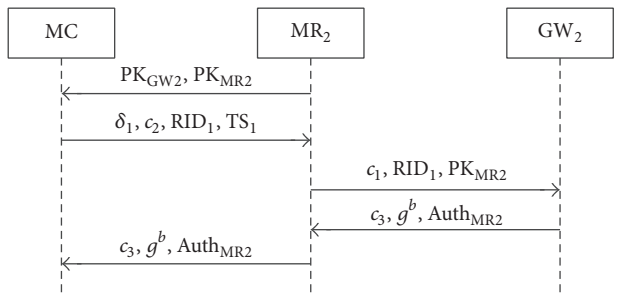


Figure 3: The workflow of Inter-WMN authentication protocol.

(2) $MC \to MR_2 : \delta_1, c_2, TS_1, RID_1$. MC calculates $c_1 = ENCR\_BB1\_PK_{GW_2}\{g^a\}$, $c_2 = ENCR\_BB1\_PK_{MR_2}\{c_1\}$, and $\delta_1 = SIGN\_PRS\_SK_{MC}\{TS_1\}$, where $g^a \in G_1$ is the parameter for session key negotiation and TS_1 is the current timestamp. MC sends δ_1, c_2, TS_1, and RID_1 to MR_2.

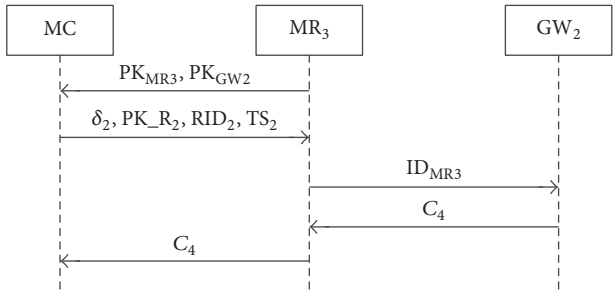


Figure 4: The workflow of Intra-WMN authentication protocol.

(3) $MR_2 \rightarrow GW_2 : c_1, PK_{MR_2}, RID_1$. After receiving (2) from MC, MR_2 checks the freshness of TS_1. If fresh, MR_2 decrypts c_2 to obtain c_1. MR_2 then sends c_1, RID_1, and PK_{MR_2} to GW_2. Meanwhile, MR_2 utilizes PRS-Verify-sign to verify δ_1 through requesting the ring members public key from TR in terms of RID_1. If δ_1 is valid, MC is regarded as a legal user.

(4) $GW_2 \rightarrow MR_2 : c_3, Auth_{MR_2}, g^b$. After receiving (3) from MR_2, GW_2 decrypts c_1 to obtain g^a, choose $g^b \in G_1$ and generate the warrant $W_{r_2} = sk_{GW_2} H_1(ID_{r2})$, where sk_{GW_2} is GW_2's private key. GW_2 computes $AUTH_{MR_2} = sk_{GW_2} H_1(PK_{MR_2})$, session key $K_{GW_2\text{-}MC} = g^{ab}$, and $c_3 = Enc\_K_{GW_2\text{-}MC}\{W_{r_2}\}$. GW_2 then sends c_3, $Auth_{MR_2}$, and g^b to MR_2. Finally, GW_2 stores $K_{GW_2\text{-}MC}$.

(5) $MR_2 \rightarrow MC : c_3, Auth_{MR_2}, g^b$. MR_2 relays c_3, $Auth_{MR_2}$, and g^b to MC when getting (4) from GW_2.

After receiving (5) from MR_2, MC calculates session key $K_{MC\text{-}GW_2} = g^{ab}$ to decrypt c_3 for obtaining W_{r_2}. MC checks $e(P, Auth_{MR_2}) \stackrel{?}{=} e(PK_{GW_2}, H_1(PK_{MR_2}))$, if equal, MC makes sure to access a legal WMN. MC then calculates $U = g^r$ and $V = H_2(RID_2 \parallel PK\_R_2)$, where $r \in Z_q^*$. MC stores U, V, and $K_{MC\text{-}GW_2}$.

3.5. Intra-WMN Authentication Protocol. After finishing Inter-WMN authentication, MC will obtain W_{r_2} issued by GW. When MC moves from one MR to another in the same WMN, we use CLS [14] to achieve efficient Intra-WMN authentication. As shown in Figure 1, assuming that MC and MR_2 finished Inter-WMN authentication, when MC wants to move from MR_2 to MR_3, the Intra-WMN authentication protocol is triggered as shown in Figure 4.

(1) $MR_3 \rightarrow MC : PK_{MR_3}, PK_{GW_3}$. MR_3 broadcasts PK_{MR_3} and PK_{GW_2} to MC.

(2) $MC \rightarrow MR_3 : \delta_2, PK\_R_2, TS_2, RID_2$. MC calculates $h = H_2(TS_2 \parallel U \parallel RID_2 \parallel PK\_R_2)$ and $\delta_2 = rP - h(W_{r_2} + SK\_R_2 V)$, where U and V are generated and stored in the process of Inter-WMN authentication. TS_2 is the current timestamp. MC sends TS_2, δ_2, PK_R_2, and RID_2 to MR_3.

(3) $MR_3 \rightarrow GW_2 : ID_{MR_3}$. After receiving (2) from MC, MR_3 checks the freshness of TS_2. If fresh, MR_3 adopts CLS-Verify to verify δ_2. If δ_2 is valid, MC is regarded as a legal user. MR_3 then sends ID_{MR_3} to GW_2.

(4) $GW_2 \rightarrow MR_3 : C_4$. After receiving ID_{MR_3}, GW_2 uses the previously saved key $K_{GW_2\text{-}MC}$ to encrypt ID_{MR_3} to produce the ciphertext C_4. Then, GW_2 sends C_4 to MR_3.

(5) $MR_3 \rightarrow MC : C_4$. MR_3 relays C_4 to MC after getting (4) from GW_2.

MC uses the previously saved key $K_{GW_2\text{-}MC}$ to decrypt C_4. If the decryption is successful, MC makes sure to access a legal MR.

4. Security Analysis of the Proposed Scheme

In order to prove the security of our scheme, we first take a fundamental security analysis. Then we choose SVO logic [20] to analyze the proposed protocols. SVO logic was presented by Syverson and van Oorshot in 1994 based on BAN logic, GNY logic, AT logic, and VO logic [21]. SVO holds the features of complete semantics, expansibility, and practicality.

4.1. Fundamental Security Analysis. According to the mobile network architecture shown in Figure 1, we will first present fundamental security analysis of the proposed scheme in the following aspects: anonymity, unforgeability, and reliability.

Anonymity. During Inter-WMN authentication, the accessed network checks the legality of MC through verifying the signature $\sigma_1 = SIGN\_PRS\_SK_{MC}\{TS_1\}$ offered by MC. The accessed network is able to know the ring where MC comes from but cannot tell the real identity of MC since it is hidden in the ring. So the anonymity of MC is guaranteed. In addition, when handover occurred, accessed network verifies the certificateless signature $\sigma_i = rP - h(W_{r_i} + SK\_R_i V)$ to authenticate MC. In this paper, the proposed scheme adopts enhanced certificateless signature mechanism: $V = H_2(RID_i \parallel PK\_R_i)$, $h = H_2(TS_2 \parallel U \parallel RID_i \parallel PK\_R_i)$, and $\sigma_i = rP - h(W_{r_i} + SK\_R_i V)$. Thus, with the help of the ring, the identity of MC is also kept private to achieve anonymity.

Unforgeability. Firstly, only TR can calculate the authority for the proxy group. If the adversary does not know TR's private key, he fails to compute the legal authority. Secondly, the only legal proxy signer can generate legal proxy ring signature. If the adversary cannot obtain the authority, he cannot generate the legal signature. Thus, the proxy ring signature is unforgeable. Finally, only trusted GW can issue W_{r_i} to foreign MC, if the adversary does not know GW's private key for certificateless signature, the legal cannot be computed. Moreover, if the adversary cannot obtain the other part of the private key SK_R_i, the legal certificateless signature also cannot be computed. Consequently, certificateless signature is unforgeable based on the security of related entity's private key.

Reliability. In Inter-WMN authentication, if adversary does not know the BB1 secret key of GW_2, then $c_1 = \text{ENCR\_BB1\_PK}_{GW_2}\{g^a\}$ cannot be decrypted. The adversary thus cannot negotiate the correct key with MC. So GW_2 is legal. Likewise, if adversary does not know MR_{2BB1_SK}, he fails to decrypt $c_2 = \text{ENCR\_BB1\_PK}_{MR_2}\{c_1\}$ to obtain c_1, thus MR_2 is legal. Furthermore, the legal proxy ring signature cannot be generated since adversary does not know MC_{PRS_SK}, so the Inter-WMN authentication protocol is reliable. In addition, during Intra-WMN authentication, adversary fails to generate legal signature σ_2, if he cannot obtain W_{r_2}, then MC is thus legal.

4.2. Security Proof of the Proposed Protocols under SVO. SVO logic is not only semantic sound, but also convenient. In terms of our scheme, SVO owns advantages over other logic analysis methods in the following aspects: (1) The axioms in SVO can be adjusted or expanded easily to meet the security proof needs rather than BAN or other logical approaches. (2) SVO is detailed and legible which helps to accurately express the actual meaning of the protocol and thus avoid the misunderstandings. (3) SVO is rigorous and reliable, and the semantics is clear. We first give the grammatical components of SVO logic as follows.

P believes X: indicating that P believes that proposition is right.

P received X: indicating that P received the message including X.

P says X: indicating that P sends a message including X.

P controls X: indicating that P is a trusted authority on X.

P sees X: indicating that P possesses message X.

fresh(X): indicating that X is random number generated in running scheme.

$P \overset{K}{\longleftrightarrow} Q$: indicating that K is a key shared exclusively by P and Q.

$\{X\}_K$: indicating that the ciphertext is output by encrypting X through key.

$[X]_K$: indicating that the message is generated by signing X through key.

$\text{PK}_\sigma(A, K)$: indicating that K is the public signature verification key associated with principal A.

$\text{PK}_\delta(A, K)$: indicating that K is the key agreement key associated with principal A.

$\text{PK}_\psi(A, K)$: indicating that K is the public encryption key associated with principal A.

$\text{SV}(X, K, Y)$: indicating that given signed message X, applying K to it as a signature verification key verifies Y as the message signed with the corresponding private key.

SVO logic includes two initial rules and twenty axioms, part of which are regular axioms and others are axiom templates that include formula variables. We only present part of the axioms used in the following security proof. All the axioms can be found in [20].

Two inference rules are as follows:

(1) Modus ponens MP: φ and $\varphi \supset \psi$ infer ψ

(2) Necessitation Nec: $\vdash \varphi$ infer $\vdash P$ believes φ

φ and ψ are metalinguistic symbols used to refer to arbitrary formula. $\vdash$ is a metalinguistic symbol. $\vdash \varphi$ means that φ is a theorem.

There are twenty SVO axioms. We list only several axioms associated with this article. For any principal P, Q and formula φ, ψ:

(A1) P believes φ and P believes $(\varphi \supset \psi) \supset P$ believes ψ

(A2) $\text{PK}_\sigma(Q, K)$ and R received $X \wedge \text{SV}(X, K, Y) \supset Q$ says Y

(A3) P received $(X_1, \ldots, X_n) \supset p$ received X_i

(A4) P received $\{X\}_K$ and P sees $K^{-1} \supset P$ received X

In SVO, some generic goals should be satisfied. This does not mean a definitive list of the goals that our protocol should meet. In our paper, we should achieve the mutual authentication between MC and MR. For this purpose, we just need that MR and MC could make sure of the legality for each other. So on the basis of the generic goals, we make the appropriate modifications. The goals of Inter-WMN authentication protocol could be described as follows.

(G1′) MR believes $[\text{TS}_1]^{-1}_{K_s}$

(G2′) MC believes $[H(\text{PK}_{\text{MR}})]^{-1}_{K_{\text{GW}}}$

SVO Logic Initial Assumptions

(P1) MC believes $\text{PK}_\sigma(S, K_s)$

(P2) MC believes $\text{SV}([\text{TS}_1]^{-1}_{K_s}, K_s, \text{TS}_1)$

(P3) MC believes fresh(TS_1)

(P4) MR believes (MC says $(\text{TS}_1, \text{RID}_i) \supset \text{TS}_1$)

(P5) MR believes MC says $\text{TS}_1 \supset$ MC says TS_1

(P6) MR believes MR received $\{\{*_1\}_{K_{\text{GW}}}\}_{K_{\text{MR}}}, *_2, \text{RID}_i, [*_3]_{*_4}$

(P7) MR believes MR received $\{\{*_1\}_{K_{\text{GW}}}\}_{K_{\text{MR}}}, *_2, \text{RID}_i, [*_3]_{*_4} \supset$ MR received $\{\{*_1\}_{K_{\text{GW}}}\}_{K_{\text{MR}}}, \text{TS}_1, \text{RID}_i, [\text{TS}_1]^{-1}_{K_s}$

(P8) GW believes $\text{PK}_\sigma(\text{GW}, K_{\text{GW}})$

(P9) GW believes $\text{SV}([H(\text{PK}_{\text{MR}})]^{-1}_{K_{\text{GW}}}, K_{\text{GW}}, H(\text{PK}_{\text{MR}}))$

(P10) MC believes (GW says $(H(\text{PK}_{\text{MR}})) \supset H(\text{PK}_{\text{PK}_{\text{MR}}})$)

(P11) MC believes GW says $H(\text{PK}_{\text{MR}}) \supset$ GW says $H(\text{PK}_{\text{MR}})$

(P12) MC believes MC received $\{[*_5]^{-1}_{K_{\text{GW}}}\}_{K_{\text{GW-MC}}}, *_6, [*_7]_{*_8}$

(P13) MC believes MC received $\{[*_5]^{-1}_{K_{\text{GW}}}\}_{K_{\text{GW-MC}}}, *_6, [*_7]_{*_8} \supset$ MC received $\{[*_5]^{-1}_{K_{\text{GW}}}\}_{K_{\text{GW-MC}}}, g^b, [H(\text{PK}_{\text{MR}})]^{-1}_{K_{\text{GW}}}$

Where K_s is the public key for proxy signer and TS_1 is the current timestamp, $*_i$ means the part that subject cannot understand. The proof is as follows.

From (P6), (A1), (A3), and Nec, we have

$$\text{MR believes MR received } [*_3]_{*_4}. \quad (2)$$

From (2), (P7), (A1), (A3), and Nec, we have

$$\text{MR believes MR received } [TS_1]^{-1}_{K_s}. \quad (3)$$

From (P5), (P1), (P2), (3), (A1), (A2), and Nec, we have

$$\text{MR believes MC says } [TS_1]^{-1}_{K_s}. \quad (4)$$

From (4), (P4), and (A1), we have the following.

MR believes $[TS_1]^{-1}_{K_s}$; *(GI′) is then proved*. In the same way as above, we can get

$$\text{GW believes } [TS_1]^{-1}_{K_s}. \quad (5)$$

From (P12), (A1), (A3), and Nec, we have

$$\text{MC believes MC received } [*_7]_{*_8}. \quad (6)$$

From (6), (P13), (A1), (A3), and Nec, we have

$$\text{MC believes MC received } [H(PK_{MR})]^{-1}_{K_{GW}}. \quad (7)$$

From (P11), (P8), (P9), (7), (A1), (A2), and Nec we have

$$\text{MC believes GW says } [H(PK_{MR})]^{-1}_{K_{GW}}. \quad (8)$$

From (8), (P10), and (A1), we have the following.

MC believes $[H(PK_{MR})]^{-1}_{K_{GW}}$; *(G2′) is thus proved*.

Similar to Inter-WMN authentication protocol, the goal of Intra-WMN authentication is also mutual authentication between MR and MC. The difference is that the MR is in MC's accessed WMN. The security proof of Intra-WMN authentication protocol is described as follows:

(G3′) MR believes $[TS_2]^{-1}_{K_{MC}}$

(G4′) MC believes $[H(PK_{MR})]^{-1}_{K_{GW}}$

SVO Logic Initial Assumptions

(P14) MC believes $PK_\sigma(MC, K_{MC})$

(P15) MC believes $SV([TS_2]^{-1}_{K_s}, K_s, TS_2)$

(P16) MC believes $\text{fresh}(TS_2)$

(P17) MR believes (MC says $(TS_2, RID_i) \supset TS_2$)

(P18) MR believes MC says $TS_2 \supset$ MC says TS_2

(P19) MR believes MR received $PK_\sigma(W_{r_i}, K_{W_{r_i}}), *_1, RID_i, [*_2]^{-1}_{K_{MC}}$

(P20) MR believes MR received MR received $PK_\sigma(W_{r_i}, K_{W_{r_i}}), *_1, RID_i, [*_2]^{-1}_{K_{MC}} \supset$ MR received $PK_\sigma(W_{r_i}, K_{W_{r_i}}), TS_2, RID_i, [TS_2]^{-1}_{K_{MC}}$

(P21) GW believes $PK_\sigma(GW, K_{GW})$

(P22) GW believes $SV([H(PK_{MR})]^{-1}_{K_{GW}}, K_{GW}, H(PK_{MR}))$

(P23) MC believes (GW says $(H(PK_{MR})) \supset H(PK_{PK_{MR}})$)

(P24) MC believes GW says $H(PK_{MR}) \supset$ GW says $H(PK_{MR})$

(P25) MC believes MC received $\{[*_3]_{*_4}\}$

(P26) MC believes MC received $\{[*_3]_{*_4} \supset$ MC received $[H(PK_{MR})]^{-1}_{K_{GW}}\}$

Where TS_2 is the current timestamp, $*_i$ means the part that subject cannot understand. The proving process is shown as follows.

From (P19), (A1), (A3), and Nec, we have

$$\text{MR believes MR received } [*_2]^{-1}_{K_{MC}}. \quad (9)$$

From (9), (P20), (A1), (A3), and Nec, we have

$$\text{MR believes MR received } [TS_2]^{-1}_{K_{MC}}. \quad (10)$$

From (P18), (P14), (P15), (10), (A1), (A2), and Nec, we have

$$\text{MR believes MC says } [TS_2]^{-1}_{K_{MC}}. \quad (11)$$

From (11), (P17), and (A1), we have the following.

GR believes $[TS_2]^{-1}_{K_{MC}}$; *(G3′) is proved*.

From (P25), (A1), (A3), and Nec, we have

$$\text{MC believes MC received } [*_3]_{*_4}. \quad (12)$$

From (12), (P26), (A1), (A3), and Nec, we have

$$\text{MC believes MC received } [H(PK_{MR})]^{-1}_{K_{GW}}. \quad (13)$$

From (P24), (P21), (P22), (13), (A1), (A2), and Nec, we have

$$\text{MC believes GW says } [H(PK_{MR})]^{-1}_{K_{GW}}. \quad (14)$$

From (14), (P23), and (A1), we have the following.

MC believes $[H(PK_{MR})]^{-1}_{K_{GW}}$; *(G4′) is thus proved*.

5. Simulation and Performance Analysis

CPS-WMN has limited resource in the computation ability of nodes and operating bandwidth, so the performance of authentication scheme plays an important role in the practicability of CPS-WMNs. The simulation and performance analysis focus on the efficiency of system initialization and the handover process. In addition, in order to demonstrate the high efficiency of our scheme, we give a comparison analysis between our scheme and PEACE [15].

5.1. Simulation Environment. We do simulations for PRS and PEACE using OMNET++ (4.4) simulation platform to get average results based on 20-time experiments. In the process of bilinear group instantiation, we use Tate pairing in the MNT curve [22].

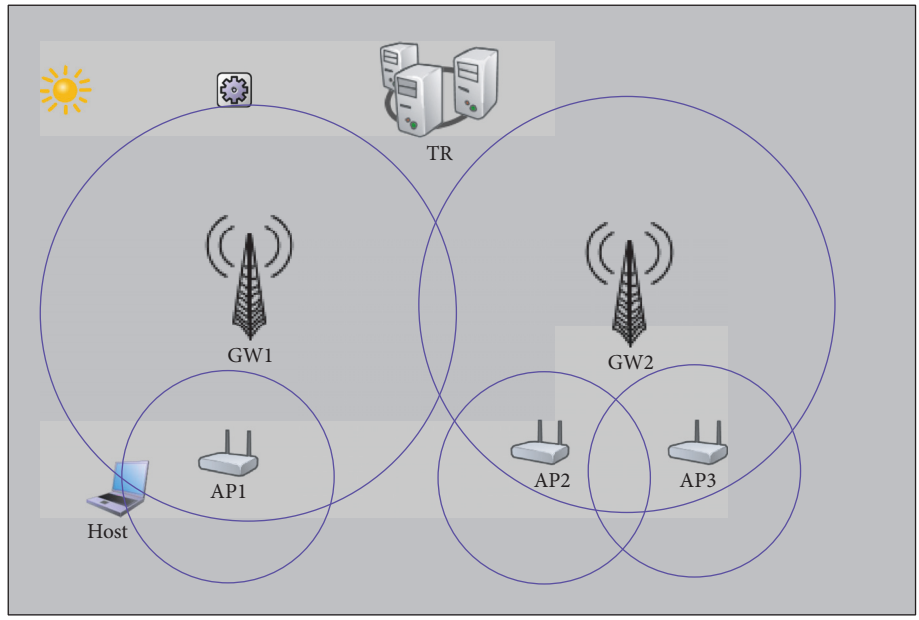


Figure 5: Simulation network topology.

As shown in Figure 5, the initial topological structure of simulation environment is composed of one TR, two GWs, three APs, and one host. These nodes are arranged in a 420 m 300 m simulation space according to the hierarchical network architecture. The TR generates initial parameters for the system. The wireless covering radius is 100 m. AP represents MR, whose covering radius is 45 m. TR, GW, and AP are fixed nodes. Host represents MC, which will take a movement from coordinate (10,250) to coordinate (400,250) by speed 1 m/s. During this process, host firstly accesses the coverage of AP1 and triggers the Inter-WMN authentication. Then, host leaves AP1 to AP2 and the Inter-WMN authentication takes place again. When host moves on from AP2 to AP3, the Intra-WMN authentication protocol should be executed. The details of the parameters and values are shown in Table 2.

(1) The internal structure of the network node shown in Figure 6.

(2) Wlan and eth module: implementation of ethernet and 802.11 capabilities.

(3) NetworkLayer: to achieve network-level functions and as the interface of upper and lower layer.

(4) TCPapp: template for TCP applications.

(5) RoutingTable: the table of routing status.

(6) InterfaceTable: the table of network interfaces.

(7) NotificationBoard: notification about "events" such as wireless handovers.

5.2. Performance Analysis of System Initialization. The delay of system initialization is the period from the simulation start to the first movement of the host. The relationship between the number of nodes and system initialization delay is shown in Figure 7, where the number of nodes could be adjusted as needed. The system initialization includes authorization from original signer to proxy signers, the public key registration for ring members, and the generation of public and private keys for the ring members. Figure 6 shows that the delay of system initialization would increase with the increasing network scale.

Table 2: Parameters and values.

Parameters	Values
Scenario area	420 m × 300 m
Number of nodes	7
Routing protocol	AODV
MAC protocol	IEEE 802.11
Channel	Wireless channel
Simulation time	480 S
Packet length	512 bytes
Node energy	1 J

5.3. Performance Analysis of Authentication Protocols. In this section, we focus on the delay of Inter-WMN authentication and Intra-WMN authentication. The delay of Inter-WMN authentication means the period from AP receiving an access requirement of a new host to the end of Inter-WMN authentication. The delay of Intra-WMN authentication is the period from AP receiving a handover requirement of a host to the end of Intra-WMN authentication.

Figure 8 shows the relationship between the number of ring members and the delay of access authentication scheme. From the result we can see that the efficiency of Intra-WMN authentication is higher than that of Inter-WMN authentication with the increasing number of ring members. During Inter-WMN authentication, the main cost is from

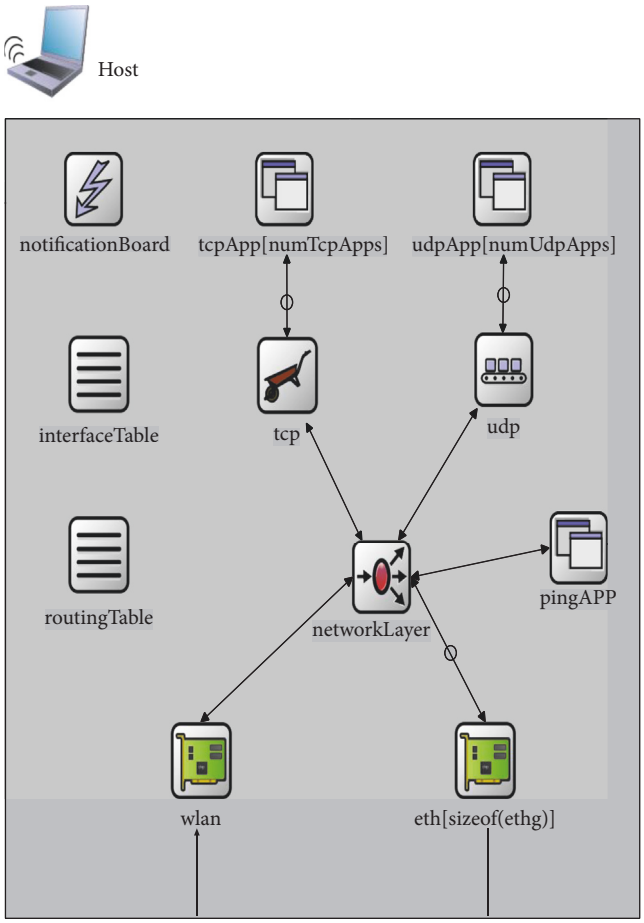


Figure 6: Node internal structure.

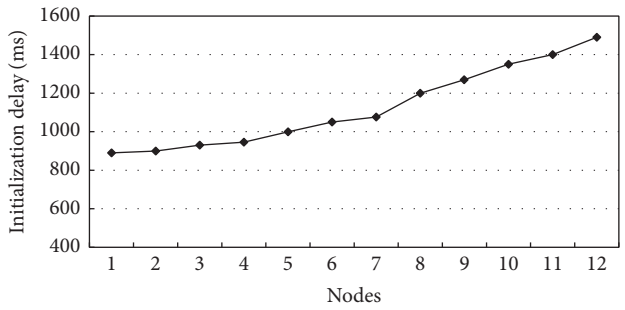


Figure 7: Relationship between system initialization delay and the number of nodes.

verifying the proxy ring signature. For the use of high-efficient ring setup policy, the verifier could acquire all ring members' public keys from TR at once, which help to reduce the delay of communication. In addition, in the process of Intra-WMN authentication, the utilization of certificateless signature makes the scheme independent of the number of ring members that would not lead to obvious delay.

5.4. The Efficiency Analysis of Intra-WMN Authentication Protocol. As shown in Figure 9, we make the comparison analysis of Intra-WMN authentication delay between PRS and PEACE [15]. The delay of PRS is obviously lower than PEACE since PEACE adopts multiple bilinear pairing operations and exponential operations which lead to high computation cost. In the Intra-WMN authentication, we use more efficient certificateless signature which only includes two scalar multiplications in group and one hash operation. Moreover, we just need one bilinear pairing operation, two exponential operations, and one hash operation during the verification process. Thus, the computation cost is obviously reduced in PRS.

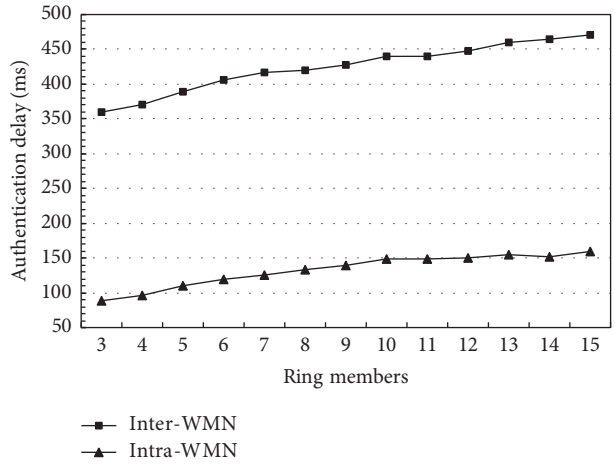


Figure 8: Relationship between authentication delay and the number of ring members.

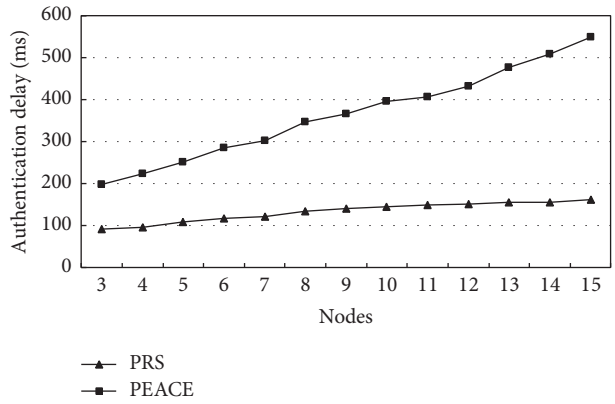


Figure 9: Comparison of the Intra-WMN authentication delay between PRS and PEACE.

In short, the main cost of PRS is from the process of system initialization, while the access authentication delay is obviously dropped down. In addition, the delay of access authentication will not elevate much with the increasing number of nodes in the ring. Although the delay of system initialization increases with the increasing number of ring members, the result of simulation shows that the delay would be controlled in a reasonable range. Comparing to the typical scheme (PEACE), our proposed scheme performs more efficiently, especially during the Intra-WMN authentication.

We further compared the computational overhead of PRS scheme and PEACE scheme during the signing and

Table 3: Comparison of the computational overhead between PRS and PEACE.

Scheme	Signing algorithm	Verifying algorithm
PEACE	2BP + 8SM	(3 + 2|URL|) BP + 6SM
Our scheme	1SM + 2E	3BP + E

verifying phases. In Table 3, BP represents a bilinear mapping operation, SM represents scalar multiplication in $G1$, E represents exponentiation in $G1$, and |URL| represents the time of searching revocation list. From the result we can see that PRS performs more efficiently than PEACE in terms of computational overhead.

6. Conclusions

Anonymous access authentication is an essential approach to address the security issue of CPS-WMNs. In this paper, we propose a novel anonymous access authentication scheme based on proxy ring signature for CPS-WMNs. The scheme is elaborated with the hierarchical mobile network architecture and the corresponding mutual authentication protocols, which achieve high-efficient mutual authentication and satisfy the privacy requirements. The fundamental security and the security proof of the authentication protocols under SVO logic demonstrate the robustness of our scheme. Moreover, the simulation and performance analysis show that the proposed scheme owns higher efficiency and adaptability than the typical.

In our future research, some novel and robust encryption and signature mechanisms will be introduced to make our scheme more resilient. Moreover, how to secure the routing procedure of WMNs under the proposed hierarchical architecture forms another future task.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by National Natural Science Foundation of China under Grant no. 61402095 and Grant no. 61300196 and China Fundamental Research Funds for the Central Universities under Grant no. N120404010 and Grant no. N130817002. This work was also supported in part by Soonchunhyang University Research Fund and the Scientific and Technological Research Program of Chongqing Municipal Education Commission (KJ1500440).

References

[1] Z. Ning, F. Xia, X. Kong, and Z. Chen, "Social-oriented resource management in cloud-based mobile networks," *IEEE Cloud Computing*, vol. 3, no. 4, pp. 24–31, 2016.

[2] Z. Ning, F. Xia, X. Hu, Z. Chen, and M. S. Obaidat, "Social-oriented adaptive transmission in opportunistic internet of smartphones," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 2, pp. 810–820, 2017.

[3] X. Hu, X. Li, E. C.-H. Ngai, V. C. M. Leung, and P. Kruchten, "Multi-dimensional context-aware social network architecture for mobile crowdsensing," *IEEE Communications Magazine*, vol. 52, no. 6, pp. 78–87, 2014.

[4] X. Hu, J. Zhao, B.-C. Seet, V. C. M. Leung, T. H. S. Chu, and H. Chan, "S-aframe: agent-based multilayer framework with context-aware semantic service for vehicular social networks," *IEEE Transactions on Emerging Topics in Computing*, vol. 3, no. 1, pp. 44–63, 2015.

[5] Z. Ning, L. Liu, F. Xia, B. Jedari, I. Lee, and W. Zhang, "CAIS: a copy adjustable incentive scheme in community-based socially aware networking," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 4, pp. 3406–3419, 2017.

[6] X. Hu, T. H. S. Chu, V. C. M. Leung, E. C.-H. Ngai, P. Kruchten, and H. C. B. Chan, "A survey on mobile social networks: applications, platforms, system architectures, and future research directions," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1557–1581, 2015.

[7] Q. Liu, X. Hu, E. C. Ngai et al., "A security patch addressing bandwidth request vulnerabilities in the IEEE 802.16 standard," *IEEE Network*, vol. 30, no. 5, pp. 26–34, 2016.

[8] Z. Ning, Q. Song, L. Guo, Z. Chen, and A. Jamalipour, "Integration of scheduling and network coding in multi-rate wireless mesh networks: optimization models and algorithms," *Ad Hoc Networks*, vol. 36, pp. 386–397, 2016.

[9] X. Hu, T. H. S. Chu, H. C. B. Chan, and V. C. M. Leung, "Vita: a crowdsensing-oriented mobile cyber-physical system," *IEEE Transactions on Emerging Topics in Computing*, vol. 1, no. 1, pp. 148–165, 2013.

[10] C. Li, U. Nguyen, and H. Nguyen, "Efficient authentication for fast handover in wireless mesh networks," *Computers and Security*, vol. 47, pp. 124–142, 2013.

[11] Y. Yu, Z. Ning, and L. Guo, "A secure routing scheme based on social network analysis in wireless mesh networks," *Science China Information Sciences*, vol. 59, no. 12, article 122310, 2016.

[12] D. S. Wong, "Security analysis of two anonymous authentication protocols for distributed wireless networks," in *Proceedings of the 3rd IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom '05)*, pp. 532–536, Kauai Island, Hawaii, USA, 2005.

[13] M. Ayyash, H. Elgala, A. Khreishah et al., "Coexistence of WiFi and LiFi toward 5G: concepts, opportunities, and challenges," *IEEE Communications Magazine*, vol. 54, no. 2, pp. 64–71, 2016.

[14] Y. Li, F. Yao, T. Lan, and G. Venkataramani, "SARRE: semantics-aware rule recommendation and enforcement for event paths on android," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 12, pp. 2748–2762, 2016.

[15] K. Ren, S. Yu, W. Lou, and Y. Zhang, "PEACE: a novel privacy-enhanced yet accountable security framework for metropolitan wireless mesh networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 21, no. 2, pp. 203–215, 2010.

[16] V. S. Miller, "Use of elliptic curves in cryptography," in *Proceedings of the Advances in Cryptology (CRYPTO '85)*, Lecture Notes in Computer Science, pp. 417–426.

[17] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," *SIAM Journal on Computing*, vol. 32, no. 3, pp. 586–615, 2003.

[18] V. Kumar and R. Kumar, "Prevention of blackhole attack using certificateless signature (CLS) scheme in MANET," in *Security*

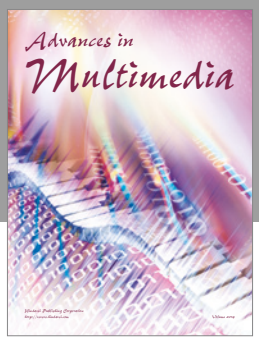
Solutions for Hyperconnectivity and the Internet of Things, vol. 130, IGI Global, 2016.

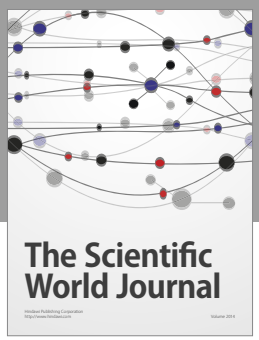
[19] Y. Yu, C. Xu, and X. Huang, "An efficient anonymous proxy signature scheme with provable security," *Computer Standards and Interfaces*, vol. 31, no. 2, pp. 348–353, 2009.

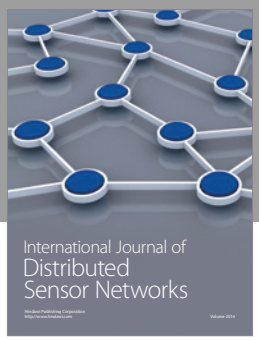
[20] P. F. Syverson and P. C. van Oorschot, "On unifying some cryptographic protocol logics," in *Proceedings of the 1994 IEEE Symposium on Research in Security and Privacy*, pp. 14–28, May 1994.

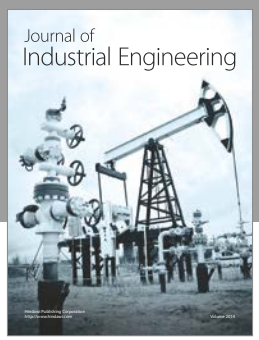
[21] W. Zhao, A. Zhang, J. Li et al., "Analysis and design of an authentication protocol for space information network," in *Proceedings of the IEEE Military Communications Conference (MILCOM '16)*, pp. 43–48, Baltimore, MD, USA, 2016.

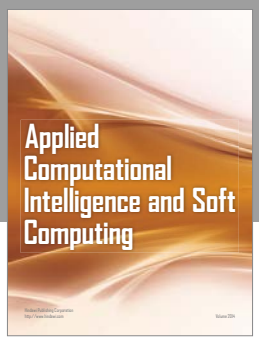
[22] S. D. Galbraith, K. Harrison, and D. Soldera, "Implementing the tate pairing," in *Proceedings of the International Algorithmic Number Theory Symposium*, pp. 324–337, Sydney, Australia, 2002.

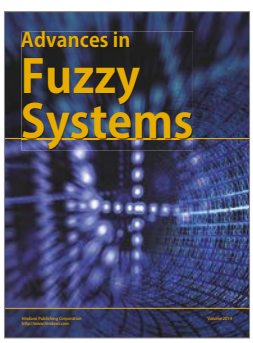


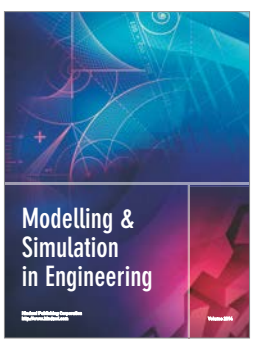


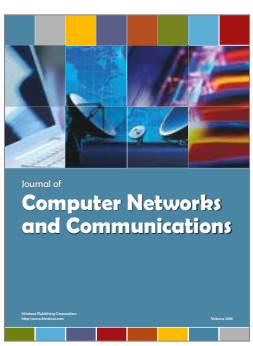












Hindawi
Submit your manuscripts at
https://www.hindawi.com