Gao *et al. EURASIP Journal on Wireless Communications and Networking* (2016) 2016:193
DOI 10.1186/s13638-016-0685-2

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Anonymous authentication scheme based on identity-based proxy group signature for wireless mesh network

Tianhan Gao*, Fangting Peng and Nan Guo

Abstract

Access security is the key obstacle of the rapid popularization of wireless mesh network (WMN). We suggest the proxy group signature scheme based on identity in this paper. This scheme is combined with proxy group signature and identity-based group signature, based on designated hierarchical proxy architecture for WMN. An anonymous mutual authentication scheme is thus achieved, which not only simplifies the complex management of PKI but also guarantees anonymous authentication and owns high handover authentication efficiency. Performance and security analysis show that the scheme in this paper is efficient and resilient to a series of security and anonymity attacks.

Keywords: WMN, Access authentication, Privacy preserving, Proxy group signature, Certificate-based signature

1 Introduction

Compared with traditional wireless self-organized network (MANET), wireless mesh network (WMN) owns higher reliability, larger data throughput, and lower disturbance, as well as stronger scalability due to its unique mesh structure. As a result, WMN is able to provide high-speed wireless access service for mobile users in a wide area. WMN is now attracting more and more attentions in both academia and industry [1].

WMN is a kind of wireless multi-hop radio network, whose promotion and deployment depend heavily on security issues relative to cable network and WLAN [2]. To keep malicious nodes from accessing and provide reliable service to WMN users, two-way authentication between mesh client (MC) and access network is necessary and becomes the foundation of the whole WMN security [3]. However, users' privacy information is always carried in the authentication signaling. So to protect user's privacy is important during mutual authentication in the research of WMN access security [2].

For the past few decades, scholars have lots of researches in WMN access security, which aim at achieving safe and efficient access authentication systems. In Ref [4], the authors applied identity-based encryption and signature scheme to WMN access authentication. Mutual authentication is adopted between MC and authentication server without the protection of MC's privacy. Ref [5]'s authors utilized Tor (The Onion Router Protocol) to protect the security of WMN router and the privacy of MC. But access authentication is ignored. Moreover, the extra-expense for saving and maintaining a routing table made the scheme not profitable. The authors of Ref [6] adopted Ring Signature for WMN anonymous authentication and communication. However, each MR needs to manage two certificates, which results in extra-burden. Besides, the cost for handling ring signature during authentication is large.

We proposed a new scheme, which is the combination of proxy group signature and identity-based group signature, based on designated hierarchical proxy architecture for WMN. An anonymous mutual authentication scheme is thus achieved, which not only simplifies the complex management of PKI but also guarantees anonymous authentication and owns high handover authentication efficiency. Security and performance analysis show that our scheme is efficient and is resilient to a series of security and anonymity attacks.

Our paper is organized as follows. Section 2 reviews the cryptographic primitives. The identity-based proxy

*Correspondence: gaoth@mail.neu.edu.cn
Software College, Northeastern University, No. 3–11, Wenhua Road, Heping District, Shenyang, China

Springer Open

© 2016 The Author(s). **Open Access** This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

group signature scheme was presented in Section 3. The anonymous access authentication scheme with different roaming is in Section 4. We provide security and performance analysis in Section 5. Last, we make the conclusion in Section 6.

2 Preliminaries

2.1 Bilinear pairings

G_1, G_2, and G_T are groups of the same prime order q. Consider that discrete logarithm problem(DLP) is hard in G_1, G_2, and G_T [8]. A bilinear paring can be defined if the mapping e:$G_1 \times G_2 \rightarrow G_T$ satisfying the following properties.

(1) Bilinearity:
$e\left(g_1^a, g_2^b\right) = e(g_1, g_2)^{ab}$ if $g_1 \in G_1, g_2 \in G_2, a, b \in Z_q^*$;
(2) Non-degeneracy:
$e(g_1, g_2)^{ab} \neq 1_T$ if 1_T is a generator of group G_T.
(3) Computable:
As how to compute $e(g_1, g_2) \in G_T$, there existed an efficient algorithm.

2.2 Hard problems and security assumptions

G_1 and G_2 are cyclic groups of prime order q, and P is a generator of group G_1. For bilinear pairing $e : G_1 \times G_1 \rightarrow G_2$ as well as a, b, c, x, $y \in Z_q^*$, the assumptions that related to this paper are described as followings.

(1) Computational Diffie-Hellman (CDH) problem:
Sample:(P, aP, bP) for some $a, b \in Z_q^*$
Output: abP
(2) CDH assumption:
There does not exist an efficient PPT (probabilistic polynomial time) algorithm in G_1 to solve CDH problem.
(3) Decisional Diffie-Hellman (DDH) problem:
Sample:(P, aP, bP, cP) for some $a, b, c \in Z_q^*$
Output: True if $c = abmodq$ and false if otherwise.
(4) Gap Diffie-Hellman (GDH) group:
If there exists an efficient PPT algorithm to solve the DDH problem and no PPT algorithm to solve the CDH problem, then G_1, a prime group, is defined as a GDH group.
(5) q-Strong Diffie-Hellman (q-SDH) problem:
Instance: $q+1$ tuple $< P, xP, x^2P \ldots x^qP >$ belongs to GDH group G_1.
Output: $\left(y, \frac{1}{x+y}P\right)$.
(6) q-SDH assumption:
There does not exist an efficient PPT algorithm to solve q-SDH problem.
(7) Bilinear Diffie-Hellman (BDH) problem:
Instance: (P, aP, bP, cP) in random
Output: $e(P, P)^{abc}$
(8) BDH assumption:
No efficient PPT algorithm exist here to solve BDH problem under the condition $< G1, G2, e >$.

2.3 Certificate-based signature

Based on the certificate-based encryption (CBE) scheme [7, 11], Kang et al. presented certificate-based signature(CBS) scheme . First of all, users' public and private keys are generated by public parameters. Then users apply certificates from CA as part of temporary signing key. And it addressed the key escrow problem. Besides, it is not necessary to establish the secure channel between users and CA. The process of CBS is described as below.

(1) CBS.Setup:
Given cyclic groups G_1 and G_2 generated by CA and the bilinear pairing $e : G_1 \times G_1 \rightarrow G_2$; CA computes system public key $PK_c = S_cP$ after choosing generator $P \in G_1$ and random private key $S_C \in Z_q^*$; CA selects two hash functions $H_1 : \{0,1\}^* \rightarrow G_1$, $H_2 : \{0,1\}^* \times G_1 \rightarrow Z_q^*$. $(G_1, G_2, e, q, P, PK_C, H_1, H_2)$ is published.
(2) CBS.UserKeyGen:
Users select their own private key $S_A \in Z_q^*$ randomly to compute public key $PK_A = S_AP$.
(3) CBS.CertGen:
Users send their PK_A and authentication information(such as ID_A) to CA to verify their identity. If valid, CA calculates $P_A = H_1(PK_C||PK_A||\mathrm{ID_A}) \in G_1$ then generates certificate $\mathrm{Cert}_A = S_CP_A$ which is sent to users.
(4) CBS.SignKeyGen:
Users compute $P_A^{'} = H_1(PK_A||\mathrm{ID}_A) \in G_1$ and $S_A = S_CP_A + S_AP_A^{'} = \mathrm{Cert}_A + S_AP_A^{'}$.
(5) CBS.Sign:
Given message m, users select $r \in Z_q^*$ and generate the signature $\sigma = (U_1, U_2, V)$, where $U_1 = rP_A, U_2 = rP_A^{'}, h = H_2(U_1, U_{2.}, m)$, and $V = (r+h)S_A = (r+h)(S_CP_A + S_AP_A^{'})$.
(6) CBS.Verify:
Verifier will check whether $e(PK_C, U_1 + hP_A)e(PK_A, U_2 + hP_A^{'}) =?e(P, V)$ when given the signature σ to confirm the validity of σ. Returns 1 if valid, else returns 0.

3 Identity-based proxy group signature

Identity-based Proxy Group Signature (IPGS) scheme is the combination of proxy group signature [9] and identity-based group signature [10]. In IPGS, the signing rights can be delegated in turn from the initial signer to proxy signer then to group manager. Anyone in this group can sign a message for the initial signer. As for the verifier, the only thing he can do is to verify the validity of a signature but cannot tell which specific group member generates

the signature. The group manager is responsible for setting up the group. When dispute happens, only the group manager can disclose signer's real identity. The process of IPGS is described as following.

(1) IPGS.Setup:
Original signer generates two cyclic groups G_1 and G_2 of prime order q and the bilinear pairing $e : G_1 \times G_1 \rightarrow G_2$. Then he selects a generator $P \in G_1$ and random number $S_O \in Z_q^*$ as private key. The corresponding public key $PK_O = S_O P$; Three hash functions $H_1 : \{0,1\}^* \rightarrow G_1, H_2 : \{0,1\}^* \times G_1 \rightarrow G_1$, and $H_3 : G_1 \rightarrow G_1$ are also selected. $(G_1, G_2, e, q, P, PK_O, H_1, H_2, H_3)$ is published. Proxy signer selects private key $S_D \in Z_q^*$ and figures out the public key $PK_D = S_D P$. Group manager selects group private key $S_g \in Z_q^*$ and computes group public key $PK_g = S_g P$.

(2) IPGS.Auth:
Original signer generates the warrant $\text{auth}' = S_O H_3(PK_D)$ which is sent to proxy signer. Proxy signer verifies auth' through $e(P, \text{auth}')=?e(PK_O, H_3(PK_D))$, then computes another warrant $\text{auth} = S_D H_3(PK_g) + \text{auth}'$ for group manager.

(3) IPGS.Join:
It is necessary to execute the following protocol if a user (group member) wants to join a group. $r \in Z_q^*$ was the long-term private key selected by the group member and then it figures out the public key $Q_{\text{ID}}=H_1(\text{ID})$; Group member sends ID, rP to group manager to compute $S_{\text{ID}} = S_g H_2(Q_{\text{ID}}||rP)$. Then group manager distributes S_{ID} and auth to group member through secure channel; (S_{ID}, r) is the group member's private key; the public key is Q_{ID}.
Group member selects $x_i \in Z_q^*, i = 1, 2, ...k$ and sends ID, $S_{\text{ID}}, rP, x_i P$, and $rx_i P$ to group manager through secure channel.
Group manager verifies $S_{\text{ID}} =?S_g H_2(Q_{\text{ID}}||rP)$ and $e(rx_i P, P) =?e(x_i P, rP)$. If successful, group manager sends $S_i = S_g H_2(T||rx_i P)$ to user. T presents the life cycle of the private key. User needs to update the private key if T is expired. $(S_i, rx_i P)$ is the user's group signing key.

(4) IPGS.Sign:
Signer signs the message m through computing $U = rx_i P, V = rx_i H_2(Q_{\text{ID}}||T||U), H = H_2(m||V)$ and $W = rx_i H + S_i$ then generates signature $\sigma = (U, V, W, T)$. σ and along with warrant auth will be sent to verifier by signer.

(5) IPGS.Verify-auth:
If T is fresh, verifier verifies auth first by checking $e(P, auth) =?e(PK_P, H_3(PK_{DM}))e(PK_{DM}, H_3(PK_g))$.

(6) IPGS.Verify-sign:
If auth is successfully tested, verifier computes $Q = H_2(T||U), H = H_2(m||V)$ then verifies the signature by checking $e(P, W) =?e(PK_g, Q)e(U, H)$. If the equation holds, returns 1, else returns 0.

IPGS is the foundation of our proposed scheme in this paper to achieve anonymous access authentication. In Ref. [9], authors show that IPGS is safe under q-SDH assumption. IPGS simplifies the management and maintenance of the certificate for both signer and verifier.

4 Anonymous access authentication scheme

4.1 Proxy-based hierarchical network architecture

The relevant notations and explanations used in our scheme are shown in Table 1.

We present a proxy-based hierarchical network architecture shown as Fig. 1 [12]. TR is the first layer. As the architecture's root trust, TR generates public parameter and distributes warrant to the second-layer entities, Domain Managers(DMs).

After getting the warrant from TR, DM delegates the signing rights to the third-layer entities, a quantity of WMN groups which includes GW, several mesh routers and MCs. As the manager of a WMN group, GW holds the group master key and allocates private key for every member in the group. Besides, GW issues the certificates for legitimate roaming users.

4.2 Trust model

As shown in Fig. 2, our trust model is set up under the hierarchical network architecture. The following trust assumptions are given. (1) TR is trusted by all the entities of the network. (2) There is no trust between DMs

Table 1 Notations and explanations

Notations	Explanations
ID_A	Identity of entity A
TS	Current time stamp
$\text{A} \rightarrow \text{B}$ {M}	Entity A sends message M to entity B
SIGN_ALG(M)	Use ALG to sign M
MSK_i	Master key of group *i*
PK_A/SK_A	Entity A's public/private key pair
ENCR_ALG_PK(M)	Use ALG to encrypt M with public key PK
$A_{ALG\_PK/SK}$	Entity A's public/private key pair in ALG
CERT_A_WMN_i	A's certificate at WMN group *i*
$\text{M}_1 \parallel \text{M}_2$	Concatention of M_1 and M_2
Auth_A	Entity A's warrant for proxy signature
K_{A-B}	Shared key between A and B
$\text{SE}_K(\text{M})$	Encrypt M with shared key K

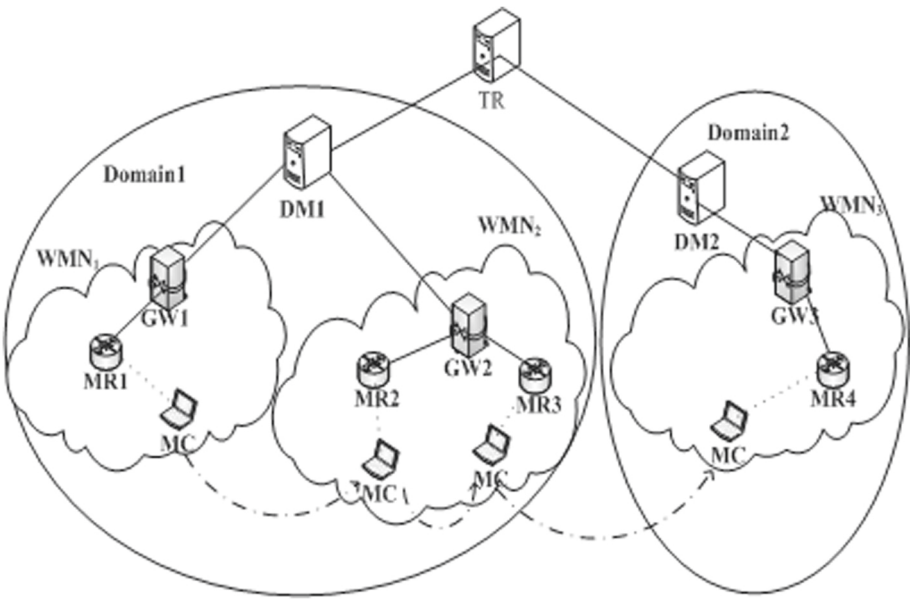

Fig. 1 Proxy-based hierarchical network architecture

in different domain. (3) GWs in the same domain own mutual trust to each other. (4) Within the same WMN group: GW and MR trust each other. MC trusts GW and MR in the same group. MC trusts all the GW's public keys in the same group. (5) MC does not trust the entities in the access WMN group, vice versa. The main goal of our authentication scheme is to establish trust between MC and the access network.

4.3 Adversary model

In this paper, we assume that adversary owns the ability to launch both active and passive attacks. The adversary

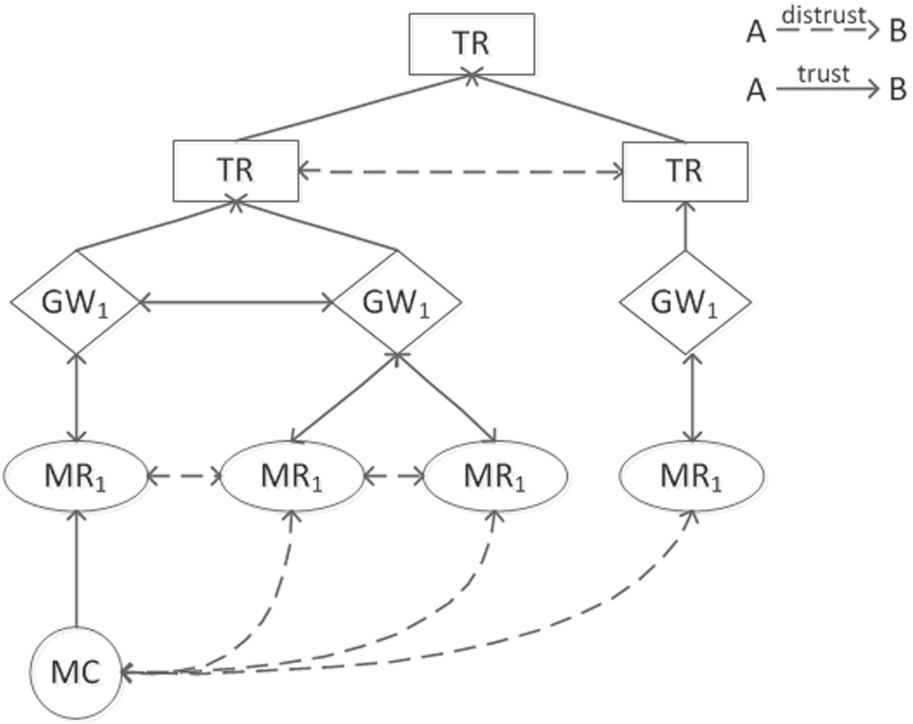

Fig. 2 Trust model

can break all the nodes and eavesdrop all the communications between nodes in our network. While it does not mean that the adversary holds boundless information stealing and computing capacity. In other words, the adversary cannot guess the private key of the relevant nodes and decrypt the ciphertext or fake the digital signature of intercepted message. It implies that CDH, BDH, and q-SDH assumptions are effective for the adversary.

4.4 Intra-domain authentication protocol

We design intra-domain authentication protocol with the help of IPGS, CBS, and BF scheme [13]. The protocol includes initial authentication protocol as well as handover authentication protocol.

4.4.1 System initialization

As a root trust, TR generates system public parameter Param $= \{G_1, G_2, e : G_1 \times G_1 \rightarrow G_2, P \in G_1, PK_{TR}, H_1 : \{0,1\}^* \rightarrow G_1, H_2 : \{0,1\}^* \times G_1 \rightarrow Z_q^*, H_3 : G_1 \rightarrow G_1, H_4 : \{0,1\}^* \times \{0,1\}^* \rightarrow Z_q^*, H_5 : G_1 \times G_1 \rightarrow G_2\}$ for IPGS, CBS, and BF. At the same time, TR publishes Param for all the entities in the system. Assume that DM and GW have completed IPGS. Auth and get warrants before MC's roaming. Besides, entities in the third layer have completed IPGS.join and obtain the corresponding warrant and public/private keys.

4.4.2 Initial authentication protocol

It will trigger the initial authentication protocol when MC leaves its WMN group for another WMN group in the same domain. In Fig. 1, MC moves from WMN_1 to WMN_2 and connects with MR_2. It is necessary for MC and MR_2 to execute mutual authentication protocol. The details of the protocol are described in Fig. 3.

(1) $MR_2 \rightarrow MC\{PK_{MR2}, PK_{g2}, auth_{MR2}, PK_{DM1}\}$
MR_2 broadcasts $PK_{MR2}, PK_{g2}, PK_{DM1}, auth_{MR2}$ to MC. After the message was received, MC chooses $MC_{CBS\_SK} = S \in Z_q^*$ and figures out $MC_{CBS\_PK} = SP, \delta_1 = SIGN\_IPGS(TS_1), c_1 = ENCR\_BF\_GW_2(g^a), c_2 = ENCR\_BF\_MR_2(c_1)$, where TS_1 is the current time stamp, g^a is the key negotiation parameter. MC sends $PK_{g1}, c_2, \delta_1, MC_{CBS\_PK}, PK_{MC}, TS_1$ to MR_2.

(2) $MC \rightarrow MR_2\{PK_{g1}, c_2, \delta_1, MC_{CBS\_PK}, TS_1\}$
MR_2 checks TS_1's freshness after receiving the access authentication message from MC. If TS_1 is fresh, c_2

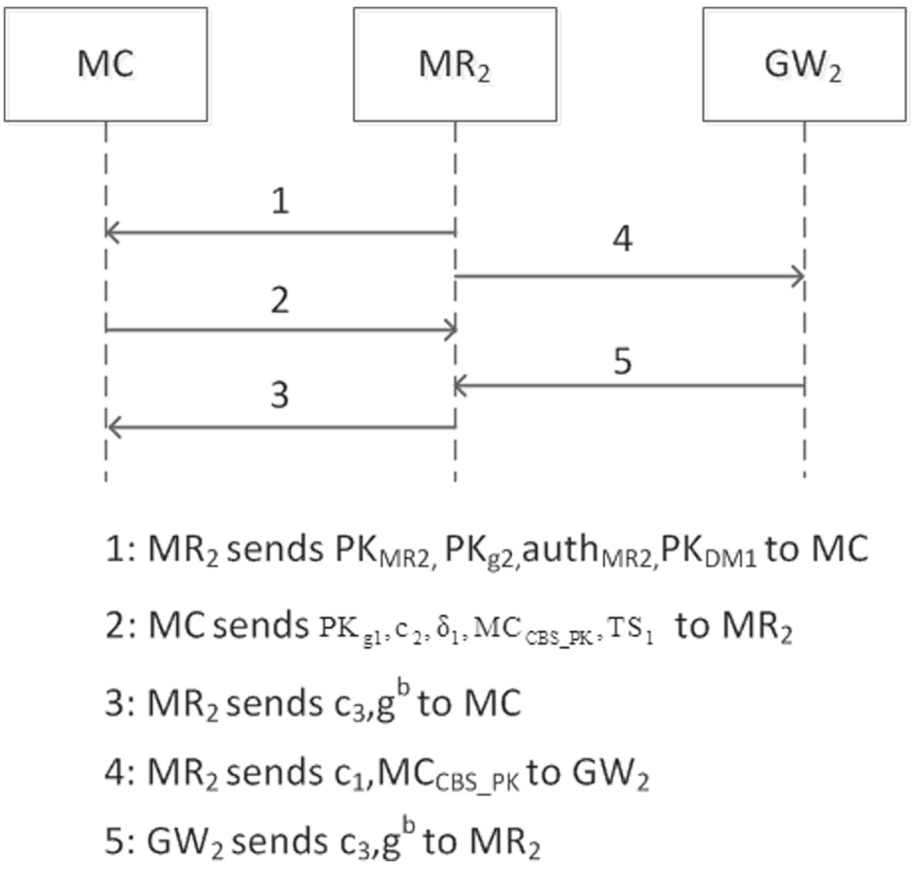

Fig. 3 Initial authentication protocol

will be decrypted by MR_2 to get c_1. Then c_1, MC_{CBS_PK} will be sent to GW_2. MR_2 verifies group signature δ_1 through IPGS.Verify-sign. If δ_1 is legitimate, MC is regarded as a legal user by MR_2.

(3) $MR_2 \rightarrow GW_2\{c_1, MC_{CBS\_PK}\}$
While getting the message from MR_2, GW_2 decrypts c_1 to get g^a. GW_2 generates negotiation parameter g^b and $CERT\_MC\_g_2 = S_{g2}P_A$, where $P_A = H_1(PK_{GW2}||MC_{CBS\_PK})$. GW_2 derives shared key $K_{GW2-MC} = g^{ab}$ and $c_3 = SE_{K_{GW2-MC}}(CERT\_MC\_g_2)$. c_3, g^b are then sent to MR_2. Meanwhile, GW_2 stores K_{GW2-MC}.

(4) $GW_2 \rightarrow MR_2\{c_3, g^b\}$
MR_2 transfers c_3, g^b to MC after receiving the message from GW_2.

(5) $MR_2 \rightarrow MC\{c_3, g^b\}$
When getting message from MR_2, MC computes the shared key $K_{GW2-MC} = g^{ab}$ and uses it to decrypt c_3 and then to get CERT_MC_g2. If the certificate is normally decrypted, MC makes sure to access to a legitimate WMN. MC also computes CBS's signing key $MC_{CBS\_SK\_SIGN} = CERT\_MC\_g_2 + MC_{CBS\_SK}P_A^{'}$, where $P_A^{'} = H_1(MC_{CBS\_PK})$. Finally, MC stores $P_A^{'}$ and K_{GW2-MC}.

4.4.3 Handover authentication protocol

When MC roams from one MR to another in the same WMN group, handover authentication protocol should be executed between MC and new access MR. As shown in Fig. 1, when moving from MR_2 to MR_3 in WMN_2, MC needs to take handover authentication with MR_3 following the steps in Fig. 4.

(1) $\{R_3 \rightarrow MC\{PK_{MR3}, PK_{g2}, auth_{MR3}, PK_{DM1}\}$
MR_3 broadcasts PK_{MR3}, PK_{g2}, PK_{DM1} to MC. MC computes $\delta_2 = SIGN\_CBS(TS_2)$, $c_4 = ENCR\_BF\_PK_{MR3}(g^c)$, where TS_2 is the current time stamp, g^c is the key negotiation parameter. MC then sends $MC_{CBS\_PK}, \delta_2, c_4, TS_2$ to MR_3.

(2) $MC \rightarrow MR_3\{MC_{CBS\_PK}, \delta_2, c_4, TS_2\}$
MR_3 will check the freshness of TS_2 when received the authentication message from MC. If TS_2 is fresh, MR_3 verifies δ_2 through CBS.Verify. If δ_2 is valid, MR_3 regards MC as a legal user. MR_3 decrypts c_4 and chooses g^d as the key negotiation parameter. MR_3 computes $K_{MR3-MC} = g^{cd}, c_5 = SE_{K_{GW2-MC}}(PK_{MR3})$. MR_3 then sends g^d, c_5 to MC and stores K_{MR3-MC}.

(3) $MR_3 \rightarrow MC\{g^d, c_5\}$
MC computes $K_{MC-MR3} = g^{cd}$ when receiving message from MR_3 and decrypts c_5 with its private key. If the plaintext includes PK_{MR3}, MC confirms to access a legitimate network. Finally, MC keeps K_{MC-MR3}.

4.5 Inter-domain authentication protocol

When MC leaves its own WMN for another in the different domain,it needs to take inter-domain authentication with the access WMN. As Fig. 1 shows, MC leaves WMN2 in $domain_1$ for WMN_3 in $domain_2$ and connects with MR_4, and it needs to complete mutual

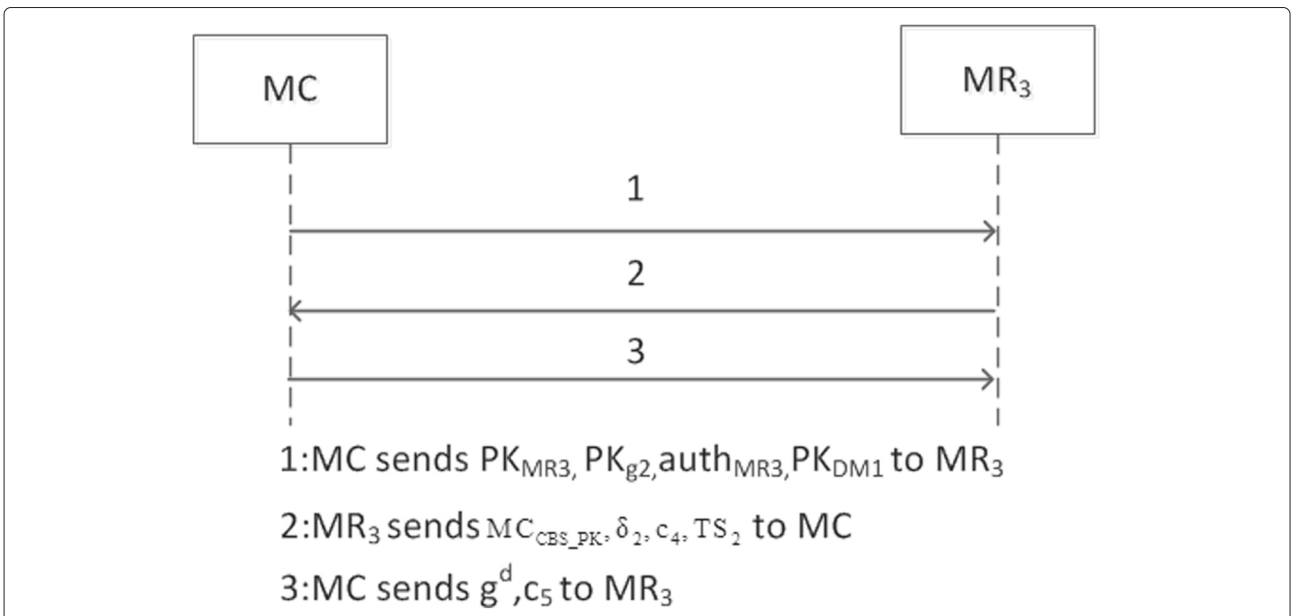

Fig. 4 Handover authentication protocol

authentication with MR_4. The difference between inter-domain authentication protocol and initial authentication protocol is whether to verify the group public key of the other group. In our roaming scenario, MC and MR_4 should utilize IPGS.Verify-auth to verify PK_{g3} and PK_{g1}, respectively, during inter-domain authentication. While the other procedures are totally the same as initial authentication protocol.

5 Discussion

5.1 Security analysis

According to Fig. 1, we make security analysis of our scheme in terms of reliability, traceability, anonymity, and unforgeability.

5.1.1 Reliability

First, adversary could not decrypt $c_1 = \text{ENCR\_BF\_PK}_{\text{GW2}}(g^a)$ if he does not know $\text{GW}_{\text{2BF\_SK}}$ due to the fact that BF is safe under BDH assumption during initial authentication [13]. Thus, adversary cannot get g^a. He cannot negotiate correct shared key with MC. So GW_2 is legitimate. Similarly, adversary could not decrypt $c_2 = \text{ENCR\_BF\_PK}_{\text{MR2}}(c_1)$ if he does not know $\text{MR}_{\text{2BF\_SK}}$. Then GW_2 cannot get c_1. So MR_2 is legitimate. Besides, adversary cannot generate a legitimate group signature if he does not know $\text{MC}_{\text{IPGS\_SK}}$ due to the security of IPGS under q-SDH assumption [9]. So MC is legitimate. In conclusion, our initial authentication protocol is reliable.

Second, adversary could not decrypt $c_4 = \text{ENCR\_BF\_PK}_{\text{MR3}}(g^c)$ if he does not know $\text{MR}_{\text{3BF\_SK}}$ during handover authentication. Thus, he cannot get g^c. As a result, adversary cannot negotiate correct shared key with MC. So MR_3 is legitimate. Meanwhile, adversary could not generate legitimate certificate-based signature if he does not get $\text{MC}_{\text{CBS\_SK}}$ or MC does not obtain CERT_MC_g_2 [11]. So MC is legitimate. To sum up, our handover authentication protocol is reliable.

Finally, the analysis of reliability of inter-domain authentication protocol is the same as initial authentication protocol.

5.1.2 Traceability

When a MC behaves illegally in a certain visiting WMN, the group manager(GM) should be equipped with the ability to disclose the real identity of that MC.

To achieve the traceability goal, GM first sends group signature $\delta_1 = \text{SIGN\_IPGS}(\text{TS}_1)$ to the GM of MC's home WMN group who is able to open δ_1 and trace the real identity of MC with the clue of $U = rx_iP$.

5.1.3 Anonymity

During initial authentication and inter-domain authentication process, access network can verify MC by checking whether the group signature $\delta_1 = \text{SIGN\_IPGS}(\text{TS}_1)$ is legal or not. The access network only knows which group MC belongs to but cannot tell MC's real identity information. MC's privacy is thus guaranteed. Access network verifies MC through $\delta_2 = \text{SIGN\_CBS}(\text{TS}_2)$ to handover authentication. We modify the CBS certificate as $\text{CERT\_MC\_}g_2 = S_{g2}P_A, P_A = H_1(\text{PK}_{\text{GW2}}||\text{MC}_{\text{CBS\_PK}})$. MC's privacy is guaranteed since no identity information is included in the certificate.

5.1.4 Unforgeability

First, only TR can generate DM's warrant. Adversary cannot compute legitimate warrant if he does not know TR's private key. Only DM who obtain warrant form TR can compute WMN group's warrant. Adversary cannot compute legitimate warrant if he does not know DM's private key. Hence, warrant is unforgeable on the basis of private key's security.

Second, only legitimate group member owns private key issued by GM to generate legitimate group signature. Adversary cannot compute legitimate group signature if he does not know group member's private key. As a result, group signature is unforgeable on the basis of private key's security.

Finally, only MC can generate legitimate CBS signature. Adversary cannot compute legitimate CBS signature if he does not know $\text{MC}_{\text{CBS\_SK}}$. Consequently, CBS signature is also unforgeable on the basis of private key's security.

5.2 Performance analysis

We use NS2 (Network Simulation version2) [14–17] to simulate ad hoc on-demand distance vector routing (AODV) protocol, our proposed scheme(HPAA) and JSEN [6]. We analyze the access authentication efficiency of these schemes in terms of handover delay.

According to the scenario defined in Fig. 1, the experimental environment is constructed within a rectangular area of 1000 m × 1000 m as shown in Fig. 5. MAC layer is assumed to be 802.11 MAC protocol. AODV is adopted as routing protocol. The simulation is under wireless environment as AODV does not support promiscuous mode between cable and wireless. FTP traffic flow is built between MC and CN through TCP at application layer, which begins at 1.0 s and finishes at 88.0 s. When simulation begins, MC moves from MR1 to MR4 at the speed of 10 m/s. The simulation time is 90 s. In the whole simulation, MC handovers three times. (1) MC moves from MR1 to MR2. Initial authentication protocol is executed among MC, MR2, and GW2; (2) MC leaves MR2 for MR3. Handover authentication occurs between MC and MR3; (3) MC moves on from MR3 to MR4. Inter-domain authentication protocol is triggered.

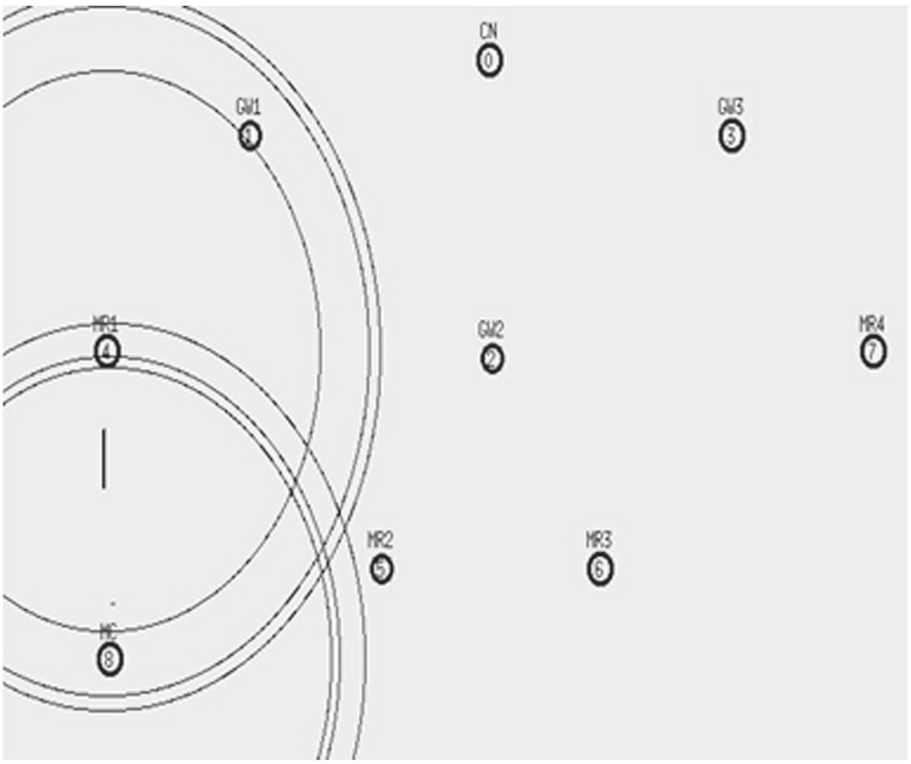

Fig. 5 NS2 simulation scenario

5.2.1 Handover delay analysis

Handover delay is defined as a kind of communication interrupt between CN and MC when handover occurs. Handover delay can be analyzed through the serial number and receiving time of the TCP packet from CN to MC. Simulations are done for AODV, JSEN, and HPAA to observe their differences in handover delay. In order to eliminate the error and interference, all the experimental results are the average value of 20 times' simulation.

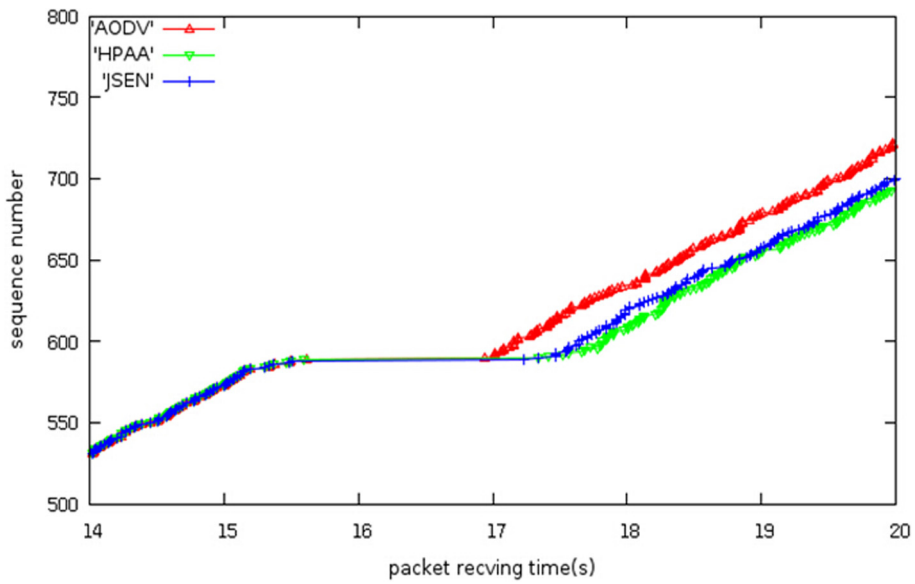

Fig. 6 Relationship between serial number and receiving time (first handover)

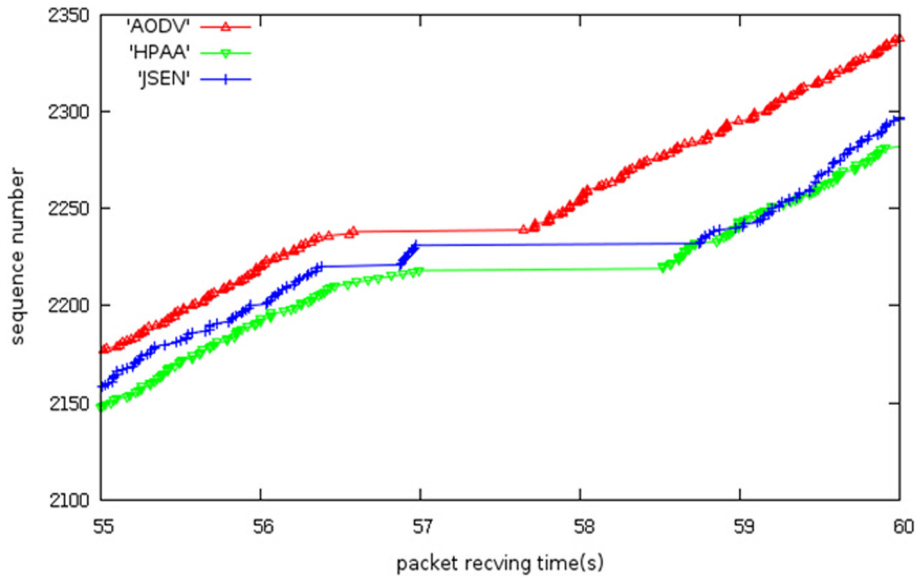

Fig. 7 Relationship between serial number and receiving time (second handover)

Figure 6 shows the results when MC handovers for the first time. The handover delay of AODV, JSEN, and HPAA is 1.2, 2.1, and 1.8 s, respectively. Figure 7 shows the simulation results when MC handovers for the second time. The handover delay of AODV, JSEN, and HPAA is 1.1, 1.7, and 1.5 s, respectively. Figure 8 shows the simulation results while MC handovers for the third time. The handover delay of AODV, JSEN, and HPAA is 1.2, 2.2, and 2.1 s, respectively.

From the above results, we can draw the following conclusions. Mutual authentication is introduced in HPAA and JSEN together with some specific signature scheme for privacy protection. Compared with AODV, which has no concern of privacy-preserved authentication, the handover delay of HPAA and JSEN is obviously higher. However, the handover delay of HPAA is superior to JSEN, even approaches AODV with average 0.6 s higher, due to the introduction of CBS, shared-key negotiation method,

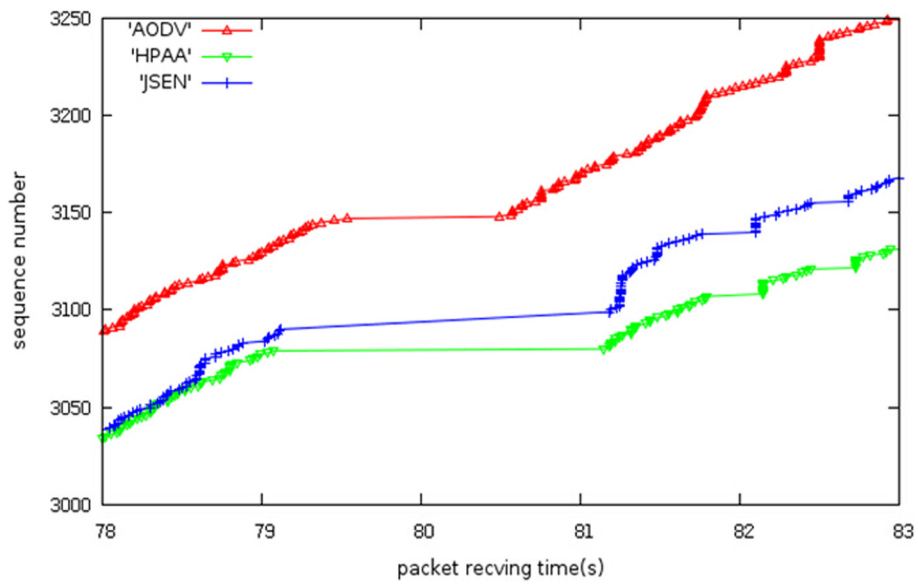

Fig. 8 Relationship between serial number and receiving time (third handover)

and other optimizations during the handover authentication procedure.

6 Conclusions

Our scheme is different from other similar works because we combined the proxy group signature and identity-based group signature. And it has high efficiency and has less expense for saving and maintaining a routing table.

In this paper, we propose a proxy-based authentication scheme which is aimed at anonymous authentication for WMN. The scheme owes the following advantages.

(1) MC's privacy is safe due to the anonymous authentication;
(2) The interactions are eliminated between home network and access network. This is because identity-based proxy group signature scheme makes a great effect;
(3) The authentication delay no longer exists because of the implementation of efficient handover authentication by CBS.

Security and performance analysis show that our scheme is secure and efficient. How to integrate our scheme into the existed authentication protocol forms [18–20] our future research work.

Acknowledgements
This work was supported by the National Natural Science Foundation of China under Grant No. 61300196, 61402095, and China Fundamental Research Funds for the Central Universities under Grant No. N130817002, N120404010.

Competing interests
The authors declare that they have no competing interests.

Received: 30 March 2016 Accepted: 9 August 2016
Published online: 24 August 2016

References

1. Z Wang, Ma Maode, W Liu, X Wei, A unified security framework for multi-domain wireless mesh networks [J]. Lect. Notes Comput. Sci. **7043**, 319-329 (2011)
2. R Di Pietro, S Guarino, NV Verdeb, J Domingo-Ferrerc, Security in wireless ad-hoc networks - A survey [J]. Int. J. Comput. Commun. **51**(10), 1-20 (2014)
3. T Gao, N Guo, K Yim, Q Wang, PPS: A Privacy-Preserving Security Scheme for Multi-operator Wireless Mesh Networks with Enhanced User Experience [J]. Sci. Inf. Syst. **11**(3), 975–999 (2014)
4. Z Wang, WJ Liu, A Wireless mesh network authentication method based on identity based signature [C]. International Conference on Wireless Communications, NETWORKING and Mobile Computing. **46**, 1-4 (2009)
5. R Li, L Pang, Q Pei, Anonymous communication in wireless mesh network[C]. Comput. Intell. Secur. Int. Conf. IEEE. **2**, 416–420 (2009)
6. J Sen, Secure and Privacy-Preserving Authentication Protocols for Wireless Mesh Networks [M]. Applied Cryptography and Network Security, ISBN: 978-953-51-0218-2, InTech, 3-34 (2012)
7. A Shamir, in *Proceedings of CRYPTO '84*. Identity-based cryptosystems and signature schemes[C]. Advances in Cryptology (Springer, Berlin Heidelberg, 1985), pp. 47-53
8. VS Miller, in *Advances in Cryptology Proceedings of CRYPTO'85*. Use of elliptic curves in cryptography[C] (Springer, Berlin Heidelberg, 1986), pp. 417-426
9. KL Wu, J Zou, XH Wei, et al., Proxy group signature: a new anonymous proxy signature scheme[C]. International Conference on Machine Learning and Cybernetics. **3**, 1369-1373 (2008)
10. D Liang, X Guo-Zhen, An ID-based group signature scheme [J]. Comput. Sci. **32**(11), 69–71 (2005)
11. BG Kang, JH Park, SG Hahn, *A certificate-based signature scheme [M]. Topics in Cryptology*. (Springer, Berlin Heidelberg, 2004), pp. 99-111
12. T GAO, N GUO, ZL ZHU, Access authentication for HMIPv6 with node certificate and identity-based hybrid scheme[J]. J. Softw. **23**(9), 2465–2480 (2012)
13. D Boneh, M Franklin, *Identity-based encryption from the Weil pairing[C]. Advances in Cryptology*. (Springer, Berlin Heidelberg, 2001), pp. 213–229
14. A Ortega, et al., Proposal DNP3 protocol simulation on NS-2 in IEEE 802.11g wireless network ad hoc over TCP/IP in smart grid applications [C]. Innovative Smart Grid Technologies. **3**, 25–31 (2015)
15. B LI, G-g ZHANG, J-j ZHAO, Research and simulation of wireless mesh network model [J]. Comput. Simul. (4), 270–273 (2013)
16. S ZHENG, W-q WU, Q-y ZHANG, N-t ZHANG, Routing protocol based on energy aware in ad hoc network[J]. J. Commun. **33**(04), 9–16 (2012)
17. S Xu, Y Yang, Protocols simulation and performance analysis in wireless network based on NS2 [C]. International Conference on Multimedia Technology. **1**, 638–641 (2011)
18. A Skovoroda, D Gamayunov, Securing mobile devices: malware mitigation methods [J]. J. Wirel. Mob. Netw. Ubiquit. Comput. Dependable Appl. (JoWUA). **6**(2), 78–97 (2015)
19. L Nkenyereye, BA Tama, Y Park, KH Rhee, A fine-grained privacy preserving protocol over attribute based access control for VANETs [J]. J. Wirel. Mob. Netw. Ubiquit. Comput. Dependable Appl. (JoWUA). **6**(2), 98–112 (2015)
20. K Sun, Y Kim, Flow mobility management in PMIPv6-based DMM (Distributed Mobility Management) Networks[J]. J. Wirel. Mob. Netw. Ubiquit. Comput. Dependable Appl. (JoWUA). **5**(4), 120-127 (2014)

Submit your manuscript to a SpringerOpen journal and benefit from:

► Convenient online submission
► Rigorous peer review
► Immediate publication on acceptance
► Open access: articles freely available online
► High visibility within the field
► Retaining the copyright to your article

Submit your next manuscript at ► springeropen.com