Wang et al. EURASIP Journal on Wireless Communications and Networking (2018) 2018:200
https://doi.org/10.1186/s13638-018-1217-z

EURASIP Journal on Wireless Communications and Networking

RESEARCH

Open Access

An anonymous batch handover authentication protocol for big flow wireless mesh networks

Dongcheng Wang[1,2], Li Xu[1,2*], Feng Wang[1,2] and Qikui Xu[3]

Abstract

Wireless mesh network (WMN), as a new generation of wireless network technology, has raised increasing concerns in recent years. Due to the strong mobility nature of the clients in WMNs, the handover events frequently occur. Therefore, taking into consideration the openness of the wireless communication channel, the handover authentication protocols for WMNs have to be both efficient and secure, which remains a challenge. In this paper, an anonymous batch handover authentication protocol is proposed using group signature technique to pre-distribute handover keys. Unlike existing protocols based on group signature, the proposed protocol does not involve group signature correlation operations in the handover authentication phase, hence achieving a better performance.

Keywords: Wireless mesh networks, Handover authentication, Privacy-preserving, Bath authentication

1 Introduction

With the explosive growth of the number of mobile devices and their widespread use in our daily life, more and more wireless network architectures have been proposed in order to provide better network access services. As one of the key technologies of the new generation of wireless networks, wireless mesh networks (WMNs) have been widely recognized and applied in recent years. WMNs consist of a number of mesh routers (MRs) and mesh clients (MCs), and an authentication server (AS), where MRs have powerful resources while MCs have limited resources but strong mobility [1, 2].

With the rapid development of network technology, how to protect users' sensitive data privacy (such as users' location information, patients' symptom information, and users' financial information) is increasingly important [3–6]. Therefore, an anonymous handover authentication protocol is required to ensure that only legitimate MCs access the network without divulging its private information and legitimate MRs provide network access service. An anonymous handover authentication protocol cannot only provide mutual authentication between MCs and MRs, but also produce a session key for secure communication between them.

To assist understanding, a typical WMN handover authentication scenario is shown in Fig. 1, where three types of entities participate in a typical WMN handover authentication scenario, which are mesh clients (MCs), mesh routers (MRs), and an authentication server (AS). A mesh client, MC_i in this scenario, must register in the AS to access the wireless mesh network. After MC_i anonymously accesses the network by connecting to MR_1, it may roam to the new MR (i.e., MR_2). In this process, MC needs to execute the handover authentication protocol in order to prove its legitimacy to MR_2 and access the network. MR_2 will authenticate legitimate MC and reject illegal request. At the same time, MR_2 must prove its legitimacy to MC_i by executing the handover authentication protocol. After a successful handover authentication, a session key is established between the authenticated MC_i and MR_2 to protect the subsequent communication.

Some issues must be taken into account when designing an efficient and secure anonymous handover authentication protocol for WMNs. First, due to the openness of wireless network, an anonymous handover authentication protocol requires a high security level to protect networks

*Correspondence: xuli@fjnu.edu.cn
[1]School of Mathematics and Informatics, Fujian Normal University, Fuzhou, Fujian, China
[2]Fujian Provincial Key Laboratory of Network Security and Cryptology, Fuzhou, Fujian, China
Full list of author information is available at the end of the article

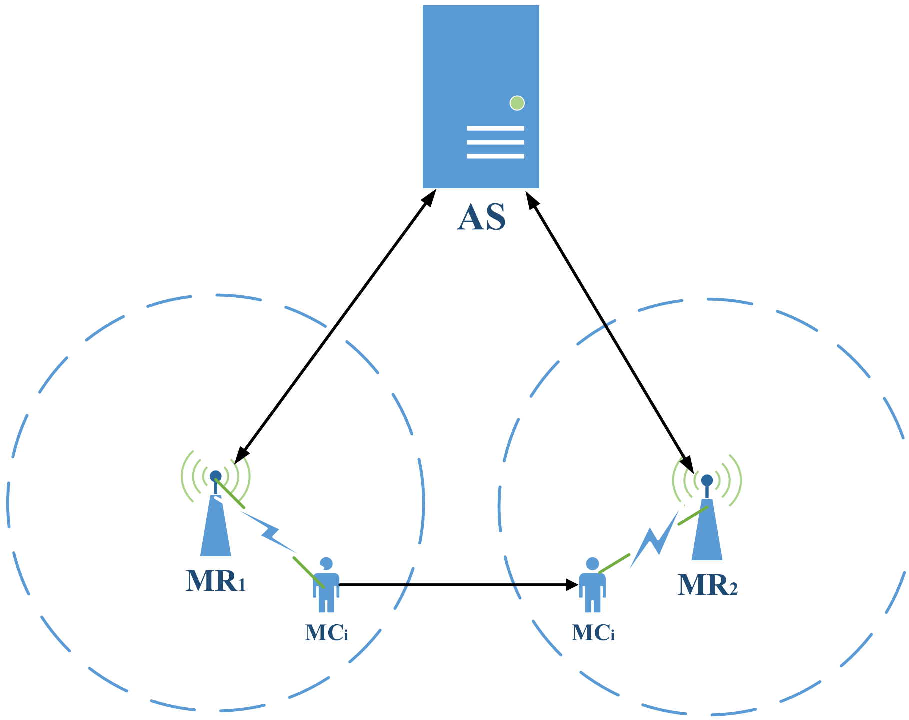

Fig. 1 Typical handover authentication scenario for wireless mesh networks. This figure describes a typical wireless mesh network handover authentication scenario. Three types of entities participate in this scenario, which are mesh clients (MCs), mesh routers (MRs), and an authentication server (AS)

against various attacks. Second, most users prefer a wireless network that provides not only internet services, but also privacy protections such as their identities and locations. Therefore, an anonymous handover authentication protocol should provide privacy protection for users. Last but not least, an anonymous handover authentication protocol must have a high efficiency and low computational complexity, as MCs are generally constrained by limited power and processing capabilities.

1.1 Related work

To guarantee the security of handover authentication process, many handover authentication protocols have been proposed in the last several years. In this section, a brief review of these protocols is provided.

An efficient handover authentication protocol can be implemented by using tickets. In our previous works [7], we presented a handover authentication protocol by using tickets for wireless mesh networks. Li et al. [8] and Li et al. [9] also presented their handover authentication protocols by using tickets to improve performance. In these protocols [7–9], entities pre-apply different kinds of tickets from ticket agents who are trusted by entities to issue and manage tickets. In the handover authentication process, entities authenticate each other by exchanging tickets. The authentication process does not need complex operations such as bilinear pairing and elliptic curve scalar multiplication, so the authentication efficiency is high. However, these protocols do not provide privacy protections, leading to a potential release of users' private information, such as identity, location, and motion trajectory.

To protect users' privacy, Tsai et al. [10], Fu et al. [11], and Zhu et al. [12] respectively presented anonymous handover authentication protocols, which effectively protected the privacy of users from attackers. However, these protocols need at least three-way handshakes to implement the handover authentication process, which is associated with a high communication cost and authentication delay. To improve performances, Yang et al. [13] and He et al. [14] proposed anonymous handover authentication protocols, which only involved two-way handshakes. Later, Yang et al. [13] presented an anonymous handover authentication protocol by using group signature technique, where each access point (AP) is the group manager of an independent group signature system, and in the handover authentication process, mobile clients only need to send a group signature generated by an AP (AP_1) to a new AP (AP_2). If the group signature is valid, AP_2 will authenticate the mobile client; otherwise, AP_2 will reject the request. He et al. [14]

described an anonymous handover authentication protocol by using pseudo identities. Mobile clients pre-apply pseudo identities ($PID_1 \dots PID_n$) from AS. The handover authentication process can be completed only by sending a PID (PID_i). However, both [13, 14] are based on bilinear pairings which have a high computational cost. To achieve a better performance, our previous works [15] and Chaudhry et al. [16] respectively used elliptic curve cryptography (ECC) to construct the protocols. However, both [15, 16] incur high computation overhead at the mobile client side and cannot provide batch authentication as well.

1.2 Our contribution

In this paper, we present a new anonymous handover authentication protocol which has higher efficiency and less computational complexity compared to other related protocols. To be more specific, our main contributions of this paper can be summarized as follows:

- First, we present a new efficient and secure anonymous handover authentication protocol which supports batch authentication using group signature.
- Second, we present an analysis of the computation cost of the proposed anonymous handover authentication protocol and related anonymous handover authentication protocols to demonstrate that ours has a better performance.

1.3 Organization of the paper

The remainder content of this paper is organized as below. The methods that we used are proposed in Section 2. The background of the elliptic curve group and security requirements are proposed in Section 3. The proposed anonymous handover authentication protocol is presented in Section 4. The security analysis and performance evaluation of the proposed anonymous handover authentication protocol are proposed in Sections 5 and 6 respectively. A conclusion is made in Section 7.

2 Methods

Due to the open environment of wireless mesh networks and strong mobility of mesh clients, it is necessary to design a secure and efficient handover authentication protocol to guarantee the quality of network service and to protect mesh clients' privacy. We proposed an anonymous handover authentication protocol based on group signature to improve handover authentication efficiency and to protect mesh clients' privacy in this paper. By using group signature, elliptic curve cryptography(ECC), and message authentication code, the proposed protocol can effectively protect mesh clients' real identity information, locations, and motion trajectory. There are three major participants in the proposed protocol, i.e., authentication server, mesh routers, and mesh clients. In terms of assessment, we used security analysis and performance analysis to measure the quality of the proposed protocol.

3 Preliminaries

3.1 Elliptic curve group

Let F_q be a finite prime number field, E/F_q be an elliptic curve defined over F_q, and P be an element of a large prime order q in E/F_q. The point on E/F_q together with an extra point Θ called the point at infinity form a group $G = \{(x,y) : x,y \in F_q; (x,y) \in E/F_q\} \cup \{\Theta\}$. G is a cyclic additive group of composite order q. Z_q^* is a set of integers which elements are less than the prime number q. Besides, scalar multiplication over E/F_q can be computed as follows: $tP = \underbrace{P + P + \cdots + P}_{t}$.

There exist the following problems over the elliptic curve group.

Computational Diffie-Hellman (CDH) problem: For random chosen values $a, b \in Z_q^*$ and the generator P of G, given aP and bP, it is computationally intractable to compute the value abP.

Decisional Diffie-Hellman (DDH) problem: For random chosen values $a, b, c \in Z_q^*$ and the generator P of G, given aP, bP and cP, it is computationally intractable to verify whether or not $cP = abP$, that is, equal to confirm whether or not $c = ab \bmod q$

3.2 Security requirements

To guarantee a secure communication, an anonymous handover authentication protocol should be able to satisfy the following requirements [17–19]:

1. Mutual authentication: To ensure only legitimate MCs access Internet services through legitimate MRs, an anonymous handover authentication protocol should provide mutual authentication between MCs and MRs.
2. User anonymity: An anonymous handover authentication protocol should provide user anonymity to ensure that MCs are anonymous to adversary including the MRs.
3. Non-traceability: An anonymity handover authentication protocol should be able to support non-traceability to protect MCs being tracked by adversaries.
4. Session key establishment: After implementation of the protocol, MCs will share a session key with MRs to guarantee session security.
5. Revocability: An anonymity handover authentication protocol should be able to allow AS to revoke targeted MCs which break the stipulated regulations.

6 Attack resistance: An anonymity handover authentication protocol should be able to withstand various attacks such as replay attack and man-in-the-middle attack.

4 The proposed anonymous handover authentication protocol

In this section, we propose an anonymous handover authentication protocol for WMNs using group signature with privacy protection.

There are five phases in the proposed protocol: the system initialization phase, the group establishment phase, the pre-distribution of handover authentication key phase, the handover authentication phase, and the batch handover authentication phase.

4.1 System initialization phase

It is assumed that the AS is a trusted third party. Unlike the protocols presented in the paper [13, 14], the proposed protocol does not involve bilinear pairing operations. In the system initialization, the AS executes the following operations to generate system parameters:

1. AS chooses a prime number q and determines the tuple $\{F_q, E/F_q, G, P\}$;
2. AS chooses $x \in Z_q^*$ as the master key and computes the system public key $P_{pub} = x \cdot P$;
3. AS chooses secure hash functions: $H_1 : \{0,1\} \rightarrow Z_q^*, H_2 : \{0,1\}^* \times G \rightarrow Z_q^*$;
4. AS publishes $\{F_q, E/F_q, G, P, P_{pub}, H_1, H_2\}$ as system parameters.

AS generates key pairs for MRs using system parameters and the master key. It is assumed that ID_{MR_j} is MR$_j$'s unique identity. AS randomly chooses $r_{MR_j} \in Z_q^*$ and computes $R_{MR_j} = r_{MR_j} \cdot P$, $h_{MR_j} = H_2\left(ID_{MR_j}, R_{MR_j}\right)$ and $s_{MR_j} = r_{MR_j} + x \cdot h_{MR_j}$. Then, AS sends (s_{MR_j}, R_{MR_j}) to MR$_j$ over a secure channel. On receiving it, MR$_j$ computes the public key $PK_{MR_j} = s_{MR_j} \cdot P$ and publishes PK_{MR_j}.

4.2 Group establishment phase

Unlike the protocol presented in paper [13], we just add routers to the group. Therefore, the MC is not involved in the group signature operation.

1. Let AS be the group manager of an independent group signature system. AS executes the key generation algorithm to generate the group key pair (G_{msk}, G_{pub}) and MR$_j$'s group private key G_{sk_j}. Then, AS sends G_{sk_j} to MR$_j$.
2. Let MR$_j$ be the group member and save the group private key received from AS securely.

Different group signature schemes can be selected according to the network capabilities.

4.3 Pre-distribution of handover authentication key phase

If the users connect to the network for the first time, they have to execute traditional authentication protocols (e.g., IEEE 802.1x standard) or other access authentication protocols. In our protocol, when a MC (MC$_i$) anonymous accesses the network by connecting to a MR (MR$_1$) for the first time, it has to execute the access authentication protocol proposed in [20]. Then, it would share a session key (*SSK*) with the MR$_1$. In order to improve the handover efficiency, as shown in Fig. 2, MC$_i$ can pre-calculate the handover key (*HDK*) and securely send it to MR$_1$. After receiving it, MR$_1$ sends it to neighbor routers. Due to the characteristics of the group signature, the proposed protocol can effectively protect the users' privacy comparing with the protocols proposed in the paper [7–9].

1. MC$_i$ randomly selects $a, b \in Z_q^*$ and computes $A = a \cdot P, B = b \cdot P, m = Enc_{SSK}(A||B)$. Then, MC$_i$ sends m to MR$_1$.
2. After receiving m, MR$_1$ uses the session key (*SSK*) to decrypt it. $A, B = Dec_{SSK}(m)$. Then, MR$_1$ generates a valid group signature of A, B. $\delta = Sig_{G_{sk_1}}(A||B)$. Note that δ is the signature of A and B. It is assumed that MR$_1$ has m neighbor routers. Finally, MR$_1$ uses neighbor routers' public keys to encrypt δ. $\zeta_j = Enc_{P_{MR_j}}(\delta||A||B)(j = 1, \ldots, m)$. Then, MR$_1$ sends ζ_j to MR$_j$. If MC$_i$ accesses the network for the first time, MR$_1$ encrypts A, B, and *SSK* using system public key P_{pub} and sends it to AS; otherwise, MR$_1$ encrypts the previous handover key (A', B') and (A, B) using system public key P_{pub} and sends it to AS.
3. After receiving ζ_j, MR$_j$ decrypts it using sk_{MR_j} to obtain $\delta, A, B = Dec_{sk_{MR_j}}(\zeta_j)$ and using group public key to verify δ. If the signature δ is valid, MR$_j$ saves A and B.

4.4 Handover authentication phase

When roaming to a new MR (MR$_j$), MC$_i$ has to execute the handover authentication process to access the network. In our proposed protocol, as shown in Fig. 3, MC$_i$ and MR$_j$ only need to use the handover key (*HDK*) which is pre-calculated by MC$_i$ and saved in MR$_j$'s buffer to implement mutual authentication. The detailed information exchanging for the handover authentication phase is shown below. In contrast to protocols proposed in the paper [10–12], the presented protocol requires only two-way handshakes to complete the handover authentication process which can effectively reduce the communication cost.

1. $\mathbf{MC}_i \rightarrow \mathbf{MR}_j : \langle \delta_{MC_i}, B, ID_{MR_j}, T_{MC_i} \rangle$
   MC$_i$ selects a time stamp T_{MC_i} and computes $\delta_{MC_i} = a + b \cdot H_1\left(T_{MC_i}, ID_{MR_j}\right)$. MC$_i$ sends the

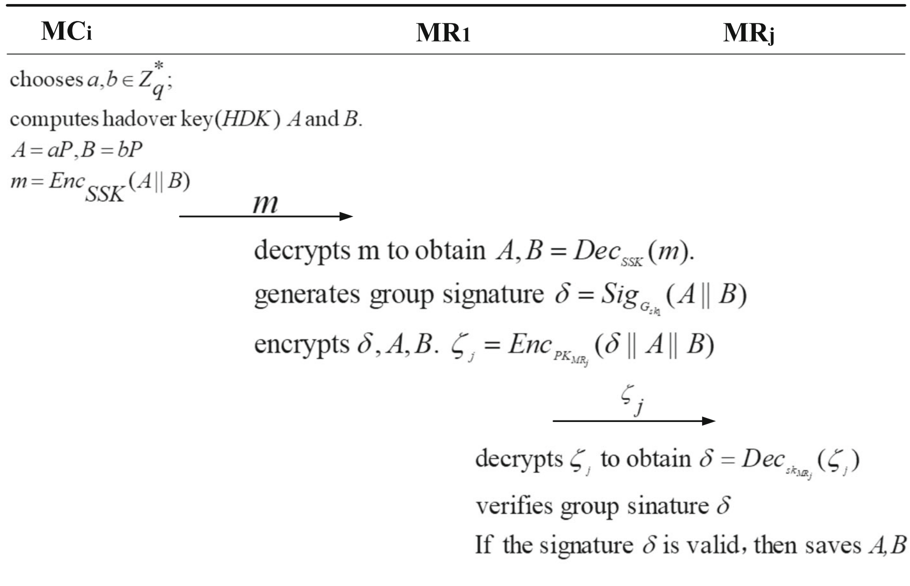

Fig. 2 Pre-distribution of handover authentication key phase. This figure describes the parameters exchanged in the pre-distribution of handover authentication key phase

authentication request $\langle \delta_{MC_i}, B, ID_{MR_j}, T_{MC_i} \rangle$ to MR$_j$ over a public channel.

2 $\mathbf{MR}_j \rightarrow \mathbf{MC}_i : \langle MAC_{MR_j}, T_{MR_j}, ID_{MR_j}, B, C \rangle$
After receiving authentication request message $\langle \delta_{MC_i}, B, ID_{MR_j}, T_{MC_i} \rangle$, MR$_j$ checks if T_{MC_i} is fresh. If not, MR$_j$ rejects the process; otherwise, MR$_j$ checks whether $\delta_{MC_i} \cdot P = A + H_1(T_{MC}, ID_{MR_i}) \cdot B$ holds or not. If not, MR$_j$ rejects the session and, otherwise, authenticates MC$_i$ and randomly selects $c \in Z_q^*$, and computes $C = c \cdot P$. After then, MR$_j$ computes $SSK_{MR_j} = c \cdot A$ as the session key. Then, MR$_j$ selects a time stamp T_{MR_j} and computes $MAC_{MR_j} = H_2(A, B, C, ID_{MR_j}, T_{MR_j})$. MR$_j$ sends $\langle MAC_{MR_j}, T_{MR_j}, ID_{MR_j}, B, C \rangle$ to MC$_i$.

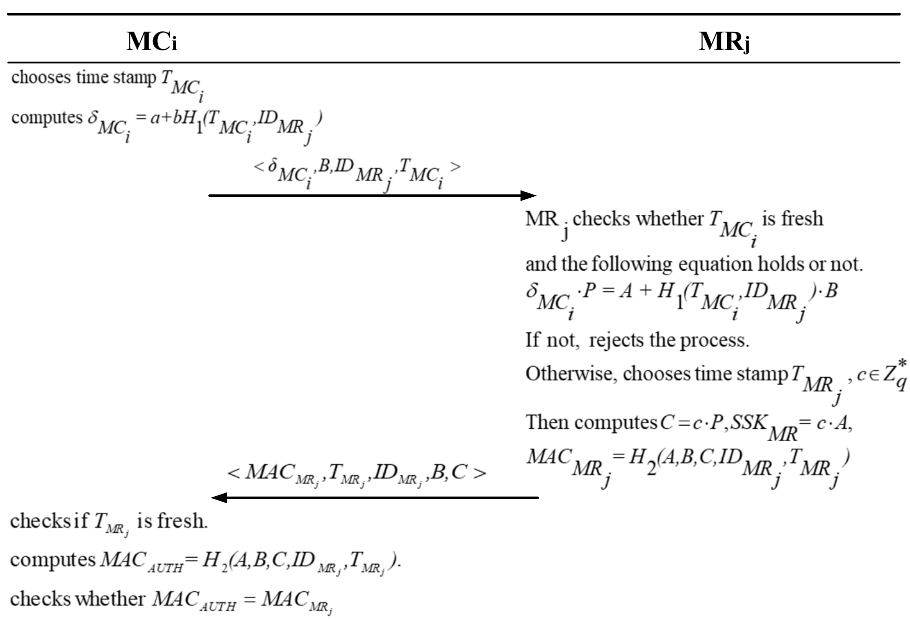

Fig. 3 Handover authentication phase. This figure describes the parameters exchanged in the handover authentication phase

3 After receiving response message $\langle MAC_{MR_j}, T_{MR_j}, ID_{MR_j}, B, C\rangle$, MC_i checks if T_{MR_j} is fresh. If not, MC_i rejects the process; otherwise, MC_i computes $MAC_{AUTH} = H_2(A, B, C, ID_{MR_j}, T_{MR_j})$. MC_i will reject MR_j's response if $MAC_{MR_j} \neq MAC_{AUTH}$ and, otherwise, authenticates MR_j and computes $SSK_{MC} = a \cdot C$ as the session key.

4.5 Batch handover authentication phase

A mesh router MR_j receives a mount of handover authentication request messages simultaneously when the number of MCs is too large. The presented protocol can support batch authentication. Upon receiving n request messages $\{\delta_{MC_k}, B_k, ID_{MR_j}, T_{MC_k}\}, (k = 1, 2 \ldots, n)$, MR_j runs the following process to verify the validity of those request messages simultaneously.

1 After receiving n authentication request messages $\{\delta_{MC_k}, B_k, ID_{MR_j}, T_{MC_k}\}$, $(k = 1, 2 \ldots, n)$, MR_j checks if T_{MC_k} is fresh. If not, MR_j rejects the process;
2 MR_j checks whether Eq. (1) holds or not. If not, MR_j rejects the session;

$$(\delta_{MC_1} + \delta_{MC_2} + \ldots + \delta_{MC_n}) \cdot P = \sum_{k=1}^{n}(A_k) + \sum_{k=1}^{n}(H_1(T_{MC_k}, ID_{MR_j}) \cdot B_k) \tag{1}$$

Therefore, the presented anonymous handover authentication protocol is able to provide batch verification, which will reduce the amount of calculations by half.

5 Security analysis

This section shows that the presented protocol supports the security requirements given in Section 3.

5.1 Mutual authentication and session key establishment

After a MC (MC_i) anonymously accesses the network, in order to improve the handover efficiency, MC_i chooses $a \in Z_q^*$ and computes $A = a \cdot P$. Then, MC_i sends A to MR_1 which is providing network access services for it, and MR_1 sends A to neighbor routers by executing the process given in Section 4. In the handover authentication phase, MC_i uses a to generate a signature and sends the request authentication message to a new MR (MR_j). As the parameter a is chosen by MC_i, only MC_i can use a to generate a valid signature that can be verified using A. Simultaneously, as mentioned in Section 4, only an authorized MR can decrypt the ciphertext and obtain A. Therefore, only a legitimate MR can generate a valid response message MAC_{MR_j} to prove itself. Hence, the mutual authentication can achieve in the proposed protocol. If MC_i and MR_j authenticate each other, they will compute the session key like this: $SSH_{MC} = a \cdot C = c \cdot A = SSK_{MR}$. This session key exchanging process is accomplished based on CDH problem.

5.2 User anonymity

In order to protect MCs' privacy, in the pre-distribution of handover authentication key phase, MCs choose a different parameter to compute the handover key (HDK) each time, and those parameters are not related. In the handover authentication phase, the information that the authentication process interacts does not involve MCs' real identity information. Therefore, the proposed protocol can effectively protect MCs' privacy.

5.3 Non-traceability

In the pre-distribution of handover authentication key phase, when the MR (MR_1) receives a handover key (HDK) from the MC (MC_i), it generates a valid group signature over HDK and encrypts it by using its neighbor routers' public keys. Finally, MR_1 anonymously sends ciphertext to its neighbor routers. Due to the characteristic of group signature, in the handover authentication phase, adversaries and other MRs cannot know which mesh router this MC is switching from. Therefore, it can protect MCs' trajectory privacy. At the same time, adversaries and the MRs are unable to determine if the two authentication processes belong to the same MC.

5.4 Revocability

In the handover authentication phase, MR_j uses the handover key $\left(A'\right)$ which saves in its buffer to verify the legitimacy of the MC (MC_i). After then, MC_i pre-computes another handover key (A) for next handover authentication interacting with MR_j during the communication session, and MR_j uses AS's public key P_{pub} to encrypt $\left(A', A\right)$ and sends it to AS. This can help the AS revoke the targeted MC when the MC breaks the laws or violates the stipulated regulations.

5.5 Replay attack and man-in-the-middle attack

In the wireless environment, the proposed protocol should be able to resist various types of attacks. For eavesdropping, adversaries can capture the data package that transmits between MRs and MCs. However, they cannot acquire the content of packets. This is due to the fact that the content of packets are encrypted by the SSK. In terms of replay attack, MCs add a time stamp in the signature to constitute a request message while MRs add a time stamp in the response message too. Therefore, due to the time stamp, any replay messages must be beyond the service expiration time in the proposed protocol. If the adversaries update the time stamp T_{MC}, the verification of signature will fail due to the different T_{MC}. Additionally,

Table 1 Performance analysis and comparison of each protocol

Protocols	Tsai et al. [10]	Yang et al. [13]	Su et al. [15]	Islam et al. [21]	Our protocol
T_H	2	3	2	2	2
T_P	1	0	0	0	0
T_E	9	4	5	8	3
Batch	Yes	No	No	No	Yes
Comput.cost (ms)	39.93	8.84	11.05	17.86	6.63

the man-in-the-middle attack also has been solved in our protocol. The session key exchange in our protocol is designed based on the CDH. Both the MR and MC exchange packets by checking the Diffie-Hellman public components and generate session keys, which can achieve mutual authentication in the proposed protocol. Thus, the attacker cannot implement the man-in-the-middle attack successfully.

6 Performance analysis result and discussion

An anonymous handover authentication protocol should not only be able to support the security requirements to protect MCs' privacy and resist attacks, but also have high efficiency. In this section, the performance of our protocol was evaluated and compared with other closely related protocols [10, 13, 15, 21]. The evaluation and comparison results show in Table 1. For convenience, some notations are defined as follows:

- T_H: the communication cost between the MC and MR
- T_P: the time complexity of bilinear pairing operation
- T_E: the time complexity of elliptic curve scalar multiplication operation
- *Batch*: supports bath authentication or not

In handover authentication protocol, re-authentication delay refers to from beginning to the end of the handover authentication phase. Here we do not consider those efficient operations that have little effect on the handover authentication delay (such as hash evaluation and so on) and communication costs are directly determined by the number of communications between the MC and the MR. Hence, we analyzed our communication costs by comparing the number of handshake times (T_H) with other protocols. From Table 1, we can see that [13] needs three-way handshake in handover authentication, while others only take two-way handshake. In terms of the computation cost, compared with [10], our protocol cannot only complete a handover authentication without complex bilinear pairing operation, but also take less T_E operations. Besides, the computation cost is obviously reduced in our protocol compared with other related protocols [15, 21]. The proposed protocol only needs to take two T_E operations to complete a handover authentication process, while [15, 21] must take five and eight respectively. Additionally, only the protocol presented in Tsai et al. [10] and our protocol can support batch authentication which can substantially reduce computation load. According to [22], the running time of pairing operations T_P and elliptic curve scalar multiplication operation T_E are about 20.04 ms and 2.21 ms. As shown in Table 1, the total handover authentication delay of the protocol we put forward is about $2T_H + 6.63$ ms, and [10, 13, 15, 21] are about $2T_H + 39.93$ ms, $3T_H + 8.84$ ms, $2T_H + 11.05$ ms, and $2T_H + 17.86$ ms respectively. Therefore, from the performance analysis, we can conclude that the proposed protocol achieves a better performance than other closely related ones [10, 13, 15, 21].

7 Conclusions

In this paper, we propose a security and high efficiency anonymous handover authentication protocol for wireless mesh networks. By using group signature and message authentication code, the proposed protocol can effectively protect mesh clients' real identity information, locations, and motion trajectory. Through security and performance cost analysis, the proposed protocol has been proven to meet security requirements and computational efficiency.

Abbreviations

AP: Access point; AS: Authentication server; CDH: Computational Diffie-Hellman; DDH: Decisional Diffie-Hellman; ECC: Elliptic curve cryptography; MC: Mesh client; MR: Mesh router; WMN: Wireless mesh network

Funding

This work was supported by the National Natural Science Foundation of China (Grant No. 61771140, No. 61702100, No. U1405255), Natural Science Foundation of Fujian Province (Grant No. 2013J01222 and No. 2016J01287), Fujian Normal University Innovative Research Team (Grant No. IRTL1207), Fujian Province Department of Education Project (Grant No. JAT160123), Fuzhou Science and Technology Bureau Project (Grant No. 2015-G-59), and Fujian Province University industry Cooperation of Major Science and Technology Project (Grant No. 2017H6005). China Postdoctoral Science Foundation (No. 2017M612107, No. 2018T110636).

Authors' contributions

WDC, XL, and WF designed and analyzed the anonymous batch handover authentication protocol for big flow wireless mesh networks. XQK participated in the discussion of protocol designed and modified the English expressions. All authors read and approved the final manuscript.

Competing interests

The authors declare that they have no competing interests.

Publisher's Note

Author details

[1]School of Mathematics and Informatics, Fujian Normal University, Fuzhou, Fujian, China. [2]Fujian Provincial Key Laboratory of Network Security and Cryptology, Fuzhou, Fujian, China. [3]Faculty of Science, The University of Sydney, Sydney, New South Wales, Australia.

Received: 20 January 2018 Accepted: 30 July 2018
Published online: 13 August 2018

References

1. T Fowler, Mesh networks for broadband access. IEE Rev. **47**(1), 17–22 (2001)
2. IF Akyildiz, X Wang, W Wang, Wireless mesh networks: a survey. Comput. Netw. **47**(4), 445–487 (2005)
3. Y Yang, X Zheng, X Liu, S Zhong, Chang V, Cross-domain dynamic anonymous authenticated group key management with symptom-matching for e-health social system. Futur. Gener. Comput. Syst. **84**, 160–176 (2018)
4. D He, S Chan, M Guizani, Handover authentication for mobile networks: security and efficiency aspects. IEEE Netw. **29**(3), 96–103 (2015)
5. Y Yang, X Zheng, W Guo, X Liu, Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system. Inf. Sci, 1–26 (2018). https://doi.org/10.1016/j.ins.2018.02.005
6. Y Yang, X Liu, RH Deng, Y Li, Lightweight sharable and traceable secure mobile health system. IEEE Trans. Dependable Secure Comput. (2017). https://doi.org/10.1109/TDSC.2017.2729556
7. L Xu, Y He, X Chen, X Huang, Ticket-based handoff authentication for wireless mesh networks. Comput. Netw. **73**, 185–194 (2014)
8. C Li, UT Nguyen, HL Nauyen, MN Huda, Efficient authentication for fast handover in wireless mesh networks. Comput. Secur. **37**, 124–142 (2013)
9. GG Li, X Chen, JF Ma, in *Proceedings of the 6th IEEE International Conference on Wireless Communications Networking and Mobile Computing, WiCOM2010, Chengdu, Sichuan, China, September 23-25, 2010*. A ticket-based re-authentication scheme for fast handover in wireless local area networks, (2010), pp. 1–4
10. J Tsai, N Lo, Provably secure anonymous authentication with batch verification for mobile roaming services. Ad Hoc Networks. **44**, 19–31 (2016)
11. A Fu, Y Zhang, Z Zhu, Q Jing, J Feng, An efficient handover authentication scheme with privacy preservation for IEEE 802.16m network. Comput. Secur. **31**(6), 714–749 (2012)
12. H Zhu, X Lin, M Shi, P Ho, X Shen, PPAB: a privacy-preserving authentication and billing architecture for metropolitan area sharing networks. IEEE Trans. Veh. Technol. **58**(5), 2529–2543 (2009)
13. G Yang, Q Huang, DS Wong, X Deng, Universal authentication protocols for anonymous wireless communications. IEEE Trans. Wirel. Commun. **9**(1), 168–174 (2010)
14. D He, D Wang, Q Xie, K Chen, Anonymous handover authentication protocol for mobile wireless networks with conditional privacy preservation. Sci. China Inf. Sci. **60**(5), 1–17 (2017)
15. B Su, L Xu, F Wang, Z Lin, An anonymity handover authentication protocol based on group signature for wireless mesh network. J. Commun. **37**, 174–179 (2016)
16. SA Chaudhry, MS Farash, H Naqvi, SH Islam, T Shon, A robust and efficient privacy aware handover authentication scheme for wireless networks. Wirel. Pers. Commun. **93**(2), 311–33 (2017)
17. D He, C Chen, S Chan, J Bu, Secure and efficient handover authentication based on bilinear pairing functions. IEEE Trans. Wirel. Commun. **11**(1), 48–53 (2012)
18. Q Han, Y Zhang, X Chen, H Li, J Quan, in *Network and System Security - 6th International Conference, NSS 2012, Wuyishan, Fujian, China, November 21–23, 2012. Proceedings*. Efficient and robust identity-based handoff authentication in wireless networks, (2012), pp. 180–191
19. Z Wan, K Ren, B Preneel, in *Proceedings of the First ACM Conference on Wireless Network Security, WISEC 2008, Alexandria, VA, USA, March 31 - April 02, 2008*. A secure privacy-preserving roaming protocol based on hierarchical identity-based encryption for mobile networks, (2008), pp. 62–67
20. Z Zhang, Q Qi, N Kumar, N Chilamkurti, H Jeong, A secure authentication scheme with anonymity for session initiation protocol using elliptic curve cryptography. Multimed. Tools Appl. **74**(10), 3477–3488 (2015)
21. SH Islam, MK Khan, Provably secure and pairing-free identity-based handover authentication protocol for wireless mobile networks. Int. J. Commun. Syst. **29**(17), 2442–2456 (2016)
22. D He, J Chen, J Hu, An id-based proxy signature schemes without bilinear pairings. Ann. Telecommun. **66**(11–12), 657–662 (2011)