International Journal of Research (IJR) Vol-1, Issue-7, August 2014 **ISSN 2348-6848**

Capable of Handover Certification with Conditional Privacy for Wireless Networks

R. Swathi[1] & S. Mangayarkarasi[2]

[1]M.Phil., Research Scholar , School of Computing Science.
VELS University, Pallavaram. India

[2]Asst. Professor., Research Scholar , School of Computing Science.
VELS University, Pallavaram. India

ABSTRACT

The existing mechanisms for handover authentication is designing a secure authentication module, and protect users' privacy information when they are authenticated by the access points for data access. Further, most existing approaches do not support user revocation. In this paper, we present a secure and efficient authentication protocol named Handauth. Similar to the existing mechanisms but, Handauth provides user authentication and session key establishment. However, compared to other well-known approaches, Handauth not only enjoys both computation and communication efficiency, but also achieves strong user anonymity and untraceablility, forward secure user revocation, conditional privacy-preservation, AAA server anonymity, access service expiration management, access point authentication, easily scheduled revocation, dynamic user revocation and attack resistance.

Keywords—Access Point, privacy, revocation, Handover authentication, wireless networks.

1 INTRODUCTION

NOWADAYS, various wireless networks such as telecommunication systems, roadside-to-vehicle communication systems and WLANs have become widely available and interconnected. To provide seamless access services for mobile users (MUs) (e.g., PDA, laptop computer, smart phone and vehicle) without being limited by the geographical coverage of each access point, handover authentication modules have been deployed. The technology implemented, as shown in Fig. 1, a typical handover authentication scenario involves three parties: mobile users, access points (APs) and an Authentication, Authorization, and Accounting (AAA) server. Before entering the network, an MU selects an AAA server for registration, then subscribes services and connects to an AP for accessing data. When the MU moves from the current AP (i.e., AP1) into a new AP (i.e., AP2), handover authentication should be performed at AP2. Here, the two circles indicate the transmission ranges of AP1 and AP2, respectively. Through handover authentication, AP2 authenticates the MU to protect itself from illegitimate access. At the same time, a session key should be established between the MU and AP2 to protect the user's data against attacks.

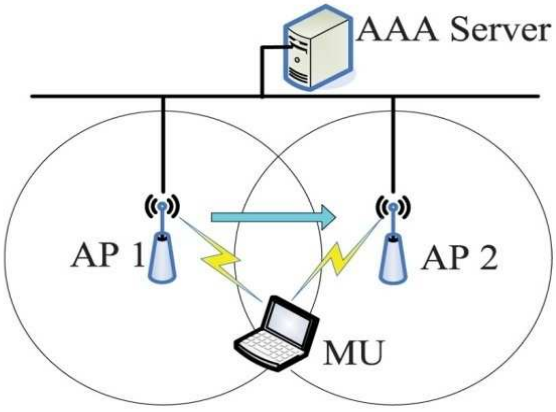

Fig. 1. Handover authentication overview.

2 REQUIREMENTS

A secure and efficient handover authentication protocol should satisfy the following requirements:

2.1. User authentication.

2.2. Session key establishment.

2.3. Low communication cost and computation complexity. In general, an MU does not have sufficient resources in comparison with fixed nodes such as APs. Therefore, a handover authentication process should minimize energy consumption of MUs. Additionally, such a process should be fast enough to maintain persistent connectivity.

2.4. Strong user anonymity and untraceablility. It allows an MU not to expose its private information to eavesdroppers or APs.

2.5. Provision of user revocation mechanism with forward secrecy. Due to some reasons (e.g., the subscription period of a user has expired or a user's secret key has been compromised), handover authentication should allow an AP to find out whether an MU is revoked. At the same time, however, it should also guarantee the anonymity of the revoked user's before the revocation, which means forward secure user revocation.

2.6. Conditional privacy preservation. Although it is desirable to provide strong user anonymity and untraceablility, and also the AAA server to reveal the related private information (e.g., identity, position) of a user in case of emergency.

2.7. AAA server anonymity. The identity of its AAA server should also be hidden from eavesdroppers and the legitimate network entities except the visited AP [17]. Otherwise, the real identity of an MU may be discovered by analyzing the traffic between a visited AP and its AAA server.

2.8. Local access service expiration. With the involvement of the AAA server, each MU should be permitted to access the services only during its subscription period. For example, in mobile phone services, it is necessary for the AAA server to precisely control the service time of an MU according to service payments and managements.

2.9. Local AP validation. Most handover authentication schemes just consider the authentication of MUs by the visited AP. However, it is also important that each MU is able to verify that the visited AP is authorized by the AAA server to offer access services without the help of its AAA server. Otherwise, an imitated AP will easily obtain the private information of the MUs who carelessly connect to it.

2.10. Easily scheduled revocation. To be more practical, it should easily allow a scheduled revocation after which a user will resume the services without reregistering to the AAA server. For example, a user may plan to suspend the services for a few months.

2.11. Provision of dynamic user revocation mechanism. Due to some reasons (e.g., a user's secret key has been compromised or a user has misbehaved), revocation of misbehaving users should take place at any time to prevent these users from the safety of other users and the network provider. Note that different from Requirements 8 and 10, dynamic user revocation occurs before the subscription period of a user expires.

2.12. Attack resistance. Clearly, handover authentication protocol should have ability to

resist various kinds of attacks (e.g., Denial-of-Service (DoS) attacks).

3 THE CRYPTOGRAPHIC PRIMITIVE OF HANDAUTH

A viable approach is for each user to send a login request to the AP through a basic group signature technique. A basic group signature scheme allows one member of the group to sign a message such that any verifier can just verify if the message is originated from a group member without knowing the identity of the actual sender.Only the group manager can lift the anonymity of a signature and reveal the identity of the singer who created it. Group membership is controlled by the group manager, who generates the group's public key and provides individual members with their secret signing keys. To further support user revocation with forward secrecy, the group manager has to change and redistribute the group public key and secret keys of all but the revoked users. Therefore, it incurs enormous loads to no revoked users.

3.1 FSR-GS Technique

A FSR-GS [21] is a tuple *(G.Kg, G.Enroll, G.Revoke, G.Sign, G.Ver, G.Open)* of probabilistic polynomial-time algorithms and one interactive mechanism. The parties involved in the FSR-GS include a group manager, a group member (i.e., a signer) and a verifier.

A more suitable approach is to use forward secure revocable group signature technique. Forward secure revocation allows a revoked group member to preserve the anonymity of its signatures generated before the revocation. However, we observe that although FSR-GS techniques have been proposed by researchers for a long time, most of the existing FSR-GS schemes are not suitable for the construction of efficient handover authentication.

Very recently, the most efficient method of this kind is proposed in [21]. It has constant signing and verifying complexity, and constant size in signature, public key, and signing key. Also it does not require updates of public key or signing key when member joining or leaving occurs.

4 HANDAUTH: THE PROTOCOL

4.1. System Setup Phase: In Handauth, we have the following system setup:

A. The AAA server acts as the group manager of an FSR-GS[21] system and has a master key pair *(mpk, msk)* and the initial membership information. Additionally, the AAAserver also has a signing/verification key pair *(sk, pk)* of a conventional digital signature scheme, e.g., Elliptic Curve Digital Signature Algorithm (ECDSA).

B. The AAA server issues the master public key to all APs. Additionally, each AP shares a session key with the AAA server, respectively.

C. The entire service provision time is divided into time intervals in the unit of hour, day, or month. We assume the AAA server sets day as the interval unit. In this case, the time interval has the format "YYYY/MM/DD." At the beginning of each day, each AP downloads the latest membership information from the AAA server.

D. Each AP has a signing/verification key pair (sk_{AP}, pk_{AP}) of a conventional digital signature scheme, e.g., ECDSA. The ID and public key of each AP are publicly known to all the users who are within the network controlled by the AP. In order that each MU is able to use the verification key (public key of AP) of the AAA server to verify that the serving AP is authorized by the AAA server to offer access services (i.e., Requirement 2.9), the digital certificate should be issued by the AAA server. Alternatively, when subscriber U_i registers to the AAA server, the certificates of all APs are

loaded on U_i (e.g., built in the web browsers of all

subscribers). The visited AP also broadcasts the latest membership information. Suppose for an AAA server, there are currently revoked subscribers. Since, user revocation key of each user U_i is secretly shared between U_i and the AAAserver, no one except the AAA server can learn any information from the membership information.Each MU can verify those two information by using the AAA server's public key .

4.2. New User Joining Phase

Before accessing the network, an MU has to authenticate itself to the AAA server by in-person contact. For subscriber U_i, the AAA server is to generate a user signing key, a (public) user membership key, and a user revocation key .The AAA server delivers all these keys and public key to U_i using a secure transmission protocol (e.g., wired transport layer security protocol). Note that the AAA server maintains a subscriber list, which is composed of every subscriber's related keys (e.g., user membership key, user revocation key) and expiration time. It is clear that different subscribers may have different expiration time. Obviously, the above procedure is invoked whenever a user wants to register with the AAA server.

4.3. Handover Authentication Phase

The handover authentication protocol which is carried out between a mobile user U_i and the visited access point AP2 is as follows. U_i first sends a login request to AP2 for mutual authentication. Then, AP2 checks the validity of U_i, establishes a session key and then gives a response to U_i. Subsequently, U_i validates AP2, establishes the session key and then responds to AP2. Finally, AP2 notifies the AAA server of the authentication result , that satisfy Requirement 2.2. This procedure shows in the Figure - 2,.AP2 uses the secret key to encrypt the group signature message and then delivers it to the AAA server. Upon receiving this message, the AAA server can obtain the identity of U*i*, which means that the AAA server can provide conditional privacy. Thus, it is shown that Handauth can achieve Requirement 2. 6. Since APs only notify the AAA server of the authentication result after performing the handover authentication, this step does not affect the authentication time.

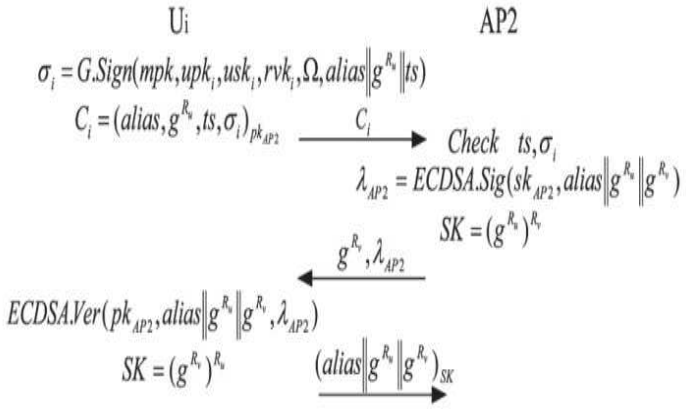

Fig. 2, Authentication procedure of Handauth.

4.4. Supporting Local Access Service Expiration

The AAA server maintains a subscriber list, which is composed of every subscriber's related keys (e.g., user membership key, user revocation key) and expiration time. Once a subscriber U*i*'s service subscription expires, its signing key should be invalidated from then on. In this case, the AAA server needs to updates its membership information. This shows that Handauth can achieve Requirement 2. 8.

4.5. Supporting Scheduled Revocation Easily

In practice, some users may need a predefined revocation period. *For example*, a mobile phone user may want to suspend the services for three months. A natural method is for such a user to reregister to the AAA server and then receive a new user signing key, a new user membership key, and a new user revocation key.Obviously, this method causes inconveniences. Therefore, to address this issue, Handauth provides a feasible approach as follows. We assume that a subscriber U_m is revoked at the interval t1 and hopes to resume the services of the same AAA server with his previous keys (i.e., user signing key, user membership key, and user revocation key) at the interval t_2, where $t_2 > t_1$. Subsequently, U_m resumes the services automatically and exactly at t_2, without the necessity to visit the AAA server. Hence, Handauth can satisfy Requirement 2.10.

4.6. Provision of Dynamic User Revocation Mechanism

There may be misbehaving users in the system. In this case, the AAA server can identify these misbehaving users in step 4 of the handover authentication procedure, and then revoke them. Therefore, Handauth can meet Requirement 2.11.

4.7. Design for Strong User Anonymity & Untraceablility

The restriction on handover authentication with user anonymity is that the standards of current wireless technologies, such as Bluetooth, require manufacturers to assign an identification number (i.e., MAC address) to every device (i.e., Laptop PC). The MAC address is like an annoying tag attached to a mobile device, anytime, and anywhere. Obviously, such a practice exposes the ID of a mobile device at the MAC address. However, current handover authentication techniques do not consider this security issue. For Handauth, this weakness is to replace the MAC address with a user alias. Alias collision should not be a serious problem in this case and can be prevented in many ways, for instance, by adding a time stamp or random number. For example, the packet sizes of the MUs have been exploited to identify different users [23]. Since all existing handover authentication do not consider this issue, they fail to provide user anonymity and untraceability. A feasible way is that each MU should frequently change its physical layer properties or information. For instance, to address this issue, each MU should frequently change its

TABLE
Functionality Comparison between Handauth and Related Work

Protocols	HMZCJ [14]	Scheme of [13]	CHCBGR [16]	SFRIC [10]	method of [11]	CJKY [12]	Handauth
Number of parties	3	3	3	2	2	2	2
Strong user anonymity and untraceablility	No	No	No	No	No	No	Yes
Conditional privacy preservation	Yes	Yes	Yes	No	No	No	Yes
AAA server anonymity	No	No	No	No	No	No	Yes
Local access service expiration	No	No	No	Yes	Yes	Yes	Yes
Local AP validation	No	No	No	No	No	No	Yes
Easily scheduled revocation	No	No	No	No	No	No	Yes
Dynamic user revocation	Yes	Yes	Yes	No	No	No	Yes
Attack-resistance	No	No	No	No	No	No	Yes

frame sequence number, packet size, and signal strength, by using some ways (e.g., random number generator).It satisfy

Requirement2.4.

5 SECURITY ANALYSES

Mutual authentication. AP authentication is done then the user is sure about the identity of the visited AP. Since only AP2 has session key, no other APs can compute a valid digital signature on U_i's. Only the AAA server can generate a valid certificate for AP2, and the identity of AP2 and its public key pk_{AP2} are included the certificate. Therefore, other APs cannot cheat by using different public keys or different IDs. Thus, Handauth can satisfy Requirement 9. Since the group signature message is encrypted using *AP2*'s public key, only AP2 can use its private key to obtain such a group signature message and then obtain the identity of U_i's AAA server. Thus, the identity of *U_i's* AAA server can be hidden from eavesdroppers and the legitimate network entities except the visited AP (i.e., AP2). That is, Handauth can meet Requirement 2.7. Subscriber authentication is achieved only a legitimate subscriber of the AAA server can generate a valid group signature on *Ui's.* Thus, Handauth can satisfy Requirement 2.1. According to the above analysis, Handauth can provide mutual authentication.

Strong user anonymity and untraceablility. An adversary (including eavesdroppers) and APs are not able to obtain the identity of the real signer since they do not have the trace key *tk*, which is preserved only by the AAA server. That is to say, when the handover authentication runs, the visited AP is just able to determine whether an MU is the subscriber of the AAA server, but it cannot derive any further identity information about the MU. User untraceability is also achieved by the anonymity of the group signature.

6 HOW HANDAUTH DIFFERS FROM OTHER NETWORKS

6.1. GSM (Global System for Mobile) In telecommunication systems, the GSM [1] communication system are intended to provide user privacy by using a temporary identity called Temporary Mobile Subscriber Identity (TMSI) to identify an MU. However, a user's real identity called International Mobile Subscriber Identity (IMSI) is sent to the visited AP over the air in plaintext during the authentication process; thus, eavesdroppers over the radio network can easily identify the subscriber by its IMSI. Obviously, GSM cannot satisfy Requirement 2. 4.

6.2. UMTS (Universal Mobile Telecommunication system) The thirdgeneration mobile cellular communication system UMTS [2], though enhanced from GSM, uses the same mechanism to provide anonymity for MUs. That is, UMTS also uses IMSI for the first registration at the visited AP, and obtains some TMSIs for subsequent sessions. Likewise, UMTS cannot achieve Requirement 2. 4.

Finally, we make the functionality comparisons of Handauth and the well-know approaches [10], [11], [12], [13], [14], [16] in the above Table.

7 ADVANTAGES OF HANDAUTH

Thus, once Handauth is built on the scheme of [21], it can achieve scalability and dynamic participation. The time of each protocol run is independent of the number of MUs and revoked users. More specifically, it is constant. Thus, Handauth is efficient even in a large-scale network with many subscribers and many revoked users.

8 CONCLUSIONS

Moreover, we have proposed a novel protocol named Handauth to achieve secure and efficient handover authentication. The protocol satisfies a set of important requirements which have not been addressed by earlier works. The security analysis and

experimental results show that the proposed approach is feasible for real applications.

REFERENCES

[1] European Telecomm. Standards Inst. (ETSI), GSM 02.09: Security Aspects, 1993.

[2] 3rd Generation Partnership Project, 3GPP Specification: 3GPP TS 33.102, 3G Security, Security Architecture, Dec. 2002.

[3] P. Funk and S. Blake-Wilson, "EAP Tunneled TLS Authentication Protocol (EAP-TTLS)," IETF Internet Draft, draft-ietf-pppext-eap-ttls-05.txt, July 2004.

[4] A. Palekar et al., "Protected EAP Protocol (PEAP)," IETF Internet Draft, draft-josefsson-pppext-eap-tls-eap-06.txt, Mar. 2003.

[5] S. Pack and Y. Choi, "Fast Handoff Scheme Based on Mobility Prediction in Public Wireless LAN Systems," Proc. IEE Comm., vol. 151, no. 5, pp. 489- 495, Oct. 2004.

[6] C.-C. Chang, C.-Y. Lee, and Y.-C. Chiu, "Enhanced Authentication Scheme with Anonymity for Roaming Service in Global Mobility Networks," Computer Comm., vol. 32, no. 4, pp. 611-618, 2009.

[7] D. He and S. Chan, "Design and Validation of an Efficient Authentication Scheme with Anonymity for Roaming Service in Global Mobility Networks," Wireless Personal Comm., vol. 61, no. 2, pp. 465-476, 2011.

[8] H. Wang and A.R. Prasad, "Fast Authentication for Inter-domain Handover," Proc. Int'l Conf. Telecomm. (ICT '04), 2004.

[9] J. Choi and S. Jung, "A Secure and Efficient Handover Authentication Based on Light-Weight Diffie-Hellman on Mobile Node in FMIPv6," IEICE Trans. Comm., vol. E-91B, no. 2, pp. 605-608, 2008.

[10] Y. Kim, W. Ren, J. Jo,M. Yang, Y. Jiang, and J. Zheng, "SFRIC: A Secure Fast Roaming Scheme in Wireless LAN Using ID-Based Cryptography," Proc. Int'l Conf. Comm. (ICC '07), 2007.

[11] J. Choi and S. Jung, "A Handover Authentication Using Credentials Based on Chameleon Hashing," IEEE Comm. Letters, vol. 14, no. 1, pp. 54-56, Jan. 2010.

[12] J. Choi, S. Jung, Y. Kim, and M. Yoo, "A Fast and Efficient Handover Authentication Achieving Conditional Privacy in V2I Networks," Proc. Int'l Conf. Smart Spaces and Next Generation Wired/Wireless Networking, S. Balandin et al., eds., pp. 291-300, 2009.

[13] D. He and S. Chan, "A Secure and Lightweight User Authentication Scheme with Anonymity for the Global Mobility Network," Proc. Int'l Conf. Network-Based Information Systems (NBiS '10), pp. 305-312, 2010.

[14] D. He, M. Ma, Y. Zhang, C. Chen, and J. Bu, "A Strong User Authentication Scheme with Smart Cards for Wireless Communications," Computer Comm., vol. 34, no. 3, pp. 367-374, 2011.

[15] C.-C. Chang and H.-C. Tsai, "An Anonymous and Self-Verified Mobile Authentication with Authenticated Key Agreement for Large-Scale Wireless Networks," IEEE Trans. Wireless Comm., vol. 9, no. 11, pp. 3346-3353, Nov. 2010.

[16] C. Chen, D. He, S. Chan, J. Bu, Y. Gao, and R. Fan, "Lightweight and Provably Secure User Authentication with Anonymity for the Global Mobility Network," Int'l J. Comm. Systems, vol. 24, no. 3, pp. 347-362, 2011.

[17] D. Samfat, R. Molva, N. Asokan, "Untraceability in Mobile Networks," Proc. MobiCom '95, pp. 26-36, 1995.

[18] E. Bresson and J. Stern, "Efficient Revocation in Group Signatures," Proc. Conf. Public Key Cryptography (PKC '01), 2001.

[19] T. Nakanishi and Y. Sugiyama, "A Group Signature Scheme with Efficient Membership Revocation for Reasonable Groups," Proc. Australasian Conf. Information Security and Privacy (ACISP '04), 2004.

[20] T. Nakanishi, H. Fujii, Y. Hira, and N. Funabiki, "Revocable Group Signature Schemes with Constant Costs for Signing and Verifying," Proc. Conf. Public Key Cryptography (PKC '09), 2009.

[21] H. Jin, D. Wong, and Y. Xu, "Efficient Group Signature with Forward Secure Revocation," Proc. Int'l Conf. Security Technology (SecTech '09), 2009.

[22] K. Zeng, K. Govindan, and P. Mohapatra, "Non-Cryptographic Authentication and Identification in Wireless Networks," IEEE Wireless Comm., vol. 17, no. 5, pp. 56-62, Oct. 2010.

[23] J. Pang, B. Greenstein, R. Gummadi, S. Seshan, and D. Wetherall, "802.11 User Fingerprinting," Proc. MobiCom '07, pp. 99-110, 2007.