Chapter 36
Comments on "A Robust User Authentication Protocol with Privacy-Preserving for Roaming Service in Mobility Environments"

Xinglan Guo, Lei Yang, Tsu-Yang Wu, Lili Chen, and Chien-Ming Chen

Abstract Roaming service under the global mobile network (GLOMONET) means that users who use mobile devices can still use mobile devices in other regions or countries after leaving their region or country. When mobile users use roaming services, the communication information transmitted by wireless channels is easy to be tampered with and eavesdropped on by attackers. These attacks may expose the identity and location of remote users. Thus, mutual authentication among mobile users, foreign agents, and home agents play an important role. To ensure a secure roaming service in a mobile network, it is necessary to design an efficient and secure solution. Recently, Shashidhara et al. proposed a user authentication protocol for roaming service in the GLOMONET. In this paper, we find that there are some security vulnerabilities in their protocol, including perfect forward secrecy (PFS), key compromise impersonation attacks (KCIA), and known-session-specific temporary information attacks (KTIA).

36.1 Introduction

The rapid development of wireless networks [11] has brought great convenience to people's lives, in which there is a special network environment called global mobility network (GLOMONET) [1, 2, 9, 10, 14]. GLOMONET refers to a new network environment that can provide global roaming service for communication. With the rapid development of communication technologies, mobile users can access the services through roaming technologies. In this environment, the mobile user registers with the home agent. To obtain the service of the foreign network, it needs the help of the home agent to realize the authentication and establish a session secret key [6, 18–20] between the mobile user and the foreign agent. However, the communication transmitted in the mobile network environment is easily vulnerable to various attacks [4]. Thus, it is necessary to protect the privacy of users as well as

X. Guo · L. Yang · T.-Y. Wu (✉) · L. Chen · C.-M. Chen
College of Computer Science and Engineering, Shandong University of Science and Technology, Qingdao 266590, China

T.-Y. Wu et al. (eds.), *Advances in Smart Vehicular Technology, Transportation, Communication and Applications*, Smart Innovation, Systems and Technologies 250,
https://doi.org/10.1007/978-981-16-4039-1_36

to design authentication protocols to ensure the realization of secure communication [5, 7, 12, 15–17, 21].

In 2009, Chang et al. [3] proposed an enhanced authentication protocol to maintain the anonymity of mobile users for roaming services in global mobile networks. However, this protocol cannot guarantee anonymity and confidentiality. To improve their protocol, Zhou et al. [23] proposed a secure authentication protocol. Unfortunately, their protocol is also vulnerable to forgery attacks, replay attacks, and insider attacks. In 2016, Gope et al. [8] proposed an effective authentication protocol. However, the cost of this protocol is computationally expensive. Xu et al. [22] analyzed Gope et al.'s protocol and found that the protocol is vulnerable to replay attacks and clock synchronization problems. Then, a new user authentication protocol is proposed.

Recently, Shashidhara et al. [13] analyzed Xu et al.'s protocol and found that the protocol is vulnerable to denial of service attacks, privileged-insider attacks, and impersonation attacks. To solve these security problems, they further proposed a lightweight user authentication protocol with privacy preservation. In this paper, we analyze Shashidhara et al.'s authentication protocol and point out its security vulnerabilities, including perfect forward secrecy (PFS), key compromise impersonation attacks (KCIA), and known-session-specific temporary information attacks (KTIA).

36.2 Review of Shashidhara et al.'s Protocol

In this section, we review the initialization phase, registration phase, login phase, and authentication phase of the protocol. The symbols used in this protocol are described in Table 36.1.

Table 36.1 Notations

Symbol	Description
$\mathrm{PSW}_{\mathrm{MU}}$	Password of the mobile user
$\mathrm{ID}_{\mathrm{MU}}, \mathrm{ID}_{\mathrm{HA}}, \mathrm{ID}_{\mathrm{FA}}$	Identities of MU, HA and FA
SK_F	Shared-secret key of HA and FA
SK_H	Secret key of HA
K_{MU}	Counter value of MU
SK	Session key
A	Adversary

36.2.1 Initialization Phase

The protocol includes three roles. Mobile User (MU), Foreign Agent (FA), and Home Agent (HA). In the initialization phase, FA obtains a dynamic Diffie–Hellman secret key SK_F from HA, where $\mathrm{SK}_F = h(\mathrm{ID}_{\mathrm{FA}} \parallel \mathrm{SK}_H)$.

36.2.2 Registration Phase

The registration phase of the protocol is that MU registers with HA. The registration of MU follows the following steps.

(1) MU selects identity $\mathrm{ID}_{\mathrm{MU}}$, password $\mathrm{PSW}_{\mathrm{MU}}$ and randomly generates a random number R_M, then MU computes a pseudo identity $\mathrm{AID} = h(\mathrm{ID}_{\mathrm{MU}} \parallel R_M)$, and sends $M_m = \{\mathrm{AID}\}$ to HA through secure channel.

(2) HA computes $\mathrm{RID} = h(\mathrm{AID} \parallel \mathrm{SK}_H)$ after receiving message M_m from MU, and initializes K_{MU} to 0. Then, HA stores $\{\mathrm{AID}, K_{\mathrm{MU}}\}$ in its own database. Finally, HA sends $M_h = \{\mathrm{RID}, K_{\mathrm{MU}}, h(.)\}$ to MU through secure channel.

(3) After MU receives the message M_h from HA, MU computes two values: $\mathrm{AC} = \mathrm{RID} \oplus h(\mathrm{PSW}_{\mathrm{MU}} \parallel R_M)$, $LA = h(\mathrm{ID}_{\mathrm{MU}} \parallel \mathrm{PSW}_{\mathrm{MU}} || R_M)$. Finally, MU stores $\{\mathrm{AC}, \mathrm{LA}, R_M, K_{\mathrm{MU}}\}$ in the smart card.

36.2.3 Login and Mutual Authentication Phase

This is an authentication protocol based on three parties. When MU wants to access a foreign network through roaming service, to ensure secure communication, MU and FA need to be authenticated by HA. The authentication steps are as follows.

(1) First of all, MU enters its own $\mathrm{ID}_{\mathrm{MU}}$ and password $\mathrm{PSW}_{\mathrm{MU}}$ in the smart device, and computes $\mathrm{LA}^* = h(\mathrm{ID}_{\mathrm{MU}} \parallel \mathrm{PSW}_{\mathrm{MU}} \parallel R_M)$ through the R_M obtained from the smart card, then MU verifies $\mathrm{LA}^* \overset{?}{=} \mathrm{LA}$. If equal, login to smart card is successful. Otherwise, the login fails.

(2) After successful login, MU generates a random number N_{MU}, and computes $\mathrm{RID} = \mathrm{AC} \oplus h(\mathrm{PSW}_{\mathrm{MU}} \parallel R_M)$, $A_M = h(\mathrm{ID}_{\mathrm{MU}} \parallel R_M) \oplus N_{\mathrm{MU}}$, $V_1 = h(\mathrm{RID} \parallel K_{\mathrm{MU}}) \oplus N_{\mathrm{MU}}$. Finally, MU transmits the login request $M_1 = \{A_M, V_1, \mathrm{ID}_{\mathrm{HA}}\}$ to FA through public channel.

(3) After receiving the message M_1 from MU, FA generates a random number N_{FA}, and computes $B_M = h(A_M \parallel \mathrm{SK}_F) \oplus N_{\mathrm{FA}}$, $V_2 = h(B_M \parallel \mathrm{SK}_F \parallel V_1)$. FA transmits authentication request $M_2 = \{B_M, V_1, V_2, \mathrm{ID}_{\mathrm{FA}}\}$ to HA through public channel.

(4) After receiving the message M_2 from FA, HA verifies the $\mathrm{ID}_{\mathrm{FA}}$, and if it exists, HA finds the $\mathrm{SK}_F = h(\mathrm{ID}_{\mathrm{FA}} \parallel \mathrm{SK}_H)$ associated with the $\mathrm{ID}_{\mathrm{FA}}$. HA computes

$V_2^* = h(B_M \parallel \mathrm{SK}_F \parallel V_1)$, and verifies $V_2^* \overset{?}{=} V_2$. If equal, HA believes that FA is legal. Otherwise, the certification is terminated. HA computes $\mathrm{RID}^* = h(\mathrm{AID} \parallel \mathrm{SK}_H)$, $N_{\mathrm{MU}}^* = h(\mathrm{RID}^* \parallel K_{\mathrm{MU}}) \oplus V_1$, $V_1^* = h(\mathrm{RID}^* \parallel K_{\mathrm{MU}}) \oplus N_{\mathrm{MU}}^*$ and verifies $V_1^* \overset{?}{=} V_1$. If equal, HA believes that MU is legal. Otherwise, authentication is terminated. HA computes $A_M^* = (\mathrm{AID} \parallel R_M) \oplus N_{\mathrm{MU}}^*$, $N_{\mathrm{FA}}^* = h(A_M^* \parallel \mathrm{SK}_F) \oplus B_M$, $N_M^* = h(\mathrm{RID}^* \parallel N_{\mathrm{MU}}^*) \oplus N_{\mathrm{FA}}$, $V_3 = h(\mathrm{ID}_{\mathrm{HA}} \parallel A_M^* \parallel \mathrm{SK}_F)$, $V_4 = h(\mathrm{RID}^* \parallel \mathrm{ID}_{\mathrm{FA}} \parallel K_{\mathrm{MU}})$. Then HA updates $K_{\mathrm{MU}} = K_{\mathrm{MU}} + 1$ and stores in database of HA. Finally, HA transmits authentication request $M_3 = \{N_M^*, V_3, V_4\}$ to HA.

(5) After receiving authentication request M_3 from HA, FA computes $V_3^* = h(\mathrm{ID}_{\mathrm{HA}} \parallel A_M \parallel \mathrm{SK}_F)$, and verifies $V_3^* \overset{?}{=} V_3$. If it is equal to V_3, FA believes that HA and MU are legal. Otherwise, the communication will be terminated. Then, FA computes $\mathrm{SK} = h(N_{\mathrm{FA}} \parallel A_M \parallel \mathrm{ID}_{\mathrm{HA}})$, and finally FA transmits message $M_4 = \{N_M^*, V_4\}$ to MU.

(6) After receiving message M_4 from FA, MU computes $V_4^* = h(\mathrm{RID} \parallel \mathrm{ID}_{\mathrm{FA}} \parallel K_{\mathrm{MU}})$, and verifies $V_4^* \overset{?}{=} V_4$. If equal, MU believes that FA and HA are legal. Otherwise, the certification is terminated. Then, MU computes $N_{\mathrm{FA}} = h(\mathrm{RID} \parallel N_{\mathrm{MU}}) \oplus N_M^*$, $\mathrm{SK} = h(N_{\mathrm{FA}} \parallel A_M \parallel \mathrm{ID}_{\mathrm{HA}})$, and finally MU updates $K_{\mathrm{MU}} = K_{\mathrm{MU}} + 1$ and stores it in the smart card.

36.3 Statement of the Problem

This paper is about the protocol of Shashidhara et al. In this section, we analyze the protocol and point out three security vulnerabilities, violation of perfect forward secrecy (PFS), key compromise impersonation attacks (KCIA), and known-session-specific temporary information attacks (KTIA). PFS means that although the server's long-term private key is compromised by the adversary (A), the former session keys can also be protected. KCIA refers to that if A can obtain a long-term private key of the user, then A can impersonate as another legitimate user. KTIA means that the exposure of the random number will lead to the exposure of the session key.

In this paper, we suppose A has the following abilities. A can access the public communication channel. And A may obtain a dynamic Diffie–Hellman secret key SK_F from HA, where $\mathrm{SK}_F = h(\mathrm{ID}_{\mathrm{FA}} \parallel \mathrm{SK}_H)$, and direct access a random number N_{FA}.

36.3.1 Perfect Forward Secrecy

To compute the session key, A may follow the following steps.

(1) A can first intercept the login request $M_1 = \{A_M, V_1, \mathrm{ID}_{\mathrm{HA}}\}$ and authentication request $M_2 = \{B_M, V_1, V_2, \mathrm{ID}_{\mathrm{FA}}\}$ transmitted on the public channel. A can

obtain parameters $\{A_M, \mathrm{ID}_{\mathrm{HA}}, B_M, \mathrm{ID}_{\mathrm{FA}}\}$ from the two requests for subsequent computation of session key.

(2) A uses $\{\mathrm{ID}_{\mathrm{FA}}, B_M, A_M\}$ in intercepted message M_2 and SK_H to compute $\mathrm{SK}_F = h(\mathrm{ID}_{\mathrm{FA}} \parallel \mathrm{SK}_H)$, $N_{\mathrm{FA}} = h(A_M \parallel \mathrm{SK}_F) \oplus B_M$ to get the value N_{FA} required for session key computation.

(3) Finally, A can successfully compute $\mathrm{SK} = h(N_{\mathrm{FA}} \parallel A_M \parallel \mathrm{ID}_{\mathrm{HA}})$.

Therefore, the protocol of R. Shashidhara et al. cannot provide PFS.

36.3.2 Key Compromise Impersonation Attacks

To impersonate as a legitimate FA, A may follow the following steps.

(1) Firstly, A can intercept the authentication request $M_2 = \{B_M, V_1, V_2, \mathrm{ID}_{\mathrm{FA}}\}$ and login request $M_1 = \{A_M, V_1, \mathrm{ID}_{\mathrm{HA}}\}$ transmitted on the public channel, and compute $\mathrm{SK}_F^* = h(\mathrm{ID}_{\mathrm{FA}} \parallel \mathrm{SK}_H)$ with SK_H obtained by A.

(2) Then, A generates a random number N'_{FA}, and computes $B'_M = h(A_M \parallel \mathrm{SK}_F^*) \oplus N'_{\mathrm{FA}}$, $V'_2 = h(B'_M \parallel \mathrm{SK}_F^* \parallel V_1)$. A can form an effective authentication request $M'_2 = \{B'_M, V_1, V'_2, \mathrm{ID}_{\mathrm{FA}}\}$ and send it to HA.

(3) After receiving the message M'_2 from A, HA verifies the $\mathrm{ID}_{\mathrm{FA}}$, and if it exists, HA finds the $\mathrm{SK}_F^* = h(\mathrm{ID}_{\mathrm{FA}} \parallel \mathrm{SK}_H)$ associated with the $\mathrm{ID}_{\mathrm{FA}}$. HA computes $\mathrm{SK}_F^* = h(\mathrm{ID}_{\mathrm{FA}} \parallel \mathrm{SK}_H)$, $V_2^* = h(B'_M \parallel \mathrm{SK}_F^* \parallel V_1)$, and verifies $V_2^* \overset{?}{=} V'_2$. If equal, HA believes that A is a legal FA. Otherwise, the certification is terminated. HA computes $\mathrm{RID}^* = h(\mathrm{AID} \parallel \mathrm{SK}_H)$, $N_{\mathrm{MU}}^* = h(\mathrm{RID}^* \parallel K_{\mathrm{MU}}) \oplus V_1$, $V_1^* = h(\mathrm{RID}^* \parallel K_{\mathrm{MU}}) \oplus N_{\mathrm{MU}}^*$ and verifies $V_1^* \overset{?}{=} V_1$. If equal, HA believes that MU is legal. Otherwise, authentication is terminated. HA computes $A_M^* = h(\mathrm{ID}_{\mathrm{MU}} \parallel R_M) \oplus N_{\mathrm{MU}}^*$, $N'_{\mathrm{FA}} = h(A_M^* \parallel \mathrm{SK}_F^*) \oplus B'_M$, $N'_M = h(\mathrm{RID}^* \parallel N_{\mathrm{MU}}^*) \oplus N'_{\mathrm{FA}}$, $V'_3 = h(\mathrm{ID}_{\mathrm{HA}} \parallel A_M^* \parallel \mathrm{SK}_F^*)$, $V'_4 = h(\mathrm{RID}^* \parallel \mathrm{ID}_{\mathrm{FA}} \parallel K_{\mathrm{MU}})$. Then, HA updates $K_{\mathrm{MU}} = K_{\mathrm{MU}} + 1$ and stores in database of HA. Finally, HA transmits authentication request $M'_3 = \{N'_M, V'_3, V'_4\}$ to HA.

(4) After receiving authentication request M'_3 from HA, A computes $V_3^* = h(\mathrm{ID}_{\mathrm{HA}} \parallel A_M \parallel \mathrm{SK}_F^*)$, and verifies $V_3^* \overset{?}{=} V'_3$. If it is equal to V'_3, A believes that HA and MU are legal. Otherwise, the communication will be terminated. Then, A computes $\mathrm{SK} = h(N'_{\mathrm{FA}} \parallel A_M \parallel \mathrm{ID}_{\mathrm{HA}})$ and transmits message $M'_4 = \{N'_M, V'_4\}$ to MU.

(5) After receiving message M'_4 from A, MU computes $V_4^* = h(\mathrm{RID} \parallel \mathrm{ID}_{\mathrm{FA}} \parallel K_{\mathrm{MU}})$, and verifies $V_4^* \overset{?}{=} V'_4$. If equal, MU believes that A and HA are legal. Otherwise, the communication is terminated. Then, MU computes $N'_{\mathrm{FA}} = h(\mathrm{RID} \parallel N_{\mathrm{MU}}) \oplus N'_M$, $\mathrm{SK} = h(N'_{\mathrm{FA}} \parallel A_M \parallel \mathrm{ID}_{\mathrm{HA}})$, updates $K_{\mathrm{MU}} = K_{\mathrm{MU}} + 1$, and stores it in the smart card. So A can get the session key SK by impersonating FA.

Therefore, the protocol of R. Shashidhara et al. is vulnerable to KCIA.

36.3.3 Known-session-specific Temporary Information Attacks

To compute the session key, A may follow the following steps.

(1) A can first intercept the login request $M_1 = \{A_M, V_1, \mathrm{ID}_{\mathrm{HA}}\}$ transmitted on the public channel. A can obtain parameters$\{A_M, \mathrm{ID}_{\mathrm{HA}}\}$ from the request for subsequent computation of session key.
(2) A can obtain a random number N_{FA} generated by FA.
(3) Finally, A can successfully compute $\mathrm{SK} = h(N_{\mathrm{FA}} \parallel A_M \parallel \mathrm{ID}_{\mathrm{HA}})$.

Therefore, the protocol of R. Shashidhara et al. is vulnerable to KTIA.

36.4 Conclusion

This paper is about the protocol of Shashidhara et al. We carefully analyze their proposed protocol and point out three security vulnerabilities, including PFS, KCIA, and KTIA. It is contrary to the protocol of Shashidhara et al. that the protocol is unable to resist some well-known attacks and cannot guarantee secure communications. We hope that this research can guide researchers to design a more secure protocol for roaming services in mobile environments.

References

1. Alveras, D., Grotschel, M., Jonas, P., Paul, U.: Survivable mobile phone network architectures: models and solution methods. IEEE Commun. Mag. **36**(3), 88–93 (1998)
2. Buttyan, L., Gbaguidi, C.: Extensions to an authentication technique proposed for the global mobility network. IEEE Trans. Commun. **48**(3), 373–376 (2000)
3. Chang, C.C., Lee, C.Y., Chiu, Y.C.: Enhanced authentication scheme with anonymity for roaming service in global mobility networks. Comput. Commun. **32**(4), 611–618 (2009)
4. Chen, C.M., Xu, L., Wang, K.H., Liu, S., Wu, T.Y.: Cryptanalysis and improvements on three-party-authenticated key agreement protocols based on chaotic maps. J. Int. Technol. **19**(3), 679–687 (2018)
5. Chen, C.M., Wang, K.H., Fang, W., Wu, T.Y., Wang, E.K.: Reconsidering a lightweight anonymous authentication protocol. J. Chin. Inst. Eng. **42**(1), 9–14 (2019)
6. Chen, C.M., Xiang, B., Wang, K.H., Yeh, K.H., Wu, T.Y.: A robust mutual authentication with a key agreement scheme for session initiation protocol. Appl. Sci. **8**(10), 1789 (2018)
7. Chen, C.M., Xiang, B., Wang, K.H., Zhang, Y., Wu, T.Y.: An efficient and secure smart card based authentication scheme. J. Int. Technol. **20**(4), 1113–1123 (2019)
8. Gope, P., Hwang, T.: Lightweight and energy-efficient mutual authentication and key agreement scheme with user anonymity for secure communication in global mobility networks. IEEE Syst. J. **10**(4), 1370–1379 (2016)
9. Hwang, K.F., Chang, C.C.: A self-encryption mechanism for authentication of roaming and teleconference services. IEEE Trans. Wirel. Commun. **2**(2), 400–407 (2003)

10. Karuppiah, M., Saravanan, R.: A secure authentication scheme with user anonymity for roaming service in global mobility networks. Wirel. Pers. Commun. **84**, 2055–2078 (2015)
11. Lee, C.C., Hwang, M.S., Liao, I.E.: Security enhancement on a new authentication scheme with anonymity for wireless environments. IEEE Trans. Ind. Electron. **53**(5), 1683–1687 (2006)
12. Lee, C.C., Yang, C.C., Hwang, M.S.: A new privacy and authentication protocol for end-to-end mobile users. Int. J. Commun. Syst. **16**(9), 799–808 (2003)
13. Shashidhara, R., Bojjagani, S., Maurya, A.K., Kumari, S., Xiong, H.: A robust user authentication protocol with privacy-preserving for roaming service in mobility environments. Peer-to-peer networking and applications **13**, 1943–1966 (2020)
14. Suzuki, S., Nakada, K.: An authentication technique based on distributed security management for the global mobility network. IEEE J. Sel. Areas Commun. **15**(8), 1608–1617 (1997)
15. Tzeng, Z.J., Tzeng, W.G.: Authentication of mobile users in third generation mobile systems. Wirel. Pers. Commun. **16**, 35–50 (2001)
16. Wang, Y., Liu, Y., Ma, H., Ma, Q., Ding, Q.: The research of identity authentication based on multiple biometrics fusion in complex interactive environment. J. Netw. Intell. **4**(4), 124–139 (2019)
17. Wu, T.Y., Lee, Y.Q., Chen, C.M., Tian, Y., Al-Nabhan, N.A.: An enhanced pairing-based authentication scheme for smart grid communications. J. Ambient Intell. Hum. Comput. (2021), https://doi.org/10.1007/s12652-020-02740-2
18. Wu, T.Y., Lee, Z., Obaidat, M.S., Kumari, S., Chen, C.M.: An authenticated key exchange protocol for multi-server architecture in 5g networks. IEEE Access **8**, 28018–28096 (2020)
19. Wu, T.Y., Lee, Z., Yang, L., Luo, J.N., Tso, R.: Provably secure authentication key exchange scheme using fog nodes in vehicular ad hoc networks. J. Supercomput. (2021). https://doi.org/10.1007/s11227-020-03548-9
20. Wu, T.Y., Wang, T., Lee, Y.Q., Zheng, W., Kumari, S., Kumar, S.: Improved authenticated key agreement scheme for fog-driven IoT healthcare system. Secur. Commun. Netw. **2021**, 6658041 (2021)
21. Wu, T.Y., Yang, L., Lee, Z., Chen, C.M., Islam, S.H.: Improved ECC-based three-factor multiserver authentication scheme. Secur. Commun. Netw. **2021**, 6627956 (2021)
22. Xu, G., Liu, J., Lu, Y., Zeng, X., Zhang, Y., Li, X.: A novel efficient MAKA protocol with desynchronization for anonymous roaming service in global mobility networks. J. Netw. Comput. Appl. **107**, 83–92 (2018)
23. Zhou, T., Xu, J.: Provable secure authentication protocol with anonymity for roaming service in global mobility networks. Comput. Netw. **55**(1), 205–213 (2011)