Journal of Engineering and Applied Sciences 14 (14): 4713-4716, 2019
ISSN: 1816-949X

Privacy Preserving Handover Authentication Protocol for Wireless Mobile Communication Networks

T. Senthil Kumar and S. Prabakaran
SRM Institute of Science and Technology, Department of Computer Science and Engineering, Chennai, India

Abstract: In wireless mobile network, during handoff technique, authentication is required in order to transfer the information in secured way. Hence, in this study, we propose a privacy preserving handoff authentication protocol for wireless mobile networks. In this protocol, Attribute Based Signature (ABS) is applied for handoff authentication between the mobile node (UE) and the BS. The attributes considered are pseudo id of the UE, time slot and location information. Whenever, the UE decides to handoff to a selected BS it signs the message using its attribute List L and the Secret Key (SK) and transmit to BS. The BS verifies the signature and generates a blind signature which is transmitted to the UE. UE verifies the blind signature and creates the Session Key (SK) for that slot. By simulation results, we show that the proposed technique enhances the network security.

Key words: Secret key, attributes, transmit, blind signature, simulation, handoff

INTRODUCTION

Wireless Mobile Communication (WMC) is one of the latest developing technology of telecommunication networks. Though currently we are using 3rd (3G) and 4th Generation (4G) of WMC, most of the services are based on the 2G standard of WMC. Moreover, the security framework of 4G utilizes the same concept as that of 3G network (Parne *et al*., 2018). The major components involved in WMC are Mobile Nodes (MNs), Access Points (APs) and Authentication Server (AS). MNs could move from 1 place to another 1 while APs have a limited geographical coverage. As a consequence, the handover occurs frequently. It needs an efficient security handover protocol when the handover occurs. An essential goal of the handover protocol is authentication. It aims to guarantee only valid MNs could access wireless networks and prevent illegal access request from adversaries (Zeng *et al*., 2018). After registering to an AS, the MN can access the network and acquire network service from an associated AP. When an MN moves from one AP to another, it should perform a handover authentication to the new AP to protect them from unauthorized user access or unauthorized access by legitimate users (Chen *et al*., 2017).

Designing a secure handover authentication technique and providing strong anonymity for global mobility networks become challenging, due to their limited processing and power capabilities (Xie *et al*., 2014). A strict time deadline is applied over the handover process in order to mitigate the connection disruption (He *et al*., 2015). The initial authentication delay should be reduced without compromising the security (Lee *et al*., 2014). In vertical handover process, the access point changes from 1 to another such that the data transmission of the session is maintained consistently (Qachri *et al*., 2013). Though the existing mechanisms protect the identification details of the user, the location information is not well guarded which is a serious threat (Mohanaprasanth *et al*., 2013). In this research, we propose a privacy preserving handoff authentication protocol for wireless mobile networks.

Literature review: Zeng *et al*. (2018) have proposed attribute-based anonymous handover authentication protocol for wireless networks. It applies Attribute-Bases Signature (ABS) scheme in which a specific set of user attributes is used to generate the public keys. A mutual authentication scheme was then developed based on ABS. This protocol ensures privacy preservation, user revocation and session key updation.

Chain *et al*. (2016) have proposed an authentication scheme for roaming which applies elliptic curve based anonymous login method. It provides balanced session key generation between the sending and receiving parties. The integrity of the session key is verified using the Burrows-Abadi-Needham logic (BAN-logic).

Corresponding Author: T. Senthil Kumar, SRM Institute of Science and Technology, Department of Computer Science and Engineering, Chennai, India

Wang and Hu (2014) have discussed the security attacks and improvements over the handover authentication protocol PairHand. Then they have developed a method to resolve the key recovery attack over PairHand by reducing the number of captured signatures. To overcome the security flaws of improved PairHand protocols, a secure authentication mechanism was proposed.

Wang *et al.* (2017) have proposed provably secure handover authentication scheme for based on Elliptic Curve Cryptography (ECC). This scheme overcomes the security attacks over the PairHand protocol by integrating the blind signature and identity-based signature schemes. It achieves batch verification for handover authentication and does not involve any bilinear pairing computations.

He *et al.* (2013) have studied the current roaming authentication techniques. They have resolved the issues of privacy-preserving universal authentication protocol, named, Priauth, they have then suggested some simple and efficient patches for solving the vulnerabilities.

MATERIALS AND METHODS

Proposed solution: In this study, we propose a privacy preserving handoff authentication protocol for wireless mobile networks. In this protocol, Attribute Based Signature (ABS) is applied for handoff authentication between the mobile node (UE) and the BS. The attributes considered are pseudo id of the UE, time slot and location information. Whenever the UE decides to handoff to a selected BS, it signs the message using its attribute list L and the Secret Key (SK) and transmit to BS. The BS verifies the signature and generates a blind signature which is transmitted to the UE. UE verifies the blind signature and creates the Session Key (SK) for that slot.

Handover authentication: In this protocol, Attribute Based Signature (ABS) is applied for handoff authentication between the mobile node (UE) and the BS. UE obtains its private Key K_{prG} and revocation information $Q_{i,j}$ for each timestamp Ts_j. Consider the following details:

- Z = Specified access structure
- CDS = Common Digital Signature
- TS = Timestamp
- ID_{UEj} = Identity of UE_j
- $Q_{i,j}$ = Revocation information with time interval index TS_j for UE_i
- Y = Attribute list (pseudo id, time slot and location information) owned by UE
- K_{prG} = Be the secret private key of UE_i on Y
- u, v = Random numbers in X^*_p
- δ_i, δ_j = Digital signature of UE_i and BS, respectively
- K_s = Session key
- c = Message to be encrypted
- g = The generator of prime order
- W_j = Revocation list that includes the revocation information related to TS
- K_{sec} = The secret key

The steps involved in this technique are as follows:

- The UE sends a registration/authentication request to the SeNB through secure channel
- On receiving the request, the SeNB generates pseudo ID for UE, p, K_{pri} and shares these value with UE through the secure channel
- UE_i acquires Z from the beacon message from BS_j
- If its Y satisfies the access structure, then UE_i initially selects a random number $u \in^*_p$ and generates the following:

$$\delta_i = \text{ABS.Sign}(c, Y, K_{prG})$$

where, $c = ID_{UEj} \| g^u_0 \| TS \| Q_{i,j}$

- UE_i forwards the $\{c, \delta_i\}$ to BS_j
- BS_j validates the TS (Case 1) to prevent the replay attack and performs revocation (Case 2)

Case 1:

- If the validation is successful, then BS_j verifies the signature
- If the signature is valid, then BS_j selects a random number $v \in X^*_p$ and computes the following:

$$\delta_j = \text{CDS.Sign}\{c', K_{prG}\}$$

where $c' = ID_{UEj} \| g^u_0 \| g^v_0$

- On the other hand, if the signature is invalid then BS_j rejects it

Case 2:

- The server generates the revocation list W_j and sends it to each UE with a K_{sec}
- Upon receiving W_j, each UE_i updates the $Q_{i,j}$
- For any, $Q_{i,j} \in W_{j-1}$

$$Q_{ij-1} = \overline{H_{K\,sec}(Q_{ij-1})}$$

- UE stores both W_j and W_{j-1} in its internal data store

- UE_i verifies whether the received message is in W_j. If available then the user is revoked and handover request is rejected. Otherwise, proceed with next step
- BS_j sends $\{c', K_{prG}\}$ back to UE_i
- BS_j computes the session key $K_s = (g^u{}_0)^v$ and deletes the random number v from the memory
- Upon receiving $\{c', K_{prG}\}$, UE_i verifies δ_j as per CDS.Ver (.)
- If the value is 1, then UE_i generates the session key $K_s = (g^v{}_0)^u$ and erases the random number u from its memory
- UE_i generates the $(ID_{UEj}\|g^u{}_0\|g^v{}_0)k_s$ and sends it to Bs_j Here $(N)_K$ refers to the symmetric key K to encrypt a message N
- After receiving the encrypted message, BS_j verifies the signature and blinds it with two random elements $\mu, v \leftarrow x_P^*$

$$C'' = (ID_{UEj} + \mu g^u{}_0 + v g^v{}_0)k_s$$

Computes $m' = H_1(m, c'')$ $m = m'^{-v} \bmod p$

- m is sent to UE_j
- UEi feedbacks the value e = k+mxmodp to BS_j
- BS_j verifies the following equation:

$$[e]^{g^u_0} = [m]^{g^v_0} = c'$$

- If the equation holds good, then BS_j believes that they have established a session key K_s for that time slot

Otherwise, it rejects the access request.

RESULTS AND DISCUSSION

Simulation parameters: We use NS2 to simulate our proposed Privacy Preserving Handover Authentication (PPHA) scheme. The performance of PPHA scheme is compared with Attribute based Anonymous Handover (AAHA) scheme (Zeng *et al*., 2018). The simulation settings and parameters are summarized in Table 1. The simulation topology is shown in Fig. 1.

Performance metrics

Computational cost: To evaluate the bandwidth consumption of the re-authentication, all transaction message size between different network entity sections in 1 round authentication session are calculated.

Authentication success ratio: Authentication Success Ratio (ASR) is given by:

Table 1: Simulation parameters

Variables	Parameters
Number of cells	18
Number of users per cell	6
Number of Service Providers (SP)	6
Area size	1000×1000 m
Simulation time	50 sec
Traffic model	Constant Bit Rate (CBR)
Propagation	Two ray ground
Antenna	Omni antenna
Number of attackers per cell	1

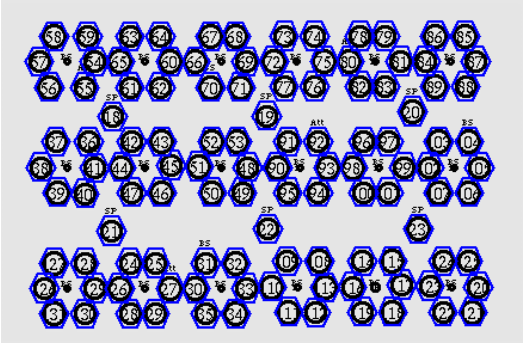

Fig. 1: Simulation topology

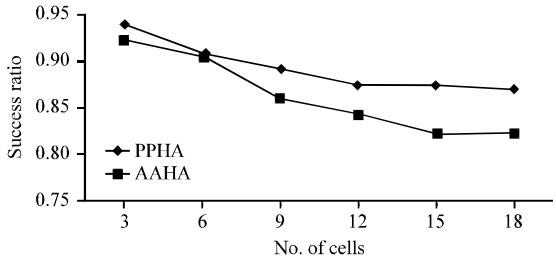

Fig. 2: Authentication success ratio for different cells

$$ASR = no\_suc\_auth/auth\_att$$

where, no_suc_auth and auth_att are the total number of successful authentications made and total number of authentication attempts, respectively. In the simulation experiment, the mutual authentication is performed between the users of different cells by varying the number of user cells from 3-18. The number of attackers per cell is kept as 1.

Figure 2 shows the authentication success ratio measured for PPHA and AAHA schemes. As seen from the figure, the success ratio of PPHA decreases from 0.83-0.36 and the success ratio of AAHA decreases from 0.68-0.27, when the number of cells is increased. But the success ratio of PPHA is 3.5% higher when compared to AAHA.

Figure 3 shows the computational cost involved in PPHA and AAHA schemes. As depicted by the figure,

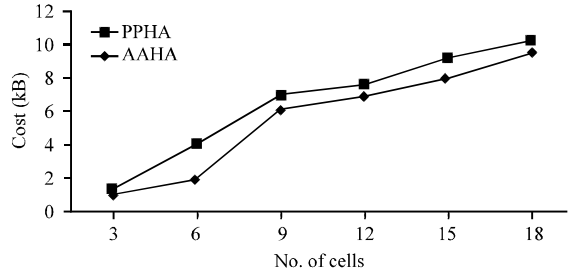

Fig. 3: Computational cost for different cells

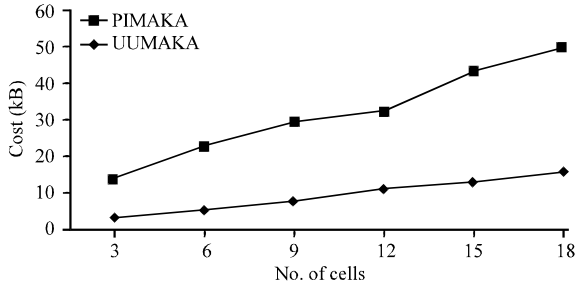

Fig. 4: Communication cost for different cells

the computational cost of PPHA increases from 0.4-9.1 kB and the computational cost of AAHA increases from 1.8-27.1 kB, when the number of cells is increased. Since, PPHA does not involve the computations of bilinear pairings, it has 19% lesser computational cost than AAHA scheme.

Figure 4 shows the communication cost involved in PPHA and AAHA schemes. As depicted by the figure, the communication cost of PPHA increases from 3.2-15.7 kB and the computational cost of AAHA increases from 14.4-49.5 kB, when the number of cells is increased. Since, PPHA does not involve the computations of bilinear pairings it has 30% lesser communication cost than AAHA scheme.

CONCLUSION

In this study, we have proposed a privacy preserving handoff authentication protocol for wireless mobile networks. In this protocol, Attribute Based Signature (ABS) is applied for handoff authentication between the mobile node (UE) and the BS. The attributes considered are pseudo id of the UE, time slot and location information. Whenever, the UE decides to handoff to a selected BS it signs the message using its attribute List L and the Secret Key (SK) and transmit to BS. The BS verifies the signature and generates a blind signature which is transmitted to the UE. UE verifies the blind signature and creates the Session Key (SK) for that slot. By simulation results, we have shown that the proposed technique enhances the network security.

REFERENCES

Chain, K., W.C. Kuo and J.C. Cheng, 2016. A novel mobile communications authentication scheme with roaming service and user anonymity. Appl. Sci., 6: 1-13.

Chen, R., G. Shu, P. Chen and L. Zhang, 2017. Enhanced security and pairing-free handover authentication scheme for mobile wireless networks. J. Phys. Conf. Ser., 910: 1-9.

He, D., C. Chen, S. Chan and J. Bu, 2013. Strong roaming authentication technique for wireless and mobile networks. Intl. J. Commun. Syst., 26: 1028-1037.

He, D., S. Chan and M. Guizani, 2015. Handover authentication for mobile networks: Security and efficiency aspects. IEEE. Network, 29: 96-103.

Lee, K., J., Deng and R. Sudhaakar, 2014. Fast authentication in multi-hop infrastructure-based mobile communication. Proceedings of the 2014 IEEE International Conference on Communications (ICC), June 10-14, 2014, IEEE, Sydney, Australia, ISBN:978-1-4799-2003-7, pp: 665-670.

Mohanaprasanth, P., B. Sridevi and S. Rajaram, 2013. Secured cost effective group handover authentication scheme for WiMAX networks. Intl. J. Adv. Res. Comput. Eng. Technol., 2: 1011-1016.

Parne, B.L., S. Gupta and N.S. Chaudhari, 2018. ESAP: Efficient and secure authentication protocol for roaming user in mobile communication networks. Sadhana, 43: 1-19.

Qachri, N., O. Markowitch and J.M. Dricot, 2013. A formally verified protocol for secure vertical handovers in 4G heterogeneous networks. Intl. J. Secur. Appl., 7: 309-326.

Wang, C., Y. Yuan and J. Wu, 2017. A new privacy-preserving handover authentication scheme for wireless networks. Sens., 17: 1-14.

Wang, W. and L. Hu, 2014. A secure and efficient handover authentication protocol for wireless networks. Sens., 14: 11379-11394.

Xie, Q., D. Hong, M. Bao, N. Dong and D.S. Wong, 2014. Privacy-preserving mobile roaming authentication with security proof in global mobility networks. Intl. J. Distrib. Sens. Networks, 2014: 1-7.

Zeng, Y., H. Guang and G. Li, 2018. Attribute-based anonymous handover authentication protocol for wireless networks. Secur. C ommun. Networks, 2018: 1-9.