Pair Hand: A Pairing-based Cryptography to Secure Handover Process

T. Sandeep & T. Venkata Naga Jayudu

Department of CSE, Intell Engineering College, Anantapur, A.P., India.
E-mail : tsandeepmca@gmail.com, tvnagajayudu@gmail.com

Abstract **–** Seamless handover over multiple access points is highly desirable to mobile nodes, but ensuring security and efficiency of this process is challenging. This paper shows that prior handover authentication schemes incur high communication and computation costs and are subject to a few security attacks. Further, a novel handover authenticatonprotocol named PairHand is proposed. PairHand uses pairing-based cryptography to secure handover process and to achieve high efficiency. Also, an efficient batch signature verification scheme is incorporated into PairHand. Experiments using our implementation on laptop PC's show that PairHand is feasible in real applications.

Keywords – Security, Privacy, Efficiency, Authentication.

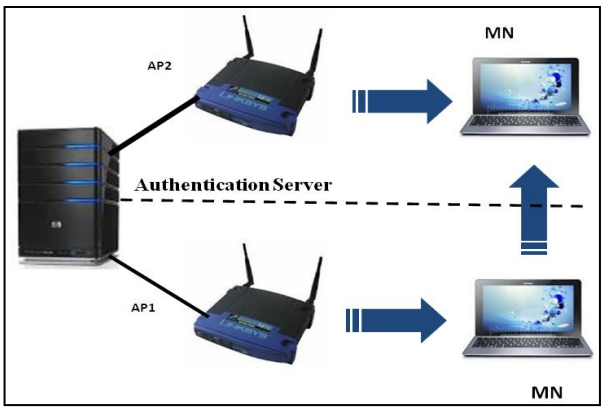
I. INTRODUCTION

Wireless internet access services are offered through interconnected mobile telecommu-nication networks, WLANs, vehicular adhoc networks. To overcome the geographical coverage limit of each access point and provide seamless access service for mobile nodes, it is important to have an efficient handover protocol. One important module in the handover protocol is authentication. Regardless of the tech-nology implemented, a typical handover authentication scenario involves three entities: mobile nodes, access points (APs) and the authentication server (AS). Before entering the network, an MN registers to AS, then subscribes services and connects to an AP for accessing the network. When the MN moves from the current AP (e.g., $AP1$) into a new AP (e.g., $AP2$), handover authentication should be performed at $AP2$. Through handover authentication, AP2 authenticates the MN to identify and reject any access request by an unauthorized user. At the same time, a session key should be established between the MN and $AP2$ to provide confidentiality and integrity of the communication session. TA deploys RSUs and registers vehicles by granting the corresponding authentication keys. Each RSU receives and then verifies the traffic safety messages from the OBUs. Designing a handover authentication protocol is not an easy task. Generally, there are two major practical issues challenging the design.

First, efficiency needs to be considered. An MN is generally constrained in terms of power and processing capability. Therefore, a handover authentication process should be computationally efficient. Further, such a process should be fast enough to maintain persistent connectivity for MNs.

Second, security and privacy are serious concerns for the handover authentication service. However, all existing handover authentication protocols are subject to a few security attacks in two aspects. On the one hand, users are deeply concerned about their privacy-related information such as the identity, position, and roaming route.

A novel handover authentication protocol called *Pair Hand*, which uses pairing based cryptography to secure handover process and to reduce the communication and computation overheads of the involved entities.



Also, it only requires two handshakes between an MN and an AP, and does not need to transmit or verify any certificate as in traditional public key cryptosystems. Further, we introduce an efficient batch signature verification scheme, in which each AP can simultaneously verify multiple received signatures.

II. PROPOSED WORK

A novel handover authentication protocol named Pair Hand is proposed. This project shows that prior handover authentication schemes incur high communication and computation costs, and are subject to a few security attacks. In this project, we propose a novel handover authentication protocol called Pair Hand, which uses pairing based cryptography to secure handover process and to reduce the communication and computation overheads of the involved entities. Also, it only requires two handshakes between an MN and an AP, and does not need to transmit or verify any certificate as in traditional public key cryptosystems. Further, we introduce an efficient batch signature verification scheme, in which each AP can simultaneously verify multiple received signatures. Pair Hand uses pairing-based cryptography to secure handover process and to achieve high efficiency. Also, an efficient batch signature verification scheme is incorporated into Pair Hand.

Request Server

If the client or a Mobile Node (MN) gets in to the system once, it may access the server through Access pointer (AP). The MN can request any process from the server such download, verify, etc.

Handover Authentication:

The handover authentication process takes place, when the AP receives a new MN. The AP sends a private key to MN and the MN will respond with message and signature. The AP verifies the signature for authentication.

Each AP broadcasts its identity as part of beacon messages that are periodically broadcasted to declare service existence.

To access the network, an MN, say i, follows the handover authentication protocol as specified below, when an AP ($AP2$) is within his direct communication range.

1) MN i picks an unused pseudo-ID $pidi$ and the corresponding private key $sH1(pidi)$.
2) With the private key $sH1(pidi)$ and message $||i = (pidi||IDAP2||ts)$, MN i can compute the signature

$i = H2(||i)||sH1(pidi)$, where a timestamp ts is added by MN i to counter replay attacks and || indicates message concatenation operation. In this case, we assume that all network entities keep loose time synchronization via some existing time synchronization mechanisms such as GPS-system. Alternatively, instead of timestamp, a random number can be used to prevent replay attacks.

3) Subsequently, MN i unicasts the access request message $\{||i, \sigma i\}$ to $AP2$.
4) Then, MN i computes the shared symmetric key with $AP2$:

$Ki-2 = \hat{}(sH1(pidi), H1(IDAP2))$. Upon receipt of $\{||i, \sigma i\}$, $AP2$ proceeds as follows.

1) Check the time stamp ts to prevent replay attack.

   Examine $ExpiryDate$ included in $pidi$ to verify the service expiration time.

2) With $params$ assigned by AS, $AP2$ checks whether signature σi is valid if $\hat{}e(\sigma i, P) = \hat{}e(H2(||i)||H1(pidi), Ppub)$), as verified below.

   $\hat{e}(\sigma_i, P) = \hat{e}(H_2(M_i) \cdot sH_1(pid_i), P)$

   $= \hat{e}(H_2(M_i) \cdot H_1(pid_i), sP) = \hat{e}(H_2(M_i) \cdot H_1(pid_i), P_{pub})$

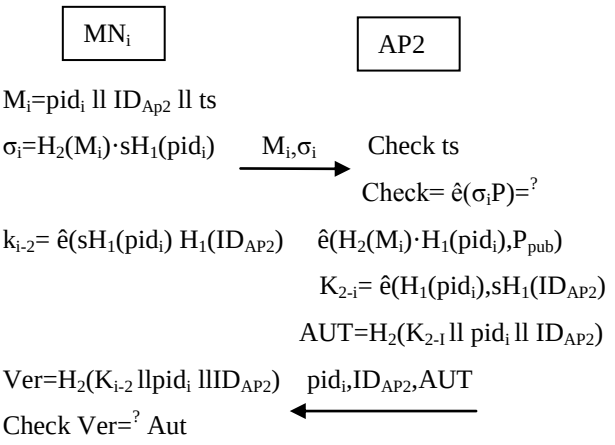
3) AP_2 further computes

   $K_{2-i} = \hat{e}\,(H_i(pid_i), sH_1(ID_{AP2})) \cdot$

   Note that K_{i-2} in equal to k_{2-i} Since

   $K_{i-2} = \hat{e}(sH_1, (pid_i), H_1(ID_{AP2})) = \hat{e}(H_1(pid_i), H_1(ID_{AP2}))^s$

   $= \hat{e}(H_1(pid_i), sH_1(ID_{AP2})) = K_{2-i}$



Batch Authentication

The batch authentication is the process of verifying information, which is received from the MN to previous AP where MN resident. The authenticated information

is checked between the MN and previous AP in new AP. If the authentication is correct, it will allow the MN to continue their status from the server.

Traffic-Aware Dynamic Routing

When the *n* number of packets moves towards the AP parallel, there the traffic may occur. To avoid the traffic during communication establishment the traffic aware-dynamic routing technique is provide.

Pairhand

A novel handover authentication protocol called *Pair Hand*, which uses pairing based cryptography to secure handover process and to reduce the communication and computation overheads of the involved entities. Also, it only requires two handshakes between an MN and an AP, and does not need to transmit or verify any certificate as in traditional public key cryptosystems. Further, we introduce an efficient batch signature verification scheme, in which each AP can simultaneously verify multiple received signatures.

III. A SECURE DYNAMIC ID BASED REMOTE USER AUTHENTICATION SCHEME FOR MULTI-SERVER ENVIRONMENT

Since the number of server providing the facilities for the user is usually more than one, the authentication protocols for multi-server environment are required for practical applications. Most of password authentic-cation schemes for multi-server environment are based on static ID, so the adversary can use this information to trace and identify the user's requests. It is unfavorable to be applied to special applications, such as e-commerce. In this project, we develop a secure dynamic ID based remote user authentication scheme to achieve user's anonymity. The proposed scheme only uses hashing functions to implement a robust authentication scheme for the multi-server environment. It provides a secure method to update password without the help of third trusted party. The proposed scheme does not only satisfy all requirements for multi-server environment but also achieve efficient computation. Besides, our scheme provides complete functionality to suit with the real applications.

IV. CONCLUSION

Some schemes cannot provide anonymity under the forgery attack. Moreover, the heavy computation cost may consume battery power expeditiously for mobile devices. A novel protocol to achieve secure and efficient handover authentication is needed.

Therefore, we proposed a novel authentication scheme to overcome these weaknesses that is efficient, secure, and suitable for battery-powered mobile devices in global mobility networks. The security analysis and experimental results shows that the proposed approach is feasible for real applications.

V. REFERENCES

[1] Secure and Efficient Handover Authentication Based on Bilinear Pairing Functions, VOL. 11, NO. 1, JANUARY 2012.

[2] European Telecommunications Standards Institute (ETSI), GSM 02.09: Security Aspects, 1993..

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

[4] "Enhanced authentication scheme with anonymity for roaming service in global mobility networks, " Computer Commun., vol. 32, no. 4, pp. 611–618, 2009.

[5] J.Choi, S.Jung, "A handover authentication using credentials based on chameleon hashing," IEEE Commun. Lett., vol. 14, no. 1, pp. 54–56,2010.

[6] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," J.Computer Security, vol. 15, no. 1, pp. 39–68, 2007.

[7] Y.-P. Liao and S.-S. Wang, "A secure dynamic ID based remote user authentication scheme for multi-server environment," Computer Standards & Interfaces, vol. 31, no. 1, pp. 24–29, 2009.

[8] H.-C. Hsiang and W.-K. Shih, "Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment," Computer Standards & Interfaces, vol. 31, no. 6, pp. 1118–1123, 2009.

[9] D. He, M. Ma, Y. Zhang, C. Chen, and J. Bu, "A strong user authentication scheme with smart cards for wireless communications," Computer Commun., vol. 34, no. 3, pp. 367–374, 2011.

[10] K. C. Barr and K. Asanovi, "Energy aware lossless data compression," ACM Trans. Comput. Syst., vol. 24, no. 3, pp. 250–291, 2006.

[11] U.S. Department of Transportation, National Highway Traffic Safety Adminstration, Vehicle Safety Communications Project, Final Repot, 2006.

[12] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," in Proc. Asiacrypt 2001, vol. 2248, pp. 514–532.

[13] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," J. Computer Security, vol. 15, no. 1, pp. 39–68, 2007.