ISSN: 2321-7782 (Online)
Volume 2, Issue 12, December 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Efficient Handover Authentication Scheme Using Bilinear Pairing

Dr. Sattar J. Aboud
Department of Computer Science and Technology
University of Bedfordshire
United Kingdom

Abstract: ***The handover over multiple access points is extremely needed in mobile nodes, but promising efficiency and security of such implementation is difficult. This paper illustrates that preceding handover authentication schemes suffer from the communication and computing costs, and are vulnerable to some security attacks. Additional, a new handover authentication scheme is presented. The proposed scheme uses pairing-typed cryptography to secure handover process and to get high efficiency. Besides, an efficient batch signature scheme is used with proposed scheme. The result shows that the performance on laptop is competitive.***

Keywords: Wireless network, cryptography, bilinear pairing, handover authentication.

I. INTRODUCTION

These days, wireless internet access services are accessible over interconnected mobile networks and vehicular ad hoc network. To conquer a geographical reporting constraint of every access point and give easy access service for mobile nodes such as smart phone, laptop and vehicle, it is vital to have an efficient handover scheme. The handover authentication general idea is illustrated in Figure 1.

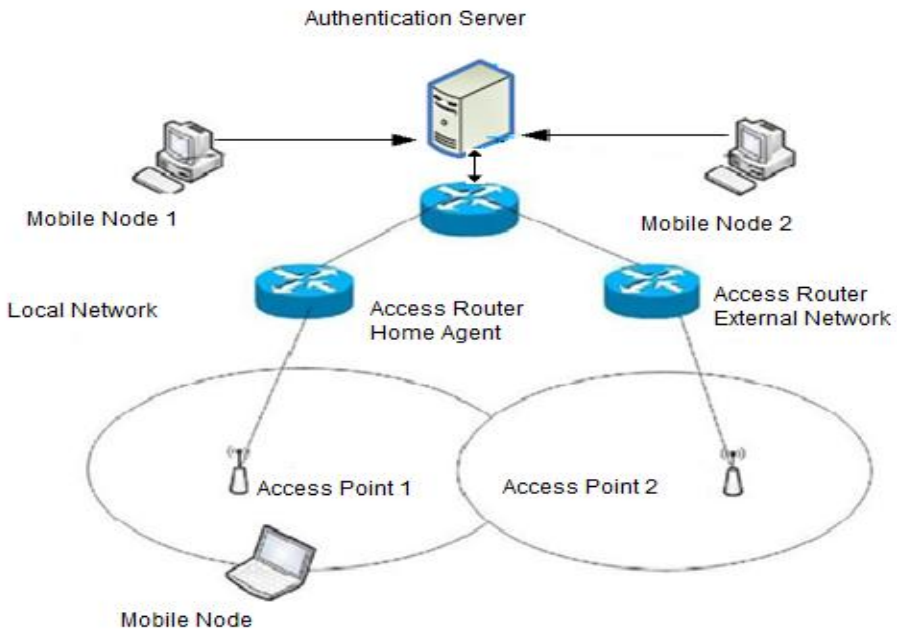

Figure 1: Handover authentication general idea

The standard handover authentication phase includes three participants; mobile node, access point and authentication server. Before ingoing the network, mobile node enrolls to authentication server, and then links to access point for accessing a network. If the mobile node goes from a present access point into the new access point, handover authentication must be done at

© 2014, IJARCSMS All Rights Reserved

access point2 ($AP2$). With handover authentication, $AP2$ authenticates the mobile node to accept or reject any access request by illegal user. Simultaneously, the session key must be created between mobile nodes and $AP2$ to gives privacy and integrity of the communication session. Additional, we show that the above process is checking by vehicular ad hoc network state. The standard vehicular ad hoc network contains the trusted authority (authentication server), the number of vehicles set by wireless on-board unit (mobile node), and some stationary roadside unit (access point). The trusted authority sets up roadside unit and registers vehicles by yielding the related authentication keys. Every roadside unit obtains and then checks the traffic safety messages from the on-board unit. Construction the handover authentication scheme is not a simple job. However, there are two matters facing the construction.

First, efficiency should be considered. The mobile node is limited in terms of influence and processing ability. So, the handover authentication process must be computationally efficient. Additional, such a process must be rapid to preserve persistent connectivity for mobile node. But, most of the current handover authentication schemes [1] suffer from communication and computing cost in five faces.

1. The standard way of doing handover authentication is to assume $AP2$ contact authentication server who works as the sponsor for vouching that mobile node is authorized subscriber. This will suffer more calculation and communication delay [2].
2. The schemes without communicating with authentication server need at least three handshakes between mobile node and $AP2$ compare with the other schemes need at least four handshakes among three participants. Data broadcast is an expensive operation in wireless networks; transfer 1-bit over the wireless medium needs over 1000 times power than the single 32-bit calculation [3].
3. To give strong security using the digital signature scheme as an effective method for handover authentication. It is not efficient in communication, since a certificate should be broadcasted together with a digital signature as the message spreads in the net. This directs to more power use on mobile node. Also, to authenticate every digital signature, the equivalent receiver needs two costly signature verification processes, since the certificate must be authenticated.
4. To give user anonymity, group signature-typed scheme have been presented in [4]. Though, the user revocation list should be distributed over the whole network in the timely way. Also, a verification delay suffered in these schemes is linearly comparative to the number of called users. Thus, the result of these schemes may weaken if the number of called users is big.
5. The access point checks every signature independently. If the arrival rate of signatures is high, the scalability problem emerges straight away; with the access point has much less time to check every received signature. For instance, in vehicular ad hoc network, every roadside unit can communicate with hundreds of on-board unit, every passing the safety related messages to the roadside unit each $100-300ms$ [5].

Second, security and privacy are grave related to the handover authentication schemes. The present handover authentication schemes [6] are subject to the security attacks form the following aspects.

1. User is extremely concerned regarding the privacy-related information like an identity. In the existing handover authentication schemes, it is understood that an access point is dependable and will keep user privacy-related information private. Such information is very sensitive and popular by many firms in which can use to enhance their business.
2. By denial-of-service attacks, hacker can use the resources of access point and authentication server to makes them less competent to serve mobile node. Such attacks are categorized by two types [7].
    - The traditional method of achieving handover authentication scheme. It needs access point to unconditionally onward any access information to authenticate server, the hacker can easily start denial-of-service on authentication server by access point.

© 2014, IJARCSMS All Rights Reserved

- To prevent such denial-of-service problem, some handover authentication schemes need mobile node and access point to be included in every scheme executed.

The rest of this paper is organized as follows. Section 2 describes the security preliminaries. Section 3 illustrates the scheme and Section 4 analyzes the scheme. Section 5 concludes the paper.

II. THE PRELIMINARIES

Suppose that G is the cyclic additive group and G_T is the cyclic multiplicative group of the same order q. Suppose P is a random generator of G. With aP represents P added to it a time. Assume that $e' : G \times G \to G_T$ is the bilinear map, which convinces the following:

1. Bilinear: $e'(aP, bQ) = e'(P, Q)^{ab}$, such that $P, Q \in G$ and $a, b \in Z_q^*$
2. Non-degenerate: $e'(P, P) \neq 1$
3. Computable: There is an efficient method to calculate $e'(P, Q)$ for any $P, Q \in G$

The group that holds this map e' is entitled the bilinear group, by which the Decisional Diffie-Hellman problem is easy to solve, while the Computational Diffie-Hellman problem is difficult to solved [15]. For instance, suppose $P, aP, bP, cP \in G$ and each $a, b, c \in Z_q^*$, there is a useful method to fix if $ab = c \bmod q$ by verifying $e'(aP, bP) \equiv e'(P, cP)$. Also, there is no method that can calculate $abP \in G$.

III. THE PROPOSED SCHEME

First, none of the presented privacy-aware cryptography schemes such as blind signature, ring signature, and group signature fits the preliminaries illustrated above. Blind signature and ring signature can only give unconditional privacy, while the proposed scheme demands conditional privacy and revocable anonymity. Presented group signature schemes give revocable anonymity, but cannot meet the efficiency. In the proposed scheme, we use the privacy protecting method using pseudonyms. As mobile node have great storage capacity, making the pre-loading of the big pool of pseudonyms from authentication server. The pre-loading method in the proposed scheme contains the pool of shorter-lived pseudonyms. The preload method has been presented by many authors and acts efficiently. For instance, it used in some presented wireless infrastructure, such as Wi-Fi networks.

A. Initiation Protocol

In this protocol, authentication server initializes an entire scheme by performing the following steps.

1. Suppose that G is the cyclic additive group
2. Assume that G_T is the cyclic multiplicative group of the same order q.
3. Suppose that P is the random generator of G.
4. Assume that $e' : G \times G \to G_T$ is the bilinear map.
5. Select an arbitrary number $d \in Z_q^*$ as a master key
6. Find a related public key $Pe = dP$
7. Select two secure hash functions h_1 and h_2, with $h_1 : (0,1)^* \to G$ and $h_2 : (0,1)^* \to Z_q^*$

© 2014, IJARCSMS All Rights Reserved

8. Determine the public keys $params\,(G, G_T, q, P, Pe, h_1, h_2)$ and hold a master key privately
9. Find $h_1(Id_{AP})$ as a public key
10. Find $dh_1(Id_{AP})$ as a private key,
11. Post $h_1(Id_{AP})$ and $dh_1(Id_{AP})$ to access point
12. If mobile node, i enrolls in authentication server with the real identity Id_i then
    1. Verify the mobile node i
    2. Select un-linkable pseudo-Ids , $PId = (pid_1, pid_2, ...)$
    3. Find a public key $h_1(pid_j)$
    4. Find a related private key $dh_1(pid_j)$
    5. Post $(pid_j, dh_1(pid_j))$ to mobile node i
    6. Mobile node i can alter its pseudo-Id to reach the position in handover authentication
    7. Insert $ExpiryDate$ to Id_{AP} , and pid_j .
    8. This kind of key can be delegated to access point so it is usable before an $ExpiryDate$

B. Handover authentication Protocol

The steps of the handover authentication protocol as follows:

Step 1: The mobile node i should do the following.

1. Choose unused pseudo-Id pid_i and a related private key $dh_1(pid_i)$
2. Find the message $m_i = (pid_i \parallel Id_{AP2} \parallel ts)$
3. Calculate a signature $s_i = h_2(m_i) \cdot dh_1(pid_i)$ by added the timestamp ts to counter replay attack. Instead of ts arbitrary number can be employed to avoid replay attacks
4. Find a shared symmetric key, $k_{i-2} = e'(dh_1(pid_i)h_1(Id_{AP2}))$
5. Send the access request information (m_i, s_i) to $AP2$

Step 2: $AP2$ should do the following:

1. Verify the time stamp ts to avoid replay attack.
2. Check $ExpiryDate$ involved in pid_i
3. Verify signature s_i by $e'(a_i, P) = e'(h_2(m_i) \cdot h_1(pid_i), P_e)$
4. Find $k_{2-i} = e'(h_1(pid_i), dh_1(Id_{AP2}))$
5. Find authentication code $Ac = h_2(k_{2-i} \parallel pid_i \parallel Id_{AP2})$
6. Post (pid_i, Id_{AP2}) and Ac to mobile node i

© 2014, IJARCSMS All Rights Reserved

Step 3: The mobile node i should do the following:

1. Verify that $v = h_2(k_{2-i} \| pid_i \| Id_{AP2})$ and compares it with Ac
2. If $v = Ac$ then
    1. Mobile node i believes that $AP2$ is valid
    2. Created the shared key k_{2-i}

   Else mobile node i rejects the connection

Step 4: $AP2$ should do the following:

1. Post (m_i, s_i) to authentication server.

Step 5: The authentication server should do the following:

1. Find the real identity of mobile node i according to a pseudo-Id comprised in m_i.

Remarks

1. This protocol allows mutual authentication between access point and authorized mobile node. It also allows one-sided anonymous authentication for a mobile node.
2. After completion the protocol, an access point and a mobile node create the shared secret key used for the communication session. Thus, a computing time by an access point for checking the single signature is included of 1 point multiplication and 2 pairing operations. The computing time of the pairing operation is higher than the cost of the point multiplication operation [8].
3. The proposed scheme can give conditional privacy. Since access point inform authentication server after done a handover authentication. This step is not influence an authentication time, and gains less overhead than other current schemes [9].

C. Denial-of Service-Attacks

To avoid a denial-of-service attack, we should do in the initialization protocol the following steps:

Step 1: The authentication server should do the following:

1. Generate arbitrarily $t-$degree polynomial $f(x,y) = \sum_{i,j=0}^{t} a_{ij=0} x^i y^j$ over a finite field F_p, with p is the prime number and it has the attribute of $f(x,y) = f(x,y)$.
2. Calculate the polynomial share of $f(x,y)$ namely $f(pid_j, y)$ if the mobile node i enrolls with authentication server, for every pseudo-Id pid_j
3. Send $f(x,y) = \sum_{i,j=0}^{t} a_{ij=0} x^i y^j$ and $f(pid_j, y)$ to mobile node i
4. Post $f(Id_{AP}, y)$ to every access point, such that Id_{AP} is an identity of access point

Step 2: The mobile node should do the following:

© 2014, IJARCSMS All Rights Reserved

1. Calculate the common key $f(pid_j, Id_{AP2})$ by calculating $f(pid_j, y)$ at point $AP2$.
2. Calculate the same key $f(pid_j, Id_{AP2}) = (Id_{AP2}, pid_j)$ by finding $f(Id_{AP}, y)$ at point pid_j

Step 3: $AP2$ should do the following:

1. Use key $f(Id_{AP}, pid_j)$ to check the access request of mobile node i before doing process verification to mitigate the denial-of-service attack
2. The verification can successfully mitigate denial-of-service attacks because an authorized user has an obvious gain over the hacker because of its previous facts on the communication key with every access point

Step 4: The mobile node should do the following:

1. Select unused pseudo-Id pid_i if $AP2$ is under attack
2. Find the authentication code $Ac2 = h_2(k \| m_i \| s_i)$, with $k = f(pid, Id_{AP2})$
3. Post Ac_2 and (m_i, s_i) to $AP2$

Step 5: $AP2$ should do the following:

1. Find the verification code $v_2 = h_2(k^* \| m_i \| s_i)$
2. Compare it with Ac_2, such that $k^* = f(Id_{AP2}, pid_i)$.
3. When such verification is successful, expensive verification on the access request

IV. Security Analysis and Performance Comparison

In this section, we discuss the security analysis and the performance of the proposed scheme:

A. *Security Analysis*

First, we analyse the security of the proposed scheme as follows:

Anonymity: In the proposed protocol, every mobile node receives a pseudo-Id and a related secret key from authentication server at the registration. This pseudo-Id used instead of the real identity in handover authentication protocol for the intent of privacy protection. However, only authentication server knows the relationship between the pseudo-Id and the actual identity. As there is no linkage between pseudo-Id and authentication server, anybody with the access point is incapable to recognize the mobile node or link two transactions in the mobile node.

Validation: This signature $s_i = h_2(m_i)dh_1(pid_i)$ is really the pseudo-Id signature. Without calculating a private key $dh_1(pid_i)$, it is infeasible to forge the valid signature. Due to the NP-hard calculation of Diffie-Hellman problem in G, it is hard to gain a private key $dh_1(pid_i)$ as (P, P_e). So, a pseudo-Id signature is un-forgeable, and a characteristic of subscription validation is reached.

***Authentication**: like subscription validation, the hacker who is not known $AP2$ private key $dh_1(Id_{AP2})$ cannot create legal authentication code Aut.*

© 2014, IJARCSMS All Rights Reserved

B. The Performance Comparisons

Table 1 illustrates the performance comparison of the proposed scheme with the other schemes. Note that the computing time of the hash function is omitted. The elliptic curve scalar multiplication operation has been presented into the results of the proposed scheme.

TABLE I
Performance Comparison between the Proposed Scheme and the Existing Schemes

Protocol	Conditional Privacy Preservation	User Anonymity & Un-traceability	DoS Attack Resistance	Communication Overheads	User Cryptography Operations
Choi *et al.*[4]	No	No	No	3δ	4 Multiplication Exponentiations + 1 RSA Verification
Yang *et al.* [8]	No	Yes	No	3δ	5.20 Elliptic Curve Scalar Multiplication
He *et al.* [2]	No	Yes	No	3δ	12.55 Elliptic Curve Scalar Multiplication + 3 Paring
Our Proposed Scheme	Yes	Yes	Yes	2δ	1 Elliptic Curve Scalar Multiplication + 1 Paring

The results are summarized in Table 2. We use MNT curve with order of 160 bits and embedding degree $r = 6$. Within this curve, elements in Z_q^*, G and G_T are denoted by 160, 161 and 960 bits. Considering the broadcast overhead, the size of every access request (m_i, s_i) is 30 bytes and the size of the reply (pid_i, Id_{AP2}, Ac) is 28 bytes, with a size of pid_i, ts, Id_{AP2} are 4, 2, 4 bytes respectively. Suppose that the mobile node runs on $1.2GHz$ processor and the access point runs on $1.6GHz$ processor, the successful handover authentication needs $7.27ms$. Presently, the clock frequency of the majority Laptop is greater than $1.2GHz$. Thus, the proposed scheme is efficient if used on mobile devices. Table 1 also illustrates the energy use at the mobile node, where it is supposed that the mobile node runs on $1.2GHz$ processor. It can be computed as $E_{MN} = T_{MN} \times C$, with E_{MN} is the energy use, T_{MN} is the whole computing time for handover authentication and C is a CPU maximum power (10.88W). For communication cost, we suppose that an expected authentication message cost between access points and authentication server is B unit and that between mobile node and access point is ρ unit. As shown in Table 1. The proposed scheme is more efficient than the well-known schemes.

TABLE II
Timings for ECSM and Pairing Operations
ECSM: Elliptic Curve Scalar Multiplication

	1.2 GHz Processor		1.6 GHz Processer		2.0 GHz Processer	
Time (ms)	ECSM	Paring	ECSM	Paring	ECSM	Paring
	1.547	3.841	0.916	2.872	0.672	2.134

Table 3 shows the execution time of evaluation $t-$degree polynomial in Laptop if t varies needs $2t$ modular multiplications and t modular additions in the finite field F_p. In the implementation, p is set to 64 bit long for standard scheme such as RC5. For instance, the execution time on $1.2GHz$ laptop is $1.645\ ms$ if $t = 500$. So, evaluation of the polynomial is quick.

TABLE III
Timing for Evolution a t-Degree Polynomial

	1.2 GHz Processor			1.6 GHz Processor			2.0 GHz Processor		
Time (ms)	t=500	t=1000	t=1500	t=500	t=1000	t=1500	t=500	t=1000	t=1500
	1.645	3.265	4.397	0.799	1.623	2.359	0.517	1.075	1.661

© 2014, IJARCSMS All Rights Reserved

V. CONCLUSION

In this paper, we introduce a new scheme to obtain secure and efficient handover authentication. The security analysis and experimental results illustrate that the present scheme is feasible for real applications. Also, we prove its security in the random oracle model. Compared with the latest handover authentication schemes, a proposed scheme has the characteristics of efficiency and security.

ACKNOWLEDGEMENT

The author wishes to extend his thanks to the University of Bedfordshire, computer science Department and Technology for their helpful suggestions and supports.

References

1. Weijia Wang and Lei Hu, "A Secure and Efficient Handover Authentication Protocol for Wireless Networks", Journal of Sensors 14, pp. 11379-11394, 2014
2. He, D. Bu, J., Chan, S., Chen, C., and Yin, M., "Privacy-Preserving Universal Authentication Protocol for Wireless Communications", IEEE Transaction Wireless Communication, Volume 10, No. 2, pp. 431–436, 2011.
3. He,D., Chen, C., Chan, S., Bu, J., "Analysis and Improvement of a Secure and Efficient Handover Authentication for Wireless Networks", IEEE Communication Letters, 16, 1270–1273, 2012.
4. Choi, J. and Jung, S., "A Handover Authentication Using Credentials Based on Chameleon Hashing", IEEE Communication Letters, Volume 14, No. 1, pp. 54–56, 2010.
5. Tsai, J., Lo, N., Wu, T., "Secure Handover Authentication Protocol Based on Bilinear Pairings", IEEE Transactions, Wireless Communication, 73, 1037–1047, 2013.
6. Choi, J., Jung, S., Kim, Y. and Yoo, M., "A Fast and Efficient Handover Authentication Achieving Conditional Privacy in V2I Networks", LNCS 5764, Springer, pp. 291–300, 2009.
7. Yeo, S., Yap, W., Liu, J., Henricksen, M., "Comments on Analysis and Improvement of a Secure and Efficient Handover Authentication Based on Bilinear Pairing Functions", IEEE Communication Letters, 17, 1521–1523, 2013.
8. Yang, G., Huang, Q., Wong, D., and Deng, X., "Universal authentication protocols for anonymous wireless communications," IEEE Transaction Wireless Communication, Volume 9, No. 1, pp. 168–174, 2010.
9. He, D., Ma, M., Zhang, Y., Chen, C., and Bu, J., "A Strong User Authentication Scheme with Smart Cards for Wireless Communications", Computer Communication, Volume 34, No. 3, pp. 367–374, 2011.

AUTHOR(S) PROFILE

Dr. Sattar J. Aboud, received his Master degree in 1982 and a PhD in 1988 in the area of computing system. The two degrees were awarded from U.K. In 1990, he joined the Institute of Technical Foundation in Iraq as an assistant professor. In 1995 he joined the Philadelphia University in Jordan as a chairman of computer science department. Then, he moved as a professor at the Middle East University for Graduate Studies, Amman-Jordan. Currently, he is a visiting professor at University of Bedfordshire in UK. His research interests include areas such as public key cryptography, digital signatures, identification and authentication, networks security and cyber security. He has supervised numerous PhDs and Masters Degrees thesis. He has published more than 100 research papers in a multitude of international journals and conferences.

© 2014, IJARCSMS All Rights Reserved