An Efficient and Secure Mutual Authentication with Key Agreement Protocol for Automobile Roaming System

Xin Xu, Ping Zhu
School of Science,
Beijing University of Posts and Telecommunications,
Beijing, China
ahtcxinxin@126.com

Xin Xu, Ping Zhu, Zheng-Ping Jin, Hua Zhang
State Key Laboratory of
Networking and Switching Technology,
Beijing University of Posts and Telecommunications,
Beijing, China

Abstract--**With the fast advance of communication technologies, there is an increasing demand of efficient operations in low-power roaming environment. Several protocols came into being successively, yet for special requirements in automobile roaming system such as low consumption, high performance and convenience, these protocols cannot achieve a proper balance between security and efficiency since these protocols pay more attention to a common network environment. In order to go out from the embarrassing situation, we commit to provide a secure and effective mutual authentication mechanism for automobile roaming scenario. Our protocol employs elliptic curve cryptography system to reduce computational and communicational cost. Moreover, we also take into account common attacks and give corresponding resist measures to ensure security. In summary, our protocol is suitable for automobile roaming scenario since it provides user's anonymity, mutual authentication and is more efficient.**

Keywords- mutual authentication; key agreement; elliptic curve cryptography; automobile roaming

I. INTRODUCTION

Wireless communication systems have captured much attention since such systems can provide more convenient services. For instance, the automobile roaming service has been derived since more people tend to choose automobile to go wherever they want to go than ever. However, because of the different network environment, some services such as alarming, mileage consumption statistic, GPS navigation are necessarily limited by the place or network switching which will bring trouble to the users. So, how can an automobile driver get services given by his/her local network when he/she is away? These new technical problems call for a roaming system allowing an automobile driver to securely and efficiently receive desirable services. In such a system, when an automobile driver (AD) roams to a foreign network managed by a foreign agent (FA), it performs authentication with the FA under the assistance of his home agent (HA) in the home network [1].After a mutual authentication ran successfully, AD will access to services provided by FA. Therefore, an authentication scheme which allows an AD to obtain the services provided from the local network without effort when AD roams a long way from local network is what we desire. In addition, one of the major challenges in designing such mutual authentication protocol is to guarantee security and low-consumption. In order to resolve this problem, many protocols have been put forward constantly [1-6].

In 1981, Lamport [7] first proposed a remote authentication scheme in which the remote server could authenticate the remote user based on identity and password over an insecure network. However, in Lamport's scheme, the trusted party has to store verification tables. The existence of verification tables brings out some security risks. Subsequently, a series of schemes [8-12] based on Lamport's scheme are proposed.

In 2004, Zhu et al. [2] presented an authentication scheme with anonymity for wireless environments which has low computation. Unfortunately, Lee et al. [3] pointed out that Zhu et al.'s protocol failed to meet mutual authentication and cannot protect against a forgery attack in 2006. In 2008, Chang et al. [4] and Wu et al. [5] proposed two enhanced authentication schemes in global mobility networks, respectively. They claimed that their schemes could resist those attacks existing in Zhu et al.'s protocol. Subsequently, Zhou et al. [6] pointed out Chang et al.'s protocol failed to protect user anonymity and session key confidentiality. They also proposed an improvement to overcome the weakness in Chang et al.'s protocol. In addition, He et al. [13] proposed their strong user authentication scheme with smart cards for wireless communications.

The above schemes cannot meet desirable security and efficiency requirements because of the inherent characters of the automobile roaming system. As a case of the vehicular system, the automobile roaming system is more suitable arrange in pairs with a technical protocol which will enable to meet some special requirements since it has low-power device and frequent movement. What is more, due to the open network, attackers may launch sundry offensives to obtain some useful information. However, the protocols in [2-6, 13] cannot guarantee adequate security owing to their wide suitability for general communication network. Besides, these protocols have congenital designing defects. For instance, the protocol in [2] cannot achieve mutual authentication and cannot protect a forgery attack. What is more, the vehicle terminal is low-power and resource-limited, wherefore the mutual authentication scheme performed among AD, FA and HA should not employ parameters with long size. However, authors in protocol [13] assumed that the bit length of user's ID is 128 bit which means the user has to bear in mind such a 128 bit identity. Thus, the

Published by Atlantis Press, Paris, France.

protocols mentioned above caught in a dilemma of security and efficiency.

In order to cope with the above problems, we will propose a protocol which will reach a good balance between security and efficiency apply to automobile roaming scenario. Our protocol employs elliptic curve cryptography for reducing computation load and guaranteeing necessary security. Especially, our protocol is tailored for the automobile roaming system, which means our protocol is more suitable for low-power automobile roaming environment than the aforementioned protocols.

II. OUR PROTOCOL

In this section, we propose our protocol. In our protocol, not only the common attacks are eliminated but also the computational efficiency is improved. Our protocol also contains three entities: the automobile driver (AD), the home agent (HA) and the foreign agent (FA). Four phases are involved in our protocol: the Registration phase, the Login phase, the Authentication phase and the Password change phase. Before the registration phase starts, HA chooses an elliptic curve $E: y^3 \equiv x^3 + ax + b (\text{mod } p)$, then HA generates a group $E_P(a,b)$ with order n, where n is a large prime number. After that, HA selects a base point $P = (x_0, y_0)$. Here, P meets the equation $nP = O$. After all of these were completed, HA chooses its private key s_H and two secret numbers x and y .Then HA compute $A = h(x \| y)$, $h(y)$ and its public key $P_{HA} = s_H \cdot P$. After that HA transmits A to FA through a secure channel. As an AD may roam to more than one place, every FA holds different the parameter A which is delivered by the same HA.

A. Registration phase

In this phase, when AD wants to be a legal user from the system, it needs to perform the following steps:

Step R1: AD chooses its password PW_{AD} and a secret number d, then AD offers its identity ID_{AD} and $h(PW_{AD} \oplus d)$ to HA through a secure channel.

Step R2: HA computes $B = h(y) \oplus h(ID_{AD}) \oplus h(PW_{AD} \oplus d)$, $r = h(s_H \| ID_{AD} \| m)$, where s_H is HA's private key, m is chosen for each users by HA and the value of m is different for each user.

Step R3: HA sends AD a smart card which stores $\{E_P, n, P, P_{HA}, B, h(y), r, h(\cdot)\}$ via a secure channel. After receiving the smart card, AD inputs d into it. Finally, the smart card contains $\{E_P, n, P, P_{HA}, B, h(y), r, d, h(\cdot)\}$.

B. Login phase

When AD roams to a foreign network managed by FA and gets the service of FA, it needs to send a login message to FA. The steps should be performed as follows:

Step L1: AD inserts his/her smart card into the card reader and inputs the identity ID_{AD} and the password PW_{AD}, then the smart card computes $B^* = h(y) \oplus h(ID_{AD}^*) \oplus h(PW_{AD}^* \oplus d)$.

Step L2: Smart card verifies B^* and B are equal or not. If they are not equal, the mutual authentication will be terminated. Otherwise, AD is considered as a legal user. Then the smart card computes $C = n_{AD1} \cdot P$, $D = n_{AD1} \cdot P_{HA}$,

$E = h[r \oplus ID_{AD} \oplus h(C \| n_{AD2})]$,

$CID_{AD} = ID_{AD} \oplus h([C]_X \oplus T_{AD})$.

Here, n_{AD1} is a secret number and n_{AD2} is a random number chosen by AD, respectively. $[\ ]_X$ is the abscissa value of a point. A timestamp T_{AD} is selected by AD to resist replay attacks.

Step L3: On the behalf of AD, the smart card sends the message $m_1 = \{D, E, CID_{AD}, n_{AD2}, T_{AD}\}$ to FA.

C. Authentication phase

In this phase, FA and AD will run a mutual authentication under the assistance of HA. The steps should be performed as follows:

Step A1: Upon receiving message m_1 from AD, FA checks the validity of the timestamp T_{AD}. If it is not valid, FA refuses the login request of AD. Otherwise, FA generates a random number n_{FA} and a timestamp T_{FA}. Then FA computes $G = h(D \| E \| CID_{AD} \| A \| n_{FA} \| ID_{FA} \| T_{FA})$. Afterwards, FA sends the message $m_2 = \{D, E, CID_{AD}, n_{AD2}, n_{FA}, ID_{FA}, T_{AD}, T_{FA}\}$ to HA.

Step A2: Upon receiving message m_2 from FA, HA checks the timestamp T_{FA} is valid or not. If it is not valid, HA terminates this mutual authentication. Otherwise, HA computes $G^* = h(D \| E \| CID_{AD} \| A \| n_{FA} \| ID_{FA} \| T_{FA})$ and checks whether the equation $G^* = G$ holds. If they are equal, HA continues to compute $C^* = s_H^{-1} \cdot D$, $ID_{AD}^* = CID_{AD} \oplus h([C^*]_X \oplus T_{AD})$ $E^* = h[r \oplus ID_{AD}^* \oplus h(C^* \| n_{AD2})]$.

Then, HA compares E^* with E .If they are equal, HA considers that AD is a legal user. If they are not equal, HA sends "This is an illegal user" to FA which indicates that this session has been failed.

Step A3: Upon confirming the legality of AD, HA computes $SK = h[C \| n_{AD2} \| n_{FA} \| ID_{AD} \| ID_{FA}]$, $K_1 = SK \oplus h(A \| n_{AD2})$, $V_1 = h(A \| n_{FA} \| ID_{HA} \| K_1)$ and $S_1 = h(r \| ID_{FA} \| n_{FA})$.

Then, HA sends $m_3 = \{K_1, V_1, S_1, ID_{HA}, T_{HA}\}$ to FA. Here, T_{HA} is the timestamp chosen by HA.

Step A4: Upon receiving message m_3 from HA, FA checks the timestamp T_{FA} is valid or not. If it is not valid, FA terminates this mutual authentication. Otherwise, FA

computes $V_1^* = h(A \| n_{FA} \| ID_{HA} \| K_1)$ and decides whether $V_1^* = V_1$ holds. If the condition meets, FA believes that AD is an authorized user. Afterwards, FA computes the session key $SK = K_1 \oplus h(A \| n_{AD2})$ and sends message $m_4 = \{ID_{FA}, n_{FA}, S_1\}$ to the AD.

Step A5: Upon receiving message m_4 from FA, AD computes $S_1^* = h[r \| ID_{FA} \| n_{FA}]$ and decides whether $S_1^* = S_1$ holds. If the condition meets, FA believes that FA is legal. Afterwards, AD computes the session key $SK = h[C \| ID_{FA} \| ID_{AD} \| n_{AD2} \| n_{FA}]$.

D. Password change phase

In this phase, AD could freely change its password when it considers the existing password has been unsafe. It needs to perform the following steps:

Step C1: Please refer to Step L1 and Step L2 in the login phase for further information.

Step C2: If AD is considered legal, it could input its new password PW_{AD}^{new}. Otherwise, the smart card will reject the password change request.

Step C3: AD chooses a new secret number d_{new} and computes $h(PW_{AD}^{new} \oplus d_{new})$. Then the smart card computes $B_{new} = h(y) \oplus h(ID_{AD}) \oplus h(PW_{AD}^{new} \oplus d_{new})$ and replaces B with B_{new} .Finally, the smart card contains $\{E_P, n, P, P_{HA}, B_{new}, h(y), r, d_{new}, h(\cdot)\}$

III. Security and Efficiency Analysis

In this section, we analyze the security and efficiency of our scheme. The results show that our scheme can resist related possible attacks and can work correctly.

A. Security analysis

We will illustrate our scheme can meet the following security attributes even if the adversary launch the above attacks. TABLE Ⅰ lists the functionality comparisons of our protocol and other related protocols.

1) User anonymity

In the registration phase of our protocol, the identity of AD is submitted via a secure channel, thus the adversary cannot obtain ID_{AD}.

In the login phase, ID_{AD} is hidden in $CID_{AD} = ID_{AD} \oplus h(E \oplus [C]_X \oplus T_{AD})$, even if an adversary intercepts D, it still cannot compute C since it failed to gain s_H.

What is more, the encrypted value $E = h[r \oplus ID_{AD} \oplus h(C \| n_{AD2})]$ is used instead of ID_{AD} in order to protect the user's status information from wrongful appropriation by an adversary even he intercepts m_1 and obtains D and E. Since the real identification of AD is never transferred as plaintext over an insecure network channel, anyone cannot reveal ID_{AD} including FA. Our protocol can guarantee user anonymity.

2) Smart card stolen attack

Supposing that an AD's smart card was been stolen and the adversary extracts the secret information $\{E_P, n, P, P_{HA}, B, h(y), r, d, h(\cdot)\}$ in it. Meanwhile, the adversary also intercepts $m_1 = \{D, E, CID_{AD}, n_{AD2}, T_{AD}\}$ through the open channel. Even after gathering this information, in order to change the user's password or login into the system by using the lost smart card, the adversary has to get real identity ID_{AD} and the password PW_{AD} correctly at the same time, but it is not possible to guess these two parameters correctly at the same time in real polynomial time since they are protected by a one-way hash function and the attacker does not have knowledge of the master secret key x .Therefore, our protocol is secure against stolen smart card attacks.

3) Session key confidentiality

In our protocol, the final session key $SK = h[n_{AD2} \| n_{FA} \| ID_{AD} \| ID_{FA} \| C]$ contains two random numbers chosen by AD and FA, respectively. The secret parameters ID_{AD} and C ensure that there is no hidden security trouble in the session key. The adversary cannot get the session key, since our protocol provides user anonymity. Besides, even if the adversary get $D = n_{AD1} \cdot P_{HA}$ and the parameter P, he cannot make a precise calculation of n_{AD1} because it hard to solve the ECDLP problem. Consequently, the session key confidentiality in our protocol can be guaranteed.

4) Masquerade attack

In our protocol, HA authenticates AD according to check whether E^* and E are equal or not. If an adversary washes to masquerade a legal user AD to receive FA's service, he must forge a login message $m_1 = \{D, E, CID_{AD}, n_{AD2}, T_{AD}\}$ contains CID_{AD} . Unfortunately, the adversary cannot compute CID_{AD} correctly without ID_{AD} and $[C]_X$. Therefore, the adversary is blind to ID_{AD} and $[C]_X$, thus cannot be authenticated by HA according to check E^* and E is equal or not.

Furthermore, assume that A is a legal but malicious user of HA, i.e., A tries to impersonate another legal user to fool FA. It is noticeable that A cannot fake a login message $m_1 = \{D, E, CID_{AD}, n_{AD2}, T_{AD}\}$ even if A chooses another random number $n_{AD1}^{'}$ to compute $C^{'}$ and $D^{'}$ since A fails to reveal ID_{AD}. Besides, r is also a stumbling block for A to impersonate a legitimate user.

B. Efficiency analysis

In this section, we evaluate the efficiency performance of our protocol and make comparisons with other related protocols.

TABLE I. FUNCTIONALITY COMPARISONSS

Protocol	[3]	[4]	[5]	[6]	Ours
User anonymity	No	No	No	Yes	Yes
Smart card stolen attack	No	No	No	Yes	Yes
User friendliness	No	Yes	No	Yes	Yes
Fairness in key agreement	No	Yes	No	Yes	Yes
Session key confidentiality	Yes	No	Yes	Yes	Yes
Masquerade attack	No	No	No	Yes	Yes

Yes: prevents the attack or provides the security property;
No: does not prevent or not provides the property.

TABLE II. EFFICIENCY COMPARISONS

COMPARE ITEMS	[4]			[6]			[13]			Ours		
	A	F	H	A	F	H	A	F	H	A	F	H
Modular exponentiation	0	0	0	2	0	1	0	0	0	0	0	0
Hash operation	7	3	8	3	2	5	8	2	3	5	3	7
XOR operation	5	2	3	2	1	2	5	0	2	5	1	5
Symmetric cryptograph operation	0	0	0	0	0	0	2	1	2	0	0	0
Asymmetric cryptograph operation	0	0	0	0	0	0	0	2	2	0	0	0
Scalar multiplications	0	0	0	0	0	0	0	0	0	2	0	1
The maximum bandwidth (bytes)	210			446			186			136		

We compare the communication efficiency in terms of the maximum bandwidth. We assume that the parameter in our protocol is 160 bits in length and identification is 160 bits in length. Meanwhile the length of the ciphertext using symmetric/asymmetric encryption and the timestamp are set as 160 bits and 64 bits in length, respectively. A hash function $h(\cdot)$ is typically instantiated with the 160-bit SHA1. TABLE Ⅱ shows the number of various operations during login and authentication phases participating tripartite should calculate.

In our protocol, the longest message contains eight points. Therefore, the maximum bandwidth for our protocol is (160×6＋64×2) ／8＝136 byte. While in [10], [12] and [13], the maximum bandwidth is (160×4＋1024＋16) ／8 ＝210 byte, (1024×3＋160×3＋16) ／8＝446 byte and (1024＋160×2＋64×2＋16) ／8＝186 byte. Obviously, our protocol has the least bandwidth cost. Next, we will compare the computational cost between our protocol and other related protocols. Table.3 shows the number of various operations during login and authentication phases participating tripartite should calculate. By comprehensive analysis, our protocol is a well-balanced candidate for automobile roaming system.

IV. CONCLUSIONS

In this paper, we proposed an efficient and secure mutual authentication with key agreement protocol employing elliptic curve cryptosystem for an automobile roaming system. Though careful analysis, our protocol can withstand various common attacks and has low communication complexity. This implied our protocol satisfied the requirements of automobile roaming system. Lastly, we compared the efficiency and security between our protocol and competitive protocols and showed that our protocol is the most suitable candidate among similar protocols in automobile roaming system.

ACKNOWLEDGMENT

This work is supported by NSFC (Grant Nos. 61202434, 61170270, 61121061), the Fundamental Research Funds for the Central Universities (Grant Nos. 2011RC0505, 2011RCZJ15, 2012RC0612, 2011YB01).

REFERENCES

[1] J.Xu, W.T.Zhu, and D.C.Feng, “An efficient mutual authentication and key agreement protocol preserving user anonymity in mobile networks,” Computer Communication.vol. 34, pp. 319–325, 2011.

[2] L.Lamport, “Password authentication with insecure communication, ”Communications of the ACM.vol. 24, pp. 770-772, 1981.

[3] C.T.Li, M.S.Hwang, “An efficient biometrics-based remote user authentication scheme using smart cards, ” Journal of Network and Computer Applications. vol.33, pp.1-5, 2010.

[4] J.K.Jan, Y.Y.Chen, “Paramita wisdom” password authentication scheme without verification tables. The Journal of Systems and Software. vol. 42, pp. 45-47, 1988.

[5] M.S.Hwang, L.H.Li, “A new remote user authentication scheme using smart cards, ” IEEE Transaction on Consumer Electronics. vol. 46, pp. 28-30, 2000.

[6] H.M.Sun, “An efficient remote use authentication scheme using smart cards, ” IEEE Consumer Electronics Society. vol. 46, pp. 958-961,

[7] H.Y.Chien, J.K.Jan, Y.M.Tseng, “An efficient and Practical Solution to Remote Authentication: Smart Card, ” Computers & Security. vol, 21(4), pp. 372-375, 2002.

[8] J.Zhu, J.Ma, “A new authentication scheme with anomity for wireless environments, ” IEEE Trans. Consum. Electron.vol. 50(1), pp. 230-240, 2004.

[9] C.C.Lee, M.S.Hwang, I.E.Liao, “Security enhancement on a new authentication scheme with anonymity for wireless environments, ” IEEE Transactions on Industrial Electronic.vol. 53(5), pp. 1683-1686, 2006.

[10] C.C.Chang, C.Y.Lee, Y.C.Chiu, “Enhanced authentication scheme with anonymity for roaming service in global mobility networks, ” Computer Communication.vol. 32, pp. 611-618, 2009.

[11] C.C.Wu,W.B.Lee,W.J.Tasur, “A secure authentication scheme with anonymity for wireless communications, ” IEEE Communications Letters.vol. 12(10), pp. 722-723, 2008.

[12] T.Zhou, J.Xu, “Provable secure authentication protocol with anonymity for roaming service in global networks, ” Computer Networks.vol. 55, pp. 205-213, 2011.

[13] D.J.He, M.D.Ma, Y,Zhang, C,Chen,J.J.Bu, “A strong user authentication scheme with smart cards for wireless communications, ”Computer Communication.vol. 34, pp. 367-374, 2011.

[14] E.J.Yoon, K.Y. Yoo, K.S.Ha, “A user friendly authentication scheme with anoynymity for wireless communications, ” Computers and Electrical Engineering.vol. 37, pp.356-364, 2011.

[15] F. Li, X. Xin, Y. Hu. “Indentity-based broadcast signcryption, ” Computer Standards and Interfaces.vol. 30, pp. 89-94,2008.