http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 10 (12): 2413-2419, 2011
ISSN 1812-5638 / DOI: 10.3923/itj.2011.2413.2419

Trusted Mobile Nodes Access Scheme under Wireless Networks

[1]Lina Sun, [2]Guiran Chang, [1]Dawei Sun, [1]Lizhong Jin, [3]Jiandong Chen and [1]Xingwei Wang
[1]School of Information Science and Engineering, Northeastern University,
Shenyang 110819, Peoples Republic of China
[2]Computing Center, Northeastern University, Shenyang,
110819, Peoples Republic of China
[3]China Coal International Engineering Group Shenyang Design and Research Institute,
110819, Peoples Republic of China

Abstract: This study propose a trusted mobile nodes access method under the wireless network. The method based on the property attestation without the third party to verify the identity of mobile node platform instead of the method based on the property certificate or based on the platform configuration. When the mobile platform identity is verified, the mobile user identity is also verified at the same time. Besides, comparing with the existing method only providing the mutual attestation between mobile user and network agent, our methods also provides the mutual attestation between mobile users. At last, we use CK model to prove the security of our protocol.

Key words: Wireless networks, trusted mobile node, trusted computing, identity attestation, security

INTRODUCTION

With the development of wireless network technology, mobile devices become more popular, such as 3G cellular, WLAN terminal, WiMAX terminals and multi-mode terminals. Although, the opening of the wireless networks brings us the convenience it also brings risk, because the mobile terminals themselves have the risks (Zhenqiang *et al*., 2010). So the security of the mobile terminals becomes one of the key technologies for the Wireless networks. September 2006 the Mobile phone Working group in trusted computing group released a Mobile Trusted Module (MTM) specification V1.0 (TCG, 2007), aimed at establishing a credible security mechanisms to protect user's privacy information and sensitive data for the mobile terminal.

Trusted computing technology is then used to enhance the integrity attestation of the access node platform (Li *et al*., 2009, 2010) but these improved methods are based on the binary method (Changxiang *et al*., 2010) which is likely to expose the platform configuration information. The Property based attestation (Sadeghi and Stuble, 2004) is used to improve the access authentication of the mobile platform (Zhenqiang *et al*., 2010). However, many kinds of certifications are used, such as the attribute certificate, membership certificate, etc., that increase the cost of the entire network because of the issue and maintaining of these certificates and also bring the security risk to the wireless networks with lower bandwidth and higher error rate of channel. Besides the mobile node has to store these certifications to finish the attestation protocol which increase the load to the mobile terminal with limited computing power and the energy.

Considering the defect of mobile terminal in computing power and communication bandwidth, we propose a trusted mobile nodes access scheme under the wireless networks, based on the identity-based cryptography (Huaxi, 2006; Qi *et al*., 2010) and property-based attestation without a trusted third party (Chen *et al*., 2008). The definition of trusted mobile node is the nodes based on the MTM. The key idea of our scheme is both of the user's identity and the platform's identity are authenticated at the same time in the access process and the platform's identity can be verified directly by any network agent but the user's identity can be verified only by his home network agent. Here the idea of identity-based authenticated key is used to construct the session key between inter-authenticated parties. When a mobile node joins into a home network, the KGC (key generation center) in the home network will issue a public/private key to it which can be verified by the home network agent to allow the wireless access server. When

Corresponding Author: Lina Sun, School of Information Science and Engineering, Northeastern University, Shenyang 110819, Peoples Republic of China

the mobile node removes into a foreign network, the foreign network agent first verifies the identity of the mobile node with the help of home network agent and then it requires the KGC in the foreign network to issue a temporal private key for the mobile node. Using theses public/private keys, the network agents and the mobile nodes as well as the inter-mobile nodes can authenticate each other by the identity-based session key. The use of symmetric key reduces the communication cost and the use of temporary identity keeps the anonymity for the mobile user. Besides, the CK model (Canetti and Krawczyk, 2001, 1998) is used to theoretically analyze and prove the security of our proposed scheme.

RELATED WORK

Here, mathematical theory and security scheme of related work are shown.

Weil paring: Let E be an elliptic curve over a base field F. Let G_1 be a cyclic additive group by P whose odder is a prime q and G_2 be a multiplicative cyclic group of the same order q. We assume that the discrete logarithm problems in both G_1 and G_2 are hard. The Weil pairing (Chen and Kudla, 2004) is defined by a bilinear map ê: $G_1 \times G_1 \neg G_2$, where G_1 corresponds to the additive group of points of E (F) and G_2 corresponds to the multiplicative group of an extension field of F. The Weil pairing ê has the following properties:

- **Bilinear:** If $P, P_1, P_2, Q, Q_1, Q_2 \epsilon G_1$ then ê (P_1+P_2, Q) = ê (P_1, Q)+ê (P_2, Q) and ê (P, Q_1+Q_2) = ê (P, Q_1)+ê (P, Q_2)
- **Non-degenerate:** There exists a $P \epsilon G_1$, such that ê $(P, P) \neq 1$, where 1 is a generator of G_2
- **Computable:** There exists an efficient algorithm for compute ê (P, Q) for any $P, Q \epsilon G_1$.

Cryptographic assumptions

Bilinear Diffie-Hellman (BDH) problem (Chen and Kudla, 2004): Let P be a generator of G_1. The BDH problem in G_1, G_2, ê is given $(P, xP, yP, zp) \epsilon G_1$ for some x, y, z chosen at random from Zq, compute $e (P, P)^{xyz} \epsilon G_2$.

OMDL (One more Discrete Logarithm) problem (Baek *et al.*, 2005): Given (q, g, e, G_1, G_2), after n queries to the challenge oracle C (.) and m queries to the Discrete Logarithm oracle $Dl_{q,g}$ (.), where m<n, compute $s_1 \ldots s_n$, where $(g^{s1} = h^1)$ and $h_1, .. h_n \epsilon G_1$ output by C (.).

Canetti-Krawczyk model: CK model is proposed by Cantti and Krawczyk which is used to analysis and design the key-exchange (EK) protocol and the details of the model can be found in the original paper (Canetti and Krawczyk, 2001, 1998).

Definition 1: A key establishment protocol π is called session key security (SK-security) if the following properties are satisfied for any adversary U in the UM:

- If two uncorrupted parties complete matching sessions then they both output the same key
- The probability that U guesses correctly the bit b (i,e., b′ = b) is no more than 1/2 plus a negligible function in the security parameter

The advantage of U is defined by $Adv_{\pi,U}(k) = |Pr [b'=b]-1/2|$, sothesecond requirement will be met if the advantage of U is negligible. If the above properties are satisfied for all KE-adversaries in the AM then π is also SK-secure in the AM.

WIRELESS NETWORK SCHEME

The basic structure of our model is shown as Fig. 1. After the legitimate MTMs join in the DAA issuer group, they obtain the DAA certificates issued by these DAA issuers. Trusted CA has two roles: one is to verify the identity of KGC (Key Generation Center) and issue the public key certificate for KGC; the other is to discuss with KGC_S and confirm the platform configuration set denoted by CS for respective access domain where KGC is located. Each access region (or called service region) has its own KGC as a trusted third party to provide key distribution services for its members, such as mobile node, network agents etc. Mobile Node (MN) embedded a legitimate MTM chip is called trusted wireless device, who can access the Internet by the wireless way. Local network, foreign network, DAA issuer group and CA group are, respectively connected to the Internet through their own network connection devices such as routers by the wired way. Suppose that between the KGCs there are trust relationships which can be achieved by the traditional PKI technology based on the public key certificates issued by CA and each network agent (the home network agent HA, the foreign network agent FA) has got the knowledge of DAA issuer's public parameters and their respective platform configuration set CS. In the next section, we describe the details of the access protocols.

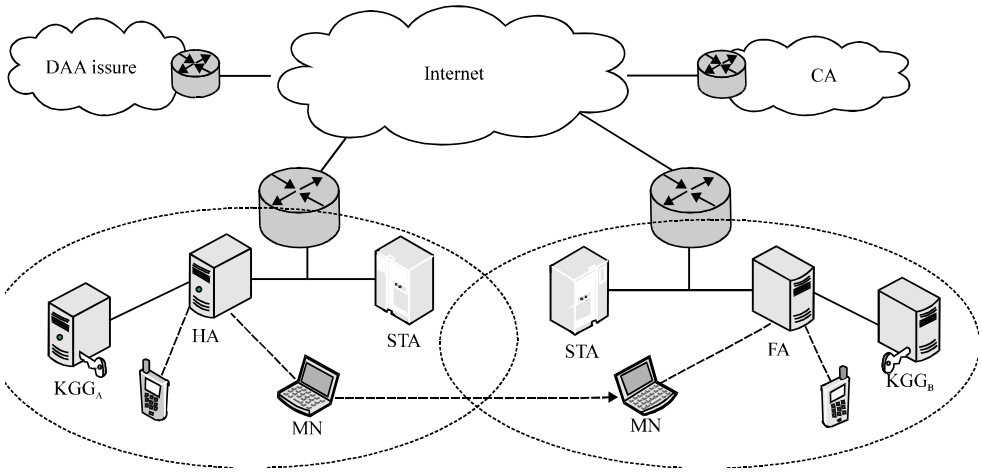

Fig. 1: Wireless network scheme

TRUSTED MOBILE NODE ACCESS PROTOCOLS

Initialization: In our model, we give some supposing as follows. First suppose that all the KGCs have the same the public parameters G_1, G_2, ê, q, P, H_1, H_2, H_3, where P is the generator of G1, the difference of KGCs are the KGC's private key (or called master key) $s \in Z^*_q$ and public key P_{sub} = sP. The feasibility of this assumption has been proved as (Huaxi, 2006; Qi *et al*., 2010; Hui *et al*., 2009); second suppose that there are two trusted authorities, say KGC_A and KGC_B which have public/private key pairs (P_{subA}, s_A) and (P_{subB}, s_B), respectively; Third suppose that there is a HA and a FA located in KGC_A and KGC_B, respectively. HA registers with KGC_A and get its private key $S_{HA} = s_A Q_{HA}$, where $Q_{HA} = H_1 (ID_{HA})$ and FA registers with KGC_B and get its private key $S_{FA} = s_B Q_{FA}$, where $Q_{FA} = H_1 (ID_{FA})$; Last suppose that each MN has got MTM certificate issued by respective DAA issuer and the certificate generation can refer to (Canetti and Krawczyk, 2001). Besides, because the case when MN registers in the home network is the special case when MN removes into the foreign homework, so we introduce the latter case. We suppose that after the register is successful, KCG_A sends the MN's public/private key (Q_{MN}, S_{MN}) to MN, where $Q_{MN} = H_2 (H_1 (ID_{MN}))$, $S_{MN} = s_A Q_{MN}$.

MN removes into the foreign network: When MN moves into a foreign network, its identity has to be verified by the foreign agent. The anonymous attestation and key agreement process are shown as Fig. 2 and the details are described as follows:

After received platform configuration set CS_B which is confirmed by CA and KGC_B and meets the platform access requirements for the foreign network, MN gives

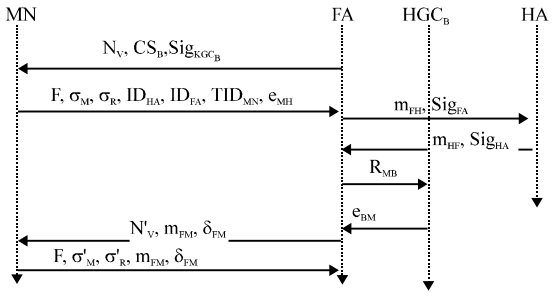

Fig. 2: MN accesses the foreign network

platform identity integrity proof based on the property and sends the proof to FA. FA first verifies the identity of MN platform and then turns to HA to require the attestation of mobile user's identity. If MN's identities including platform's identity and user's identity are verified successfully, then KGCB will send a temporary status for MN. Finally, MN can use this temporary identity to establish shared keys with FA and with other mobile nodes in the same foreign network. The authentication process of protocol mainly contains the mutual authentications between HA to MN, between FA and HA and between MN and FA.

Aiming at the authentication form HA to MN, because the flows need to be transferred by FA, so we need a mechanism to hide MN's identity as well as realize the identity authentication and then we reuse the scheme by Qi *et al*. (2010) to realize this aim; Aiming at the inter-authentications between MN and FA because MN and FA come from different network areas, so MN must get a identity issued by the KGC of FA and then we reuse the schemes by Hui *et al*. (2009) and Chen and Kudla (2004) to realize this aim. Aiming at the for the same

domain authentication both sides should establish a symmetric key. Aimed at inter-authentications between FA and HA, because is no third party, so we used the ordinary signature scheme to realize this aim. The details of our protocol are shown as follows:

Step 1: FA first verifies the MN platform's identity

Step 2: MN randomly chooses r_{MB}, r_{MH}, $r_{MF} \in_R Z^*_q$, computes the public parameters R_{MB}, R_{MF}, R'_{MF}, the temple identity of MN denoted by TID_{MN}, the session key between MN and KGC_B denoted by K_{MB} and the session key between MN and HA denoted by K_{MH}, makes the message uses m_{MH} and uses the session K_{MH} to encrypt m_{MH} denoted by e_{MH}, where $R_{MB} = r_{MB}P_{subB}$, $R_{MF} = r_{MF}Q_{MN}$, $R'_{MF} = r_{MF}P$, $TID_{MN} = r_{MH}Q_{MN}$, $K_{MB} = r_{MB}P$, $K_{MH} = H_2(\hat{e}(S_{MN}, r_{MH}Q_{HA}))$, $m_{MH} = \{ID_{HA}, ID_{FA}, ID_{MN}, r_{MH}, R_{MB}, R_{MF}, R'_{MF}\}$, $e_{MH} = E_{K_{MH}}(m_{MH})$. MN sends $\{F, \sigma_M, \sigma_R, ID_{HA}, ID_{FA}, TID_{MN}, e_{MH}\}$ to FA

Step 3: After received the message from MN, FA gets the timestamp T_{FA}, makes the message $m_{FH} = \{ID_{HA}, ID_{FA}, TID_{MN}, e_{MH}, T_{FA}\}$, computes a signature on m_{FH} using FA's private key $Sig_{FA} = E_{S_{FA}}(H_3(m_{FH}))$ and sends $\{m_{FH}, Sig_{FA}\}$ to HA

Step 4: After received the message from FA, HA first verifies the timestamp T_{FA} and the signatures Sig_{FA}. If the verifications are successful, HA computes the session key between HA and MN denoted by K_{HM}, where $K_{HM}H_1\hat{e}(TID_{MN}, S_{HA})$. Then decrypts e_{MH} using K_{HM}, gets ID_{MN} and r_{MH} and verifies the equation $r_{HM}H_1\hat{e}(ID_{MN}) = TID_{MN}$. If the verification is successful, HA trusts MN's identity according to the Eq. 1, makes the message $m_{HF} = \{ID_{HA}, ID_{FA}, TID_{MN}, R_{MF}, R'_{MF}, R_{MB}, T_{HA}\}$, computes $Sig_{HA} = E_{S_{HA}}(H_3(m_{HF}))$ and sends $\{m_{HF}, Sig_{HA}\}$ to FA:

$$K_{HM} = \hat{e}(r_{MH}Q_{MN}, s_AQ_{HA}) = \hat{e}(S_{MN}, r_{MH}Q_{HA}) = K_{MH} \quad (1)$$

Step 5: After received the message from HA, through checking the timestamp and the signature, FA trusts the identity of MN user which has been verified by a trust HA. Then FA sends R_{MB} to KGC_B

Step 6: After received news from FA, KGC_B issues a temporal private key S'_{MN} to MN, computes the session key K_{BM} between KGC_B and MN and use this session key to encrypt temporal private key denoted by e_{BM}, where $S'_{MN} = s_BQ_{MN}$, $K_{BM} = s_B^{-1}R_{MB}$, $e_{BM} = E_{K_{BM}}(S'_{MN}, expiry)$, expiry denotes the expiry time of S'_{MN}. KGC_B sends e_{BM} to FA

Step 7: FA randomly chooses $r_{FM} \in_R Z^*_q$ and a nonce N'_v, computes $R_{FM} = r_{FM}Q_{FA}$, $R'_{FM} = r_{FM}P$ and the session key between FA and MN denoted by K_{FM}, makes the message m_{FM} and computes a MAC value on m_{FM} denoted by δ_{FM}, where $K_{FM} = H_2(\hat{e}(S_{FA}, R_{MF}+r_{FM}Q_{MN}))$, $m_{FM} = \{ID_{HA}, ID_{FA}, TID_{MN}, R_{FM}, R'_{FM}, R_{MF}, R'_{MF}, e_{BM}\}$, $\delta_{FM} = MAC_{K_{FM}}(m_{FM})$. FA sends $\{N_v, m_{FM}, \delta_{FM}\}$ to MN

Step 8: After received news from FA, MN first uses K_{MB} to decrypt e_{BM} and gets the temporary secret key S'_{MN} and expiry, according to the Eq. 2. During the expiry date of S'_{MN}, MN computes the session key between MN and FA denoted by K_{MF} and verifies δ_{FM}, where $K_{MF} = H_2(\hat{e}(S'_{MN}, R_{FM}+r_{MF}Q_{FA}), r_{MF}R'_{FM})$. If the verification is successful, MN trusts FA's identity according to the Eq. 3. Then MN gives the platform identity proof on N'_v including a commitment F', a TPM signature σ'_M and a ring signature σ'_R. MN makes the message m_{MF} and computes a MAC value on m_{MF} denoted by δ_{MF}, where $m_{MF} = \{TID_{MN}, ID_{HA}, ID_{FA}, R_{MF}, R'_{MF}, R_{FM}, R'_{FM}\}$, $\delta_{MF} = MAC_{K_{MF}}(m_{MF})$. MN sends $\{F', \sigma'_M, \sigma'_R, m_{FM}, \delta_{MF}\}$ to FA:

$$K_{BM} = s_B^{-1}R_{MB} = PP_{subB}^{-1}P_{subB}r_{MB} = r_{MB}P = K_{MB} \quad (2)$$

$$K_{MF} = H_2(\hat{e}(Q_{MN} + Q_{FA})^{s_B(r_{MF}+r_{FM})}, r_{FM}r_{MF}P) = K_{FM} \quad (3)$$

Step 9: FA first verifies σ'_M, σ'_R and then uses K_{FM} to verify δ_{MF}. If all validations are successful, FA trusts the MN's identity including MN's platform identity and user identity according to the Eq. 3

SECURITY ANALYSIS

Because MN joins the Internet through the home agent is the example of through the foreign agent, so we analysis the access process when MN moves to the foreign network and through the FA to join the Internet in detail. To describe easily, the access process through FA is called ID based Mobile Node Foreign Access (IDMA). In the following sections, the authentication security and anonymity of IDMA protocol is proved.

Here we adopt CK model to give the authentication security proof. CK model has been used to prove the security of key exchange (EK) protocol (Canetti and Krawczyk, 2001; Huaxi, 2006). According to the design principle for secure KE protocols in CK, if π is a secure KE protocol in the Authenticated-links Model (AM) and C is an authenticator, then $C(\pi)$ is a secure KE protocol in the unauthenticated-links model (Canetti and Kaawczyk, 1998), we give the authentication security proof for IDMA protocol. First, we give the security IDMA protocol in

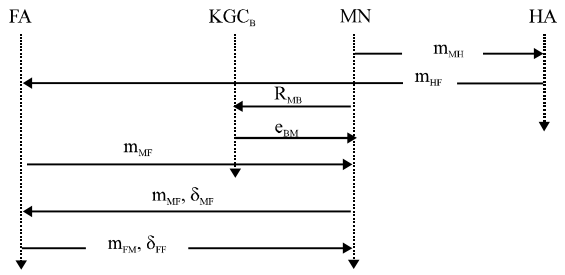

Fig. 3: IDMA in AM

AM; then we construct the security authenticators; At last get the security IDMA protocol in UM by combination and optimizing.

Secure IDMA protocol in AM: According to the definition of adversary scheme in the AM, the messages between MN and HA or between MN and KGC_B can be transferred honestly by FA. So here we suppose there is direct link between MN and HA as well as between MN and KGC_B. Next we give the description of IDMA in AM seen as Fig. 3:

Step 1: MN randomly chooses $r_{MH} \in_R Z^*_q$, computes $K_{MH} = H_2(\hat{e}(S_{MN}, r_{MH}Q_{HA}))$, $TID_{MN} = r_{MH}Q_{MN}$ and $e_{MH} = E_{K_{MH}}(ID_{MN}, r_{MH})$, makes the message $m_{MH} = \{ID_{HA}, ID_{FA}, TID_{MN}, R_{MF}, R'_{MF}, e_{Mh}\}$ and then sends m_{MH} to HA

Step 2: HA computes $K_{MH} = \hat{e}(TID_{MN}, S_{HA})$, decrypts e_{MH} and verifies the equation $TID_{MN0} = r_{MH}.Q_{MN}$. If the verification is successful, it means HA trusts MN's user identity. Then HA makes the message $m_{HF} = \{ID_{HA}, ID_{FA}, TID_{MN}, R_{MF}, R'_{MF}\}$ and sends m_{HF} to FA

Step 3: MN randomly chooses $r_{MB} \in_R Z^*_q$, computes $R_{MB} = r_{MB}P_{subB}$ and $K_{MB} = r_{MB}P$ and then sends R_{MB} to KGC_B

Step 4: KGC_B issues a temporary secret key $S'_{MN} = s_B Q_{MN}$ for MN and computes $K_{BM} = s_B^{-1}R_{MB}$ and $e_{BM} = E_{K_{BM}}(S'_{MN}, expiry)$, where expiry represents the period of validity for S'_{MN}. KGC_B sends e_{BM} to MN

Step 5: FA randomly chooses $r_{MH} \in_R Z^*_q$ and a nonce N, computes $R_{FM} = r_{FM}Q_{FM}$, $R'_{FM} = r_{FM}P$, makes the message $m_{FM} = \{ID_{HA}, ID_{FA}, TID_{MN}, R_{FM}, R'_{FM}, CS_B\}$ and sends m_{FM} to MN

Step 6: MN randomly chooses $r_{MF} \in_R Z^*_q$, computes $R_{MF} = r_{MF}Q_{MN}$, $R'_{MF} = r_{MF}P$, $K_{MF} = H_2(\hat{e}(S'_{MN}, R_{FM}, r_{MF}Q_{FA}), r_{MF}R'_{FM})$ and platform configuration information $\{F, \sigma_M, \sigma_R\}$, makes the message $m_{MF} = \{m_{FM}, R_{MF}, R'_{MF}, F, \sigma_M, \sigma_R\}$, computes $\delta_{MF} = MAC_{K_{MF}}(m_{MF})$ and then sends $\{m_{MF}, \delta_{MF}\}$ to FA

Step 7: FA computes $K_{FM} = H_2(\hat{e}(S_{FA}, R_{MF}, r_{FM}Q_{MN}), r_{FM}R'_{MF})$ and verifies the equation $\delta_{MF} = MAC_{K_{MF}}(m_{MF})$. If the verification is successful, it means FA trusts MN's identity. Then FA computes $\delta_{FM} = MAC_{K_{MF}}(m_{MF})$ and sends $\{\delta_{FM}, m_{MF}\}$ to MN

Step 8: MN verifies the equation $\delta_{FM} = \delta_{MF}$. If the verification is successful, it means MN trusts FA's identity

Next, we prove that the IDMA protocol is SK-secure in the AM.

Theorem 1: IDMA protocol is SK-secure in the AM, if the TPM signature and ring signature schemes are secure, the BDH problem, OMDL problem, discrete logarithm problem are hard and the encryption algorithm EK is secure against chosen message attack, as well as HA is trust and MN?HA and FA are uncorrupted.

Proof: According to the definition 1, if we what to prove IDMA protocol is SK-secure in the AM, we must give the proof that our protocol satisfied the two properties.

Proof (sketch) (i): When MN、HA and FA are uncorrupted, it is clear that when the IDMA protocol is finished, according the Eq. 3, we can get the conclusion that $K_{MF} = K_{FM}$ which means both MN and FA output the same session key. The first property had been proved over.

Proof (sketch) (ii): In order to prove our IDMA protocol satisfied the second properties, we give a theorem 2 described below.

Theorem 2: If the advantage of U to break IDMA protocol denoted by $Adv_{IDMA,U}(k) = |Pr[b' = b]-1/2|$ is non-negligible, then U can solve the BDH problem or OMDL problem or Discrete Logarithm problem or break the ring signature or TPM signature.

Proof: If U can successfully attack session key between MN and FM, three conditions are must satisfied together: 1) U can successfully forge a platform property (proof; 2) U can successfully get the temporary secret key S'_{MN}; 3) U can break the session key protocol between MN and FA.

Proof (sketch) (1): Because we use the method of Chen *et al.* (2008) to prove the platform's identity and this method has been proved that it is satisfied with the evidence authentication (Chen *et al.*, 2008). From the conclusion of Chen *et al.* (2008), we get the following conclusion: (1) the max probability that U break this method is:

$$q^2/2^{l\Phi}+\varepsilon_{TPM}+\varepsilon_{ring}+\varepsilon_{dlog}$$

where, ε_{TPM}, ε_{ring} and ε_{dlog}, respectively denotes the probability of U to forge a TPM signature, forge a ring signature and solve a discrete logarithm problem, $q^2/2^{l\Phi}$ is negligible in the security parameter and (2) this probability is negligible.

Proof (sketch) 2): From Fig. 3, we can see S'_{MN} is sent to MN from KGC_B by the form of $E_{K_{BM}}(S'_{MN})$. So if U what to get S'_{MN}, it must break the encryption algorithm E_K which is semantically secure against an adaptive chosen ciphertext attack or compute the session key K_{BM} which is an OMDL problem seen formula 2. We use $Adv_{E_K,U}$ and $Adv_{OMDL,U}$ to, respectively denote the advantage of U to break a security encryption algorithm E_K and solve an OMDL problem. So the max probability of U to successfully get the temporary identity secret key S'_{MN} is

$$\max\{Adv_{E_K,U}+1/2, Adv_{OMDL,U}+1/2\}$$

Proof (sketch) 3): From Fig. 3, we can see the session key protocol between MN and FA is based on the method of (Huaxi, 2006), where the protocol is proved to be SK-security under the BDH assumption. Here, we use $Adv_{BDH,U}$ to denote the advantage of U to break a BDH problem. So the max probability of U to successfully break a BDH problem is $Adv_{BDH,U}+1/2$.

So the probability of U to guess the session key K_{MF} successfully can be computed using formula 4:

$$\begin{aligned}&\min\{\max\{Adv_{E_K,U}+1/2, Adv_{OMDL,U}+1/2\}, Adv_{BDH,U}+1/2, q^2/2^{l_\Phi}+\varepsilon_{TPM}+\varepsilon_{ring}+\varepsilon_{dlog}\}\\&=\min\{\max\{Adv_{E_K,U}, Adv_{OMDL,U}\}, Adv_{BDH,U}, q^2/2^{l_\Phi}+\varepsilon_{TPM}+\varepsilon_{ring}+\varepsilon_{dlog}\}+1/2\end{aligned} \quad (4)$$

So the advantage of U to break the session key K_{MF} is:

$$\begin{aligned}&Adv_U(k)=|\min\{\max\{Adv_{E_K,U}, Adv_{OMDL,U}\}, Adv_{BDH,U}, q^2/2^{l_\Phi}+\varepsilon_{TPM}+\varepsilon_{ring}+\varepsilon_{dlog}\}|\\&\le \max\{Adv_{E_K,U}, Adv_{OMDL,U}, Adv_{BDH,U}, q^2/2^{l_\Phi}+\varepsilon_{TPM}+\varepsilon_{ring}+\varepsilon_{dlog}\}\end{aligned} \quad (5)$$

So if $Adv_U(k)$ is non-negligible, according to the formula 5, at least one of the $Adv_{E_K,U}$, $Adv_{OMDL,U}$, $Adv_{BDH,U}$, $q^2/2^{l\Phi}$, ε_{TPM}, ε_{ring} and ε_{dlog} has to be non-negligible, however this contradicts with the supposing conditions. Theorem 2 has been proved over.

By now, the theorem 1 is proved to end which means the IDMA protocol is SK-secure in the AM. Next we show some authenticators used in our scheme.

MT-authticators: We use the identity authenticator based on the anonymity identity $\lambda_{ENC,TID,T}$ (Qi *et al*., 2010), the message transport authenticator based on the anonymity identity $\lambda_{OMDL,T}$ (Hui *et al*., 2009), the signature authenticator based on the timestamp $\lambda_{Sig,T}$ (Tin *et al*., 2004) and the session key authenticator based on MAC $\lambda_{MAC,K}$ (Boyd *et al*., 2004), to emulate the message flows, respectively from MN to HA, from MN to KCG_B, between HA and FA as well as between FA and MN. The details can be seen as from studies of Qi *et al*. (2010), Hui *et al*. (2009), Tin *et al*. (2004) and Boyd *et al*. (2004).

Secure IDMA protocol in UM: We use the authenticators $\lambda_{ENC,TID,T}$, $\lambda_{OMDL,T}$, , $\lambda_{Sig,T}$ and $\lambda_{MAC,K}$ to our protocol in the AM to obtain a secure protocol in the UM, shown as Fig. 2. Its SK-security follows from Definition 1. In the next section, we give the definition of anonymity.

CONCLUSION

In this study, we propose a trusted platform access method under the wireless network. We use the method based on the property attestation without the third party to verify the identity of mobile node platform instead of the method based on the property certificate or based on the platform configuration. We use the way of consulting between CA and KGC to confirm the platform configuration set. The advantage is on the one hand, the security of platform configuration set is provide by the participation of two trusted third parties; on the other hand, avoid mobile platform access monopoly caused by each network. Besides, in terms of mobile user identity authentication, our protocol not only provides the mutual attestation between mobile user and network agent but also provides the mutual attestation between mobile users. At this point, previous agreements do not have this feature. Besides, based on CK model, our method has been proved to satisfy the authentication security and anonymity.

ACKNOWLEDGMENTS

This study is supported by the National Natural Science Foundation of China under Grant No. 61070162, 71071028, 60802023 and 70931001; the Specialized Research Fund for the Doctoral Program of Higher Education under Grant No. 20100042110025 and 20070145017; the Fundamental Research Funds for the Central Universities under Grant No. N100604012, N090504003 and N090504006.

REFERENCES

Baek, J., R. Safavi-Naini and W. Susilo, 2005. Universal designated verifier signature proof (or how to efficiently prove knowledge of a signature). Proceedings of the 11th International Conference on the Theory and Application of Cryptology and Information Security, Dec. 4-8, Chennai, India, pp: 644-661.

Boyd, C., W. Mao and K.G. Paterson, 2004. Key agreement using statically keyed authenticators. Proceedings of the 2nd International Conference on Applied Cryptography and Network Security, (ICACNS'04), (ICACNS'04), pp: 248-262.

Canetti, R.B. and H. Kaawczyk, 1998. A modular approach to the design and analysis of authentication and key exchange protocols. Proceedings of the 13th Annual ACM Symposium on Theory of Computing, May 24-26, New York, USA., pp: 419-428.

Canetti, R. and H. Krawczyk, 2001. Analysis of key exchange protocols and their use for building secure channels. Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques: Advances in Cryptology, (ICTACTAC'01), London, UK, pp: 453-474.

Changxiang, S., Z. Huanguo and W. Huaiming, 2010. Research and development for trusted computing. Sci. China, 40: 139-166.

Chen, L. and C. Kudla, 2004. Identity based authenticated key agreement protocols from pairing. Proceedings of the 16th IEEE Computer Security Foundations Workshop, 30 June-2 July, IEEE, pp: 219-233.

Chen, L., H. Lohr, M. Manulis and A.R. Sadeghi, 2008. Property-based attestation without a trusted third party. Proceedings of the 11th International Conference on Information Security, (ICIS'08), Springer-Verlag Berlin, pp: 31-46.

Huaxi, P., 2006. An identity based authentication model for multi-domain. Chin. J. Comput., 29: 1271-1281.

Hui, Z., L. Hui, S. Wanli and W. Yumin, 2009. Id-based wireless authentication scheme with anonymity. J. Commun., 30: 130-136.

Li, Y., M. Jianfeng and Z. Jianming, 2009. Trusted and anonymous authentication scheme for wireless networks. J. Commun., 30: 29-35.

Li, Y., M. Jiangeng, P. Qingqi and M. Zhuo, 2010. Direct anonymous authentication scheme for wireless networks under trusted computing. J. Commun., 31: 98-104.

Qi, J., M. Jianfeng, L. Guangsong and L. Hongyue, 2010. Identity-based roaming protocol with anonymity for heterogeneous waterless networks. J. Commun., 31: 138-145.

Sadeghi, A.R. and C. Stuble, 2004. Property-based attestation for computing platforms: Caring about properties, not mechanisms. Proceedings of the 2004 Workshop on New Secruity Paradigms, Sept. 20-23, Nova Scotia, Canada, pp: 66-77.

TCG, 2007. TCG mobile trusted module specification version 1.0. Revision 1, 12 June 2007, Trusted Computing Group.

Tin, Y.S.T., H. Vasanta, C. Boyd and J.M.G. Nieto, 2004. Protocols with security proofs for mobile applications. Proceedings of the ACISP, (ACISP'04), Sydney, Australia, pp: 358-369.

Zhenqiang, W., Z. Yanwei and Q. Zirui, 2010. Access mechanism of TMP under mobile network. J. Commun., 31: 158-169.