Improving Security and Efficiency in Mobile IP Networks

[1]Thilagavathy R,PG Scholar-Communication Engineering,
[2]Dr.Uma.S, Associate Professor-Department of ECE,
Coimbatore Institute of Technology, Coimbatore, India

***Abstract*—The emergence of mobile devices or mobile nodes allows the users to access the network when they are on the move. As users move frequently from one network to another network a new IP address is assigned to the mobile node every time when it visits a new network. The change in IP address is informed to other nodes is dealt by Mobile IP.The ID based protocol minimizes the registration delay through a minimal usage of the identity (ID)-based signature scheme that eliminates expensive pairing operations.The proposed protocol takes, advantages of self-certified key for PKI(public key infrastructure). To provide explicit authentication for self-certified key, we propose to use a concept of self-certificate. It is a user-generated certificate for the self-certified public key by signing the public key and relevant information with the private key corresponding to the public key. In this scenario, user can renew his key pairs by himself without any interaction with CA, while keeping the authenticity of CA's certification. CA can also use the same revocation mechanism as that of certificate-based scheme to revoke an issued key.As an application of self-certificate, we present a secure transaction scheme with mobile agents in hostile environment. This paper describes a version of this protocol that uses elliptic curves and eliminates the impersonation attacks. Numerical analysis and computer simulation results demonstrate that the proposed protocol outperforms the existing ones in terms of the registration delay and the computational load on a Mobile Node while improving security.**

Keywords—Mobile IP, registration, ID-based, user anonymity, authentication,self certified key,self certificate.

I. INTRODUCTION

WIRELESS COMMUNICATION, is undergoing a rapid growth.With the convergence of wireless and IP,both data and voice communications rely increasingly on IP based technologies. Next-generation mobile networks will be envisioned as all IP-based networks [1], [2]. Security support is indispensable for Wireless Communication.Mobile IP [3],[4] was designed to support mobility within the network. In MIP each mobile node (MN) is identified by its home agent (HA) and home address in the home network. While roaming away from home to a visiting network, a mobile node is associated with a care-of address (COA), which gives information about its current address. MN registers the COA at its home agent.

Then the HA will redirect the data packet destined to the MN's home address to MN's foreign agent (FA) at the visiting network and finally to the MN's COA. Anonymity in the sense hiding the identity of nodes.As a form of remote redirection that involves all the mobility entities, the registration part of mobile IP is very crucial and must be guarded against any malicious attacks [5] ,that might try to take illegitimate advantages from any participating principals.

The Basic mobile IP protocol [3],[4] use secret keys with manual key distribution for authentication of control messages.This approach is not scalable.The scalability is provided by certificate-based public key infrastructure(CA-PKI) known as Jacob's proposal.This proposal is used for the authentication among mobile node (MN), foreign agent (FA) and home agent (HA)[6];however it is computationally expensive and low bandwidth of MN to get the Certificate Revocation List(CRL) from issuing CA leads to serious problem. Later proposed protocol ,employ minimal use of the public key cryptography proposed by Suf and Lam[7].This proposal minimize computing power and provides scalability; nevertheless, their registration delay is somewhat long.The another approach proposed by yang[8] combines minimal public key with session key to produce a secure key in mobile node registration protocol;provides high security and thereby increasing the registration delay.

To achieve a better performance ,research works employ the identity based public key cryptography to exclude time consuming certificate operation,however these works are at conceptual level and cannot be used for real system.Hence there is need to introduce specific ID-based signature scheme into mobile IP registration with user anonymity,which can lead to a secure and efficient registration.In this paper, a novel ID-based mobile IP registration protocol featured with user anonymity. There are four major contributions in this paper: 1) the paper introduces the ID-based signature (IBS) scheme without pairings for the authentications between FA and HA to minimize the registration delay because it eliminates expensive pairing operations; 2) the proposed protocol achieves user's anonymity by letting MN transmit a temporary identity (TID) instead of its true identity; 3) the proposed

protocol employs the nonces from MN, HA, and FA to prevent all possible replay attacks; 4) in order to optimize the proposed protocol, the secret keys K'_{MN-HA} and K_{MN-FA} are generated by MN,rather than transmitted to MN over links. Numerical analysis and computer simulation results demonstrate that the proposed protocol outperforms the existing ones while providing stronger security.

In traditional certificate-based public key infrastructures, a user's public key is authenticated by means of a trusted third party's (TTP_1) explicit signature on the public key. *Self-Certified keys* [14] are an efficient alternative in which the user's public key is extracted using the *identity* of the user and TTP's signature on this identity. E-mail addresses and IP addresses are two good examples of identities. Self-certified keys are related to *identity-based cryptography.* Unfortunately,many self-certified schemes suffer from the *key escrow* problem, meaning that TTP gains access to the user's private key as well. Avoiding this problem is a desirable property of self-certified key issuing protocols

Related Work. Ateniese et al. presented a selfcertified, identity-based (SCID) scheme which uses multiplicative groups and is based on the Nyberg-Rueppel signature scheme [15]. While a solution was presented to the key escrow problem by blinding TTP to the user's private key, this solution is susceptible to impersonation attacks and requires a proof of knowledge to be used securely.

Contributions. The blind key issuing protocol using elliptic curve groups is presented, which does not require an proof of knowledge and is not susceptible to impersonation attacks. Eliminating the proof of knowledge is shown to reduce the complexity of the key issuing protocol.

Applications. Self-certified keys and identity-based schemes are well-suited for dynamic networks, where efficient and compact authentication is needed. Elliptic curves also provide small key and signature sizes, which can be an advantageous feature in dynamic networks.

Here ,the ID based signature scheme into mobile IP registration with user anonymity is compared with the self certified key issuing protocol using elliptic curves in mobile IP registration.

The rest of this paper is organized as follows: Section II Background of the IBS scheme without pairings. Section III proposes new mobile IP registration protocol based on the IBS scheme without pairings and describes the adversary models in mobile IP, and then presents the protocol goals.Section IV Self certified key issuing protocol.Section V numerical analysis and NS2 implementation are given in Section VI. Finally, the paper concludes in Section VII.

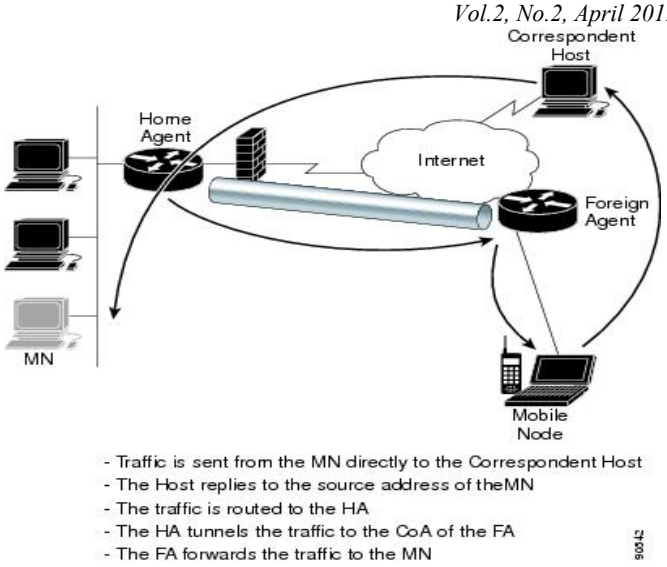


Fig.1 MIP Registration

II.BACKGROUND

The concept of IBS was introduced by Shamir in 1984. The idea is to let a user's identity to be used as his public key.The corresponding private key of user can be generated by a publicaly trusted Key Generating Server(KGS).The IBS scheme is proved to be secure in terms of existential unforgeability against the chosen message and ID attacks. The case of implementation and degree of security depends on choice of this curve **E.**In the IBS system,**G** is an order **p** cyclic subgroup of an elliptic curve **E** over a finite field **F**, such that the elliptic curve discrete log problem (ECDLP) is intractable.

Setup: Given security parameter k $\in$ N, the KGS generates system parameters and a master public/secret key pair as follows: (1) choose a generator *P*of *G*, pick a random $x \in RZp$ and compute $Ppub = xP$; (2) set the master public key $mpk = Ppub$ and the master secret key $msk = (x, Ppub)$; (3) choose two hash functions $H1 : \{0, 1\}^* \rightarrow Zp$ and $H2 : \{0, 1\}^* \rightarrow Zp$; (4) publish system parameters _*E/***F**, *P, p, Ppub,H*1,*H*2_ and keep *x* secret.

Extract: Given a user's identity $ID \in \{0, 1\}^*$, the KGS generates the user's private key *usk* as follows: (1) pick a random $r \in RZp$ and compute $R = rP$; (2) compute $s = r - cx \pmod p$, where $c = H1(Ppub, ID,R)$; (3) set *usk* to (*c, s, ID, Ppub*) and transport it to the user securely.

Sign: To sign a message $m \in \{0, 1\}^*$ under the private key $usk = (c, s, ID, Ppub)$, the user takes the following steps: (1) pick a random $t \in RZp$ and compute $T = tP$; (2) compute $e = H2(Ppub, ID,m,T, c)$ and $\pi = t - es \pmod p$; (3) return the user's signature $\sigma = (c, T, \pi)$ on message *m*.

Verify: A verifier checks the user's signature $\sigma = (c, T, \pi)$ on message m as follows: (1) compute $e = H2(Ppub, ID, m, T, c)$; (2) output: **accept** if $c = H1(Ppub, ID, cPpub+e-1(T-\pi P))$, **reject** otherwise.

III. PROPOSED SCHEME

In this section , we propose new ID-based mobile IP registration protocol with user anonymity, and specify the adversary models in mobile IP, which are security threats and attacks that mobile entities have faced in mobile IP registration, and then present the protocol goals.

A. Notations

We will use the notations in Table I to describe the proposed protocol.

TABLE I
NOTATION

Symbol	Description
M,N	Concatenation of two messages *M* and *N*,in the order specified
‖	Concatenation of two data
Request	A bit pattern indicating a request
Reply	A bit pattern indicating a reply
Result	A value indicating result of the request
Advertisement	A bit pattern indicating an advertisement
MN_{HM}	MN's home address
MN_{COA}	MN's care-of-address
HA_{id}	HA's IP address as its ID
FA_{id}	FA's IP address as its ID
N_{MN}, N_{HA}, N_{FA}	Nonces issued by MN, HA, and FA, respectively
K_{MN-HA}	Shared keys between MN and HA
K_{FA-HA}	Shared keys between FA and HA
K_{MN-HA}	Shared keysbetween MN and FA
mpk	The master public key
msk	The master secret key
usk_{FA} , usk_{HA}	The private key of FA and HA respectively
σ_F	FA's signature on M3
σ_H	HA's signature on M4
‹M›K	MAC value of message M under key K
A→B:M	A sends the message M to B
{M}K	Encryption of message M under key K
Key-Request	A bit pattern indicating session key request
Key-Reply	A bit pattern indicating session key reply

B. Protocol Description

Both FA and HA in the mobile IP system employ the ID-based public key infrastructure, in which the private key usk_{FA} of a FA is (c_{FA} , s_{FA}, ID_{FA}, P_{pub}) and the private key usk_{HA} of a HA is (c_{HA}, s_{HA}, ID_{HA}, P_{pub}).

1)*Mobile node initial registration in its home network:*

When a mobile node is added to the mobile IP system, the new node's home agent first verifies the node's identity ID_{MN} and shares a secret key K_{MN-HA} with it. Then HA produces a nonce N_{HA} and computes MN's temporary identity ($ID_{MN}||N_{HA}$), where $H:\{0,1\}^* \rightarrow \{0,1\}^*$. HA will pick $t_\alpha \in_R Z_P$, and compute $\alpha = t_\alpha P$ to be used by MN in next registration.Finally, HA allocate data ($H(ID_{MN}||N_{HA})$, K_{MN-HA}, $N_{HA,\alpha}$) to the MN securely.

2) Mobile node location registration with its HA in a foreign network:

Fig. 2. shows the proposed mobile IP registration protocol that proceeds as follows:

• ***Agent Advertisement:***

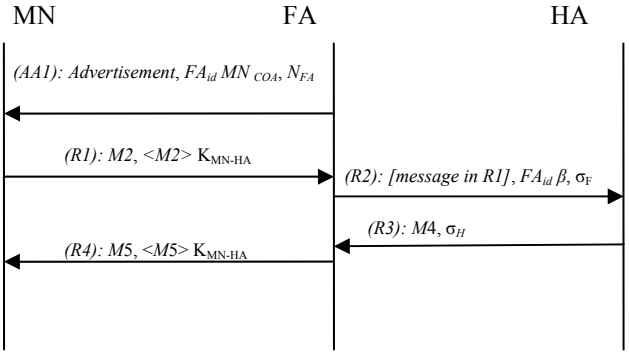
(AA1) FA → MN : *M*1

where $M1 = Advertisement, FA_{id}, MN_{COA}, N_{FA}$

• ***Registration:***

(R1) MN → FA : $M2, \langle M2 \rangle K_{MN-HA}$

where $M2 = Request, Key\text{-}Request, , HA_{id}, MN_{COA}, N_{HA,} N_{MN}$, N_{FA}, FA_{id} , α, $H(ID_{MN} || N_{HA})$



$M2 = Request, Key\text{-}Request, FA_{id}, HA_{id}, MN_{COA,} N_{HA}$, N_{MN}, N_{FA}, α , $H(ID_{MN}||N_{HA})$

$M3$ = [message in R1], FA_{id}, β $\sigma_F = Sig(usk_{FA}, M_3) = (c_F, T_F, \pi_F)$

$M4 = M5, \langle M5 \rangle K_{MN-HA}$, N_{FA}, { K_{MN-FA} } K_{FA-HA}

$\sigma_H = Sig(usk_{HA}, M4) = (c_H, T_{H,}, \pi_H)$

$M5 = Reply, Result, Key\text{-}Reply, MN_{HM,} HA_{id}$, N_{MN}, N'_{HA}, σ'

Fig. 2. Proposed mobile IP registration protocol

On receipt of agent advertisement, MN generates a registration request consisting of , the non-authentication Extensions (N_{FA}, FA_{id}, α, $H(ID_{MN}||N_{HA})$), and Mobile-Home Authentication Extension $\langle M2 \rangle K_{MN-HA}$ .Then MN sends request to FA.

(R2) FA → HA : $M3, \sigma_F$

where $M3$ = [message in R1], $FA_{id,} \beta$

$\sigma_F = Sig(usk_{FA}, M3) = (c_F , T_F , \pi_F)$

Upon receipt of R1, FA validates N_{FA}. If the nonce is valid,FA picks $t_\beta \in_R Z_P$ computes $\beta = t_\beta P$, and generates the signature σ_F on the message $M3$ using its private key usk_{FA} (see Section II). Then FA appends the non-authentication Extensions (FA_{id}, β) and the Foreign-Home Authentication

Extension σ_F to the request message from MN and sends it to HA. If the nonce is not valid, FA ignores the registration request and sends MN a reply with suitable denial code.

(R3) HA → FA : $M4, \sigma_H$

where

$M4 = M5, \langle M5 \rangle K_{MN-HA}, N_{FA}, \{ K_{MN-FA} \} K_{FA-HA}$

$M5 = Reply, Result, Key\text{-}Reply, MN_{HM}, HA_{id}, N'_{HA}, N_{MN}, \alpha'$

$\sigma_H = Sig(usk_{HA}, M4) = (c_H, T_H, , \pi_H)$

When HA receives the request, it will check if FA_{id} in $M3$ equals FA_{id} in R1. If these two values are equal, HA validates N_{HA}; otherwise it rejects the request with a denial code. If the received N_{HA} is correct, HA checks if the signature σ_F is valid; otherwise it rejects the request with suitable denial code. If the signature verification algorithm returns **accept** (see Section II), HA has authenticated FA successfully, otherwise HA returns a reply with suitable denial code. Then HA uses $H(ID_{MN}||N_{HA})$ in $M2$ to find the shared secret K_{MN-HA} in HA's database and validates $\langle M2 \rangle K_{MN-HA}$ with K_{MN-HA}. If the calculated $\langle M2 \rangle K_{MN-HA}$ equals the received $\langle M2 \rangle K_{MN-HA}$, HA has authenticated MN successfully; **otherwise** HA sends a reply with suitable denial code.

If the above verification succeeds, HA will accept MN's request, dynamically assign a home address to MN, and store the new mobility binding of MN_{HM} and MN_{COA}. Then HA computes $K_{FA-HA} = t_\alpha \beta$ and erase t_α. Afterwards, HA updates the registration parameters as follows: a) HA picks $t'_\alpha \in {}_R Z_P$, and computes $\alpha' = t'_\alpha P$ for MN's next registration; b) it produces a new nonce N'_{HA} and computes MN's new temporary identity $H(ID_{MN}||N_{HA})$; c) it generates the new key K'_{MN-HA} *MN-HA* and secret key *KMN-FA* via the HMAC-SHA-1 one-way function [10]–[13]:

$$K'_{MN-HA} = HMAC{-}SHA{-}1(K_{MN-HA}, N'_{HA}||N_{MN}||HA_{id}) \quad (1)$$

$$K_{MN-FA} = HMAC{-}SHA{-}1(K_{MN-HA}, N_{HA}||N_{MN}||FA_{id}) \quad (2)$$

d) HA overlays (ID_{MN}, $H(ID_{MN}||N_{HA})$, K_{MN-HA}, N_{HA}, α, t_α) with (ID_{MN}, $H(ID_{MN}||N'_{HA})$, K'_{MN-HA}, N'_{HA}, α', t'_α) for MN's next registration.

Finally, HA constructs a registration reply message as follows: a) HA computes the Mobile-Home Authentication extension $\langle M5 \rangle K_{MN-HA}$; b) it generates the signature σ_H on the message $M4$ using its private key usk_{HA} (c_{HA}, s_{HA}, ID_{HA}, P_{pub}). c) HA appends the non-authentication Extension α', the Mobile-Home Authentication Extension $\langle M5 \rangle K_{MN-HA}$, the non-authentication Extension (N_{FA}, $\{ K_{MN-FA} \} K_{FA-HA}$), and the Foreign-Home Authentication Extension σ_H to the fixed portion of the registration reply and transmits the reply to FA.

(R4) FA → MN : $M5, \langle M5 \rangle K_{MN-HA}$

On receiving the reply from HA, FA validates N_{FA}. If the nonce is valid, FA checks if the signature σ_H is valid; otherwise it sends a reply with a suitable denial code to MN. If the signature verification algorithm outputs **accept**, FA has authenticated HA successfully; otherwise FA returns a rejection reply to MN. If the above verification succeeds, FA will compute $K_{FA-HA} = t_\beta \alpha$ and erase t_β. Then FA decrypts $\{K_{MN-FA} \} K_{FA-HA})$ with K_{FA-HA} to get K_{MN-FA}. Finally, FA relays the reply ($M5, \langle M5 \rangle K_{MN-HA}$) to MN. Upon receipt of R4, MN validates N_{MN}. If the nonce is correct, MN compares the calculated $\langle M5 \rangle K_{MN-HA}$ with the received $\langle M5 \rangle K_{MN-HA}$; otherwise MN's registration attempt fails. If these two MAC values are equal, MN computes K'_{MN-HA} and K_{MN-FA} according to (1) and (2). Then MN generates the new TID $H(ID_{MN} || N'_{HA})$ and overlay (ID_{MN}, $H(ID_{MN} || N'_{HA})$, K_{MN-HA}, N_{HA}, α) with (ID_{MN}, $H(ID_{MN} || N'_{HA})$, K'_{MN-HA}, N'_{HA}, α')for the next registration.

3) Tunneling:

When HA intercepts a datagram destined for MN, HA encapsulates the datagram and then routes it to the Careof Address through a tunnel. After arriving at the end of the tunnel, the datagram is decapsulated and then correctly delivered by FA to MN.

C. Adversary Models in Mobile IP

1) Denial-of-Service (DoS) attacks: a) A malicious node can impersonate a legal MN to generate a bogus registration request specifying his own IP address as Care-of Address and thus redirect the latter's traffic toward itself and causing the legal MN to lose its network connectivity; b) an attacker may intercept the registration reply message from HA to a legal MN, causing the MN to receive maliciously altered traffic or to lose the parameters synchronization with its HA and resulting in unsuccessful registration afterwards .

2) Replay attacks: a) By eavesdropping, an attacker can store a valid registration request that has been accepted by HA and replay it later for directing packets to MN's previous location; b) an attacker first records a valid request and its corresponding reply from some pervious run of successful registration. Then the attacker replays the request and corresponding reply to FA in turn. FA believes that the registration is one generated by a legitimate MN and HA. Therefore, the attacker spoofs FA and can use resources on FA's local network for free.

3) Passive eavesdropping: In mobile IP registration, passive eavesdroppers are mainly interested in two pieces of information: a) the secret keys exchanged among mobile entities; b) a mobile user's identity information.

IV ELLIPTIC CURVE SELF CERTIFIED KEY ISSUING PROTOCOL

Self-certified keys are an efficient alternative to certificate based PKI. Instead of verifying public keys using an explicit signature on a user's public key, the public key is extracted directly from TTP's signature on the user's identity. This reduces the storage and computational requirements.While the extracted public key cannot be explicitly verified, resulting signatures will not verify unless the extracted key is authentic. If the message signature fails to verify, it is unknown whether the user's signature on the message is invalid or the extracted public key is invalid (or both).

A Self-Certified Identity based (SCID) scheme based on the Nyberg-Rueppel signature[15] scheme was presented in where the focus is on provable security. As such, exponentiation of separate generators to the power of the hash values from H takes place. No such exponentiation is present here, as the focus is on efficiency and practicality. While it was noted that elliptic curve groups provide an efficient setting, all of the notation therein is for multiplicative groups. The scheme is presented below. Let $k_{(i)}$ be random integers in Z^*_r.

Setup: Primes r, q such that r | (q − 1) are chosen, as well as a generator g of order r. TTP generates a private key s_T and public key w_T as

$w_T = gs \pmod q$, where $s_T \in Z^*_r$

Keygen To generate a key pair on user A's identity IDA, TTP calculates

$r_A = g^k H(IDA) \pmod q$

$s_A = -k - s_T r_A \pmod r$ (4)

and escrows (r_A, s_A) to A.

$$TTP \rightarrow A : k_A G$$

$$TTP : (r_A, b_A) = COMPRESS (K_A G + K_T G)$$

$$r_A = r_A + H(ID_A)$$

$$s_A = k_T - r_A s_T \pmod r$$

$$A \rightarrow TTP : (r_A, b_A, s_A)$$

$$s_A = k_A + s_A \pmod r$$

Extract: To extract A's public key $w_A = g_{SA}$ on identity ID_A given public value r_A, B calculates

$$w_A = \frac{H(ID_A)}{w_D^{rA} r_A} \pmod q$$

$$W_A = DECOMPRESS (r_A - H(ID_A), b_A - r_A w_T)$$

$$W_A = DECOMPRESS (\overline{r_A} + H(ID_A) - H(ID_A), b_A) - r_A W_T$$

$$= k_A G + k_T G - r_A s_T G = (k_A + k_T - r_A s_T) G$$

$$= (k_A + \overline{s_A}) G = s_A G$$

The key issuing protocol Keygen only reaches Trust Level1(user's private key and can therefore impersonate the user without being detected). Note that (r_A, s_A) is simply a Nyberg-Rueppel signature by TTP on the message IDA. A's private key is s_A while r_A is used by other users to reconstruct A's public key as shown in Extract. The public key is correct:

$$w_A = \frac{H(ID_A)}{w_D^{rA} r_A} = \frac{H(ID_A)}{g^{s_T r_A} g^k H(ID_A)} = \frac{1}{g^{-k - s_A + k}} = g^{sA}$$

As with Nyberg-Rueppel signatures, existential forgery is still possible. In this case, if two users have identities that hash to the same value, they can impersonate the other user.

V PERFOMANCE EVALUATION

A. Simulation Setup

Simulations are carried out to evaluate the performance of the proposed protocol, based on NS2. For Yang's protocol [8], RSA with a 1024-bit modulus and the public exponent of $e = 2^{16} + 1$ is used for sufficient security and fast computation. Therefore, an RSA public key consists of a pair (*n, e*), resulting in a total size of 131 bytes. In addition, an RSA signature consists of a single 1024-bit value. FA and HA's IP address of 32 bits are used as their ID and certificate expiration time can be encoded in 2 bytes. An RSA certificate ‹ID_A, (*n, e*), *exp,*CA's signature› will be a total of 265 bytes in length. For self-certified public key protocols , the modulus 1024 bits, which can provide the required security. For the proposed protocol, *p* is a 160-bit Solinas prime in the IBS scheme. Such choices of *p* deliver a comparable level of security to 1024-bit RSA.

In order to simulate realistic scenarios, we have imported traffic flows as the background load between HA and FA. First, we study the performance of the proposed protocol by varying the number of mobile nodes and their registration delay.Secondly, we study the signalling traffic by increasing number of nodes.

B. Simulation Results

1) Registration delay:

It is clear that the performance of CA-PKI based protocol is restricted by the heavy certificate-based public key cryptography operations on MN. Therefore, the basic protocol, Yang's protocol and the proposed protocol are implemented. Because the registration delay varies over the course of a simulation, it is helpful to look at the time average for this statistics.

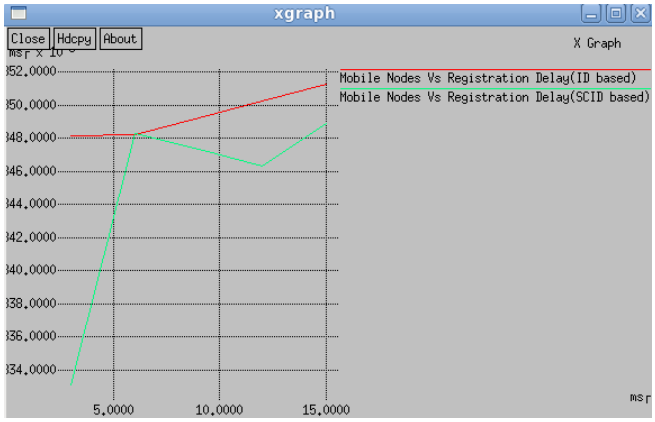


Fig. 3 Registration delay for various number of nodes

TABLE I
Registration Delay of various protocol

Protocol	MN-FA	FA-HA	HA-FA	FA-MN	Total Reg. Delay
Basic	2.7191	1.004	1.0144	2.7031	7.4406
CA-PKI	7.6417	5.9266	6.3170	7.6457	27.61663
Yang	2.7934	16.056	15.0117	2.8007	36.6618
Proposed	3.3813	7.647	1.0156	2.7615	14.8054

From figure.3,
we have the following five observations: (1) compared to Yang's protocol, the average registration delay of the proposed protocol is drastically reduced for two main reasons: a) the proposed protocol eliminates certificate-based operations and does not employ expensive pairings; b) $K'_{MN\text{-}HA}$ and $K_{MN\text{-}FA}$ are not transmitted by HA to MN but generated locally by MN, leading to the save of the time spent in transmitting these two keys over links and the associated encryption and decryption at HA and MN;(2) the proposed protocol takes a little more time than the basic protocol, because the proposed protocol provides much stronger security and there exists a trade-off between the security and efficiency;(3) the registration delay of the proposed protocol is smaller than that of the ID based protocol. It is clear that the secret key distribution in the proposed protocol is better. These observations confirm that the proposed protocol minimizes the registration delay while improving the security. The simulation results agree with the analytical results. For example, the registration delay of the proposed protocol is reduced up to 49.3 percent approximately, compared to Yang's protocol.

2) Registration signaling traffic:

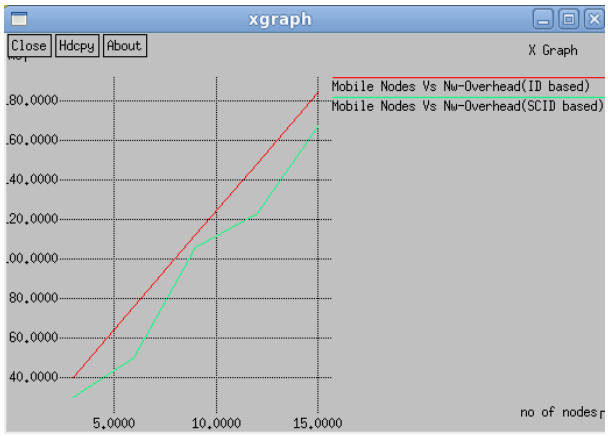
Compared to Yang's protocol ,the proposed protocol saves the communication bandwidth between FA and HA because of no RSA signature and certificate of large size in the exchanged messages; messages between MN and FA of the proposed protocol slightly longer for security consideration.The proposed protocol has less message size.Hence proposed protocol has less registration signalling traffic with stronger security.

Table II lists the message sizes of four protocols.

TABLE II
Message Size of various protocol

Protocol	MN-FA	FA-HA	HA-FA	FA-MN
Basic	50	50	46	46
CA-PKI	66	578	582	66
Yang	50	50	46	46
Proposed	82	176	146	48

3) Computational load on MN: The basic protocol only needs two SHA operations since it maintains the lowest level of security; Yang's protocol needs nine DES operations on MN; However, the proposed protocol only performs three SHA operations on MN considering offline computation. Although the variant protocol seems to save SHA on generating the keys, it needs more SHA operations while validating MAC due to the longer message *M*5. Moreover, the proposed protocol can generate the keys offline.Therefore,the proposed protocol can save the computation time and battery consumption on MN while improving the security.



In conclusion, the proposed protocol outperforms the existing protocols in terms of the registration delay, the registration signaling traffic, and the computational load on a MN while providing the improved security.

VI CONCLUSION

Thus,Elliptic curve SCID scheme has less registration delay in comparison with Elliptic curve Id based registration scheme.Improvement is done by integrating it with the AAA for its flexible mobility among different administrative domains.The protocol has also extended to the Bluetooth communication. Moreover,the replay attacks can be prevented using nonces from MN,HA and FA.Therefore, efficiency and security of the network using propsed protocol is better than the previous other protocol.

REFERENCES

[1] C. Politis, K. A. Chew, N. Akhtar, M. Georgiades, R. Tafazolli, and T.Dagiuklas, "Hybrid multilayer mobility management with AAA context transfer capabilities for all-IP networks," *IEEE Wireless Commun.*, vol.11, no. 4, pp. 76-88, Aug. 2004.

[2] S. J. Kwon, S. Y. Nam, H. Y. Hwang, and D. K. Sung, "Analysis of a mobility management scheme considering battery power conservation in IP- based mobile networks," *IEEE Trans. Veh. Technol.*, vol.53, no.6, pp.1882-1890, Nov. 2004.

[3] C. Perkins, "IP mobility support," IETF RFC 2002, Oct. 1996.

[4] C. Perkins, "IP mobility support for IPv4," IETF RFC 3344, Aug.

2002.

[5] W. Haitao and Z. Shaoren,"The security issues and countermeasures in mobile IP," in *Proc. IEEE ICII'01*, vol. 5, pp. 122-127, 29 Oct. 2001.

[6] J. Zao, S. Kent, J. Gahm, G. Troxel, M. Condell, P. Helinek, N.Yuan , and I. Castineyra, "A public-key based secure mobile IP," *Wireless Netw.*, pp. 373-390, May 1999.

[7] Sufatrio and K.Y. Lam, "Mobile-IP Registration Protocol: a Security Attack and New Secure Minimal Pubic-key based authentication ,Proc.1999 Intnl. Symp. Parallel Architectures, Sep. 1999.

[8] C.Y. Yang and C.Y. Shiu, "A Secure Mobile IP Registration Protocol,"Int. J. Network Security,vol. 1, no. 1, pp. 38-45, Jul. 2005.

[9] Lanjun Dang, Weidong Kou, *Senior Member, IEEE,* Hui Li, Junwei hang, Xuefei Cao, Bin Zhao, and Kai Fan"Efficient ID-Based Registration protocol Featuredwith User Anonymity in Mobile IP Networks " *IEEE Wireless Commun.*, vol.9, no. 2, pp. 594-604, Feb.2010.

[10] L. Salgarelli, M. Buddhikot, J. Garay, S. Patel, and S. Miller,"Efficient authentication and key distribution in wireless IP networks," *IEEE Wireless Commun.*, vol. 10, no. 6, pp. 52-61, Dec. 2003.

[11] P. Calhoun, T. Johansson, C. Perkins, and P. McCann, "Diameter MIPv4 application," IETF RFC 4004, Aug. 2005

[12] C. Perkins and P. Calhoun, "Authentication, authorization, and Accounting (AAA) registration keys for mobile IP," IETF RFC 3957,Mar. 2005.

[13] Rathi.S,Thanushkodi.K, "Performance Analysis of Mobile IP Registration Protocols,"*WSEASTRANCATIONS on COMPUTERS,*Issue 3,Volume 8,pp. 538-548March 2009.

[14] M. Girault. Self-certified public keys. In D.W. Davies,editor, *Advances in Cryptology - EuroCrypt '91*, pages 490–497, Berlin, 1991. Springer-Verlag. Lecture Notes in Computer Science Volume 547.

[15] Billy Bob Brumley " Blinding Self-Certified Key Issuing Protocols Using Elliptic Curves" TKK T-110.5290 Seminar on Network Security 2006-12-11/12