Mobile IP Registration Protocols: A Survey

Senthil Kumar Mathi
Department of CSE
Amrita Vishwa Vidyapeetham
Coimbatore, Tamil Nadu, India

M.L.Valarmathi
Department of CSE
Government College of Technology
Coimbatore, Tamil Nadu, India

ABSTRACT

IP Mobility which was established to facilitate mobility within a worldwide system of interconnected computer networks gives a scalable solution for different networks. As the commercial use of the internet becomes common for IP Mobility through the wireless communication, it is necessary to construct a secure IP Mobility in a registration process which informs the location of the portable systems such as mobile devices to the home network. While registering the locality with the packet transmission by the portable system, the security issues are of paramount importance and this registration must be secured against any cruel attacks that might attempt to acquire unauthorized advantages from any participating principals. The need for secure way to do Mobile IP registration has given rise to a number of protocols. This paper discusses the various existing Mobile IP Registration protocols. The simulation and comparisons has been conducted on the different protocols with the security parameters and registration time to evaluate each protocol's efficiency.

General Terms

IP Mobility, IP Security, Public Key Infrastructure, Hierarchical mobility, Certificateless signature and Identity-Based Public Key Cryptosystem.

Keywords

Authentication, Confidentiality, Non-repudiation, Registration delay, Replay attack and User anonymity.

1. INTRODUCTION

Mobile computing is becoming omnipresent. The past few years have seen a proliferation of portable computers and laptops. However, current internet routing protocols (IP, OSI etc.) require the network address to be changed when a host moves to a new location [1]. This is inconvenient for laptops and other mobile stations. The Mobile IP Protocol (MIP) [2] handles this problem using Mobility Agents. Mobility agents keep track of mobile hosts and are responsible for routing packets to them. Agents, however, use static IP for routing their packets. Mobile IP is simple in the sense that it uses the existing mechanisms of IP Encapsulation [3, 4], ICMP messages and ARP. So the next generation mobile based networks [5, 6] will be identified as all IP-supported networks.

2. MOBILE INTERNET PROTOCOL

2.1 An Overview

The original IP was designed for stationary hosts because the part of the address defines the network to which the host is attached. The address is valid only when the host is attached to the network. If network changes the address is no longer valid. When a host moves from one network to another, the IP addressing structure needs to be modified. The host has its original address in the IP header [7]; called the home address and a temporary address called care-of-address (CoA). The home address is fixed; it associates the host to its home sub network.

When a host moves from one network to another, the CoA changes; it is associated with the foreign network, the network to which the host moves. In Figure.1, The source S sends a packet to a Mobile Node (MN). The Home Agent (HA) intercepts the packet, encapsulates and tunnels it to a Foreign Agent (FA). The FA then decapsulates it and hands it to the MN.

2.2 Working Mechanism of Mobile IP

The FA consistently advertises their occurrence by the use of agent advertisement messages. The MN accepts these advertisements and finds whether it is on its home network or a foreign network. When MN detects it is at home, it operates without mobility services. When recurring to its home network, it deregisters with the HA through the exchange of registration request and reply messages. When the MN detects that it has moved to a foreign network, it acquires a care-of address on the foreign network. The CoA can be either be obtained from agent advertisements (FA's CoA), or by some other mechanism like DHCP (a co-located care-of address). MN then registers its new CoA with its home agent through registration request and reply messages, possibly via its FA. Datagrams sent to MN are intercepted by HA, encapsulated and tunnelled to the mobile's CoA without any cruel attacks [8]. They are received at the tunnel endpoint by FA (or by MN itself), decapsulated and handed to MN. The datagrams sent by MN are routed to their destination by static IP routing.

3. MIP REGISTRATION PROTOCOLS

3.1 Base Protocol

The base protocol uses nonce or timestamp to provide replay protection. This protocol is self-synchronizing [2, 9] and two nodes with nonces only require the pseudo-random number generators. However, two nodes using timestamps must have sufficiently synchronized time-of day clocks and require clock resynchronization in case the timestamp is not valid. The high level representation of this registration protocol of the IP Mobility can be given as follows.

(1) $MN \rightarrow FA : M_1, <M_1>S_{MN\text{-}HA}$

where M_1 = Request, FA_{id}, HA_{id}, MN_{HM}, MN_{COA}, N_{HA}, N_{MN}

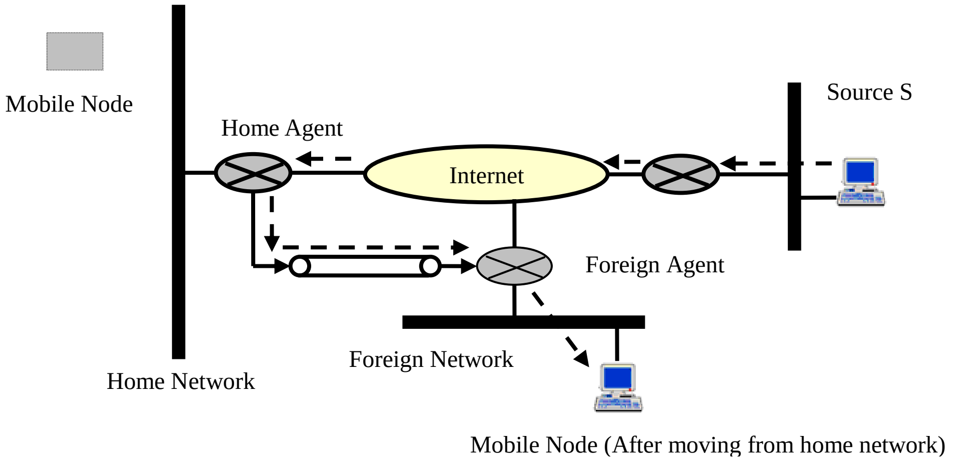

Fig 1: Mobile IP model

(2) FA → HA : M_1, $<M_1>S_{MN-HA}$

(3) HA → FA : M_2, $< M_2>S_{MN-HA}$

where M_2 = Reply, Result, FA_{id}, HA_{id}, MN_{HM}, N'_{HA}, N_{MN}

(4) FA → MN : M_2, $<M_2>S_{MN-HA}$

3.2 A Secure Registration Protocol for Wireless Internet

A Secure registration protocol [10] is proposed to implement Mobile IP environment with the communication model through two way authentication by symmetric encryption between MN and HA, MN and HA, and MN and FA for secure transmission of messages. This protocol is similar to basic protocol but with the security in terms of authentication and location privacy through certain entries such as temporary number, node identification number etc., to guarantee the secure communication. The registration protocol can protect the transmission from attacks such as reply and wiretap and also attain the position privacy of the mobile node.

3.3 A Secured Registration Protocol for MIP

In this approach [11], the certified public key mechanism is used to provide mutual authentication which is not available in the secure registration protocol between FA and HA for secured registration and also distinctively FA and HA sign on each message sent to each other and verify the signature on the message received from each other. The mutual authentication between MN and HA is provided in the already existing security association between them. The session key between the MN and FA is proposed by the mobile node and forwarded to FA by HA. It is used in succeeding communication between MN and FA to prevent unauthorized access and man-in-the-middle attack.

3.4 CA - PKI Based Protocol (Jacob's Protocol)

The secret key based authentication in basic Mobile IP protocol is not a scalable approach. This reason is main motivation for Certificate Authority – Public Key Infrastructure (CA-PKI) based authentication proposed by Jacob. The Jacob's method [12] defines a new certificate extension message format intended to carry information about certificates, which now must always be appended in all the control messages. Jacob's method allows Mobile Nodes and Mobility Agents to use:

- X.509 digital certificates
- Public keys
- Digital signatures

3.5 A Public-Key Based Secure Mobile IP

Here [13], a public key management system is used to satisfy the security aspects of Mobile IP by authenticating Mobile IP control messages and protecting packet redirection with IPSec protocols. Both authenticated registration and the end-to-end IPSec (IP Security) tunnelling has been provided. The protocol describes the design and the implementation of a public key management system that can be used with IETF basic and route optimized Mobile IP. This system is known as the Mobile IP Security (MoIPS) system, was built upon a DNS based X.509 PKI and the innovation in cross certification and zero-message key generation. The scheme gives cryptographic keys for authenticating Mobile IPv4 location management messages and establishing IPSec tunnels for Mobile IP based redirected packets.

3.6 Minimal Public Key Based Protocol (Lam's Protocol)

To get better scalability, CA-PKI is used for the authentications among mobile node, foreign agent, and home agent [14]; however, this approach has a requirement on the mobile node to perform heavy certificate-based public key cryptography operations. A method in [15] is proposed by Sufatrio and Lam which aims to provide public key based authentication and a scalable solution for authentication while sets only minimal computing on the mobile host and as follows. Some new notations related to public-key operations as in Lam's protocol:

• CA	- Certification Authority;
• K_{HA}, K_{FA}, K_C	- Public key of HA, FA, and CA respectively;
• K^{-1}_{HA}, K^{-1}_{FA}, K^{-1}_{CA}	- Private key of HA, FA, and CA, respectively;

- $<<M>>K^{-1}_A$ - Digital signature of M using private key of A;
- $Cert_{HA}$, $Cert_{FA}$ - Certificate of HA and FA respectively;

Agent Advertisement:

(AA1) FA → MN : M_1, $<<M_1>>K^{-1}_{FA}$, $Cert_{FA}$
where M_1= Advertisement, FA_{id}, MN_{COA}

Registration:

(R1) MN → FA : M_2 , $<M_2>S_{MN-HA}$
where M_2 = Request, FA_{id}, HA_{id}, N_{HM}, MN_{COA}, N_{HA}, N_{MN}

(R2) FA → HA : [message in R1], N_{FA}

(R3) HA: (upon receipt of R2)

- validate $<M_2>S_{MN-HA}$ using S_{MN-HA} and check whether FA_{id} in AA1 = FA_{id} in M_2
- validate CertFA based on existing PKI at HA and $<<M1>>K^{-1}_{FA}$ using authenticated K_{FA} and continue with the following steps.

(R4) HA → FA: M_3, $<<M_3>>K^{-1}_{HA}$, $Cert_{HA}$
where M_3 = M_4, N_{FA} and M_4 = Reply, Result, FA_{id}, HA_{id}, MN_{HM}, N'_{HA}, N_{MN}, $<M_4>S_{MN-HA}$

(R5) FA: (upon receipt of R4)

- validate $N_{FA,}$ $Cert_{HA}$ and $<<M_3>>K^{-1}_{HA}$ using authenticated K_{HA}
- log this message as a proof of serving MN and continue with the following steps.

(R6) FA → MN: M_4

(R7) MN: (upon receipt of R6)

- validate $<M_4>S_{MN-HA}$ using S_{MN-HA}

3.7 MIP Registration with AAA Protocol

The scheme proposed in [16] is used to provide concurrently the public key cryptosystem and symmetric cryptosystem to carry out the task of Mobile IP registration for authentication, authorization and accounting (AAA) for reducing the computation complexity. In addition, this method ensures the security aspects such as authentication, unforgeablility and nonrepudiation, and it is competent to oppose from the replay attack. In this proposal, an MN can use three kinds of registration.

1) The MN asks for entering an administrative domain.

2) When an MN which is a registrant of an administrative domain first arrives at a foreign domain, it must register with its home authority (AAAH) and wait till the local authority (AAAF) obtains the proof of that the MN is legal.

3) The MN must register when it micro-moves within the same foreign domain.

3.8 MIP Registration Scheme for Hierarchical Mobility Management

When an MN roams in a visited domain, it does the following two types of registrations.

1) Home registration which is performed when the MN first arrives at the visited domain.

2) Micro-moving registration which is performed when the MN micro-moves from one FA to another within the same visited domain.

In the above described scenario, ensuring security among the communication parities has become an important problem to avoid possible attacks. There are number of protocols were proposed to solve this problem, but they are suffered from a long delay caused by the MN frequently roaming to different agents in the same visited domain. The new FA must authenticate the mobile node via the mobile node's HA. To reduce the overhead of authentication and home registration, the registration process [17], propose a secure Mobile IP registration scheme with hierarchical mobility management. In this method, one-way hash function and symmetric cryptosystem are used to reduce the computation cost of authentication. Besides, it deploys a group key for each FA, to make simpler the authentication procedure between the MN and visited FA.

3.9 Secure and Scalable MIP Registration Scheme Using PKI

It is necessary and frequent process in the mobile communication network not to disconnect service session during the handoff, this registration scheme [18] was suggested a new optimized registration process with authentication using PKI. Normally, the followings include a secure mobile IP registration scheme using PKI

1) Initial registration is done when a mobile node turns its power on with its home network.

2) Refreshing is done. It means that MN updates its location registration without moving around.

3) Handoff Registration

Generally, security level enhancement is inversely proportional to scalability of the network. The performance of this authentication scheme using PKI may be certainly worse than the legacy standard that uses the pre-shared secret since the proposed scheme takes longer time to validate certificates.

3.10 A Secure MIP Authentication based on Identification Protocol

For the registration with the home network, in this protocol [19], the Mobile IP authentication is provided based on an identification scheme by using one-way function. It ensures a secure Mobile IP Authentication between MN and HA, and FA and HA against certain attacks such as replay attack and man-in-the middle attack. Additionally, its implementation is expected to be efficient, since MN is at no cost from the necessity to perform the public key-based operations.

3.11 Yang's Protocol

Subsequently, other Mobile IP registration protocols [20-22] are proposed, which involve only the nominal use of the public key cryptography to avoid drawback on the mobile node to perform heavy certificate-based public key cryptography operations; one of such Yang's protocol [23] proposes the secure key combine minimal public key besides produce the communication session key in mobile node registration protocol. The Yang's protocol proceeds as follows with the sequence of steps:

Step1: Agent → MN: M_1
where M_1 = Advertisement; FA_{id}, $MN_{COA,}$ N_{FA}
Step 2: MN → FA: HA_{id}, MN_{HM}, MN_{COA}, N_{FA},
$S_{MN\text{-}HA}<M_2>$
where M_2 = Request, FA_{id}, HA_{id}, MN_{HM}, MN_{COA},
N_{HA}, N_{MN}, N_{FA}
Step 3: FA → HA: M_3
whereM_3 = $K_{HA}\{K^{-1}{}_{FA}$ $<<S_{MN\text{-}HA}\{M_2\}$, $MN_{HM}>>\}$,
$S_{MN\text{-}HA}\{M_2\}$, HA_{id}, $Cert_{FA}$
Step 4: HA → FA: M_4
where M_4 = $K_{FA}\{K^{-1}{}_{HA}$ $<<M_5$, S_{sk}, N_{FA}, $MN_{COA}>>$,
M_5, S_{sk}, N_{FA}, $MN_{COA}\}$, FA_{id}, $Cert_{HA}$ and
M_5 = S_{sk} {Reply, Result, FA_{id}, HA_{id}, MN_{HM},
$N'_{HA}\}$, $S_{MN\text{-}HA}$ $\{S_{sk}$, $S'_{MN\text{-}HA}$, $N'_{MN}\}$
Step 5: FA → MN: M_5
where M_5 = S_{sk}\{Reply, Result, FA_{id}, HA_{id}, MN_{HM},
$N'_{HA}\}$, $S_{MN\text{-}HA}$ $\{S_{sk}$, $S'_{MN\text{-}HA}$, $N'_{MN}\}$
Step 6: MN

After receiving the successful registration reply from HA, the mobile node uses the new nonce for next registration.

3.12 ID-Based Secure Session Key Exchange Scheme

AAA protocol has not an adequate authenticating procedure since the computing capability of a MN increases when it is distributed new session keys during handoff every time and also a key sharing using a symmetric key cannot guarantee the security. ID-Based Secure Session Key Exchange Scheme [24] compares with the basic AAA protocol [25] and AAA with the ID-based mechanisms [26] and provides better latency up to about 63% compared to them and it uses ID-based cryptography to strengthen the security and when the MN moves to a new network, a FA reuses previous session keys encrypted by a public key for the fast handoff.

3.13 Secure MIP Registration Based on AAA

For simplifying registration key distribution in Mobile IP registration, a new key management scheme [27] based on AAA Protocol is introduced and it reduces the delay connected with the AAA protocol. In order to build simplified key distribution and to reduce the delay caused by the AAA protocol, the registration key distribution in AAA protocol is disconnected from the base registration protocol. The non-repudiation based on a hash chain is also provided in this protocol.

3.14 MIP Registration from Pairings

The problem of improving both the security of the Mobile IP registration and the efficiency including the latency, the throughput and the security cost is an important issue for Mobile IP based networks. To achieve this, the method in [28] combines both the symmetric cryptosystem with the ID-based non-interactive key agreement from parings. They are used to reduce the latency, the throughput and the security cost and also the authentication is optimized for the MN.

3.15 Secure MIP Registration Scheme with AAA from Parings

A secure ID-based Mobile IP registration with AAA from pairings to reduce the registration delay [29] is based on the previous work [28]. The work reduces the registration delay of the protocol in [30] from 420.201ms to 23.766 ms. The features of this protocol includes the dynamic key generation, user privacy based on TMSI (Temporary Mobile Subscriber Identity) and symmetric (sym) encryption and the mutual authentication among MN, AAAH and AAAF. However, the work is not addressed for the session set-up between MN and the correspondent node.

3.16 Anonymous Registration Scheme

User anonymity can be introduced to prevent an attacker from tracking user's moving history and current location, which is a serious violation in the development of wireless networks. An important issue in the anonymous registration of Mobile IP is to lessen the registration delay while enhancing security. The method for Mobile IPv4 in [31] resolves this problem by the non-interactive authentication from pairings [32] in the Identity-Based Public Key Cryptosystem (ID-PKC) to reduce the security cost.

In ID-PKC, the user's public key can be obtained and used without a certificate authority-based operations, this simplifies the certificate handling process. The scheme reduces both the on-line pairing operation time and the inter-domain communication round trip time based on the dynamic one-way authentication key for providing the non-interactive authentication.

3.17 Time invariant and Time-variant Public Keys Based Protocols

The two protocols [33] time invariant and time variant uses the self certified Diffie-Hellman key exchange systems to generate the secret key between FA and HA. In disparity to the conventional PKI, some of the protocols require the certificateless public key cryptography [34]. The self-certified public keys [35] are not entailing the use of certificates for the authenticity of public keys. Thus, there is no sequence of certificate authorities in it. They can be proved to be secure [36], with which to spawn the secret keys of the MAC for the authentications between the agents in the Mobile IP environment. The variation between two protocols is that the generation of the secret keys between domains based on the time-invariant and time-variant. As a result, the time invariant provides better efficiency and time variant provides stronger security. These protocols lie between security and efficiency. These two schemes include the features parameter resynchronization, user anonymity through temporary identity of MN, and replay attack.

3.18 MIP registration in Certificateless PKI

Further these protocols which are described above, the various schemes for registration [37-39] were proposed in IP Mobility for IPSec, GSM, and one-way function but they were not developed with the intention to balance both the security and the efficiency. To address this issue, the certificateless signature scheme in [40] is introduced and it is more efficient than those methods [41-46] which are based on the same scheme because of less pairing computations and shorter public keys. For registration, a secure and efficient Mobile IP protocol [47] using certificateless signature scheme is proposed to lessen the registration delay during the registration part through nominal convention of an efficient certificateless signature scheme between FA and HA. The parameters of this protocol can be kept resynchronised by reusing the initial values in the Mobile IP registration in case the synchronisation between mobile nodes and the home agent is lost. In addition, User anonymity service has been provided in this protocol and it is achieved via a temporary identity transmitted by a mobile user, instead of its true identity and also the replay protection from FA is included in the registration messages to prevent a possible replay attack.

Table 1. Authentication analysis of registration protocols

Registration Protocol	MN-FA	FA-HA	MN-HA
Base [2], [9]	None	None	MAC (Static key)
Protocol in [10]	Symmetric encryption	Symmetric encryption	Symmetric encryption
Protocol in [11]	None	Certified public key	Certified public key
Protocol in [13]	None	None	Symmetric encryption
Lam [15]	None	None	Digital Signature
Protocol in [16]	None	None	MAC
Protocol in [17]	Digital Signature	Digital Signature	Digital Signature
Protocol in [18]	IPSec Tunnelling	Tunnelling with firewall	IPSec Tunnelling
Protocol in [19]	Certificate from CA	Certificate from CA	Certificate from CA
Yang [23]	None	Digital Signature	Symmetric encryption
Protocol in [24]	Signature	Signature	Signature
Protocol in [27]	PKI Certificate & MAC	PKI Certificate & MAC	PKI Certificate &MAC
Protocols in [28], [29]	HMAC	HMAC	HMAC
Protocols in [31], [33]	None	MAC (static/dynamic key)	MAC (dynamic key)
Protocol in [47]	None	Digital Signature	MAC (dynamic key)
Protocol in [50]	Certificate	Certificate	Certificate
Protocol in [51]	TTP	MAC (static/dynamic key)	MAC (dynamic key)
Protocol in [52]	None	MAC (static/dynamic key)	MAC (dynamic key)
ID Based [71]	None	IBS without pairings	MAC (dynamic key)

Table 2. Confidentiality analysis of registration protocols

	Base [2], [9]	Jacob [12]	Lam [15]	Other protocols
MN-FA	None	None	Yes	Yes
FA-HA	None	None	None	Yes
MN-HA	Yes	Yes	Yes	Yes

3.19 Scalable and Practical Authentication Protocol in MIP (Lee's Protocol)

The IPsec [48] is not suitable to Mobile IP because the IPsec is too heavy to be executed at the mobile node and related with the home address and the mobile node should acquire a new address whenever it moves to a foreign network. So it is necessary to locally authorize mobile users for efficient authentication in Mobile IP networks [49], which is based on the authentication between MN and the agents. Thus, a practical Mobile IP authentication protocol [50] is used for public key cryptography merely in the opening authentication for the registration between the communication parties. It is compatible with the conventional Mobile IP protocol and provides scalability for the number of mobile nodes.

3.20 A Scalable and Secure MIP Registration

The protocol in [51] provides the scalable solution for authentication for Mobile IPv6 based network by extending Internet Protocol version 4 (IPv4). It allows translucent routing of datagrams between a MN and a Corresponding Node (CN), as the MN moves from the current network to visited network and changes its point of attachment. The authentication between MN and CN enables the MN to communicate with the CN directly which resolves the triangle routing problem in IPv4 based networks. Here the MN sends the authentication request to the HA and the FA verifies and authenticates the MN and forward the message to CN. The CN validates the MN, calculates the shared secret and sends response to MN. Finally, the MN calculates the shared secret and validates the CN. Then, the MN and CN can directly communicate each other.

3.21 MIP Registration in Certificateless PKI without Pairing

The protocol in [47] entails bilinear paring operation which requires expensive operations. To address this problem, the protocol [52] which is based on certificateless public key encryption without pairings [53], is introduced to minimize the registration time. The features of the scheme includes the mutual authentication between MN, FA and HA, and local key generation. In addition, both the anonymous scheme and the replay protection service from a FA are provided in the registration packets of the protocol.

3.22 VHAHA Secure Registration

For a fault-tolerant characteristic in IP Mobility, the various approaches [54 - 65] were proposed for the recovery of HA for both Mobile IPv4 and Mobile IPv6 based networks. But all of them do not concern with the security of the registration messages and other issues of the mobile network. Thus, to provide the security aspects and efficiency consideration in registration, Virtual Private Network (VPN) based Inter Home Agent Reliability Protocol (VHAHA) [66] is established to support reliability and provides better survivability, transparent failure detection and recovery for Mobile IPv6 networks, reduced complexity of the system and workload, secure data transfer and get better overall performance.

3.23 ID-Based Registration Protocol

To develop a better registration in mobile IP, research work in [67] employ the identity (ID)-based public key cryptography (ID-PKC) [68-70] to eliminate the time-consuming certificate operations, however, these works are only at a theoretical level and lacking of a complete algorithm description, and they cannot be used in a real system. Hence, there is a requirement for introducing a specific ID based signature scheme into mobile IP registration, which can direct to a secure and efficient implementation. A protocol [71] with user anonymity is projected for IP-based mobile networks. This scheme is more efficient than other existing schemes because it does not need any pairing operations and map-to-point hash operations and it is proved to be secured in terms of existential enforceability against the chosen message and ID attacks [72]. The protocol reduces the registration delay through a minimal usage of the identity (ID)-based signature scheme that eliminates expensive pairing operations. User anonymity is achieved via a temporary identity (TID) transmitted by a mobile user, instead of its true identity. In addition replay protection from a foreign agent is incorporated in the registration messages to avoid a possible replay attack. This protocol uses Protocol Composition Logic (PCL) [73-75] to prove the correctness of the scheme.

3.23 MIP Registration in Certificateless Signature

Certificateless encryption (CLE) [34] surmounts the drawback in PKI and ID based cryptosystem. The CLE and certificates signature protocols [41, 42] are introduced for shorter certificateless public key signature scheme [76] to decrease the registration delay. Furthermore, using a temporary identity for mobile users, the scheme provides user anonymity and replay protection from a FA is included in the registration messages to prevent a possible efficient than others; therefore it is more appropriate to Mobile IP registration. The protocol in [77] introduces an efficient Mobile IP registration method, which is based on replay attack.

4. ANALYSIS OF SECURITY PARAMETERS

4.1 Authentication

In the communication network, it is very important to authenticate one another’s individuality while delivering the packets between the sender and receiver of the communication parties. For the registration of IP Mobility, the authentication of communicating entities between the mobile nodes and the agents is provided through security functions such as Trusted Third Party (TTP), digital signature, Message Authentication Code (MAC).The authentications between three entities MN, HA, and FA in Mobile IP are set up during the registration process. Table 1 shows the authentication analysis of the various protocols.

4.2 Confidentiality

The confidentiality of the data in the internet is of vital importance since it can be easily interrupted and falsified. Thus, ensuring confidentiality of communication between the source and destination is dreadfully significant in Mobile IP situation. The confidentiality service between three entities MN, HA, and FA in Mobile IP registration process for the various protocols is examined and listed in Table 2.

4.3 Attack Prevention and Location Privacy

In IP Mobility registration process, there is a chance that the attacker may be receiving the registration packets and will be able to understand them. Fundamentally, protection from replay attack is provided by ensuring that no message is processed more than once. The nonce or timestamp is used to prevent the replay attack [78] between the communication parties in the registration set-up of the IP Mobility. And also, location privacy or user anonymity is becoming increasingly important in the operational model of the Mobile IP environments. The location anonymity is provided through the temporary identity or number of the MN during the registration. Table 3 shows the replay attack prevention and location privacy analyses of the registration protocols.

5. ANALYSIS OF EFFICIENCY

5.1 Message size

The signalling traffic analysis really plays an important role in finding the efficiency of any registration protocol. In order to have the same amount of connectivity to a mobile node from HA when it roams away from its home network, and also the FA to send messages to and from the mobile node, the registration protocol causes the amount of signalling traffic for secure transmission. In the registration process, time to register with the HA by M is directly proportional to security since it introduces unacceptable delay as considerable amounts of messages between mobile node and the agents increased. The transmission of registration packets is implemented in all the protocols and each protocol specifies their message size as shown in Figure.2 in bytes. Table 4 summarizes the message size of the compared protocols between the communication entities.

Table 3. Attack prevention and Location privacy analysis of registration protocols

Registration Protocol	Replay attack prevention	Location privacy
Base protocol [2], [9]	None	None
Protocol in [11]	Yes (Nonce)	None
Protocol in [12]	None	None
Protocol in [13]	Yes (Secret key & Timestamp)	None
Protocol in [14]	Yes (Timestamp or Nonce)	Yes (Identification number)
Protocol in [17]	Yes (Nonce)	None
Protocol in [21]	Yes (Timestamp)	None
Protocol in [24]	Yes (Identity)	None
Protocol in [40]	Yes (Nonces)	Yes (TID)
Protocol in [47]	Yes (Nonce)	None
Protocol in [48]	Yes (ID- Based Secure Session key)	None
Protocols in [53], [61]	Yes (Nonces)	Yes (TID & Hash value)
Protocol in [71]	Yes (Temporary entries)	Yes (Temporary number)
Protocol in [72]	Yes (Session key)	Yes (Dynamic anonymity)
Protocol in [75]	Yes (Timestamp or Nonce)	None
Protocols in [76], [77]	Yes (Timestamp & Nonce)	Yes (TMSI & Sym.encryption)
Protocol in [79]	Yes (Secure key)	Yes (TID)
Protocol in [81]	Yes (Nonces)	Yes (TID & Hash value)

5.2 Registration Delay Comparisons

The comparison result of the registration time in milliseconds (ms) of various protocols is shown in Figure.3.

Table 4. Signaling traffic analysis of registration protocols

Protocol	MN-FA	FA-HA	HA-FA	FA-MN
Base	50	50	46	46
Jacob	224	228	64	128
Lam	178	178	174	174
Yang	66	578	582	66
Time invariant	206	364	108	54
Time variant	226	404	124	70
Certificateless PKI	78	92	92	54
ID-Based	82	176	146	48
VHAHA	206	364	108	54

The estimated registration delay by using the system parameters [24], [79-81] is shown in Table 5, and we have listed the numerical values for the registration delay for the various protocols. The registration time can be computed as follows.

Registration Time = $RREQ_{MN-FA}$ + $RREQ_{FA-HA}$ + $RREP_{HA-FA}$ + $RREP_{FA-MN}$

6. CONCLUSION

In this paper, the various aspects of different registration protocols has been discussed and examined in terms of the security parameters such as authentication, confidentiality, replay attack prevention, user anonymity and registration time. The numerical results are also compared. The extreme security may cause long registration time, especially for real-time services. Consequently for the spacious deployment of MIP, the registration must have as good a performance as possible while providing a certain level of security, for example, authentication, integrity, replay protection, secure distribution of session keys, confidentiality and anonymity. There is a trade-off between security issues and efficiency in terms of the registration time; hence we need a protocol which can be dealt with a framework for secure and efficient Mobile IP registration which provides better security and efficiency. The pros from existing protocols can be congregated to form a new protocol in the future that is optimal in every aspect and can be applied in different wireless networks.

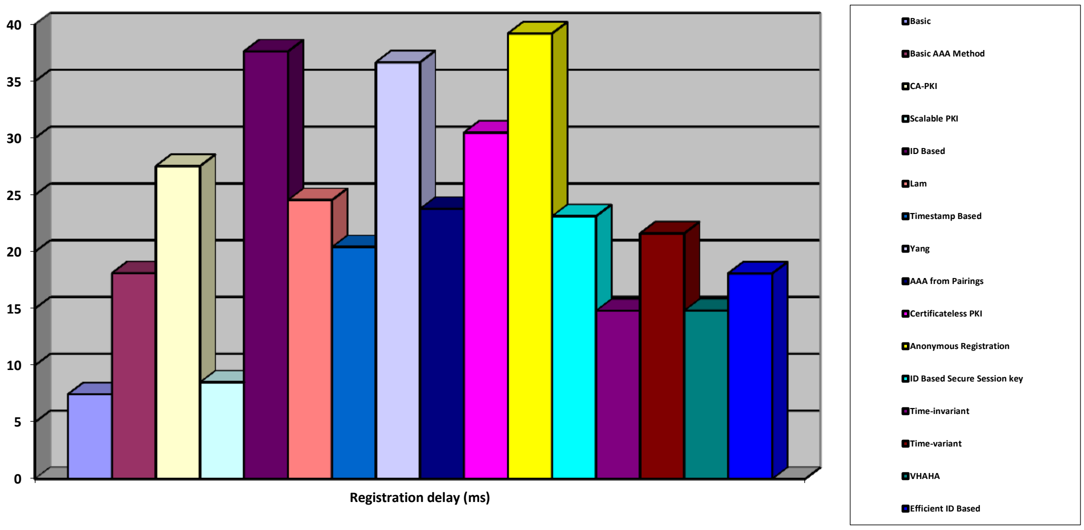

Fig 2: Registration delay of the various protocols

Table 5. Registration time of the various protocols

Protocol	**Registration time (ms)**
Base	7.441
Basic AAA method	18.1
CA-PKI	27.5312
Scalable PKI	8.5
ID Based	37.62
Lam	24.5399
Timestamp Based	20.4039
Yang	36.663
AAA from pairings	23.766
Certificateless PKI	30.478
Anonymous scheme	39.2001
ID Based SSK	23.12
Time-invariant	14.8
Time-variant	21.602
VHAHA	14.8056
Efficient ID Based	18.078

7. REFERENCES

[1] C. E. Perkins, Mobile IP, IEEE Communication Magazine, May 1997, pp. 84-99.

[2] C. Perkins, IP Mobility Support, Request for Comments RFC2002, Oct. 1996.

[3] C. E. Perkins, IP encapsulation within IP, IETF RFC, RFC2003, Oct. 1996, pp. 1-18.

[4] R. Atkinson, IP Encapsulating Security Payload (ESP), IETF RFC, RFC1827, Aug. 1995, pp. 1-27.

[5] R. Atkinson, Security architecture for the Internet protocol, IETF RFC, RFC1825 Aug. 1995, pp. 1-27.

[6] 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 Communication, vol. 11, no. 4, Aug. 2004, pp. 76-88.

[7] R. Atkinson, IP authentication header, IETF RFC, RFC1826, Aug. 1995, pp. 1-16.

[8] W. Haitao and Z. Shaoren, The Security Issues and Countermeasures in Mobile IP, 2001 Int. Conf. On Info-tech and Info-net (ICII 2001), vol. 5, Beijing, Nov. 2001, pp. 122-127.

[9] C. Perkins, IP Mobility Support for IPv4, Request for Comments RFC3344, Aug. 2002.

[10] Le-Pond Chin, A Secure Registration Protocol for Wireless Internet, Proc. IEEE PIMRC'97, Finland, Vol.2, pp.495-499, Sep.97.

[11] Jianzhu Zhang and Jon W. Mark, A Secured Registration Protocol for Mobile IP, 1999.

[12] S. Jacobs, Mobile IP Public Key based Authentication, http://search/ietf.org/internet drafts/draftjacobs-mobileip-pkiauth- 01.txt. 1999.

[13] 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 Networks, May 1999, pp. 373-390.

[14] M. Shi, X. Shen, and J.W. Mark, A light weight authentication scheme for mobile wireless Internet applications, IEEE WCNC, vol.23, 2003, pp.2126 - 2131.

[15] Sufatrio and K.Y. Lam, Mobile-IP Registration Protocol: a Security Attack and New Secure Minimal Pubic-key based Authentication, Proc.1999 International. Symposium. Parallel Architectures, Sep. 1999.

[16] C. C. Yang, M. S. Hwang, J. W. Li, and T. Y. Chang, A solution to mobile IP registration for AAA, CIC 2002, LNCS 2524, Springer-Verlag, 2003, pp. 329-337.

[17] Chou-Chen Yang, Jian-Wei Li and Ting-Yi Chang, A Novel Mobile IP Registration Scheme for Hierarchical Mobility Management, Proceedings of the 2003 International Conference on Parallel Processing Workshops (ICPPW'03), IEEE, 2003, pp.373–390.

[18] J. P. Yoo, K. Kim, H. Choo, J. I. Lee, and J. S. Song, Secure and scalable mobile IP registration scheme using PKI, ICCSA 2003, LNCS 2668, Springer-Verlag, 2003, pp. 220-229.

[19] D. H. Choi, H. Kim, and K. Jung, A secure mobile IP authentication based on identification protocol, in Proc. IEEE ISPACS 2004, Nov. 2004, pp. 709-712.

[20] Wang. L, Yang. B, A Timestamp Based Registration Protocol in Mobile IP, Journalof Xidian Universiy pp. 777–780, 2004.

[21] M. Mufti and A. Khanum, Design and implementation of a secure mobile IP protocol, in Proc. IEEE Int. Conf. Netw. Commun. 2004, June 2004, pp.53-57.

[22] S. Chung and K. Chae, An efficient public-key based authentication with mobile-IP in e-commerce, in Proc. IEEE Int. Conf. Parallel Processing 2000, 2000.

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

[24] K.C. Jeong, H. Choo, and S.Y. Ha, ID-based Secure Session Key Exchange Scheme to Reduce Registration Delay with AAA in Mobile IP Networks, LNCS 3515, Springer-Verlag 2005, pp. 510-518.

[25] C.E. Perkins, Mobile IP and Security Issue: An Overview, Proceedings of 1st IEEE Workshop on Internet Technologies and Services, 1999.

[26] B.G. Lee, D.H Choi, H.G. Kim, and S.W. Sohn, Mobile IP and WLAN with AAA authentication protocol using identity based cryptography, ICT2003 Proceedings, vol.3, pp. 597–603, February 2003.

[27] Hyun-Sun Kang, Chang-Seop Park, A Key Management Scheme for Secure Mobile IP Registration Based on AAA Protocol, IEICE Tranc. Fundamentals, Vol.E89–A, No.6 June 2006.

[28] Xuefei Cao, Weidong Kou, Lanjun Dang and Kai Fan, Efficient Mobile IP Registration from Pairings, ICWMMN2006 Proceedings, Nov.2006.

[29] Xuefei Cao, Weidong Kou, and Huaping Li, Secure Mobile IP Registration Scheme with AAA from Parings to Reduce registration delay, IEEE, 2006.

[30] Byung-Gil Lee, Doo-Ho Choi, Hyun-Gon Kim, Seung-Won Sohn and Kil-Houm Park, Mobile IP and WLAN with AAA authentication protocol using identity-based cryptography, IEEE, 2003.

[31] Xuefei Cao, Weidong Kou, Huaping Li, and Jie Xu, An Efficient Anonymous Registration Scheme for Mobile IPv4, Springer-Verlag, LNAI 4456, pp. 758–766, 2007.

[32] Sakai. R, Ohgishi. K, and Kasahara. M, Cryptosystems based on pairing, Symposium on Cryptography and Information Security (2000).

[33] L. Dang, W. Kou, J. Zhang, X. Cao, and J. Liu, Improvement of mobile IP registration protocols in mobile wireless networks, submitted to IEEE Transaction on Mobile Computing, June 2007.

[34] Al-Riyami .S, and Paterson K.G, Certificateless public key cryptography in Laih, C.S. (Ed.), Asiacrypt2003, LNCS, vol. 2894, 2003, pp. 452–473.

[35] M. Girault, Self-certified Public Keys, Advances in Cryptology (Proc. EuroCrypt 91), LNCS, vol. 547, Springer-Verlag 1991, pp. 490-497.

[36] T.C. Wu, Y.S. Chang, and T.Y. Lin, Improvement of Saeedni's Self-certified Key Exchange Protocols, Electronics Letters, vol 34, Issue: 11, 1998, pp.1094–1095.

[37] H. Haverinen, N. Asokan, and T. Maattanen, Authentication and key generation for mobile IP using GSM authentication and roaming, in Proc. IEEE ICC'01, vol. 8, June 2001, pp. 2453-2457.

[38] D. Johnson, C. Perkins, and J. Arkko, Mobility support in mobile IPv6, IETF RFC3775, June 2004.

[39] J. Xie and L. F. Akyildiz, A novel distributed dynamic location management scheme for minimizing signal costs in mobile IP, IEEE Trans. Mobile Computing, vol. 1, no. 3, July-Sept. 2002 pp. 163-175.

[40] Wun-she. Y, Swee-Hway. H, and Bok-Min.G, An efficient certificateless signature scheme, EUC Workshops 2006, LNCS, vol. 4097, pp. 322–331.

[41] M. C. Gorantla and A. Saxena, An Efficient Certificateless Signature Scheme, CIS 2005, LNAI 3802, Springer-Verlag, 2005, pp. 110-116.

[42] Zhenfeng, Z., Duncan, S.W., Jing, X., and Dengguo, F, Certificateless public-key signature: security model and efficient construction, ACNS 2006, LNCS, vol. 3989, 2006, pp. 293–308.

[43] X. Li, K. Chen, and L. Sun, Certificatelss signature and proxy signature schemes from bilinear pairings, Lithuanian Mathematical Journal, Vol. 45, No. 1, 2005, pp. 95-103.

[44] Hak S, PaeYoub, K, DongHoon, L, Jongin, L, and Kilsoo, Efficient revocation of security capability in certificateless public key cryptography in Khosla, KES 2005, LNAI, vol. 3682, pp. 453– 459.

[45] Xinyi, H., Willy, S., Yi, M., and Futai, Z, Certificateless designated verifier signature schemes, Proc. 20th Int. Conf. Advanced Information Networking and

Applications (AINA'06), Vienna, Austria, April 2006, pp. 15–19.

[46] Licheng, W., Zhenfu, C., Xiangxue, L., and Haifeng, Certificateless threshold signature scheme, CIS 2005, LNAI, vol. 3802, pp. 104–109.

[47] Dang, W.Kou, N.Dang, H.Li and B.Zhan, Mobile IP registration in Certificateless Public Key Infrastructure, IET Inf. Security (4), pp.167-173, Sep 2007.

[48] A. Patel, K. Leung, M. Khalil, and H. Akhtar, Authentication protocol for mobile IPv6, Internet standard, RFC4285, 2006.

[49] Jie Li, Hui Jing and Guojun Wang, Authentication protocols for Mobile IP networks, IEEE Computer Society, ICICIC'08, 2008.

[50] Yong LEE Goo-Yeon LEE and Hwa-Jong KIM, A Scalable and Practical Authentication protocol in Mobile IP, IEICE TRANS Communication, Vol.E91-B, February 2008.

[51] Rathi S and Thanushkodi K, A Scalable and Secure Mobile Registration Protocol for IPv6, ICGST-CNIR Journal, Volume 9, Issue 1, July 2009.

[52] Manjun Zhang, Changxing Pei, and Lanjun Dang, Efficient Mobile IP Registration in Certificateless Public Key Infrastructure Without Pairing, IEEE, 2009.

[53] J Baek, R Safavi-Naini, and W Susilo, Certificateless Public Key Encryption without pairing, LNCS, 2005.

[54] B. Chambless, and J. Binkley, Home Agent Redundancy Protocol, IETF Draft, October 1997.

[55] R. Ghosh, and G. Varghese, Fault Tolerant Mobile IP," Washington University, Tech nical Report (WUCS-98-11), 1998.

[56] J. Ahn, and C. S. Hwang, Efficient Fault-Tolerant Protocol for Mobility Agents in Mobile IP, in Proc.15th Int. Parallel and Distributed Processing Symp., California, 2001.

[57] K. Leung, and M. Subbarao, Home Agent Redundancy in Mobile IP, IETF Draft, draft-subbarao-obileipredundancy-00.txt, June 2001.

[58] M. Khalil, Virtual Distributed Home Agent Protocol (VDHAP), U.S.Patent 6 430 698, August 6, 2002.

[59] J. Lin, and J. Arul, An Efficient Fault-Tolerant Approach for Mobile IP in Wireless Systems, IEEE Trans. Mobile Computing, vol. 2, no. 3, pp.207-220, July-Sept. 2003.

[60] R. Wakikawa, V. Devarapalli, and P.Thubert, Inter Home Agents Protocol (HAHA), IETF Draft draft-wakikawamip6- nemo-haha-00.txt, October 2003.

[61] F. Heissenhuber, W. Fritsche, and A. Riedl, Home Agent Redundancy and Load Balancing in Mobile IPv6, in Proc. 5th International Conf. Broadband Communications, Hong Kong, 1999.

[62] Deng, H. Zhang, R. Huang, X. and K. Zhang, Load balance for Distributed HAs in Mobile IPv6, IETF Draft, draft-wakikawa-mip6- nemo-haha-00.txt, October 2003.

[63] J. Faizan, H. El-Rewini, and M. Khalil, Problem Statement: Home Agent Reliability, IETF Draft, draftjfaizan-mipv6-ha-reliability-00.txt, November 2003.

[64] J. Faizan, H. El-Rewini, and M. Khalil, Towards Reliable Mobile IPv6, Southern Methodist University, Technical Report (04-CSE-02), November 2004.

[65] Adisak Busaranun, Panita Pongpaibool and Pichaya Supanakoon, Simple Implement of Home Agent Reliability for Mobile IPv6 Network, Tencon, November 2006.

[66] Rathi S and Thanushkodi K, A Secure and Fault-tolerant framework for Mobile IPv6 based networks International Journal of Computer Science and Information Security, Vol. 5, No. 1, 2009.

[67] B. G. Lee, D. H. Choi, H. G. Kim, S. W. Sohn, and K. H. Park, Mobile IP and WLAN with AAA authentication protocol using Identity-based cryptography, in Proc. IEEE ICT'03, vol. 1 pp.597-603, Feb. 2003.

[68] A. Shamir, Identity-based cryptosystems and signature schemes, Advances in Cryptology- CRYPTO'84, LNCS 196, Springer-Verlag, 1985, pp. 47-53.

[69] D. Boneh and M. K. Franklin, Identity-based encryption from the Weil pairing, Advances in Cryptology-CRYPTO'01, LNCS 2139, Springer-Verlag, 2001, pp. 213-229.

[70] Zhang, S., Xu, G., Hu, Z., Yang, Y., Zhou, A Mobile IP Authentication Protocol Based on Identity, Journal of BUPT 3, 2005, pp. 86–88.

[71] Lanjun Dang, Weidong Kou, Hui Li, Junwei Zhang, Xuefei Cao, Bin Zhao, Efficient ID-based registration protocol featured with user anonymity in mobile IP networks, IEEE Transactions on Wireless Communications, Volume 9 Issue 2, February 2010, pp. 594-604.

[72] R. W. Zhu, G. Yang, and D. S. Wong, An efficient Identity-based key exchange protocol with KGS forward security for low-power devices, in X. Deng and Y. Ye (eds.): WINE 2005, LNCS 3828, Springer-Verlag, 2005, pp. 500-509 (The last edition is published in Theoretical Computer Science, vol. 378, no. 2, Elsevier, June 2007, pp. 198-207.

[73] C. He, M. Sundararajan, A. Datta, A. Derek, and J. C. Mitchell, A modular correctness proof of TLS and IEEE 802.11i, in Proc. 12th ACM Conf. Computer Commn. Security, Nov. 2005, pp. 2-15.

[74] A. Datta, A. Derek, J. C. Mitchell, and A. Roy, Protocol composition logic (PCL), Electronic Notes Theoretical Computer Science, vol. 172, Apr. 2007, pp. 311-358.

[75] A. Datta, Security analysis of network protocols compositional reasoning and complexity-theoretic foundations, Ph.D. dissertation, Dept. of Computer Science, Standford Univ., Stanford, Calif., 2005.

[76] Raylin Tso, Xun Yi, Xinyi Huang: Efficient and Short Certificateless Signature. CANS 2008, pp. 64-79.

[77] Manjun Zhang, Changxing Pei and Lanjun Dang, Efficient Mobile IP Registration in Certificateless Signature IEEE 24th International Conference on Advanced Information Networking and Applications Workshops, April 2010, pp. 363-366.

[78] C. Perkins and P. Calhoun, Mobile IPv4 challenge/response extensions, IETF RFC 3012, Nov. 2000.

[79] A. Hess and G. Shafer, Performance Evaluation of AAA/Mobile IP Authentication, Proc. 2nd Polish-German Teletraffic Symp. (PGTS 02), Gdansk, Poland, Sep. 2002.

[80] J. McNair, I.F. Akyldiz, and M.D. Bender, An Inter-system Handoff Technique for the IMT–2000 System, INFOCOM 2000, vol. 1, Mar. 2000, pp. 203–216.

[81] H. Jeon, H. Choo, and J.H. Oh, Identification Key based AAA Mechanism in Mobile IP Networks, ICCSA 2004, LNCS 3043, Springer-Verlag 2004, pp. 765-775.

[82] William Stallings, Cryptography and network security, 2nd edition, Pearson Education Limited, 2003.

[83] J. Schiller, Mobile Communications, 2nd edition, Pearson Education Limited, 2003.