Performance Analysis of Mobile IP Registration Protocols

RATHI S and THANUSHKODI K
Department of Computer Science and Engineering,
Government College of Technology, Coimbatore – 641 013, Tamilnadu, INDIA.
sai_rathi @ yahoo.com, thanush_dr @ rediffmail.com

Abstract: - Mobile IPv6 will be an integral part of the next generation Internet protocol. The importance of mobility in the Internet gets keep on increasing. Current specification of Mobile IPv6 does not provide proper support for security in the mobile network and there are other problems associated with it. This paper is concerned with security aspects of the Registration protocols in Mobile IP. Providing security in Mobile IP registration is highly important. The registration part must be guarded against any malicious attacks that might try to take illegitimate advantage from any participating principal. This paper deals with the performance analysis of various protocols available for Mobile IP registration. The parameters considered for comparison are: Data confidentiality, Authentication, Attack prevention, Registration delay and Computational complexity. This paper aims to determine the protocol which outperforms others when the parameters mentioned above are taken into consideration.

Keywords: - Mobile IP, Mobility Agents, Confidentiality, Authentication, Attack prevention and Registration delay.

1 Introduction

Mobile IP Protocol [1] is an on-going effort under IETF towards an Internet Standard that aims to support node mobility within the Internet. It is the proposed solution that operates at network-layer level to address the "node mobility problem" in current Internet architecture. This protocol defines extension mechanisms on the top of existing IPv4 to allow transparent routing of IP datagrams between a *Mobile Node (MN)* and its *Corresponding Node (CN)*, as the MN moves and changes its point of attachment on the Internet [1, 2].

In Mobile IP, a MN is given a long-term address on home network and it retains this home address regardless of its location. While MN is visiting foreign network, a Care-of-Address (COA) is also temporarily assigned to it. A network layer agent on home network called *Home Agent (HA)* should be available to maintain an association between MN's home address and its current COA, that's commonly referred as *mobility binding*. Under a valid binding of MN that it serves, HA is responsible to intercept any datagrams destined to MN's home address that reach home network and then redirect these datagrams to MN's COA. The binding itself is created and updated through the registration protocol part of Mobile IP, in which MN informs HA of its current COA possibly through a *Foreign Agent (FA)* on foreign network.

As a form of *remote redirection* that involves all the mobility entities, the registration part is very crucial and must be guarded against any malicious attacks that might try to take illegitimate advantages from any participating principals. Hence, providing communication security in Mobile IP environment is highly important.

The major goals of this study are: (i) to discuss the characteristics and requirement for the Mobile IP environment and (ii) to discuss the practical and secure points of the existing methods.

We will briefly discuss the requirements of the mobile IP services [3] before going to the second point.

User Authentication: In general, user authentication deals with the personal identity of the user before providing service. Here, the user login process can determine if this user is a legal user of the system. If the person log on is verified as a legal user, the system offers the service. The Mobile IP user authentication protocol is different from the general user service authentication protocol. Three of identification levels are required in mobile IP; the mobile node must authenticate with the foreign agent, the foreign agent with the home agent and the mobile node with the home agent. Users must be verified at all three authentication levels in order to receive service. The mobile node identity authentication process prevents illegal users from using the replay attack to acquire system services.

Confidentiality and Integrity: Both of the mobile and foreign agents communicate through wireless wave and Internet. The wireless data is easy to intercept and steal. The Internet is an open network. Data delivered through the Internet can be

easily intercepted or falsified. Therefore, insuring the confidentiality and integrity of communications data are very important in a Mobile IP environment.

Locate Anonymous: An anonymous location [21, 22, 23] is important requirement in a mobile communication system. This requirement is generally provided in a cell-phone system. This requirement provides mobile user with communications with other nodes, but the correspondent nodes cannot determine the senders' location. This requirement was previously not provided in Mobile IP services.

A simple and secure mobile IP user authentication and secure communication schemes [20, 27, 28] have the following requirements: 1) the current mobile IP communication architecture must not change. 2) The mobile node hardware is simple and does not require complicated calculations. 3) The system must not increase the number of times that communication data must be exchanged. 4) All communication data must be encrypted to insure communication confidentiality and 5) Provide the corresponding location of anonymous users in a Mobile IP environment.

With the above said requirements, this paper aims to determine the performance of various protocols available for Mobile IP environment with respect to the following parameters: Data confidentiality, Authentication, Attack prevention and Registration delay and Computational overhead [14, 16, 17, 18].

The rest of the paper is organized as follows: Section 2 reviews the Mobile IP operational model and its security problems. Section 3 briefly discusses the various Mobile IP registration protocols. The security analysis and comparisons are given in Section 4. Finally, Section 5 concludes the paper.

2 Mobile IP operational model

Mobile IP is intended to enable nodes to move from one IP subnet to another. It is just as suitable for mobility homogeneous media as it is for heterogeneous media. That is, Mobile IP facilitates node movement from one Ethernet segment to another as it accommodates node movement from an Ethernet segment to a wireless LAN, as long as the MN's IP address remains the same after such a movement. One can think of a Mobile IP as solving the "macro" mobility management problem.

2.1 Mobile IP - An overview

In Mobile IP [1, 2], a source S sending a packet to a mobile M sends the packet to a fixed IP address for M. Because of the way IP routing works, this packet is routed to the "home" subnet on which M resides when it is not mobile. If M is away from home on a foreign sub-network (Fig. 1) a Home Agent for the mobile host intercepts packets addressed to M. The home agent then encapsulates and tunnels the packet to a designated Foreign Agent on the foreign sub-network. The Foreign Agent decapsulates the packet and transmits it on the foreign network.

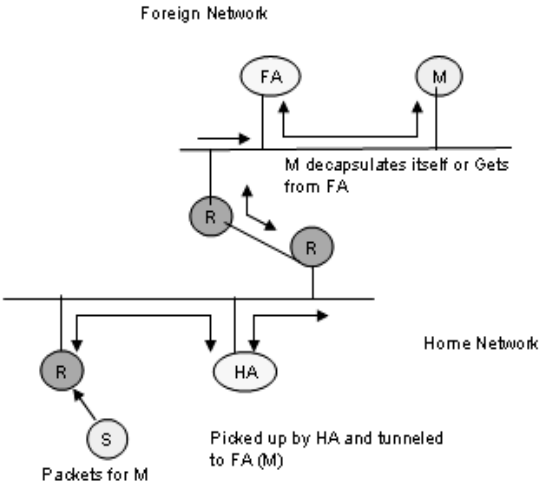

Figure 1. Mobile IP –An overview

If the mobile is using a co-located care-of address, the home agent can send the encapsulated packet to the mobile directly, bypassing the foreign agent. If M is using a co-located address, M will decapsulate the packet instead of the foreign agent.

In Fig. 1, Source S sends a packet to mobile M. The home agent HA intercepts the packet, encapsulates and tunnels it to the foreign agent FA. FA then decapsulates it and hands it to M. Alternatively, if M is using co-located care-of-address, HA sends the encapsulated packet to M directly, and M decapsulates it itself.

2.2 Functioning of Mobile IP

Home Agent (HA) and Foreign Agent (FA), frequently advertise their presence via Agent Advertisement messages. A mobile M receives these advertisements and determines whether it is on its home network or a foreign network. When M detects it is at home, it operates without mobility services. When returning to its home network, it

deregisters with HA through the exchange of Registration Request and Reply messages.

When M detects that it has moved to a foreign network, it obtains a care-of address on the foreign network. The care-of address can either be obtained from agent advertisements (a foreign agent care-of address), or by some other mechanism like DHCP (a co-located care-of address). M then registers its new care-of address with its home agent HA through Registration Request and Reply messages, possibly via its foreign agent FA. Datagrams sent to M are intercepted by HA, encapsulated and tunneled to the mobile's care-of address. They are received at the tunnel endpoint by FA (or by M itself), decapsulated and handed to M. Datagrams sent by M are routed to their destination by static IP routing.

Registration in mobile IP must be made secure so that fraudulent registration can be detected and rejected. Otherwise, any malicious user in the internet could disrupt communications between the home agent and the mobile node by the simple expedient of supplying a registration request containing a bogus care-of-address (perhaps the IP address of the malicious user). This paper is concerned with the security aspect and analysis of the various registration protocols in mobile IP.

2.3 Vulnerabilities of base protocol

Mobile IP mandates the use of Message Authentication Code (MAC) value [15] which is called *authenticator* in Mobile IP specification to ensure authentication and integrity of control-message communication only between MN and HA. But, in general it recommends all control messages between any pair of sender and receiver to be authenticated. Any algorithm for generating MAC may be used, but the default algorithm that must be supported by all Mobile IP implementations is keyed MD5 in *prefix+suffix* mode using manual key distribution.

In order to prevent replay attack on registration, Mobile IP specifies two methods that can be chosen to ensure the freshness of registration. The first method is based on *timestamp*, where MN includes its estimated current time of the day in the request. If this estimate is not sufficiently close to the HA's estimated current time of day, HA then sends non-approval in its reply but it also provides enough information for MN to synchronize its clock. The second method uses *nonce*. The basic principle of nonce replay protection is that MN includes a new pseudo-random number as nonce in every request to HA and requires HA to return this same nonce in its reply. At the same time, every reply sent by HA to MN also includes HA's nonce to be echoed later by MN in the next request. Should HA reject a request because of invalid HA's nonce, the reply also provides MN with a new nonce for the next request.

The registration protocol of Mobile IP [24, 25, 26] using shared secret key and nonce can be represented as follows:

(0) HA → MN: N_{HA} (from previous HA's reply1)
(1) MN → 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}
(2) FA→HA: M_1 ,$<M_1>S_{MN\text{-}HA}$
(3) HA → FA : M_3, $< M_3>S_{MN\text{-}HA}$
where M_3 = *Reply*, *Result*, FA_{id}, HA_{id} ,MN_{HM}, N'_{HA} , N_{MN}
(4) FA → MN : M_3 , $<M_3>S_{MN\text{-}HA}$

It is quite clear to see that the security protection [14] provided in registration protocol is intended to ensure that registration legitimately originated from MN or HA, that it has not been altered in transit, and that an old registration is not being replayed. Less clear is the security requirement from FA's point of view, since FA seems to just play a passive role. And it is exactly this subtlety that brings about a possible weakness exploited in our attack. We can notice from the protocol that after a successful registration (i.e. HA has approved MN's request and it is willing to serve MN), FA also starts serving MN and thus allowing MN to use resources in its network. This successful registration then might be taken by FA as a valid assumption that it's the legitimate MN and HA that just agreed to establish Mobile IP connection, through on a freshly-generated registration. And if the registration messages are all authenticated, FA can reasonably be sure that it deals with real MN and HA, in which FA is willing to serve for free (if under the same organization) or the bill is to be charged later (if under different organizations).

Essentially this attack works because no replay protection involving FA is employed in the protocol. It's *not enough* to say that an approved authenticated registration that has been protected using timestamp/nonce issued by HA and MN *also means* this registration must have been freshly generated from FA's point of view. This flaw can be viewed as the result of its disregarding of a basic principle for sound cryptographic protocol design, which is called the principle of "explicit communication". Specifically, the registration

doesn't include FA's replay protection that might be presumed to be not necessary or redundant after the use of nonce/timestamp from HA and MN. The absence of this information opens the door to the attack and this must be taken seriously as it indicates a flaw in the protocol design.

This attack can be prevented, simply by including additional replay protection originated from FA. One possible way is by requiring FA to include its own nonce when relaying request to HA and later expect that nonce to be echoed in the reply. As our concluding remark, of course it's possible to just say that this protocol is not really intended to be taken by FA as a proof of MN's resource consumption. Or that further security measures can be provided by some authentication, authorization, and accounting (AAA) extension [3, 4, 5] protocols that will handle this problem. On for the first argument, we argue that in that case the Mobile IP specification should have stated it clearly, as it's very likely for someone deploying Mobile IP to come to that conclusion. This then may serve as an example of practice that violates another principle of sound protocol design called the principle of "appropriate action". As for the latter argument, by considering the important role of registration in Mobile IP and to make this protocol securely complete by itself.

3 Major Protocols for Mobile IP Registration

The protocols we have considered for analyses are classified under 4 categories as follows: (i) CA-PKI based protocol [6] (ii) Minimal public key based protocol [7] (iii) Hybrid technique of Secret and CA-PKI based protocol [8] and (iv) Self certified public key based protocols [11]. The pros, cons and suggestions for each protocol are discussed.

The following notations are used in this paper to represent messages in the Mobile IP registration protocols:

- ***M, N, M || N*** Concatenation of two messages *M* and N
- 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
- ***{M}K*** Encryption of message *M* under key *K*
- ***<M>K*** MAC value of message *M* under key *K*
- $S_{MN\text{-}HA}$ ***S***ecret key between MN and HA
- ***Request*** A bit pattern indicating a request
- ***Reply*** A bit pattern indicating a reply
- ***Result*** A value indicating result of the request
- ***Key-Request*** A bit pattern indicating a session key request
- ***Key-Reply*** A bit pattern indicating a session key reply
- ***Advertisement*** A bit pattern indicating an advertisement
- H_1: $\{0,1\}^n \rightarrow \{0,1\}^n$ The one-way hash function used to generate $K_{FA\text{-}HA}$
- $K_{MN\text{-}HA}$, $K_{MN\text{-}FA}$, $K_{FA\text{-}HA}$ Shared secret keys between MN and HA, MN and FA, FA and HA
- ***A → B: M*** A sends the message M to B.

3.1 CA-PKI based protocol - Jacobs' Proposal

As mentioned before, the secret key based authentication in current Mobile IP is not scalable. Besides, it also can't provide non-repudiation that seems likely to be demanded by various parties, especially in commercial settings. These two reasons are main motivation for the certificate-based public-key cryptography authentication proposed by Jacobs [6].

This proposal is particularly interesting as it is the only attempt so far that sets out a complete specification on the use of public key cryptography for Mobile IP control messages. The proposal defines a new *Certificate Extension* message format intended to carry information about certificates, which now must always be appended in all the control messages. The protocol itself runs exactly the same as the original protocol, except that now it uses public-key generated digital signature instead of secret key based MAC value.

Besides the improvement in introducing the use of public key cryptography, the proposal itself still suffers from some drawbacks mainly due to the heavy requirements set on MN to perform demanding certificate based public key cryptography operations:

- The fact that MN is normally limited in its computing power might raise a performance problem if it has to deal with computationally expensive public-key cryptographic operations, which in general is 1000 times costly than that of secret key based algorithms [12].
- It might be a serious problem for MN with relatively low bandwidth to get the current Certificate Revocation List (CRL) from the issuing CA. Network performance could be seriously degraded if MN must always retrieve the most

recent CRL whenever a new certificate is received. This important issue is left unanswered in the proposal itself [6].

• The requirement on MN to do all necessary public key and certificate retrieval operations will require additional hardware or software that might add the complexity of its system. This in turn will give new extra administrative cost and cause greater possibility of unexpected problems to occur. Sadly enough, this extra burden must be borne by the mobile users while they are away in their trip.

3.2 Minimal Public Key Based Protocol – Suf and Lam's Proposal

In this protocol, a method [7] is proposed by Suf 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.

This protocol tries to minimize the computing power requirement as well as administration cost imposed on MN. While the protocol offers the benefit of scalability and nonrepudiation from its use of public key cryptography, its public-key operations are kept to minimal. It still makes use of secret key cryptography operations especially to be performed at MN. Thus this approach exercises a hybrid approach to this problem.

Moreover, No additional message exchange other than the original Mobile IP control messages should be required. This will maintain compatibility with the base Mobile IP and other authentication extension protocols, thus giving mobile user flexibility to choose the authentication scheme desired.

Some new notations related to public-key operations as in Suf and Lam:

- 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;

The registration protocol of Mobile IP using this approach can be represented as follows:

***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 , $<M_2>S_{MN\text{-}HA}$

where M_2 = *Request*, FA_{id} ,HA_{id} ,MN_{HM} MN_{COA} ,N_{HA} , N_{MN}

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

(R3) HA : (upon receipt of R2)

- validate $<M_2>S_{MN\text{-}HA}$ using $S_{MN\text{-}HA}$ and check whether FA_{id} in AA1 = FA_{id} in M_2
- validate $Cert_{FA}$ based on existing PKI at HA & $<<M1>>K^{-1}_{FA}$ using authenticated K_{FA} and continue with the steps in [1, 2]

(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} , $<M_4>S_{MN\text{-}HA}$

(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 steps in [1, 2]

(R6) FA → MN : M_4

(R7) MN : (upon receipt of R6)

- validate $<M_4>S_{MN\text{-}HA}$ using $S_{MN\text{-}HA}$ *and* continue with the steps in [1, 2].

Even if, this approach uses only the minimal public key based framework to prevent the replay attack; the framework must be executed using complex computations due to the creation of digital signatures by the MN. This increases the computational complexity at the MN.

3.3 Hybrid technique of Secret and CA-PKI based protocol – Yang's Proposal

To avoid the drawbacks of Suf and Lams Protocol, Yang proposes [8] the secure key combine minimal public key besides produce the communication session key in mobile node registration protocol.

The Yang's protocol [8] proceeds as follows:

S1. ***Agent → MN* : *M*1**

where *M*1=*Advertisement; $FA_{id,}$ $MN_{COA,}$ N_{FA}*

S2. ***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}

S3. ***FA → HA*: M_3**

where M_3 = $K_{HA}\{K^{-1}_{FA} << S_{MN\text{-}HA}\{M2\}, MN_{HM} >>\}$, $S_{MN\text{-}HA}\{M2\}$, HA_{id}, $Cert_{FA}$

S4. ***HA → FA*: M_4**

where $M_4 = K_{FA}\{K^{-1}_{HA} << M_5, S_{sk}, N_{FA}, MN_{COA} >>, M_5, S_{sk}, N_{FA}, MN_{COA}\}, FA_{id}, Cert_{HA}$ &

$M_5 = S_{sk}\{Reply, Result, FA_{id}, HA_{id}, MN_{HM}, N'_{HA}\}, S_{MN\text{-}HA}\{S_{sk}, S'_{MN\text{-}HA}, N'_{MN}\}$

S5. $\boldsymbol{FA \rightarrow MN: M_5}$

where $\boldsymbol{M_5 = S_{sk}\{Reply, Result, FA_{id}, HA_{id}, MN_{HM}, N'_{HA}\}, S_{MN\text{-}HA}\{S_{sk}, S'_{MN\text{-}HA}, N'_{MN}\}}$

S6. ***MN***

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

The main advantage of this method is the hardware requirements of the MN are simple. Only a secure key is needed to encrypt the communication data between the MN and the correspondent node. The mobile node does not use a public key system or complex computations, so the mobile node does not increase the overhead. Moreover, this approach provides a very strong security framework and for the first time location anonymity concept is addressed.

The drawback of this approach is the registration delay. When compared to other protocols it is considerably increasing the delay in registration. In addition to that the solution to the location anonymity is only partial.

3.4 Self certified public key based protocol

Self-certified public keys were introduced by Girault [9]. In contrast to the traditional public key infrastructure (PKI), self-certified public keys do not require the use of certificates to guarantee the authenticity of public keys. The authenticity of self-certified public key is verified implicitly by the proper use of the private key in any cryptographic applications in a logically single step. Thus, there is no chain of certificate authorities in self-certified public keys.

In the setup of self-certified public keys, a Trust Third Party (TTP) chooses an integer n as the product of two large distinct primes p and q of almost the same size, such that $p = 2p' + 1$ and $q = 2q' + 1$, where p' and q' are also primes, a base element $g \neq 1$ of order $r = p' \cdot q'$, a large integer $u < r$, and a one-way hash function h, which will output a positive integer $< p'$ and q'. The TTP makes g, u, h and n public, keeps r secret and discard p and q afterwards [10]. Next, any user U_i can register with the TTP by performing the following steps:

1. U_i randomly chooses a secret key $x_i \in z_i$, computes his public key $y_i = g^{x_i} \bmod n$ and gives y_i to the TTP.
2. The TTP prepares a string I_i associated with the personal information (name, address, etc.) of U_i and computes $w_i = (y_i - I_i)^{h(I_i)^{-1}} \bmod n$ as a witness for user U_i and sends message $\{I_i, w_i\}$ to U_i.
3. U_i verifies the identity I_i and the witness w_i by checking that $y_i = w_i^{h(Ii)} + I_i \bmod n$.

Here, the advantage of using r is that any positive integer $< p'$ and q' is invertible modulo r. This guarantees that $h(I_i)$ is co-prime to r, for any I_i, and consequently the inverse of $h(Ii)$ modulo r always exists. Note that the witness w_i cannot be computed without knowing the prime factors of n, or more properly, without knowing the trapdoor r, known only to the TTP.

In order to achieve different requirements of security and efficiency, two schemes are proposed base on self certified keys: (i) time invariant protocol and (ii) time variant protocol. The protocol 1 is more suitable for the situation that the first priority is efficiency, while the protocol 2 can offer a stronger security.

3.4.1 Time invariant protocol

The time invariant keys are generated using the following procedure:

1. *Ui* sends $\{I_i, w_i\}$ } to *Uj*.
2. *Uj* sends $\{I_j, w_j\}$ to *Ui*.
3. *Ui* computes the secret key shared with *Uj* as
$k = (w_j^{h(I_j)} + I_j)^{X_i} \bmod n$
4. *Uj* computes the secret key shared with *Ui* as
$k = (w_i^{h(I_i)} + I_i)^{X_j} \bmod n$

Since x_i is unknown, the adversary cannot pretend to act as U_i to share a secret key with U_j, and vice versa. The self-certified key exchange schemes described above can be proved to be secure [10], with which to generate the secret keys of the MAC for the authentications between FA and HA in the self-certified public keys based protocols [11].

The registration protocol of Mobile IP using this approach [11] can be represented as follows:

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 $K^0_{MN\text{-}HA}$ with it. Then HA produces a nonce N^0_{HA} and

computes MN's temporary identity $H(ID_{MN} \| N^0_{HA})$, where $H: \{0,1\}^n \rightarrow \{0,1\}^n$. Here, K^0_{MN}, and N^0_{HA} are denoted to be the initial values by the superscript 0. Finally, the data $(H(ID_{MN} \| N^0_{HA}), K^0_{MN\text{-}HA}, N^0_{HA}, w_H)$ is consigned to the MN on a secure channel. After the user initial registration step, the MN stores a initial entry $(ID_{MN}, H(ID_{MN} \| N^0_{HA}), K^0_{MN\text{-}HA}, N^0_{HA}, w_H)$ in its initial parameter memory; HA stores the same entry in its initial parameter database for the MN under its administration.

Mobile node location registration with it's HA in a foreign network

Agent Advertisement (AA1): FA → MN: $M1$

where M_1 = *Advertisement,* FA_{id}, MN_{CoA}, N_{FA}

Registration

(R1) MN → FA: M_2, $<M_2>K_{MN\text{-}FA}$

where M_2 = *Request, Key-Request,* FA_{id}, HA_{id}, MN_{CoA}, N_{HA}, N_{MN}, N_{FA}, $H(ID_{MN} \| N_{HA})$, w_H

(R2) FA: (upon receipt of R1)

- Validate N_{FA}
- Compute the key,

$$K_{FA-HA} = H_1\{[(W_h^{h(I_H)} + I_H)^{ILF}.v_H^{x_F}] \bmod n\} = H_1\{[(w_H^{h(HA_{id})} + HA_d)^{IF}.v^{x_F}] \bmod n\}$$

- Compute $MAC = <M_2 \| <M_2>K_{MN\text{-}HA} \| FA_{id} \| w_F> K_{FA\text{-}HA}$

(R3) FA → HA: M_3, $<M_3>K_{FA\text{-}HA}$

where $M_3 = M_2$, $<M_2>K_{MN\text{-}HA}$, FA_{id}, w_F

(R4) HA: (upon receipt of R3)

- Check whether FA_{id} in M 3 equals FA_{id} in R1
- Compute

$$K_{FA-HA} = H_1[(w_F^{h(I_H)} + I_F)^{x_H} \bmod n] = H_1[(w_F^{h(FA_{id})} + FA_{id})^{x_H}.\bmod n]$$

Compute $MAC^* = <M_3>K_{FA\text{-}HA}$ and compare it with $<M_3>K_{FA\text{-}HA}$ in R3. This is the authentication of HA to FA. Search in HA's dynamic parameter database. If there is an entry whose $H(ID_{MN} \| N_{HA})$ equals $H(ID_{MN} \| N_{HA})$ in M_2, HA finds out MN's true identity ID_{MN} and uses the corresponding value N_{HA} and $K_{MN\text{-}HA}$ to validate N_{HA}, and $<M_2>K_{MN\text{-}HA}$. Otherwise, HA continues to search in its initial parameter database, and then uses the corresponding initial value N^0_{HA} and $K^0_{MN\text{-}HA}$ to validate N_{HA}, and $<M_2>K_{MN\text{-}HA}$ in R1. This is the authentication of HA to MN.

- Dynamically assign a home address for the MN, and then store the new mobility binding of MN_{HM} and MN_{CoA}.
- Produce a new nonce N'_{HA} & compute MN's new temporary identity $H(ID_{MN} \| N'_{HA})$
- Generate the new secret key $K'_{MN\text{-}HA}$ and the session key $K_{MN\text{-}FA}$ via the HMAC-SHA-1 one-way function [12], [13], [14], [15]:

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

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

- Overlay (ID_{MN}, $H(ID_{MN} \| N_{HA})$, $K_{MN\text{-}HA}$, N_{HA}, w_H) in HA's dynamic parameter database with (ID_{MN}, $H(ID_{MN} \| N'_{HA})$, $K'_{MN\text{-}HA}$, N'_{HA}, w_H) for MN's next registration. Note that the initial values (ID_{MN}, $H(ID_{MN} \| N^0_{HA})$,
- $K^0_{MN\text{-}HA}$, N^0_{HA}, w_H) have been always conserved in HA's initial parameter database.

(**R5**) HA → FA: M_4, $<M_4>K_{FA\text{-}HA}$

If ID_{MN} is found out in HA's dynamic parameter database,

$M_4=M_5$, $<M_5>K_{MN\text{-}HA}$, N_{FA}, $\{K_{MN\text{-}FA}\}$, $K_{FA\text{-}HA}$

M_5 = *Reply, Result, Key-Reply,* MN_{HM}, HA_{id}, N'_{HA},N_{MN}

Else, $M4 = M5$, $<M_5>K^0_{MN\text{-}HA}$, N_{FA}, $\{K_{MN\text{-}FA}\}$, $K_{FA\text{-}HA}$

M_5 = *Reply*, *Result*, *Key-Reply*, MN_{HM}, HA_{id}, N'_{HA},N_{MN}

(**R6**) FA: (upon receipt of R5)

- Validate N_{FA}
- Validate $<M_4>K_{FA\text{-}HA}$ with $K_{FA\text{-}HA}$. This is the authentication of FA to HA.
- Decrypt $\{K_{MN\text{-}FA}\}K_{FA\text{-}HA}$ with $K_{FA\text{-}HA}$ and get the session key $K_{MN\text{-}FA}$

(**R7**) FA → MN: M_5, $<M_5>K_{MN\text{-}HA}$

(**R8**) MN: (upon receipt of R7)

- Validate N_{MN}
- Validate $<M_5>K_{MN\text{-}HA}$ with the secret key, $K_{MN\text{-}HA}$ used in R1. This is the authentication of MN to HA.
- Compute the next TID $H(ID_{MN} \| N'_{HA})$ with N'_{HA}.
- Compute $K'_{MN\text{-}HA}$ and $K_{MN\text{-}FA}$ according to (1) and (2).
- Overlay (ID_{MN}, $H(ID_{MN} \| N_{HA})$, $K_{MN\text{-}HA}$, N_{HA}, w_H) in MN's dynamic parameter memory with (ID_{MN}, $H(ID_{MN} \| N'_{HA})$, $K'_{MN\text{-}HA}$, N'_{HA}, w_H)for MN's next registration. Note that the initial values (ID_{MN}, $H(ID_{MN} \| N^0_{HA})$, $K^0_{MN\text{-}HA}$, N^0_{HA}, w_H) have been always conserved in MN's initial parameter memory.

This protocol provides strong security at the same the time Registration delay and Computational

complexity is very less when compared to other protocols.

3.4.2 Time variant protocol

To further strengthen the previous protocol, the time component can be introduced when computing the key.

The time variant keys are generated using the following procedure: Time variant approach is just similar to time invariant approach. The difference is, in key generation process the time component is also included since synchronization is difficult which make the system very secure. The key generation process is given in the following steps:

1. *Ui* randomly chooses a secret integer $t_i \in Z_u$, computes $v_i = g^{t_i}$ and sends $\{I_i, w_i, v_i\}$ to *Uj*.
2. *Uj* randomly chooses a secret integer $t_j \in Z_u$,computes $v_j = g^j \bmod n$ & sends $\{I_j, w_j, v_j\}$ to *Ui*
3. *Ui* computes the secret key shared with *Uj* as

$$k = (w_j^{h(I_j)} + I_j)^{t_i} . v_j^{x_i} \bmod n$$

4. *Uj* computes the secret key shared with *Ui* as

$$k = (w_j^{h(I_{ij})} + I_i)^{t_j} . v_i^{x_j} \bmod n$$

This protocol [11] proceeds similar to the time invariant version using the keys generated by using the above said procedure.

Because of the inclusion of the time factor, the security is very high when compared to any other protocols but the registration delay and computational cost are bit high when compared to its time-invariant counterpart.

The self certified approaches provide stronger security architecture with minimal computational overhead and delays. Also, it provides two different approaches. Based on our requirement, the appropriate method can be selected.

4. Performance Evaluation

In this section, we analyze the security of the Base protocol, CA-PKI based protocol, Minimal public key protocol, Hybrid technique of Secret and CA-PKI and Self certified protocols, followed by the comparisons.

The system parameters are shown in Table 1. The hardware platform for the FA and HA is a Pentium 4.2.1 GHz processor under Windows XP SP 1. 386; the one for the MN is a 206 MHz Strong ARM processor running Windows CE pocket PC 2002. The cryptography operation time on the FA and HA is obtained from [18], [19]; the operation time on the MN is obtained from [20].

The following attributes have been considered for our study: (i) Data confidentiality, (ii) Authentication, (iii) Attack prevention and (iv) Registration delay and (v) Computational overhead.

4.1 Confidentiality

Data delivered through the Internet can be easily intercepted and falsified. Therefore, ensuring confidentiality of communication data is very important in Mobile IP environment. The Confidentiality of the compared protocols is listed in the Table 2.

Table 2. Data Confidentiality Analysis

Protocol	MN-FA	FA-HA	MN-HA
Base	No	No	Yes
Jacob's	No	No	Yes
Suf & Lam's	Yes	No	Yes
Yang's	Yes	Yes	Yes
TimeInvariant	Yes	Yes	Yes
TimeVariant	Yes	Yes	Yes

4.2 Authentication

Prior to data delivery, both parties must be able to authenticate one another's identity. It is necessary to avoid any bogus parties from sending unwanted messages to the entities. The Mobile IP user authentication protocol is different from the general user service authentication protocol. The Table 3 shows the authentication analysis of compared protocols.

Table 3. Authentication Analysis

Protocol	MN-FA	FA-HA	MN-HA
Base	None	None	MAC
Jacob's	Digital Signature	Digital Signature	Digital Signature
Suf& Lam's	None	None	Digital Signature
Yang's	None	Digital Signature	Symmetric Encryption
Time-invariant	None	MAC (Static Key)	MAC (dynamic key)
Time-variant	None	MAC (dynamic key)	MAC (dynamic key)

Table 1. System parameters

Bit Rate			Processing time	
Wired link	100 Mbps		Routers (FA)	0.5 ms
Wireless link	2 Mbps		Routers (HA)	0.5 ms
Propagation time			Nodes (MN)	0.5 ms
Wired link	500µs		Operation time (on MN)	
Wireless link	2 ms		DES	0.007354 ms
Data Sizes			SHA	0.019111 ms
x,t	160 bits		Operation time (on FA, HA)	
			SHA-1/ DES	0.000898/0.000358 ms
			RSA 1024 Encryption /RSA 1024 Decryption	0.18 ms/4.77 ms
			RSA 1024 Signature /RSA 1024 Verification	4.75 ms/0.18 ms
			Modular Exponentiation Modulus	1.65 ms 1024 bits

Table 5. Registration delay of the protocols

Protocol	RREQ MN-FA (1)	RREQ FA-HA (2)	RREP HA-FA (3)	RREP FA-MN (4)	Total Registration Delay (1)+(2)+(3) +(4)
Base	2.719111	1.004	1.0144	2.703111	7.440622
Jacob	7.641757	5.926646	6.317046	7.645757	27.531206
Suf & Lam	2.811999	0.996646	10.877004	7.746642	22.432291
Yang	2.793416	16.056598	15.01179	2.800770	36.662574
Time-invariant	3.381333	7.64708	1.015636	2.761576	14.805605
Time-variant	3.480444	14.264934	1.017632	2.840294	21.602396

4.3 Attack Prevention

Table 4. Attack Prevention Analysis

Protocol	Replay attack	TCP Splicing attack	Guess attack
Base	No	No	No
Jacob's	No	Yes	No
Suf & Lam's	Yes	No	No
Yang's	Yes	Yes	Yes
Time-invariant	Yes	Yes	Yes
Time-variant	Yes	Yes	Yes

The nonce is used to prevent the replay attack and guess attack between the nodes. The encrypted communication data and encryption key prevents the guess and TCP splicing attack. The Table 4 shows the attack prevention analyses of the compared protocols.

4.4 Registration Delay

We compute the registration time with system parameters in Table 1 and the results are given in Table 5 and Figure 2. The registration time can be computed as follows:

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

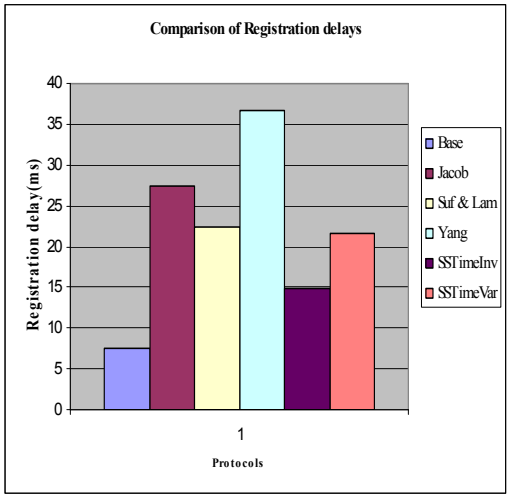

Figure 2. Comparison of Registration delays

4.5 Computational overhead

The signaling traffic of the protocols we have considered, are computed and given in Table 6 and Fig. 3. From the table, we can observe that the base protocol is having the lowest traffic. Hence complexity is less both at MNs and Mobility Agents. Also, bandwidth consumption is less. But the security is poor. Yang's protocol and Self-certified time invariant protocols are having highest overhead and strong security.

Table 6. Registration signaling traffic in bytes

Protocol	MN-FA	FA-HA	HA-FA	FA-MN
Base	50	50	46	46
Jacob's	224	288	64	128
Suf&Lam	178	178	174	174
Yang	66	578	582	66
Invariant	206	364	108	54
Variant	226	404	124	70

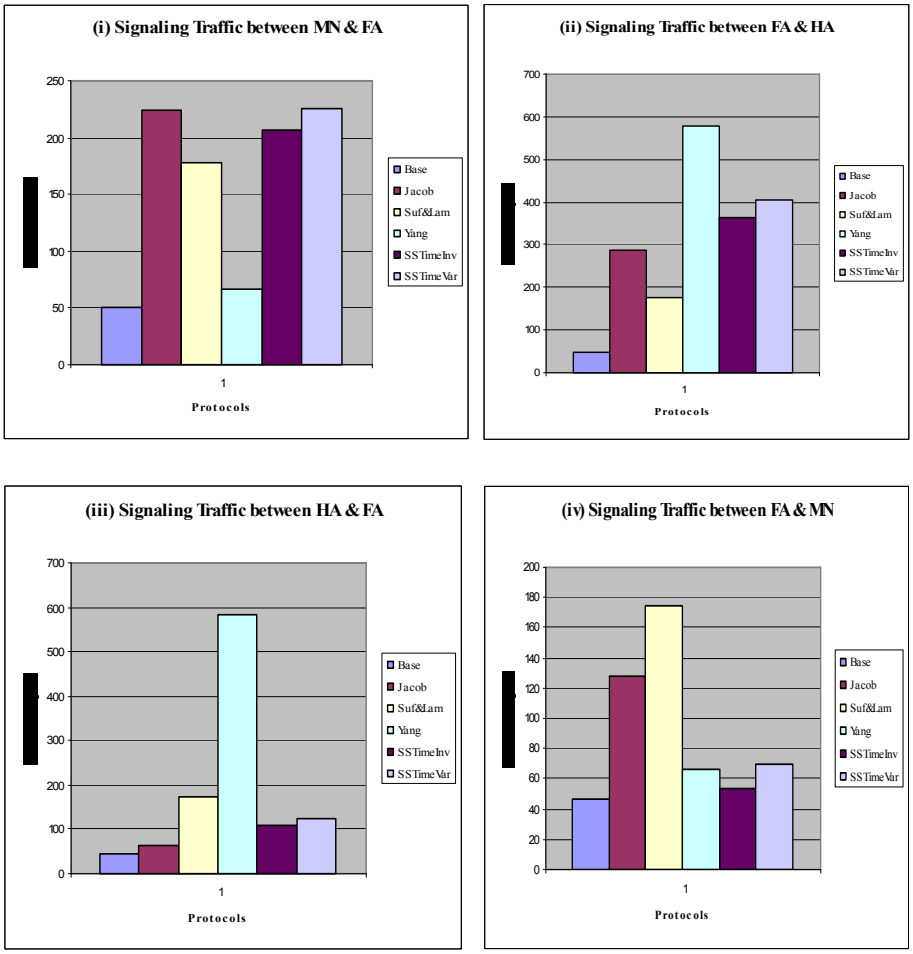

Figure 3. Signalling Traffic between (i) MN & FA, (ii) FA & HA, (iii) HA & FA and (iv) FA & MN

5 Conclusions and Future Work

Based upon the comparisons done on various protocols it is found that no one protocol can be considered as a panacea to all problems. Every protocol has its own pros and cons. Hence, based on our requirement we can select the appropriate protocol for the given application. The strong points in all protocols can be gathered together to form a new protocol in the future that is optimal in every aspect which can be applied in different wireless networks, e.g., wireless LAN, CDMA, GSM, 3G and beyond 3G wireless networks. Also, an efficient certificate-less public key cryptography into mobile IP registration can be introduced.

References

[1] C. Perkins, "IP Mobility Support," *Request for Comments (RFC)2002*, Oct. 1996.

[2] C. Perkins, "IP Mobility Support for IPv4," Request for Comments (RFC) 3344, Aug. 2002.

[3] R. Atkinson, "RFC 1825 - Security architecture for the Internet protocol," IETF RFC, pp. 1-27, Aug. 1995.

[4] R. Atkinson, "RFC 1826 - IP authentication header," IETF RFC, pp. 1-16, Aug. 1995.

[5] R. Atkinson, "RFC 1827- IP Encapsulating Security Payload (ESP)," IETF RFC, pp. 1-27, Aug. 1995.

[6] S. Jacobs, "Mobile IP Public Key based Authentication,"http: //search/ietf.org/internet drafts / draft jacobs-mobileip-pkiauth- 01.txt. 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] M. Girault, "Self-certified Public Keys," Advances in Cryptology(Proc. EuroCrypt 91), LNCS, vol. 547, pp. 490-497, Springer-Verlag 1991.

[10] 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, pp.1094–1095, 1998.

[11] L. Dang, W. Kou, J. Zhang, X. Cao, J. Liu, "Improvement of Mobile IP Registration Using Self-Certified Public Keys." IEEE Transaction on Mobile Computing, June 2007.

[12] L. Salgarelli, M. Buddhikot, J. Garay, S. Patel, and S. Miller, "Efficient Authentication and Key Distribution in Wireless IP Networks," IEEE wireless communication, pp. 52-61, Dec. 2003.

[13] P. Calhoun, T. Johansson, C. Perkins, and P. McCann, "Diameter MIPv4 Application," Request for Comment (RFC) 4004, Aug. 2005.

[14] C. Perkins and P. Calhoun, "Authentication, Authorization, and Accounting (AAA) Registration Keys for Mobile IP," Request for Comment (RFC) 3957, Mar. 2005.

[15] H. Krawczyk, M. Bellare, and R. Canetti, "HMAC: Keyed hashing for Message Authentication," Request for Comment (RFC)2104, Feb. 1997.

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

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

[18] Wei Dai, "Crypto++ 5.2.1 Benchmarks," http://www.eskimo.com/~weidai/benchmarks.html . 2004.

[19] H. Orman and P. Hoffman, "Determining strengths for Public Keys used for Exchanging Symmetric Keys," Request for Comment(RFC) 3766, Apr. 2004.

[20] P. G. Argyroudis, R. Verma, H. Tewari, and D. O'Mahony, "Performance Analysis of Cryptographic Protocols on Handheld Devices," http://www.cs.tcd.ie/publications/techreports/reports.03/TCD-CS-2003-46. pdf, 2003.

[21] 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, pp. 510-518, Springer-Verlag 2005.

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

[23] G. Cho and L. F. Marshall, "An efficient location and routing scheme for mobile computing environments," IEEE Journal Communications, vol. 13, pp. 868-879, Jun. 1995.

[24] A. Hac and L. Guo, "Mobile host protocols for the Internet," in IEEE 50th Vehicular Technology Conference (VTC 1999), vol. 5, pp. 2790 -2794, 1999.

[25] C. E. Perkins, "RFC 2003- IP encapsulation within IP," IETF RFC, pp. 1-18, Oct. 1996.

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

[27] B. Schneier, Applied cryptography (second edition). John Wiley and Sons, 1996.

[28] William Stallings, "Cryptography and network Security: Principles and Practice," 1996.