International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 5, May - 2014

Security Mechanism for Mobile IP

Khaled Mahmood Al-Adhal,
Department of CSE, Faculty of Engineering & Technology
Manav Rachna International Unniversity

Dr. S. S. Tyagi
Professor& HoD,
CSE, FET, MRIU

***Abstract*: With the evolution in the processing capabilities of wireless devices such as Smart Phones and laptops, a steady internet connection is hugely in demand. This demand is raised by the introduction of internet connectivity within the airplanes. Mobile IP is one of the protocols that have been propositioned to support user/network mobility. Mobile IP turns us on to new entities such as Home Agent and Foreign Agent to facilitate user/network mobility. As the user/network (mobile client) move from one network to another all their connections need to be handed off from one mobile agent to another to maintain unified connectivity. Effective handoff mechanism by itself is an active research discipline and security conjoined with effective handoff pioneers new challenges.**

While these security mechanisms help in upholding security and privacy of the user, they introduce superfluous processing delay thereby affecting the performance. In this paper, the authors insinuate a novel low cost security mechanism that ensures the security of the communication. It will be publicized that the proposed mechanism will secure mobile node communication without distressing the performance. While the proposed architecture necessitates the mobility agents to cache bonus information, the analysis carried out by the author's flashes that the additional cost is compensated by the added security for the communication between the mobile client and the mobility agents.

Key words: Mobile IP, Issus, Handover, IP Protocol and mobility for MIP.

1 INTRODUCTION

Access to internet has stretched a long expanse, from mere luxury to a necessity. Users expect access to the information openly offered on the internet irrespective of their current status i.e. stationary or mobile. Mobility support has become a stipulation to cater the needs of mobile internet users. Tagging mobility support to current internet infrastructure opens up a whole new set of concerns, privacy, data security, and performance to name a few.

Delivering the data to the mobile user's current location without conceding the privacy is one of the biggest trials faced by the amenity benefactors. As it has been ascertained in several of earlier research efforts, security and performance together do not work well. Performance [5] is affected negatively if an effort is made to secure the provided connection. Many researchers have tried to reach equilibrium amid security and performance while not compromising on the privacy of the mobile users. Most of such efforts revolve about using public key cryptography and pre-registration of the mobile clients.

Adjacent to security, movement between different networks also affects the performance of mobile clients.

When a mobile client moves from one network to another, the underlying infrastructure needs to move all the corresponding connections (connections established by the mobile client to the internet) to the new-fangled location. Current internet infrastructure does not support this kind of transfer inherently. This calls for patches, like Mobile IP, that are developed to support user mobility within TCP/IP protocol stack. Mobile IP [2] defines mobility support agents like Home Agent (HA) and Foreign Agent (FA) that are located in the home network and foreign network correspondingly. The HA is accountable for protecting the privacy of the mobile client. The HA intercepts all communication towards the mobile client (when mobile client is away) and securely forwards it to the mobile clients new location. The FA (of a specific network) is responsible for providing internet access to the mobile client when the remnants are visiting a foreign network. Working with HA and FA, the mobile IP protocol ensures that the current location of the mobile client is mystified from rest of the internet.

When the mobile client moves from one network to another, it has to go through a registration route. This ensures that the HA is aware of the current location of the mobile client and also allows the HA to build a secure connection between itself and the mobile client's current location. One of the significant issues with the current approaches is the registration lull [1]. Most of the current proposals suggest the mobile client to initiate the registration process after it has detected that it is in the range of a new foreign network. Depending upon the number of extensions (like security, QoS requirements etc), the time required to complete the registration process will also boost. This will adversely affect the performance of the mobile clients when they are roaming.

An alternative foremost issue is security. Most of the current proposals require the authority of a third caucus device to distribute the security keys [6]. This yet again delays the process and leaves room for security breaches.

With Traditional Security mechanisms such as IPSec, there will be an increase in the delay and reduction in the throughput [6]. Also the key negotiation and generation as required by IKE imposes a significant penalty to the throughput. One of the workarounds to address such issues is the use of key exchange servers at the home network and foreign network [1]. Exchange of keys with mobile node as well as foreign agent and home agent is allowed by the use of servers. With this solution, there is a fall in the delay but the throughput does not depreciate visibly. Also, few security concerns ascend as the key exchange server is

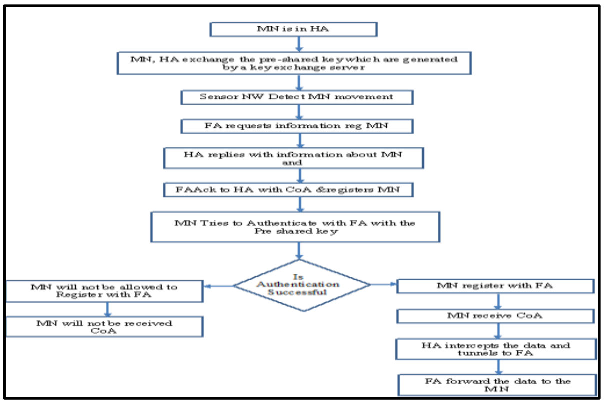
sometimes compromised and would lead to a single point of failure. Another proposal, based on the public key cryptography [6], tries to address some of these disquiets. In this scheme, the mobility agents exchange their public keys to increase security. This reduces the security risks, but the throughput alarms still remain.
Also, the delay in the key exchange process adds to the registration delay, further affecting the performance.
In this paper, the instigators endeavor to address some of these apprehensions. The authors advocate using public key encryption scheme for communication amid the mobile client and the FA. The public key exercised by the FA will be supplied by the HA during the pre-registration progression. This will warrant a well-timed and sheltered registration process. In the ensuing section, the authors confer the working of Mobile IP, which is the current mobility support protocol.

II. MOBILE IP

Mobile IP [3] is one of the first protocols developed to support user mobility. Mobile IP was designed around the tunneling principle. With the help of mobility agents (HA and FA) the protocol tunneled the datagrams destined to the mobile client to its current location. Standardized by IETF (Internet Engineering task force), mobile IP, enables a node to change its point of attachment to the internet in a manner transparent to applications running on top of the protocol stack.
Working of Mobile IP is described as below:

- When in home network, the mobile client is registered with the HA and actively participates in network operations
- When the mobile client recognizes the movement from home network to a foreign network (either through agent advertisements or timeouts), it attempts get associated with the FA of the new network.
- After layer 2 handoff (physical layer association) is complete, the mobile client generates a registration request and forwards it to the FA. The registration request will have information about the HA that will be providing mobility support to the mobile client when the client is away. The registration request will alsohave the care-of-address (COA) that is supplied by theFA in agent advertisements[8]. The COA acts as thecurrent address of the mobile client when it is in theforeign domain.
- FA re-encapsulates packet with its own address andsends it towards the HA.
- HA will perform security checks (registration requestwill also have a shared secret key that is commonbetween HA and mobile client) and once theauthenticity of the mobile client is established, the HAwill generate a registration reply. In addition, the HAinserts a route in its routing table for the mobile clientthat is pointing to the COA embedded in theregistration request [9].
- Then, the HA initiates a bidirectional tunnel betweenitself and the FA. FA acknowledges and a securecommunication path is established between the HA andFA to transport packets sourced from and destined tothe mobile client.

One of the major issues with the mobile IP approach is thesecurity. Mobile IP does not define any specific securitymechanism between the FA and the mobile client. Hence itis possible that a rogue FA could offer services to themobile client and could disrupt communication. Anotherdownside of the Mobile IP is the handoff mechanism.
Handoff process defined by the mobile IP protocol introduces latency and packet loss that are not desired fordelay sensitive and real time applications. This can bereduced using pre-registration schemes.



Fig(1) Algorithm for proposed Scheme

In the pre-registration scheme, external entities likewireless sensor networks (WSN) [7] or GPS are used totrack the movement of the mobile client. When theexternal entity detects the movement, it informs thecorresponding mobility agents i.e. HA, oFA and nFA (oFAis the FA of the network where the client is currentlyattached and nFA is the FA of the network where themobile client is moving into). The nFA generates a preregistrationrequest and forwards it to the HA. With theassumption that the node will move into the foreignnetwork, the HA authenticates the mobile node and startsforwarding traffic to both FAs until the oFA terminates theconnection. In this paper, the authors have considered theuse of WSN for movement detection.
In the next Section, the authors describe the working of theproposed protocol.

III. PROPOSED SCHEME

In order to address the security issues involved with themobility support, in the current paper, the authors proposeusing public key encryption mechanism.
The working ofthe proposed scheme is outlined in Figure 1. The proposedscheme has two stages i.e. key exchange andcommunication establishment.

A. Key exchange mechanism:

Similar to some of the other proposals, in the current work,the authors propose using public key encryption to securecommunication between the mobile client and the FA. However, unlike other proposals, the keys are generated bythe mobile client and is deposited at the HA fordistribution. This will aid in bidirectional authenticationand secure communication. Details of the key exchangemechanism are outlined below:

B. Key generation:

When mobile client is in home network,it generates a private key and sends it to the HA. The HA,using the private key sent by the mobile client, generates aset of public keys. This process could be done at the HAitself or the HA can use the services of a key server forgenerating the public keys. Once the public keys aregenerated, the HA sends an acknowledgement message tothe mobile client confirming the generation of public keys.

Once the mobile client passes through “n” foreignnetworks, it generates a new private key and sends ittowards the HA. The number of foreign networks themobile client needs to pass through before new key isgenerated depends upon the individual networkadministrators. This procedure will ensure that the securityof the mobile client communication is not compromised atany point.

C. Key distribution:

When the mobile clientaway fromthe HA, HA initializes the mobility support services for thecorresponding mobile client. Once the underlying WSNprovides the details of mobile client movement andinformation about the new foreign network the mobileclient is about to move into, the HA anticipates a preregistrationrequest from the nFA. When the nFA obtainsthe movement information from the WSN, it generates apre-registration request and sends it towards the HA. TheHA, after confirming the identity of the nFA, sends a preregistrationreply message that contains details of themobile client along with a public key that the nFA can useto communicate with the mobile client. nFA saves thisinformation in its cache and waits for the mobile client toget associated with the foreign network. One of theassumptions made here is that HA and nFA already have asecurity association between them and the communicationbetween them is secure. If this is not the case, then the HAand FA can use the mobile IP extensions for securitybetween HA and FA to establish a secure channel between them.

D. Communication establishment:

One of the main differences between the traditional mobileIP extensions and the proposed protocols is in terms of thecommunication establishment procedure. In the legacyproposals, the security between FA and mobile client isestablished after the registration process is complete (or insome cases there is no defined security mechanismbetween FA and mobile client). In the proposedarchitecture, the security mechanism is established evenbefore the mobile client gets associated with the FA. Thishelps FA in authenticating the mobile client as well ashelps the mobile client in establishing a secure channelwith the FA as soon as layer 2handoff is completed. Theproposed architecture also helps the mobile node inmaintaining better performance as the delay involved withhandoff process will be lower than many of the legacyproposals.

The working of the proposed architecture is explained below with two possible scenarios i.e. mobile clientmoving from the home network to a foreign network andmobile client moving from one foreign network to another.

- **Scenario 1:** Consider the network shown in Figure 2. Themobile client is currently in the home network and ismoving from the home network to a foreign network (FA1and FA2).

• When registered with the HA, the mobile clientgenerates a private key and shares it with the HA

• HA forwards the private key to the key exchangeserver (only if the HA is not capable of generating thepublic keys) to generate the corresponding public keys

• The key exchange server, upon receiving the privatekey from the HA, generates corresponding public keysand sends it back to the HA

• The HA then sends an ACK packet back to the mobileclient indicating that the subset of keys is successful.

• Upon receiving the ACK packet, the mobile clientstores the private key in its database

• As soon as mobile client starts moving towards FA1,sensor networks (SN1) detects it and informs both theFA1 and the HA

• FA1 triggers the pre-handoff process by enquiring HAabout the mobile clients characteristics

• HA sends the information to FA1 which contains thekey as well

• The FA1 sends an ACK packet to the HA indicatingthat it has received all the required information. Inaddition, the ACK packet contains the COA thatwould be associated with the mobile client

• When mobile client arrives in the FA1, FA1 sends a solicit message which contains the negotiation packet.The packet is encrypted with the key provided by theHA

• If the mobile client is able to decrypt the packet, itwould then send an ACK packet to the FA1 andnegotiate the encryption algorithm

• If FA1 does not receive the ACK packet, it confirmsthe user is not legitimate and informs the same to HA.

- **Scenario 2:** Consider the network shown in Figure 2. Themobile client is currently associated with FA1 and ismoving towards FA2.

• As soon as the mobile client starts moving towardsFA2, sensor networks (SN2) detects it and informsHA, FA1, and FA2

• FA2 triggers the pre-handoff process by enquiring HAabout the mobile client characteristics

• HA sends the necessary information to the FA2 whichcontains a new key that FA2 can use to communicatewith mobile client

• FA2 then sends an ACK packet to the HA, indicatingthat it has received all the required information. ThisACK packet contains the COA that would beassociated with the mobile client

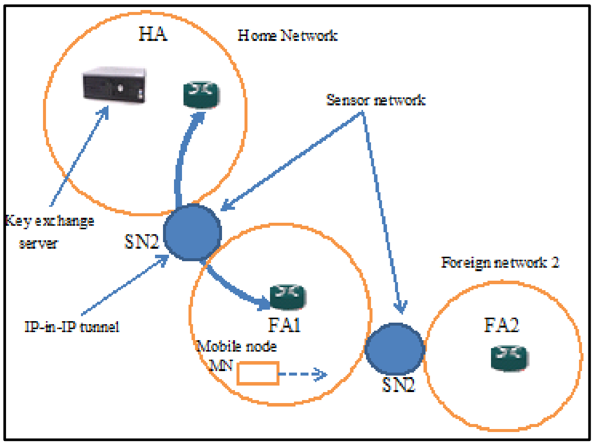
• HA creates a simultaneous binding for the mobileclient. Packets intercepted by the HA will be tunneledto both the foreign networks and as a result theremight be duplicate packets for a short duration.

Fig (2)Network proposed scheme FA1-FA2

• When the mobile client arrives in the range of FA2, FA2 sends a solicit message which contains thenegotiation packet. The packet is encrypted using the key given by the HA

• If mobile client is successfully able to decrypt thepacket, it would then send an ACK packet to the FA1and negotiate the encryption algorithm.

• Mobile client sends a registration request packet to theFA and FA will send a registration reply on behalf ofHA.
Soon after it receives the registration reply, themobile client forces a layer 2 handoff
• FA2 then forwards a message to the FA1 to delete the association details for mobile client



IV. ANALYSIS

1. *Handoff cost for traditional Mobile IP:*
As described inthe RFC 3344 [2], the movement detection in traditionalmobile IP occurs when the lifetime expires or by usingprefixes. The life time is the amount of time elapsed sincethe last agent advertisement was heard? So once thelifetime expires, the mobile client thinks that it has movedto another foreign network and starts the handoff process.
When using the prefix extensions every mobility agentneeds to add prefix elements in their advertisements. Assoon as the mobile node receives a prefix other than theone it is currently associated to, the mobile client assumes that it has moved to another network and initiates thehandoff process. One of the major disadvantages of thisapproach is the additional overhead of prefixes that every FA needs to include in the agent advertisements.
Consider lifetime expiration based handoff mechanism.
When the lifetime of the previous agent advertisementexpires, if the mobile client did not receive newadvertisement from the previous FA (oFA), the mobileclient assumes that it has moved away from the oFA.
Considering the worst case scenario where the mobileclient heard an agent advertisement just before it went outof the range of the oFA, the time required to detect themovement would be T lifetime. After it knows it has moved,the mobile client attempts to force a layer 2 handoff to thenew FA (nFA). Since, in traditional Mobile IP, a mobileclient cannot associate itself with two mobility agentssimultaneously, it will have to break the connection (layer 2) with the oFA before getting associated with the nFA.
Once the mobile client disassociates itself with the oFA, itwill try to register itself with the nFA from which it hadreceived advertisements. Let the delay involved indisassociating the mobile client from the oFA and associating with nFA (at layer 2) be TL2. If the mobileclient has not heard any new agent advertisements, then itwill try to discover an agent by performing agentsolicitation. Let the time taken by this process be TDiscovery.
Once the layer 2 handoff is done the mobile client willsend a registration request packet to the nFA in order toregister itself with the HA. Let the time taken be T (MN-FA).
The packet is then forwarded to the HA by the FA. Let thetime taken be T (FA-HA). HA sends a registration reply to theFA. Let this time taken be T(HA-FA). The packet is forwardedto the MN. Let it be T (FA-MN). Hence, the total time takenby the traditional Mobile IP to perform a handoff would be
THandoff=Tlifetime+TL2+TDiscove/ry+T(MN-FA)+T(FA-HA)+T(HA-FA)+T(FA-MN) (1)

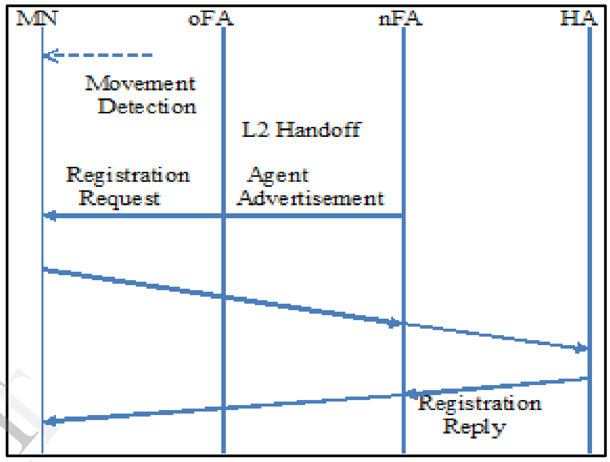


Fig (3) Timing during handoff for the Traditional Mobile IP

During the handoff time, as there is no communication between the mobile client and the HA, all the packetsdestined to the mobile client are lost. Hence the THandoffwould be the total time during which packets are lost.
2. Handoff cost while using the wireless senor network [8]: In the scheme proposed by Bahety et al, by using thewireless sensor networks, the handoff cost is significantlyreduced. The Figure 4 shows the timing diagram of theproposed mechanism by Bahety et al.

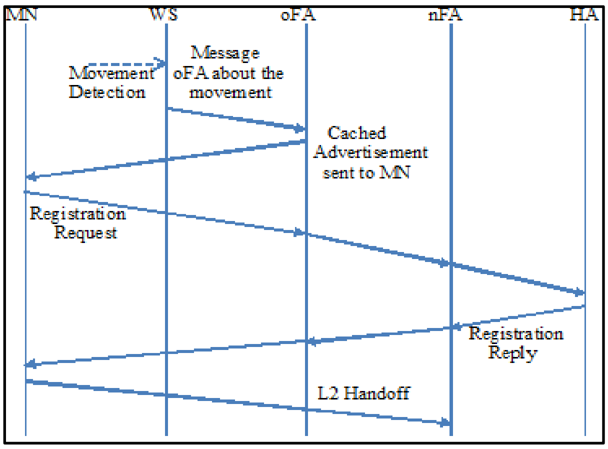


Fig (4) Timing during handoff byusing WSN

In this method, the wireless sensors which are present at the edge of the network perform movement detection. Asdescribed earlier, this method uses the STUN architectureto detect the movement of the mobile client and informsthe mobility agents regarding the same. The wirelesssensors can be installed in such a way that the L3 handoffprocess completes before L2 handoff takes place (with theassumption that the wireless cells do not overlap). Let X bea certain non-zero time taken by the wireless sensornetwork to detect that mobile client is moving in aparticular direction. The WSN then informs the FA aboutthe detection of the movement of the mobile client. Let thistime be TWS-FA. At this point the FA sends a cached agentadvertisement to the mobile client that begins theregistration process. Let the time taken be TPre-registration.

During the cached registration process the oFA would solicit on behalf of the nFA. As soon as the MN receives this new agent advertisement, it will assume that it hasmoved to an nFA. The MN sends registration request tothe FA which is then forwarded to HA. Let the time takenbe TMN-FA and TFA-HA respectively. The nFA receives aregistration reply from the HA and forwards it to the MN.

Let the time taken be THA-FA and TFA-MN respectively. Assoon as mobile client receives the registration reply, it triesto force a layer 2 handoff. Since, during the L3 handoffprocess, the mobile client will keep receiving the packetsfrom oFA , the total handoff delay would beT(WS)Handoff = TL2.

Here T(WS)Handoff is the total handoff latency using the WSNduring which the packets would get lost. Also an optimumdistance at which WSN should be installed is calculated.

The total time taken for movement detection and L3handoff is

TDetection=TMN-FA+TFA-HA+TWS-FA+THA-FA+TFA-MN (2)

3. Handoff mechanism using AAAF server: The abovediscussed approaches do not consider security parameters.

Many research efforts have indicated that traditional IPSecbased encryption is not well suited for mobilityenvironment due to performance impact as well as securityconcerns (shared secret does not provide security over long term). As discussed earlier, one of the workaround was touse AAA server based security mechanism. In the AAAserver based proposal, it is assumed that every network consists of a AAA server. It is also assumed that the AAAservers can communicate with each other and thecommunication channel established between the AAA servers is secure. In Figure 5 [4], the authors outline thetiming sequence of AAA server based secure handoff mechanism for mobility support.

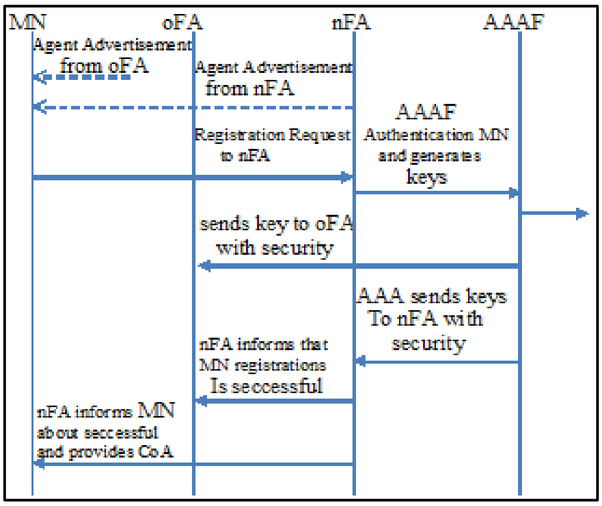


Fig (5) Timing during handoff for the scheme using AAA Servers

When the mobile client is in HA, it will obtain authentication from the AAAHome. When the mobile clientmoves from HA to the foreign network, the AAAHomeestablishes communication with the AAAForeign andprovides information about the mobile client (securitydetails). AAAHome generates a temporary security key that can be used for communication between AAAForeign andmobile client. The AAA servers generate and distribute thesecurity keys between the mobile client and the mobilityagents till the keys expire. When the mobile client moves into a foreign network, it will attempt to contact the localAAA server for authentication. Let the time taken tocomplete this authentication process be TAAAF-MN.

AAAHome distributes the session key K(MN-HA) between theHA and the mobile client. Let the time taken for thisprocess be T(AAAF-HA). AAAForeign distributes the securitykeys K(MN-FA) between mobile client and FA. AAAForeignalso distributes K(FA-HA) between the HA and FA. If oFAand nFA belong to the same domain and controlled by oneAAA server, then there exists only one securityassociation. Let the time taken to communicate between AAA server and nFA be T(AAAF-NFA). Similarly, the timetaken to establish communication between AAAForeign andoFA be T(AAAF-OFA). MN then registers with the nFA(through the oFA) and the registration request and theregistration reply are routed through the oFA. Hence thetotal handoff time would be

T(Handoff)=T(AAAF-MN+K(MN-HA)+T(AAAF-HA)+K(MN-FA)+K(FA-HA)+T(AAAF-NFA)+T(AAAF-OFA). (3)

When the mobile client moves between networkscontrolled by different AAA servers, then additional delayis introduced as the AAAHome server need to communicatewith multiple AAA servers each controlling differentforeign domains.

4. Handoff mechanism using proposed architecture: Asdiscussed earlier, by using the wireless sensor networks thehandoff delay can be reduced. Also, it was observed that,using the AAA server, it is possible to secure the communication between the mobile client and the mobilityagents. However, as described in the earlier section, AAAserver based approach adds additional delay whiledistributing the security keys. Also, it does not address thesecurity risks completely as the communication betweenthe AAA servers is also prone to security attacks.

Figure 6 shows the timing diagram of the proposed schemeduring handoff of mobile client between the home networkand the foreign network. Figure 7 shows the timingdiagram when the mobile client moves from one foreignnetwork to another.

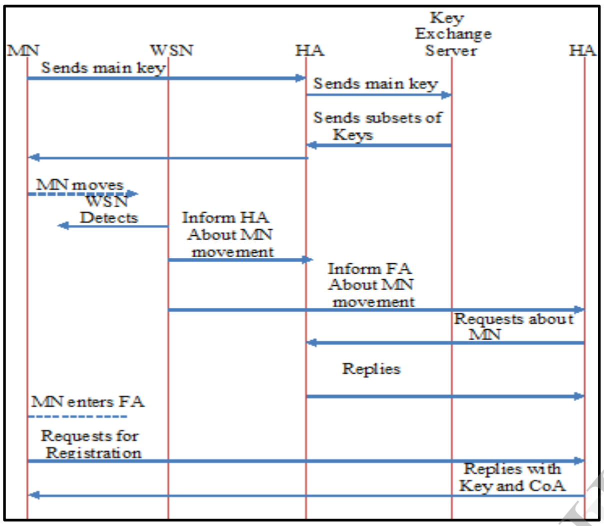


Fig (6) Timing during handoff for the proposedscheme (mobile client is moving from HA to FA)

When the network starts up mobile client is in home network. Mobile client sends a packet to the HAcontaining the private key mobile client will be using todecrypt the packets from mobility agents. The HA thenforwards the packet to the key exchange server. The keyexchange server generates a key (or it could be done at theHA itself) which is forwarded to HA. HA acknowledgesthe key to the mobile client and stores the public keys ofthe mobile client in its cache. Let the time taken togenerate the keys be TK. As the mobile client movestowards FA1, sensor networks detect the movement. Letthis time be Td. The sensor networks report mobile clientsmovement to both the HA and the FA. Let the time taken be Ti. Now the FA requests information about mobileclient from HA. Consider this time to be T(Fi-Hi). The HAreplies to the FA about the mobile client and the keysassociated with it. Let the time taken here be T(Hi-Fi). TheFA acknowledges to the HA about registration of themobile client and the associated CoA. Let the time taken be T(FA1-HA1). As the mobile client moves into the foreignnetwork, it requests registration with the FA. Consider thetime taken to transmit the registration request be T(MN-FA).

The FA sends a packet to the mobile client with its publickey and the CoA. The mobile client decrypts the packetwith its private key and extracts the CoA and the publickey of the FA. Let the time taken for this be T(FA-MN) +T(MN-FA). The HA intercepts all the packets destined to themobile client and delivers them to the destination via theFA. If the mobile client is unable to decrypt the packet sent by the FA, then it will not be able to complete theregistration process.

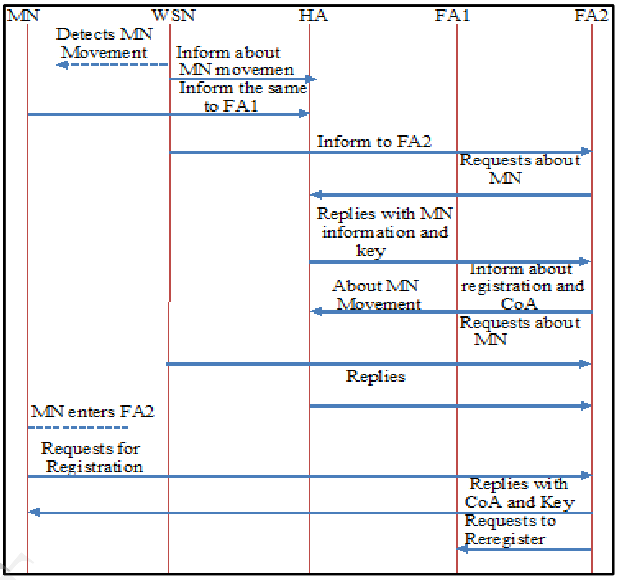


Fig (7) Timing during handoff for the proposed scheme (mobile client is moving from FA1 to FA2)

When the mobile client moves between foreign networks(FA1 to FA2), the WSN detects the movement. Let thetime taken be Td1. The sensor network reports themovement to the mobility agents i.e. HA, FA1, and FA2. Let the time taken be Ti1. The FA2 requests information about the mobile client to HA. Let the time taken be T (FA2-HA). The HA replies with the information about mobileclient to the FA2 along with the security key that need tobe used for the communication. Let the time taken be T(HAFA2).

The FA2 acknowledges to the HA. Let the time takenbe T(FA2i-HA). The registration and exchange of keys occursbetween the FA2 and the mobile client. Let the time takenbe

X=T(MN-FA)+T(FA-MN)+T(MN2-FA). (4)

Next, the FA2requests the FA1 to delete the entry for the mobile client and perform layer 2handoff. Let the layer 2 handoff delaybe TR. Hence Total handoff time (layer 3) before nthmovement and after (n+1)themovement using proposed architecture is

Total Time=TLifetime+Td1+Ti1+T(FA2-HA)+T(HA-FA2)+T(FA2i-HA)+X+L2delay+TR (4)

Comparing the four approaches described here, it can besaid that, while the proposed architecture introducesadditional protocol overhead, it provides highest securityfor the communication between the mobile clients and themobility agents. With the pre-registration process in place,the actual handoff delay will be just the layer 2 handoffdelay (similar to basic WSN based handoff approach).

Hence, the performance impact would be negligible as compared to other approaches. Since the securityassociations are established during the layer 3 handoff process the communication between the mobile client andthe mobility agents will always be secure. While, in thispaper, the authors have not discussed the securityassociations between HA and FA, that is another aspectthat could be considered for further enhancements.

5. Drawbacks: As per the proposed architecture, the mobileclient will send additional packets periodically updatingthe HA with the new security key. This will add additionaloverhead. Another drawback of the proposed architectureis the memory requirements. As the number of mobileclients supported by a home agent increases, the memoryrequired to hold the security keys will also increase.

V. CONCLUSIONS

In this paper, the authors have proposed novel securityarchitecture to secure the communication between themobile client and the mobility agents. The proposedarchitecture is designed to be light weight and has minimal impact on the performance of the mobile clients. Throughanalysis, the authors have proved that, with minimal cost,the proposed architecture provides better securitycompared to other similar approaches. As part of the futurework, the authors are looking at the ways to implement theproposed architecture and test its working. The authors arealso looking into the security of communication betweenthe mobility agents as that is one of the weak links in thecurrent.

VI. REFERENCES

1. Al Shidhani, Ali A. ; Leung, Víctor P C M "Secure and Efficient Multi-Hop Mobile IP Registration Scheme for MANET-Internet Integrated Architecture" Wireless Communications and Networking Conference,10.1109/WCSN. 2009.5434791 (WCNC), 2010 IEEE, Publication Year: 2010 , Page(s): 1 – 6.
2. C Perkins "IP Mobility Support for IPv4" RFC 3344, August 2002.
3. Charles E. Perkins, "Mobile IP" (publisher: prentic hall] (Feb.2008), second edition.
4. D Shi and C Tang, "An authentication method on security association for mobile IP fast handoff," Wireless Communications, Networking and Mobile Computing, 2005,Volume 2, 23-26 Sept. 2005 Page(s):1324 – 1327
5. Hung, T.C, Duong, V.T.T., "Performance Evaluation of Mobile IPv6 Fast Handover", Published in: Advanced Communication Technology (ICACT), 2011 13th International, Date of Conference: 13-16 Feb. 2011, Page(s): 1304 – 1308, 2011.
6. 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
7. Roja Kiran Basukala, Kyu-Jin Park, Dong-You Choi, Seung-Jo Han "Secure Mobile IP Communication in Residential Networks" 2010 IEEE 24th International Conference on Advanced Information Networking and Applications Workshops Perth, Australia, April 20-April 23-2010.
8. J.Solomon. "Mobile IP The Internet Unplugged", New Jersey. Prentice Hall International, Inc. 1998
9. Xiaoping Li, Kai Wu, "Research of Mobile IP Tunneling Mechanism", Published in: Networked Computing and Advanced Information Management (NCM), 2010 Sixth International, Date of Conference: 16-18 Aug. 2010, Page(s): 179 – 182, 2010.