Secure Authentication Mechanism in Mobile Internet Protocol Version 6

Mojtaba Sadeghi [1], Dr. Mohammad V. Malakooti [2]
[1]Faculty of Department of Computer Engineering, Islamic Azad University, UAE Branch, Dubai, UAE
Email: sadeghi_kia@yahoo.com
[2]Faculty and Head of Department of Computer Engineering, Islamic Azad University, UAE Branch, Dubai, UAE
Email: malakooti@iau.ae

Abstract

This paper presents a secure authentication method for Mobile IPv6. As a default IPsec is used for secure signaling messages between the Mobile Node and other agents in Mobile IPv6 networks. Mobile IPv6 message transactions include the Binding Updates and Acknowledgement messages as well. We propose a new mechanism for securing Mobile IPv6 signaling between Mobile Node and other agents. The proposed method consists a Mobile IPv6 message authentication option and cookie management that can be added to the current protocols for securing IPV6. Also we investigate architecture to integrate the mobility authentication signaling. This architecture is implemented and evaluated. In Mobile IPV4 protocol and also some authentication protocols of Mobile IPV6, there are some difficulties for satisfying timing requirements. We show the latency can be decrease between the Mobile IPV6 node, Home Agent and Correspondent Node with creating a cookie file keeping the mobile node identification.

Keywords: Secure, IPV4,IPV6,Mobile, Authentication

1. Introduction

The security of a mechanism and protocol depends on the reliability and infrastructure of the Internet routing. The protocol will work between mobile nodes and any other Internet node that have no previous connection or relation with, and also we assume there is not any specific global security infrastructure.

When Mobile IPV6 was developed, the built-in technology made it possible for users to change their points of attachment to the Internet while they still using the same IP connections established before. But, authentication and authorization, which are too important functions in wireless networks, were not considered during the design and creation. Therefore, this paper investigates the integration of MIPv6 and Authentication systems and develops integrated architectures as well.

The mechanism described in this paper is a simplified version of the actual Mobile IPV6 protocol. We focus on the binding-update messages sent by the mobile node to its correspondents. In fact authentication service is the most important protection and inspection services in wireless networking.

Security designing in mobile network is a critical stage in developing and establishing a Network infrastructure system. While a wireless system provides economic, convenience and efficient network , it must also be secured to prevent attack for theft and damage of data and information . A safe and secure wireless network can ensure that your data transmissions are not intercepted, abuse, misuse by unknown third-party. Unsecured wireless networks are vulnerable to many types of problems, including:

-Theft of information
-Corruption or illegal modification of data
-Interception of interaction ,transaction and communication
-Insider abusing of network data and resources

Establishing a professional and secure wireless network means implementing a framework of authentication, encryption and key management protocols[1]. We focus on authentication with IPV6 in this paper. As a description , authentication is a process of verifying that a device or user that is attempting to log in to the wireless network, should be allowed on the network. Encryption and Key Management are processes and techniques that are make more complex and scramble data so that an unauthorized user or device that receives the data cannot use that.

2. IPv6 Review

Based on the recent concerns over the lack of internet addresses and the desire to provide more functionality for modern mobile devices, an upgrade of the old and current version of the Internet Protocol (IP), called IPv4, has been established. This new version, called IP version 6 (IPv6), resolves weakness of IPv4 design issues and made a revolution in Internet in recent years. The long of addresses in IPv6 are 128 bits. The first 64 bit are used for the link prefix. Which it is assigned to every link and gets advertised through routers on that link. The second 64 bit of the address belongs to the interface identifier .There are different scopes of IPv6 addresses in networking. The different scopes can be diagnostic by looking at certain bit patterns of the address prefix.[4]

We can call the most important scopes in IPv6 as below:

- Link local: An address with a scope of link local only can be used to communicate within the node’s link. Packets with this link addresses will not be routed outside the link. The first 64 bits of this addresses are fixed and look likes this: 1111111010 0 . .

- Site local

First 10 bits Proceeding 54 bits. Link local addresses are like unique addresses inside a site. The size of a site will define by site administrator. It can be a small home network with two or three clients or even the network of a university with hundreds nodes. The first 64 bits of

site local addresses look like follows: 1111111011 0 . . . - Subnet ID
The 16 subnet bits are used to differentiate sites and First 10 bits Proceeding 38 bits last 16 bits. Protocol transitions are not easy and the transition from IPv4 to IPv6 is no exception. Protocol transitions are typically deployed by installing and configuring the new protocol on all nodes within the network and verifying that all node and router operations work successfully. Although this might be possible in a small or medium sized organization, the challenge of making a rapid protocol transition in a large organization is very difficult. Additionally, given the scope of the Internet, rapid protocol transition from IPv4 to IPv6 is an impossible issue. The designers of IPv6 recognize that the transition from IPv4 to IPv6 will take years and that there might be organizations or hosts within organizations that will continue to use IPv4 indefinitely[1]. IPv6 solves the network address limitations of the current IPv4 protocol by replacing IPv4's 32-bit addresses with 128-bit addresses.

Different elements were considered during the design of IPv6. One of this consideration is forecasting about the needs of future markets. We can guess that future of internet markets would rely on more security, high efficiency, and mobility[7].
Another successful issue of IPv6 designing is the way of internet’s transition from IPv4. This kind of transition involves with different software, hardware, protocol and infrastructure problems. Fortunately IPv6 has been developed to work with IPV4 network protocol as well. By creating a tunnel to transfer IPv6 packets or by creating a tunnel for transferring other protocol packets, IPv6 will support without requiring any fundamental changes.
When a mobile node is far from it's home agent, it sends information about its current location to the home agent. Any node that it wants to start interaction and communication with a mobile node will use the home address of the mobile node for this communication and sending packets. The home agent intercepts these packets information, and via using tunnels the packets to the mobile node's care-of address. In fact Mobile Network IPv6 uses care-of address .But for supporting route optimization for direct connection between Mobile Node and Correspondent Node, the Correspondent node will use IPv6 header than the IP encapsulation.
Mobile IPv6 technology allows a Mobile Node to move within the Internet infrastructure without loosing an old established connection. It means for a Mobile Node to be reachable at any time by a Correspondent Node it must have an address that not change. In fact this address belongs to the subnet of home network. In Mobile IPv6 this address is called, Home Address or HoA. If Mobile Node be available in its home network, all packets that want to reach to it, can reach the through the normal routing way. In this situation the Home Agent is topologically correct for the Mobile Node.
But if the Mobile Node moves to another subnet, it must to update a Care of Address that topologically this address belongs to the new network. From now Mobile Node will not be reachable through its HoA as well. Home Agent is responsible to receive all packets that destined to the Mobile Node, whenever Mobile Node is in another visited network.
Whenever Home agent receives a packet, it would establish a tunnel it to the Mobile Node's current Care of Address. It proves the Mobile Node has to update its Home Agent about its current Care of Address regular.

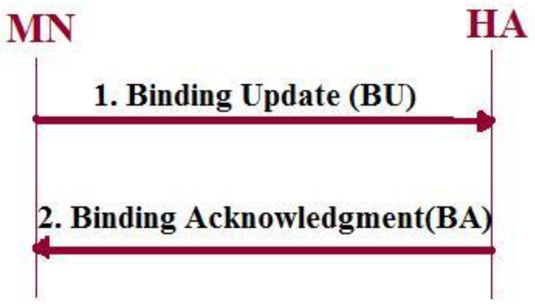

Figure 1: Simple Binding Update

It means Home Agent will forward any packets destined to the Mobile Node’s Home Address, to its current Care of Address in visited network. These packets will send through a tunnel to the Mobile Node. It should be considered that the tunnel begins from the Home Agent and will end at the Mobile Node. Mobile IPv6 works like transparent for upper layers like applications. Any time Mobile Node wants to send a packet to the Correspondent Node, it can send it direct to it's address.

3. Security on Mobile IPV6

3.1. Data Encryption and authentication protocol

One of the solution for making sure that unauthorized users or systems do not access on your wireless and mobile network is to encrypt your data and files. The famous and basic encryption method, WEP (wired equivalent privacy), unfortunately was found to be completely weak and non-stable. WEP works on a shared key technology, or password, to prevent unauthorized access.
Anyone who find the WEP key or even stronger key can join and misuse the wireless network. There is no any mechanism or technique in WEP to automatically change this key, and some tools have produced that can crack a WEP key very fast , even less that 60 sec! It means it will not take long time for an attacker to access a WEP-encrypted in wireless network. We can say the procedure of RADIUS server is receiving end user requests, then authenticating the user, and finally providing the NAS plus all of the information for it to deliver services. This protocol of authentication provides a centralized security system to control access to the network resources.
Lightweight Directory Access Protocol or LDAP is called another authentication protocol which defines organized and accessed information. As we know an authentication protocol is a set of rules for communication between server and clients. By

implementing LDAP, Network administrator can control users and clients easier with centralize and secure user information[12].
Also there are other mechanisms for mobile authenticating clients, the combination of RADIUS, EAP, and LDAP is the most common and available solution in use in business today. Each component has associated open-source software that is freely available for network administrators to download, configure, and use. Thus, with the hardware in place, installation of an authentication system is inexpensive[15].

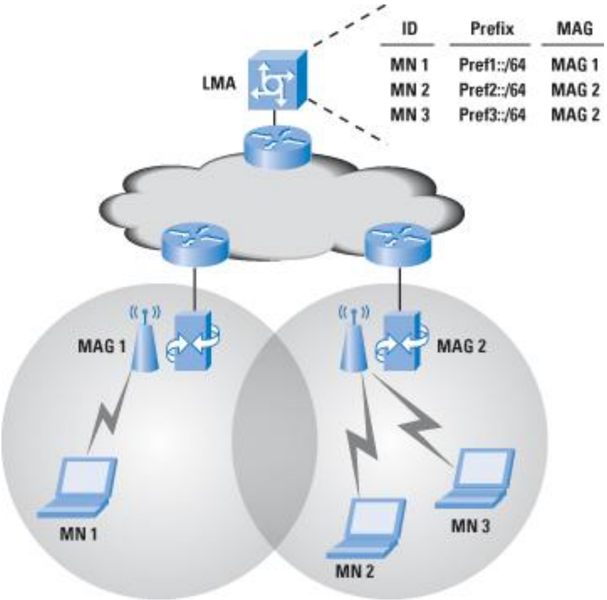

Figure 2: Mixed Mobile Authentication Protocol

3.2. Hijacking and Spoofing on Mobile IPV6 Networks

The first difficulty of IP networks is that it is difficult to know where information really comes from. An attack called IP spoofing takes advantage of this weakness. Since the source IP address of a packet has no influence to the deliverability, it can easily be changed. The attack – called spoofing – makes a packet coming from one machine appear to come from somewhere else altogether. It's obvious that IP based address is not trustable at all, because everyone can claims he is the owner of this IP address. Even after authentication step , still everything is not safe against sessions hijacking. It means after identification of a person, we can not make sure he will be the same person during the rest of that session.
That's why all source of data must authenticated during the transmission.Still most of networks in the world are based on Ethernet or cabling LANs. This type of network normally are cheap, globally available, easy understood and fast to expand. But making spying is easy in these networks, because any node is able to read every transmitted packet over the LAN.

Formally, each network card only listens and responds to the packets that specifically belongs to it, but it is not difficult to ask these devices to listen all packets during passing on the wire.
The first recommendation for all Mobile IP networks is to use encryption and authentication the data. But there are still problems on that. We should consider all encryption keys will be exchanged during communicating parties. It's a rule that encryption keys use encryption algorithms to encrypt and decrypt data.

3.3. Mobile Node MAC address and Authentication

A sorted care-of address is a care-of address that obtained by mobile node as a local IP address. This IP address will be dynamically acquire, may be through a DHCP server or via a foreign agent. After assigning a routable IP address to MN, the mobile node is now able to establish and communicate directly with it's home agent, careless of foreign agent. By implementing of this method, mobility De- capsulation has done. Sometimes Mobile Node uses the Mobile Node Identifier option to establish of communication and enable the Home Agent to start using of available authentication infrastructure. One of the most difficult step for an attacker is finding the MAC Address of wireless Lan[7].
Many of systems may trust on a faked MAC address, as an authorized wireless router or client. Attacker can start denial of service attacks by passing access control mechanisms in wireless. MAC addresses have been used as unique layer 2 for network identifier in Mobile IPV6 Networks. As we know MAC address is unique in the world for all network-based devices. Organizationally unique identifiers (OUI) has allocated to all hardware manufacturers specially network products manufacture. Generally the MAC address of a client or mobile node is used as an authentication parameter or a unique identifier for making security in authentication level.

When an attacker changes their MAC address they continue to utilize the wireless card for its intended layer 2 transport purpose, transmitting and receiving from the same source MAC. All 802.11 network protocol use their MAC addresses to be changed, with support from the manufacturer[6].
Linux users can change their MAC address with some command or programming with C program. But windows users are able to change their MAC address by configuring the properties of lan card drivers. We should care that an attacker may choose to change the MAC address for different reasons[15].

The Mobile IPv6 protocol enables a Mobile Node to move from one network to another network without the need to change its old IPv6 address. Because a Mobile Node is always routable and addressable by its home agent, which is the Mobile Node's IPv6 address. When a Mobile Node is far from its home network, messages can be routed to it using the Mobile Node’s home address. Normally the movement of a mobile node is completely invisible to transport and other layer protocols.

3.4. Mobile IPV6 Accounting

Mobile IPV6 accounting can be divided to four processes: metering, pricing, charging and billing. Actually the duty of metering process would be measure and collects the resource usage information

which is related to a single customer' service. Also the task of pricing would be the process of determining a cost per unit. Then charging process make compatible the pricing data to the usage of resource to an amount of money that we called charge. This charge has to paid by customer. And billing process obviously informs customer about the billing information[7].
In fact accounting on Mobile network means the act keeping the records for all user's usage of the source. The primary aim could be billing for any user but for security reasons we need to know each users logon and logout time, visited websites, amount of download and upload and so on.

4. New Mechanism

4.1. Mobility Message Authentication with a Cookie File

This section defines a new mechanism in mobility message authentication option that can be use to secure Binding Update and Binding Acknowledgement messages in mobile IPV6 networks. This mechanism is able to used along with IPsec or preferably as an new mechanism to authenticate Mobile node in communication with Home agent or foreign agent to Binding Update and Binding Acknowledgement messages whenever we don't have IPsec infrastructure in our network.
The simulation of the Mobile IPV6 protocols is based on the implementation of Mobile IPV6 in Network Simulator 2 (NS2). Overall implementation is based on home station, correspondent node and mobile agents. In fact base station agent will implement the functionality of home agent and foreign agent. This agent will create the Broadcasting area. This area will re-set every second. Mobile IPV6 agent finds the advertisement and registers with home agent and foreign agent based on protocol.
The registration timeout for Mobile IPV6 protocol has set for one second. It means every second updating of registration will happen.
For simulation we developed a simulated Mobile IPV6 network that considers to delay and payload. Also for the simulation of the authentication, home agent will create a cookie file as a identity file.

Based on our assumption the Mobile Node has registered with the home agent before leaving it's subnet. The Mobile Node as a personal computer has some specific details that it can save them in a cookie as a file and then encrypt the file[10]. Home Agent MUST include this option in the BA if it received this option in the corresponding BU and Home Agent has a shared-key-based mobility security association with the Mobile Node[2].

4.2. New Care-of Address and Binding Update

After detection that a Mobile Node has moved the network, new CoA allowed to access to the network, but it must inform its Home Agent regarding the new location of Mobile Node. It's a big concern in mobility that whenever a Mobile Node lost it's connectivity with its last router, until it informs its Home Agent about its new location, all messages that sent to it will lost and also it will not able to send any packet to any of correspondent nodes. Actually a Mobile Node registers its new Care of Address to its HA via sending a binding update message. Then Home agent does acknowledge this update by replying a binding acknowledgement and from that time is able to tunnel the packets from Mobile Node's home address (HoA) to the Mobile Node's in new location.
In the last step, The Mobile Node informs all of its Correspondent Node, its new location and that it is reachable with this new Care of Address. It means after registering, the Mobile Node sends a BU to all CN to inform them about its new location. By the way, there is an additional procedure for following that BUs are sent to all CNs. This one called Return Rout ability (RR) test.

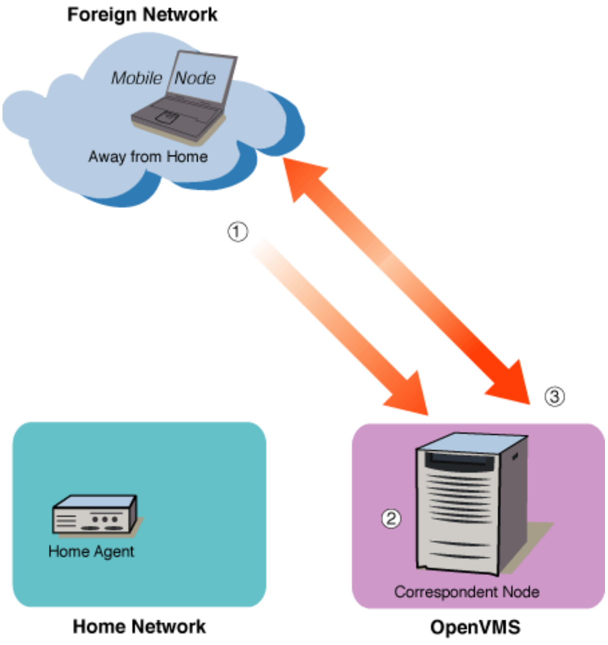

Figure 3: Secure Tunnel of MIPV6

4.3. WAP Infrastructure with Cookies

WAP protocol is a service enabler that is located between internet and mobile networks in the service layer. The service layer includes of different service enablers for mobile nodes and mobile applications.
The WAP protocol works like a secured tunnel from the mobile node to the service layer. All IP packets from a mobile node will transport via three layers of mobile networks: connectivity layer, control layer, and service layer.

4.4. Design and Implementation

Mobile IPv6 authentication relies fundamentally on IPv6 protocol functions as a standard protocol and IPv6 neighbor discovery as well[1]. It's obvious that the latency can significantly affect during following components in IPV6 Mobility[13]:
• Movement detection time (td): The time to detection and establishment for Mobile Node, when it moves to a

new location. For example the discovery of a new router.

- IPV6 Care-of-Address configuration time (ta):
The time between the establishment of movement and configuration of a globally routable IPv6 address. Duplicate address detection test is partial of this time[2].

- Context establishment time (tc): The time between establishment of a routable care-of address and the establishment of the suitable context state.

- Binding registration time (tr): The time between the sending of a binding update signal to the Home Agent to the receipt of an acknowledged Binding Update.

- Route optimization time (to): The time from registering of new Care of Address to completing route optimization with Correspondent Nodes. This time includes the return rout ability procedure time if exist, it must calculate before a Binding Update is sent by Mobile Node to a Correspondent Node[8].

In fact , the total Mobile IPV6 configuration delay (th) can be defined as the sum of these mentioned latency times as follows:
Formula 1: $th = td + ta + tc + tr + to$

4.4.1. Movement Detection Time

The movement of detection time (td) is the sum of two separate latency time:
First, Link of switching delay (Tl2) which is the time delay regarding to re-association of the wireless subnet's Access Point and Second, Link-local IPv6 address configuration delay (Tll), which is the time between the first time that Mobile Node meets a new link by receiving neighbor advertisement over its all nodes. It means movement detection time can be defined as:
Formula 2 : $td = Tl2 + Tll$

4.4.2. Care of Address Configuration Time

As we mentioned about the CoA configuration time (ta), it's a starting time from the moment of the receipt of a router advertisement till the Duplicate Address Detection and update of the routing table will complete. For stateless IPv6 address auto-configuration ta is included of the following delays:
Formula 3: $ta = TpreAd + TAddConf + TDAD + TRoutUpdt$
Meanwhile TpreAd is defined as:
TrtAd - TrtSol (if the router advertisement is requested)
TrtAdInterval / 2 (if router advertisement is cyclic)
TAddConf is the real time that Mobile Node needs to configure the address, like to Create an unique and globally routable IPv6 address. The time in stateful address auto-configuration, like DHCPv6 for Care of address can be defined as:
Formula 4: $TAddConf = TDHCPaddReq + TDHCPaddResp + TRoutUpdat$
In fact TDHCPaddReq and TDHCPaddResp will represent the transmission delay caused by stateful configuration of a care of address via a DHCP server in Mobile IPV6 network[9].

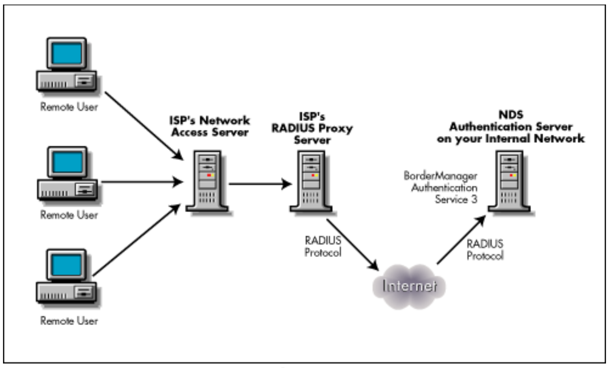
Remote User
Remote User
Remote User
ISP's Network Access Server
ISP's RADIUS Proxy Server
NDS Authentication Server on your Internal Network
BorderManager Authentication Service 3
RADIUS Protocol
Internet
RADIUS Protocol

Figure 4: Authentication Server

4.4.3. Care of Address Registration Time

Care of Address registration time or tr is defined as the transmission delay caused within registration of the Mobile Node Care of Address with its Home Agent.
Formula 5: $tr = RTMN\text{-}HA + BUproc + BAproc$

5. Delay Calculation and analyze

5.1. Authentication Delay Calculation

In this section, we quantitatively calculate and analyze the times of different phases of authentication on the security and system performance in Cookie ID based authentication and IPsec protocol with some assumption, which is the first step of the work for build up a relationship between the security and QoS[3]. Moreover the effect on the mobility security, authentication mechanism also affects on authentication delay, cost, number of message exchange, call dropping and etc[2]. Data encryption/decryption in each router involves some security processing latencies. We consider that an IPSec Mobile Network in each router take the same time. This latency lsec is evaluated with the following equation:

Formula 7 : $lsec = \frac{Dpacket}{R}$

where S*packet* is the data packet size (in bit) and R is the router encryption/decryption processing capability (in bit/s). In our assumption R is 1Mbit/Sec like a normal router. The authentication delay time is defined as the time from whenever a Mobile Node sends out the authentication request till the time that Mobile Node receives the authentication reply. The problem is during this delay, any data can be transmitted, which may interrupt or even disconnect the connections. Therefore, the call dropping will increased with the increase of authentication delay time[2].
In the other hand authentication cost is defined as the processing and signaling cost for cryptography. The total number of messages from the Mobile Node, Foreign Node and Home agent could be large if the distance between them is long[14].
It should be considered, the mobility technique and traffic mechanisms will make the authentication frequently in different scenarios because the

authentication will start whenever a Mobile Node establish a communication session.

Table 1: Symbols descriptions

Symbol	Description
Ttr	Transmission time for Mobile Node
Tu	Update Binding Time
Ta	Acknowledgment sending/receiving Time
Ted	Encryption/Decryption Time
Tr	Registration Time
Ts	Authentication request service and waiting time
Th	Home Agent updating time

Formula 8 :

Tsum = Ttr + Tu + Ta + Ted + Tr + Ts + Th

5.2. Latency and Analyze Our Mechanism

Practical of Mobile IPV6 is likely to occur where a private network is deployed over the Internet. It means this situation can hint that Foreign Agent belongs to a another subnet wants to provide mobility services. For any accounting and billing purposes, the Foreign Agent needs to track of the usage of its services by mobile nodes. We simulate the Authentication protocol of Mobile IPV6 Transport Mode. Actually the major reason for simulation is representation with the least expensive computational authentication method.

A cookie based authentication is used between the Mobile Node and Home Agent. The second association will establish between Foreign Agent and Home Agent. With the expansion of mobile security protocols and the growth of internets, all networks are trying to securely extend their wireless networks over the public infra-structure, is called Virtual Private Networks or VPN. Cookie identity authentication's functionality consists of two phases: In the first phase, mobile node and home agent involved in communication establishment and in the second phase , the home agent and foreign agent will communicate for send/receive the cookie file which is belong to mobile ipv6 node. The major difference between this two phases is that phase 1 will happen in the same subnet and naturally it's faster and easier to complete, but phase 2 must establish a communication between two different subnet. In phase 2 we recommend to establish a tunnel for higher security. The attributes of cookie file which is include Mac address, User name, Password and may extra information defined by the encryption algorithm and authentication mechanism.

Based on our assumption the maximum authentication message size would be 4096 bytes or 4KB, the transmission delay is considered 40 milliseconds, and we assume 4 Mbps for our mobile network capacity. Also IP Configuration latency on Local Site is around 20 msec and on different subnets this latency would be around 160-200 msec in Cisco standard. As a average it's considered 180 msec.

Formula 9 : IPconf-latn-local= 20 Msec,

Formula 10 : IPconf-latn-global = 180 Msec

There is an additional factors should be considered. There are additional bytes added to each packet of data sent to control errors and routing information as well. The actual numbers of these codes depend on the packet size and also protocol used in Mobile network. Generally, a typical packet of data sent will be about 90% and 10% or a bit more belongs to overhead. In order to send 4096 Bytes of data about 4506 bytes would actually need to be transmitted.

In a router with 16 MegaBITs/Sec speed transfer rate is equal to 2MB/Sec. Our Cookie file with 4506 byte would take time about 0.0023 seconds to send, assuming the source can continuously send the file and also the receiver can process it that fast and there no lost packets that need to be resent. In 802.11X protocol, router will advertise every second.

It means in the best case a Mobile Node might wait about 0 Sec and in the worst case it might to wait 1 Sec for next advertising of router and join to it. We assume 0.5 Sec for all cases as a average waiting, whenever a Mobile Node wants to find and ask a router to join to the new subnet.

Table 2 : Timing calculation

Action	In IPsec (Sec)	In Cookie ID (Sec)	Result
1st Exchange	0	0	For the first inquiry and Second exchange both are the same
2nd Exchange *(Formula 11)=* *4506b* *2,000,000b/sec* *+ 0.5=0.5023sec*	0.5023	0.5023	
Initial to Update binding (Formula 10)+Router Delay	0.6800	-- -	Update Binding is a Must in IPsec
Respond to Updating (Formula 10)	0.1800	-- -	
Refer to Home Agent*(Router Delays,10)* *0.5+0.5+0.18=1.1800*	--	1.1800	In Our Mechanism MN refer to HA
Sending Cookie File from HA to CN *(Formula 11)=* *4506b* *2,000,000b/sec* *+ 0.5=0.5023sec*	--	0.5023	HA will send the created ID cookie file to CN
Sending/Receiving Acknowledgment *Formula 11:* *0.5+0.5=1 Sec*	1.0000	--	In IPsec Acknowledgment transaction must updated
Encryption/Decryption By Tunneling *Formula7 :* *lsec = Dpacket =* *R* *4065Byte =* *0.0325Sec* *125,000Byte/Sec*	---	0.0325	Cookie file must encrypt and decrypt for security reason
Care of Address *Formula 9:* *IPconf-latn-local= 20 Msec,*	0.0200	0.0200	Assign new IPV6 address to MN
Updating HA *(Formula 11)=* *4506b* *2,000,000b/sec* *+ 0.5=0.5023sec*	0.5023	0.0023	HA already had ID from MIPV6,but in IPsec full info must updated
Total Time (Formula 8)	2.8846 Sec	2.2394 Sec	

Formula 11 :

$$\textit{Time Taken} = \frac{\textit{File Size(Kbyte)}}{\textit{Bandwidth Speed(KB/Sec)}} + \textit{Router delay (Sec)}$$

Saving time: 2.8846 – 2.2394 = 0.6452 Sec   Efficiency: % 22

6. Conclusion

We have described secured authentication Mobile IPv6 mechanism and used in the standard protocol such as IPSec. In Mobile IP network techniques, some features are unconventional because of globally working of protocols and without any global infrastructure for security challenges.

The quantitative analysis and design of Mobile IPV6 authentication with respect to the IPSec create more challenges about the authentication in IPV6 wireless networks. Overall time in IPSec in our assumption with 4KB file and 2MB/Sec router bandwidth is 2.8846 Sec. But in our mechanism with Cookie ID it decreases to 2.2394Sec . It means saving time would be 0.6452 Sec and the efficiency would be %22.

Note that we considered latency time for encryption/decryption via a tunnel from HA to CN, and obviously it takes time and cost for our mechanism[11]. We believe without making strong security, any protocol and mechanism on mobility infrastructure will not get a positive response. As result shows encryption/decryption time for Cookie ID file is 0.0325 Sec, that this time will be higher for bigger files. This time has not calculated and mentioned for IPSec protocol, because although it's strongly recommended on IPSec, but its not a Must[5].

The only disadvantage of Cookie ID mechanism could be creating cookie files on the storage of authenticator server. We can ignore these small files, because as we mentioned the size of cookie file is 4KB. Also task schedule can be configure for disk cleanup monthly, weekly or daily. It can erase these un-useful files from the storage to prevent of any confusing and conflict.

Future Researches

As the development of Mobile IP network, all security mechanisms are designed to protect valuable data and information securely. As one of the important security needed, authentication mechanism is used to identify mobile nodes, prevent unauthorized usage. Obviously authentication mechanisms will protect the communication, but they cause overheads, such as encryption and decryption load and more delay at the first of communication. Our solutions present a secure mechanism design to reduce the message exchange number during the authentication. In our proposed authentication mechanism design by Cookie ID file, we only consider a general security level hosted by two subnets. In our case for the secure authentication mechanism design by Cookie ID file in Mobile IPV6 networks, a future research is to apply this mechanism for authorization phase.

Moreover, new mechanism for authorization might be design and analyze for working with our mechanism, simultaneously. It means all rights of Mobile node can be saved on a encrypted cookie file and after authentication new server will ask authorization cookie file and run it like a batch file. It can configure and update the server and mobile node and if authentication phase has passed successfully, no need to wait for authorization level.

Moreover, latency timing can be analyzed and calculate for stateful and stateless IP address configuration. In order to using of DHCPv6 as stateful IP address configuration how much extra latency causes instead of stateless IP address configuring.

References:

[1]L. WANG, M. SONG, J. SONG, An efficient hierarchical authentication scheme in mobile IPv6 networks, School of Electronic Engineering, The Journal of China Universities of Posts and Telecommunications. China, October 2008.

[2] C. Blondia, O. Casals, Ll. Cerdà, N. Van den Wijngaert, G. Willems, P. De Cleyn,” Performance Comparison of Low Latency Mobile IP , INRIA Engineering Journal, Sophia Antipolis, pp., March 2008.

[3] H. Zhou, H. Zhang and Y. Qin, An authentication method for proxy mobile IPv6 and performance analysis, Institute of Electronic Information Engineering, Beijing Jiaotong University, Sep 2008

[4] P. Calhoun, T. Johansson, C. Perkins, T. Hiller: Diameter Mobile IPv4 Application, IETF RFC 4004, August 2008.

[5] D. Forsberg, Y. Ohba, B. Patil, H. Tschofenig, A. Yegin: Protocol for Carrying Authentication for Network Access , IETF draft, Dec 2007.

[6] M.S. Bargh, R.J. Hulsebosch, E.H. Eertink, A. Prasad: Fast Authentication Methods for Handovers between IEEE 802.11 Wireless LANs, ACM Press, Sep 2004.

[7] S. Glass, T. Hiller, S. Jacobs, and C. Perkins. Mobile IP Authentication, Authorization and Accounting Requirements. RFC2977, October 2000.

[8] T. Narten, E. Nordmark, W. Simpson, “Neighbor Discovery for IP Version 6 (IPv6)”, IETF RFC2461, August 2005.

[9] K. Chowdhury, A. Yegin: MIP6-bootstrapping via DHCPv6 for the Integrated Scenario, IETF draft, June 2006.

[10] J. Chen and K.J.R. Liu. Joint Source-channel Multi-stream Coding And Optical Network Adapter Design For Video Over IP . IEEE Transactions on Multimedia, 4(1):3–22, March 2002.

[11] D. Wei, Y. Liu, X. Yu, X. Li: Research of Mobile IPv6 Application Based On Diameter Protocol, IEEE Computer Society, 2006.

[12] P. Funk, S. Blake-Wilson: EAP Tunneled TLS Authentication Protocol Version 1, IETF draft, March 2006.

[13] A. Diab, A. Mitschele-Thiel,“ Minimizing Mobile IP Handoff Latency,” 2nd International Working Conference on Performance modeling and Evaluation of Heterogeneous Networks (HET-NET Journal, U.K., July 2006.

[14] C.F. Grecas, S.I. Maniatis, and I.S. Venieris. Towards the Introduction of the Asymmetric Cryptography. In Proceedings. Sixth IEEE Symposium on Computers and Communications, 2001, July 2001.

[15] J. C. Chen, Y. P. Wang: Extensible Authentication Protocol (EAP) and IEEE 802.1X: Tutorial and Empirical Experience, IEEE Radio Communications, Dec 2005.