Volume 2, Issue 7, July 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Analysis of Token Based Mobile IPv6 and Standard Mobile IPv6 using CPN Tool

Prof. M. N. Doja
Department of Computer Engineering
Jamia Millia Islamia, New Delhi

Ravish Saggar*
Research Scholar Singhnia University
Faculty, Banarsidas Chandiwala Institute of Information Technology, New Delhi.

Abstract - Mobile IP works like an abstractor between the Transport layer and network layer. It allows mobile devices to maintain ongoing connection irrespective of their change of networks. Mobile Internet Protocol (MIP) is defined by Internet Engineering Task Force (IETF). This standard protocol states that whenever any Mobile Node (MN) changes its location it has to register its new address i.e. Care-of-Address (CoA) with Home Agent(HA). Triangular routing is done in MIPv4 as MN directly sends messages to CN but CN sends messages to MN via HA. MPIv6 removed this triangular problem by allowing exchange of messages directly to each other only after performing Return Routability Procedure to setup secure and authenticated communication. So every time MN changes its location MN has to go through Return Router Procedure. This paper presents a Analysis of Token Based solution which can be used to avoid Return Router Procedure every time MN changes its location. Further, this paper shows that using Token Based solution will reduce the problems of Latency, Signal Overloading and Location Privacy to high extend.

Keywords – Mobile IP, MIPv4, MIPv6, Stateless Address Auto-configuration, Route Optimization, Neighbor Discovery, Triangular Routing, Ingress Filtering, Double Crossing, Issues with Mobile IP, Binding Update, Mobility Anchor Point, Public Key Encryption, security attack, Return Routability Procedure, Token, Colour Petri Net (CPN), Analysis of MIPv6 .

I. INTRODUCTION

Now a day the growth rate of mobile node is going upwards steeply. Due to this high rate in mobility the Mobility Management has become a challenging issue. Frequent change in network requires a new IP address and the packets to get routed to it. IETF defined a set of rules for this mobility, under IPv4 called Mobile Internet Protocol version 4 (MIPv4) which allows mobile devices to be associated with one permanent IP address while they freely move from one network to another network. In every foreign network they get a new IP address called Care-of Address. There are certain issues with MIPv4 like double crossing, ingress filtering and triangular routing.

To solve the problems of MIPv4, IETF has defined new protocol MIPv6, with many more enhancements. MIPv6 relishes all the advancements offered by IPv6 over IPv4 like 128-bit addressing scheme, Stateless Address Auto-Configuration, Neighbour Discovery, Route Optimization etc. and hence overcomes the issues aroused with MPIv4 including addressing issues. In MIPv6, Mobile Node after moving to another network sends a Binding Update message to both Home Agent and Correspondent Node informing them about its current IP address. But it also has issues like Update Latency, Signal Overloading and Location Privacy. Hierarchical Mobile IPv6 (HMIPv6) was proposed by IETF to overcome these issues by introducing a new router called Mobility Anchor Point (MAP). Here Mobile Node gets two temporary IP addresses – First, Regional Care-of Address which MAP uses to inform Home Agent & Correspondent Node about Mobile Node and Second, On-Link Care-of Address which Mobile Node gets in MAP's domain. Moving from one subnet to another inside one MAP's domain does not require Binding Update message to be sent to Home Agent & Remote Host, only a Local Binding Update message is sent to MAP which solves Update Latency and Signal Overloading issues upto some extend. In this paper Dynamic MAP management for HMIPv6 scheme is presented which will reduce the signal latency without compromising the efficiency event if load increases at MAP. In this there will be multilayer MAP, Super and Sub MAP. If load increases at Super MAP some load will be transferred to Sub MAP and when load goes down Sub MAP load be taken back by Super MAP. So the fall in efficiency due to heavy load will not happen.

All MIPv6, HMIPv6 and Dynamic HMIPv6, suffers with Update Latency, Signal Overloading and Location Privacy. As MN has to send BU to HA or to MAP and go through Return Routability Procedure. This paper shows the results of analysis of both Return Routability Procedure and Token Based solution. For the purpose analysis *Colour Petri Net (CPN)* tool is used.

This paper starts with a brief introduction with issues of MIPv4 then MIPv6, Token Based and at last Comparative Analysis.

II. MOBILE INTERNET PROTOCOL VERSION 4 (MIPV4)

Every Mobile Node (MN) is associated with a network called Home Network where it has a permanent IP address called Home Address. A Home Agent (HA) which is a network node generally a router which has the function of acquiring all the data that is send to the MN when the MN is outside its Home Network. When a MN moves to network other than home network then it is said to be on a Foreign Network. Since IPv4 supports only Stateful Address Auto-

configuration a DHCP server on that network provides a temporary IP address to that MN called Care-of Address (CoA). This IP address changes depending on the node's point of attachment. Foreign Agent (FA) which is a network node generally a router on the foreign network. After receiving CoA, MN registers its CoA with FA and announces its Home Address and Home Agent's address to FA. FA after registering MN registers with HA of that node by sending a message. HA in return sends a Registration Reply message informing whether it accepts registration or not. This allows the HA on home network to know exactly where the MN is located and therefore will be able to know where to send packets. If MN is unable to find a FA on foreign network then it acts as FA and then it temporary address is called Co-located Care-of Address. Each time MN changes network it gets another CoA, registers with a FA there which in turn registers with HA.

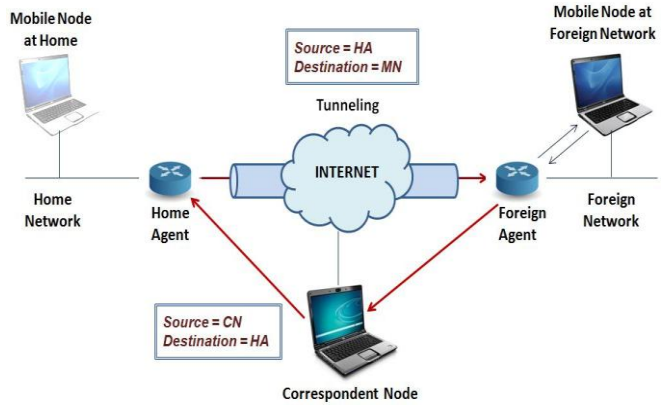

Fig 1. Working of MIPv4

In MIPv4 addresses and routers are maintained and managed with the help of ARP and ICMPv4 messages.

Correspondent Node (CN) is any node which wants to send data to MN. CN doesn't know CoA in MIPv4, it only knows Home Address i.e. permanent IP address of node. So it sends the packet with Home Address of node. Registered Home Agent receives that packet and transfers it to MN's current address where either MN directly receives it or FA receives and relays it to MN. A tunnel is set up by the HA to the CoA of node to route packet to MN which is called Tuneling. Each time CN sends packet to MN it follows the same path – from CN to HA, HA to FA, FA to MN.

But the MN sends packets using its home address, effectively maintaining the appearance that it is always on its home network. Even while the Mobile Node is wandering from one network to another, its movements are transparent to CNs. But this also gives rise to problem called Ingress Filtering.

III. ISSUES WITH MIPv4

There are certain issues with MIPv4:-

A) *Ingress Filtering*

Ingress Filtering is a technique performed by the firewall of some systems to make sure that the packets are actually from the network that they claim to be. In this technique those packets whose IP address differs from the network that the device is in are rejected. In MIPv4 the MN sends packets with Home Address while it being in foreign network and hence those packets get rejected by systems which perform Ingress Filtering. The solution to it is Reverse Tunneling. In Reverse Tunneling FA after receiving packet from MN transfers it to HA this in turn, relays it to CN.

B) *Double Crossing*

Even if CN and MN are on the same network still whenever CN wants to send a packet to MN it will follow the same path – from CN to HA, HA to FA, FA to MN i.e. the packet crosses the internet twice.

Though, the transmission would have been faster and reliable if packet travels directly from CN to MN.

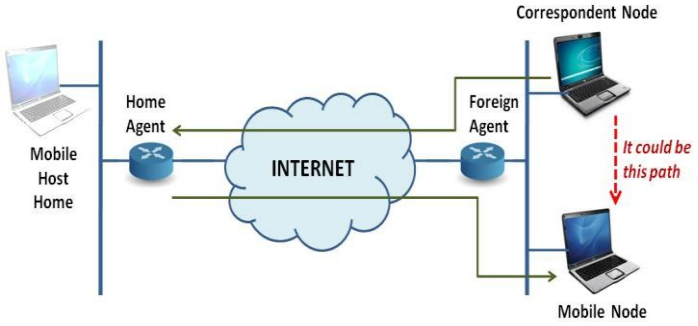

Fig 2. Each packet crosses internet twice

C) *Triangular Routing*

Since CN is unaware of the CoA of MN it always sends packet to Home Address of MN which relays it to FA which further relays it to MN. Hence a packet from CN to MN always gets routed from this triangular path.

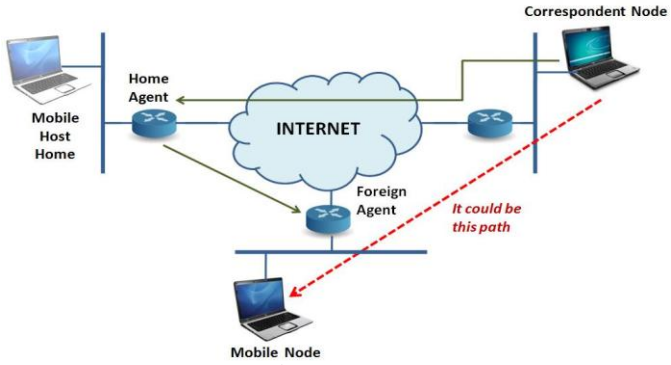

Fig 3. Packets following triangular path

Though, the transmission would have been more faster and reliable if CN knows the CoA of MN and directed the packets directly to MN's present address.

V. MOBILE INTERNET PROTOCOL VERSION 6 (MIPv6)

Main features of MIPv6 are:-

A) *Stateless Address Auto-Configuration*

In IPv6 a node can configure its own IP address with the help of Internet Control Message Protocol version 6 (ICMPv6) messages. Unlike in IPv4 where a DHCP sever provides MN with a temporary IP address. It is called stateless because no one other than the node itself manages its address, therefore no need to manage state.

B) *Neighbor Discovery Protocol*

In MIPv6, MN can automatically locate routers in the network with the use of two ICMPv6 messages – *Router Solicitation* and *Router Advertisement.*

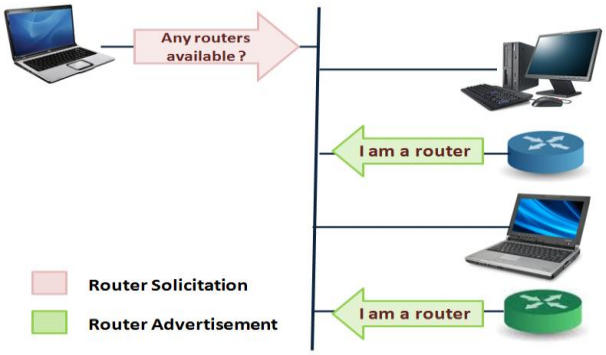

Fig 4. Router Solicitation and Advertisement

MN after reaching Foreign Network multicasts Router Solicitation message on the network. Corresponding Routers on that network responds by sending Router Advertisement message. Routers which are ready to become agents append Agent Advertisement message to the Router Advertisement message.

Stateless Address Auto-configuration takes place with the help of ICMPv6 Address Resolution messages – Neighbor Solicitation and Neighbor Advertisement.

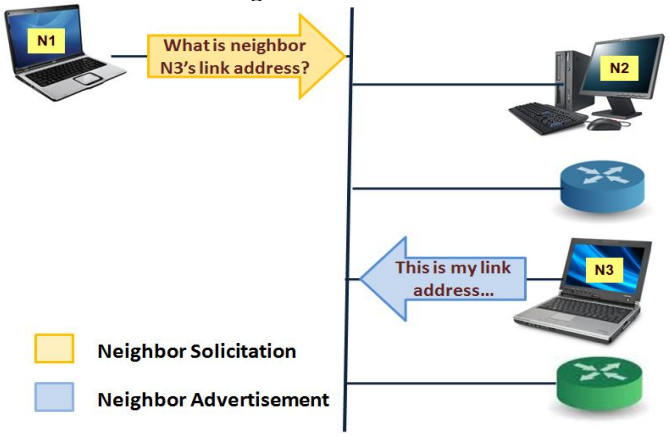

Fig 5. Neighbor Solicitation and Advertisement

Neighbor Solicitation message is sent by MN to request link layer address of neighbor, or to verify that a neighbor is still reachable and also for duplicate address detection. Neighbor Advertisement is response to Neighbor Solicitation by a node telling its link layer address. A node may also send unsolicited Neighbor Advertisement message to announce a link-layer address change.

C) *Route Optimization*

This allows a CN to send messages directly to the MN's CoA and for MN to send messages to CN using its current temporary IP address i.e. CoA, bypassing the HA. Hence it solves Ingress Filtering, Double Crossing and Triangular Routing problem.

VI. WORKING OF MIPV6

For first packet from CN to MN working of MIPv6 is same as MIPv4. CN only knows Home Address of MN; it sends the packet with destination address as Home Address of MN. Since MN is not there HA receives it and forwards it to MN's CoA.

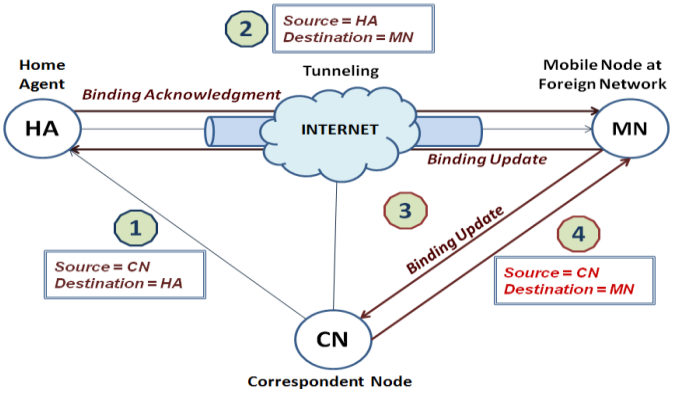

Fig 6. Working of MIPv6

But once MN knows that CN wants to communicate with it, it sends a Binding Update (BU) message to CN which contains its present IP address. CN after knowing the current location of MN sends the packet directly to MN with destination address on packet as CoA of MN. MN also sends packet directly to CN by using source address as CoA hence resolving Ingress Filtering problem.

After BU, the following packets between MN and CN are sent directly. Packets from MN to CN contains a header called Home Address Option (HAO) which tells CN that even though the packet is from source address as CoA, the node is actually from address contained in HAO. A packet from CN to MN contains a Routing Header which tells MN that even though the packet is destined to CoA, it is actually intended for Home Address.

Whenever MN changes network it sends Binding Update message to HA and CN. They sometimes respond with another message called Binding Acknowledgment (BA).

VII. ISSUES WITH MIPV6

There are certain issues with MIPv6:-

A) Update Latency

The MN is obliged to send a Binding Update message to its HA and CN each time it changes point of attachment. If HA or CN are at large distance from MN and MN is changing location frequently than update latency occurs.

B) Signaling Overhead

End-to-end path establishment is necessary for transmission and due to which BU and BA are waited for. Signals and packets get lost during waiting.

C) No Location Privacy

There is no location privacy in MIPv6 since the change in temporary local address as the MN moves exposes the MN's location to CN and potentially to eavesdroppers.

VIII. HIERARCHICAL MOBILE INTERNET PROTOCOL VERSION 6 (HMIPV6)

HMIPv6 proposes multi-level Hierarchical Network architecture. In HMIPv6 a new router called Mobility Anchor Point (MAP) is introduced. MAP is used by MN as its local Home Agent. It is similar to Foreign Agent of MIPv4 but it

need not reside in each subnet. It can be located at any level in a hierarchy of routers including the Access Routers (AR).

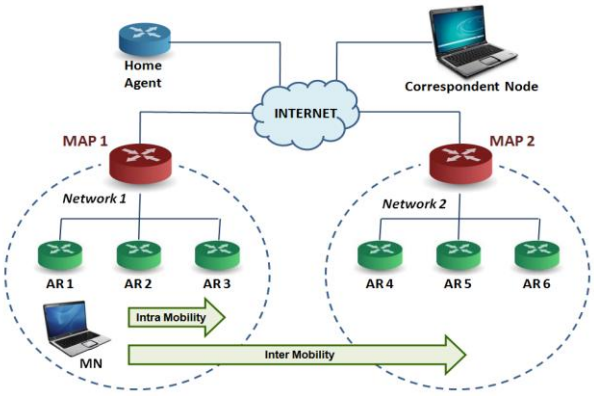

Fig 7. Working of HMIPv6

In HMIPv6, MN gets two temporary IP Address – *Regional Care-of Address (RCoA)* and *On-link Care-of Address (LCoA).* RCoA is an address which MN obtains from visited network in the MAP's domain. This is the current temporary address used by MAP to register with MN's HA i.e. HA knows RCoA of MN only. LCoA is an address obtained by MN in AR's subnet inside MAP's domain. MAP can help in providing seamless mobility for the MN as it moves from Access Router 1 (AR1) to Access Router 2 (AR2), while communicating with the CN.

Whenever MN moves from one subnet to other inside same MAP's domain i.e. Intra Mobility, only it's LCoA changes, RCoA remains the same. MN sends a Local Binding Update message to MAP in order to establish a binding between RCoA and LCoA. After a successful registration with the MAP, a bi-directional tunnel between the mobile node and the MAP is established. All packets sent by the mobile node are tunneled to the MAP.

RCoA only changes when MAP domain changes. HA and CA only knows RCoA and only MAP knows LCoA. When CN sends a packet to MN, acting as a local HA, the MAP will receive all packets on behalf of the MN it is serving and will encapsulate and forward them directly to the MN's current address i.e. LCoA.

IX. SOLUTION OF MIPV6 ISSUES WITH HMIPV6

The movement of MN remains completely transparent from CN and HA in HMIPv6. Since HA and CN only knows RCoA of MN and any change in LCoA needs only to send Local Binding Update message to MAP. Sending update messages to MAP is quite faster than sending to HA and CN. Rest all work - registering with HA, recieval of data, transmission of data - is managed by MAP. It solves the Location Privacy issue of MIPv6. HMIPv6 separates the local mobility from the global mobility hence speeds up the transmission. In MIPv6 even a movement from one subnet to other requires to send BU message to both HA and CN and this becomes issue if the distance between MN and HA or CN is large and MN is changing network frequently. Here the Update Latency problem and Signal overloading problem certainly gets solved in case of Intra or local mobility.

X. ISSUE WITH HMIPV6

When MN moves from one MAP's domain to other MAP's domain i.e. for Inter Mobility it is again inefficient. It faces higher handover latency and packet loss which decreases its overall performance.

XI. SOLUTION OF HMIPV6 ISSUES WITH DYNAMIC MAP MANAGEMENT:

Dynamic MAP Management Scheme is presented in this paper. In this scheme there will be two levels of MAP as shown in Fig 8. First level MAP will be super MAP and have two load levels Low Load (LL) level and High Load (HL) level as shown in Fig 8. These LL and HL will represent the load level of super MAP. Second level MAP will be sub MAP. This sub MAP will be activated and will take load from super MAP if the load of super MAP goes beyond HL level. This sub MAP will again be deactivated, as soon as super MAP load level goes down. So when loads goes beyond HL level load will be shared and as soon as load goes down load will be taken back from sub MAP. This scheme will work as follows:

A) When MN comes into the vicinity of AR in foreign link, it sends Registration signal to sub MAP.

B) Sub MAP will forward registration signal to super MAP after keeping a copy of registration information, although it is not an active MAP.

C) Super MAP will register all MN's entry, coming from sub MAPs. These registration information is stored in separate tables, for each sub MAP, to solve searching problem.

D) Process at serial number i to iii continues, till super MAP 's load reaches HL level.

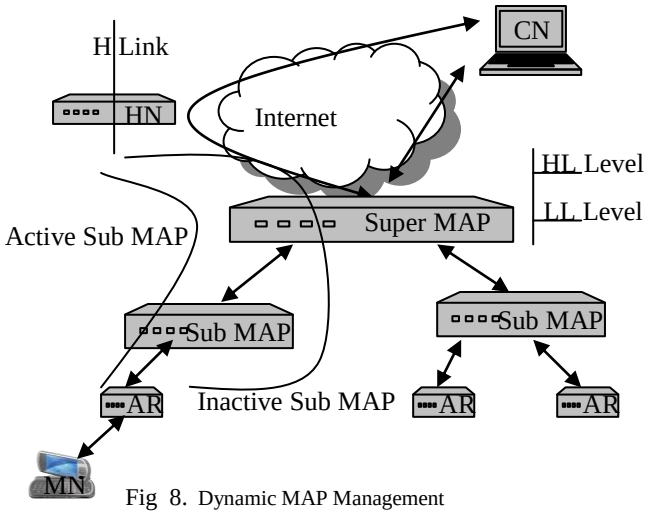

Fig 8. Dynamic MAP Management

E) As soon as super MAP load reaches HL level, it becomes necessary to immediately activate the sub MAP. For this super MAP sends load sharing signals to sub MAP's in round robin, it starts with highest number of MN's registration signals sent from sub MAP, till any one of the sub MAP sends ready signal(ready to manage all MN's sent via this particular sub MAP).

F) As soon as it receives the ready signal from sub MAP, it sends activate signal to that particular sub MAP and wait till it acknowledged back.

G) Sub MAP receives activate signal and as sub MAP has the copy of registration signals, sent to super MAP, it will just activate itself.

H) Sub MAP will now send new registration signal to all MN's,it has, HA & CN & send activated signal as acknowledgement to super MAP .

I) Super MAP, after receiving acknowledgement from sub MAP:
   (a) Encapsulates and forward those packets destine to MN, which has now been managed by sub MAP.
   (b) Reduces its load level and ask all, if any active, sub MAP's about their load, except to that sub MAP it last transferred the load.

J) All sub active MAPs response super MAP by sending their load levels after being asked or after fixed intervals.

K) Super MAP always try to vanish as many as possible sub MAP, for this it calculates new load level by adding, its load with individuals sub MAP's load, starting with lowest load sub MAP. If calculated level comes lesser then its LL Level it takes back the charge from that particular sub MAP.

L) To take back the charge Super MAP sends transfer signal to that particular sub MAP.

M) After receiving transfer signal, Sub MAP updates the registration record of super MAP, sends new registration signal of super MAP to all HA and CNs. After receiving acknowledgement from all HA and CNs, it becomes inactive. Then, it sends deactivated signal to super MAP.

Above mentioned processes ensure, to keep MAP area as bigger as possible without compromising the performance of MAP.

XII. SECURITY OF MESSAGE IN MIPV6 & DYNAMIC HMIPV6

In above all schemes, there are several types of messages involved. Binding Update (BU) message which is common in both for informing Home Agent and Correspondent Node about current location of Mobile Node and Local Binding Update (LBU) message send to MAP for binding LCoA to RCoA. One problem is Binding Update messages are not authenticated. When a MN reaches foreign network ICMPv6 messages comes into play. For searching routers as agents Router Discovery messages- Router Solicitation & Router Advertisement are used. For generating IP address Address Resolution messages – Neighbour Solicitation and Neighbour Advertisement are use. Securing all these messages is quite important because they help in finding legitimate Agent and legitimate IP address for Mobile Node. BU And LBU plays a very important role in delivery of packets to right destination. But what if there is an intruder which generates an illegitimate BU or LBU and sends it to HA or CN. CN considering that message as legitimate sends packets to intruder's address.

A) Types of Possible Attacks

1). Masquerading

Intruder pretends to be Mobile Node. Generates a fake BU or LBU and sends it to MN's HA and CN or MAP and hence all the data will get directed to it.

2). Replay attack

Intruder captures the messages coming from MN hence gets the current location of MN and then replays the message to the destination.

3). Modification of message

Intruder after capturing the BU or LBU changes the IP address of those messages so that HA, CN or MAP gets wrong CoA of MN and packets can never reach the correct MN or packets get directed to intruder instead of MN. Even the packets going from MN can also be modified in a way that they start suffering Ingress Filtering and firewall of destination rejects them even though the message was from legitimate MN. ICMPv6 messages can also be modified by intruder so that MN gets wrong router as agent or generates wrong IP address in stateless address auto-configuration.

4). Denial of Service attack

A Denial of Service attack is an attempt by attackers to prevent legitimate users of a service from using that service. It includes bandwidth consumption, consumption of scarce resources, and alteration of network components or configuration so that MN can't use service.

The solution for getting prevention from these security attacks is authentication of Binding Update message.

XIII. TOKEN BASED SOLUTION MESSAGE

For securing and authenticating Binding Update messages key based encryption can be used. Encryption is simply the obfuscation of information in such a way as to hide it from unauthorized nodes while allowing authorized nodes to see it. Public Key Infrastructure (PKI) enables users of unsecure public network to securely and privately exchange data through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority.

In Public Key Encryption both MN and HA or CN must have a key. The keys are different but are related to each other. The relationship between the keys is such that information encrypted by Key 1 can only be decrypted by its pair Key 2. If Key 2 encrypts the information, it can only be decrypted by Key 1. Another property of public key encryption is that if a node has one of the keys of a pair, it cannot compute the other key. For achieving confidentiality, encryption is performed with the public key. That way only the owner of the key pair can decrypt the information since the private key is kept secret by the owner. For providing authentication, the owner of the key pair encrypts the information with the private key. Only the correct published public key can correctly decrypt the information and thus only the owner of the key pair could have sent the information. The *integrity* of the information in transit is protected in either operation. The integrity of the information after reception can be checked if the original information was encrypted with the owner's private key.

- A *certificate authority (CA)* is an authority in a network that issues and manages security certificate and public keys for message encryption.

- A *registration authority (RA)* is an authority in a network that verifies node's request for a digital certificate and tells the certificate authority (CA) to issue it.

- A *digital signature DS[x,y,z]* is an electronic signature that can be used to authenticate the identity of the sender of a message, and possibly to ensure that the original content of the message that has been sent is unchanged. In this x has generated DS for y node using y key.
- *Digital Certificate DC[x,y]* is issued by a certification authority (CA). It contains node's name, a serial number, expiration dates, a copy of the certificate holder's public key and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. In this x has generated DC for y node.
- A*uthentication server (AS)* is an application that facilitates authentication of a node that attempts to access a network. There is one AS for every subnet.
- The *private key Pr(x,y)* is kept secret by the owner of the key pair. x denotes entity that generated it any y denotes entity for which it is generated.
- The *public key Pu(x,y)* is published with information as to who the owner is. x denotes entity that generated it any y denotes entity for which it is generated.
- *Tentative Address (TA)* is an IP Address generated by node before getting converted to permanent address.

A) *Working Of Token Based MIPv6*

The Manufacturing Company (MC) of NIC card in node, requests CA to issue Private-Public key pair and Digital Certificates. RA verifies node's request for DC and ask CA to issue it. CA issues DC that contains a Public Key Pu(CA,MC), expiration date, digital signature of issuer. Then that public key is made publicly available. The matching private key Pr(CA,MC) is also given to MC as shown in Fig 9.

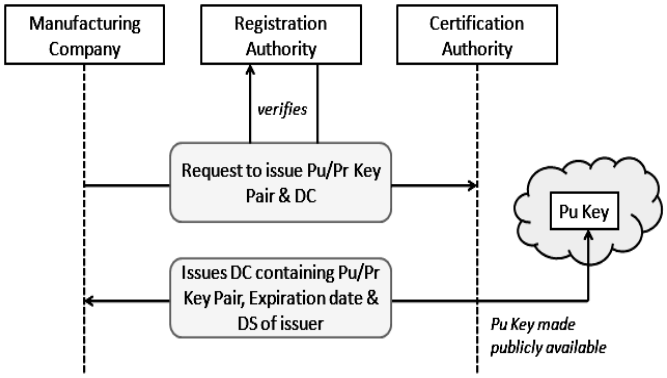

Fig 9. Request and issue of Pu/Pr Key Pair and DC

The Manufacturing Company (MC) of NIC card put DS [MC,N1,Pr(CA,MC)]. The MD1 (using hash function) is generated from Pu(CA,MC), NIC number, DC(CA,MC). Along with this MD 1, and Pu(CA, MC), NIC number, DC(CA, MC) Node1 will encrypt all the above components using Pr(CA, MC) which will give DS[MC,N1,Pr(CA,MC)]. This Digital Certificate, Digital Signature and NIC number is written on the interface card. Which is used to verify the NIC, using public key Pu(CA,CA) provided by CA.

Now, MN will first generate a TA and Pu-Pr pair Pu(N1,N1) and Pr(N1,N1). Then it will generate DS [N 1, AS 1, Pr(N 1, N 1)] and send it to AS1 with the request to provide it a Token. AS1 attached to MN, after verification of MN, will generate and provide a Token containing same TA to MN.

Correspondent Node (CN) will send its request to MN with its Token issued by it's AS. Firstly, MN will verify the CN's IP address by decrypting Token using CN's public key issued by AS and then it will verify digital signature DS issued by Manufacturing company, using public key issued to CN's interface card by RA. If it is not malicious node, MN will send its Token along with Synchronous key, encrypted using Public key of CN, to be used in further communication. After agreeing upon Synchronous key, CN will send same key, encrypted with public key of MN, to MN. Now, if MN changes its location, then MN will send its Care-of-Address to HA and to CN securely. As both, CN and HA had verified the MN and having separate shared keys, thus, MN does not have to go through return routability procedure.

XIV. ANALYSIS USING CPN TOOL :

For the purpose of analysis of Token based and standard MIPv6 CPN Tool is used. CPN Tools is a special simulation system which uses the language of Petri nets for models' representation. The system was developed in University of Aarhus in Denmark. It is used as a simulation tool to show the effectiveness of token based system over MIPv6.

For Analysis purpose of simulation, same network and ideal conditions, using different protocol under CPN tool is used. The result generated from CPN Tool, to send a single message from MN to CN, only on single location change, is shown. Multi-sets used in CPN Tools, for standard MIPv6, for MN's place's marking used was 1`(1,"BU")@0+++1`(3,"HoTI)@0 +++1`(5,"CoTI")@ and the result after first message reached to MN from CN is 1`(2,"BA")@6+++1`(4,"HoT")@15+++ 1`(6,"CoT")18+++ 1`(7,"Message")@21+++ as shown in Fig 10.

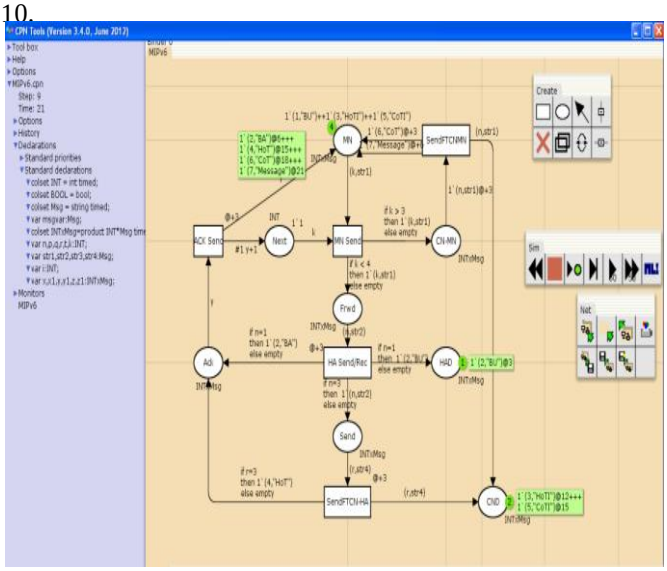

Fig 10. CPN Tool result for standard MIPv6

Multi-sets used in CPN Tools, for Token Based MIPv6, for MN's place's marking used was 1`(1,"Encrypted BU")@0+++1`(3,"Encrypted Care-of-Address")@0 and the result after first message reached to MN from CN is 1`(2," Encrypted BA")@6+++1`(4," Encrypted Message")@9 as shown in Fig.11.

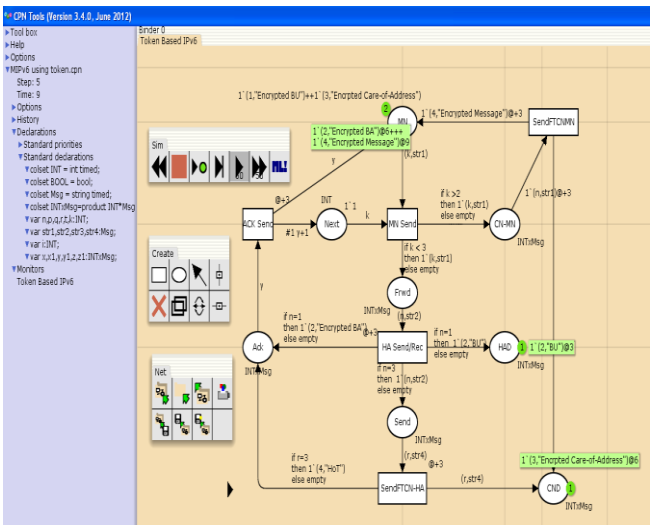

Fig 11. CPN Tool result for Token Based MIPv6

TABLE I
Result from CPN Tool

Message	**MIPv6**	**Token Based**
Initial Key setup Time	Less	High
BU To HA	Same	Same
BU To CN	High/Location Change (18 Time Unit)	Low/Location Change (6 Time Unit)
Simulation Time for 1st Message	21 Time Unit	9 Time Unit

XV. CONCLUSION

The mobility is becoming a necessity and the frequency of change of location of mobile node is going upward. Due which, it is very important to choose mobile management scheme such that the latency should be minimum and security should be very high. MIPv6 uses Return Routability Procedure to update the Care-of-Address, every time it changes, and set security key for secure communication, whereas, Token based scheme initially sets up the agreed key and if its Care-of-Address changes the same key can be used to authenticate the Mobile node.

The CPN tool is used on same network design with different protocol. The result shows that if Token based scheme is used the initial time to key setup will be high but the time required for Return Routability Procedure can be reduced drastically.

REFERENCES

[1] http://cpntools.org

[2] www.eweek.com/c/a/IT-Infrastructure/IPv4-Address-Depletion-Adds-Momentum-to-IPv6-Transition-875751/

[3] www.cisco.com/en/US/docs/ios/solutions_docs/mobile_ip/mobil_ip.html#wp1030412

[4] Tuomas Aura, "Mobile IPv6 Security", Microsoft Research ltd., Roger Needharn Building, 7 JJ Thomson Avenue, Cambridge, CB3 OFB, UK

[5] Shengling Wang, Yong Cui, Wei Li, and Jianping Wu Member, IEEE, Sajal K. Das, Senior Member, IEEE, *"Mobility in IPv6: Whether and How to Hierarchize the Network?"* IEEE Transactions on Parallel and Distributed Systems, Vol.22.

[6] Request For Comment – 5380 "Hierarchical Mobile IPv6 (HMIPv6) Mobility Management", H. Soliman, Elevate Technologies, C. Castelluccia INRIA; K. ElMalki Athonet; L. Bellier INRIA; October 2008

[7] H. Soliman, C. Castelluccia ,K. El Malki ,L. Bellier "Hierarchical Mobile IPv6 Mobility Management (HMIPv6)", RFC 4140: August 2005

[8] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[9] Carlos E. Caicedo , James B.D. Joshi and Summit R. Tuladhar; "IPv6 Security Challenges " Published by the IEEE Computer Society in Internet Computing ; Page 36 - 48 February 2009.

[10] S. Bradner and A. Mankin; Request for Comments: 1752; January 1995; "The Recommendation for the IP Next Generation Protocol"

[11] J. Arkko, J. Kempf , B. Zill and P. Nikander; March 2005; Request for Comments: 3971;"SEcure Neighbor Discovery (SEND)"

[12] T. Aura; Request for Comments: 3972; March 2005; Cryptographically Generated Addresses (CGA)

[13] Hinden, R. and S. Deering; Request for Comments: 3513; April 2003; "Internet Protocol Version 6 (IPv6) Addressing Architecture"

[14] Jonsson, J. and B. Kaliski; Request for Comments: 3447; February 2003; "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1"

[15] S. Thomson, T. Narten and T. Jinmei; Request for Comments: 4862; September 2007; "IPv6 Stateless Address Autoconfiguration"

[16] M N Doja, Ravish Saggar; "Token Based Stateless Auto-Configuration For IPv6"; International Journal of Wisdom Based Computing, Vol. 1 (3), December 2011

[17] Joseph Davies; Published By: Prentice Hall of India - 2008; "Understanding IPv6"; Second Edition; ISBN: 978-81-203-3463-2.

[18] Andrew S. Tanenbaum; "Computer Networks" ,Fourth Edition; Pearson Education -2006;ISBN 81-7758-165-1.

[19] Silvia Hagen; "IPv6 Essentials", Second Edition; O'Reilly Media – January 2007; ISBN 10 81-8404-281-7.

[20] D.A. Zaitsev, T.R. Shmeleva "Simulating of Telecommunication Systems with CPN Tools" Issue plan 2005/2006

