# A Secure Route Optimization Protocol in Mobile IPV6

**D.Kavitha**[1] **Dr.K.E.Sreenivasa Murthy**[2] **S.Zahoor ul Huq**[3]

*G.PullaReddy Engg. college G..Pullaiah College of Engg. & Technology G..Pulla Reddy Engg. college*
*Kurnool , Andhra Pradesh , India.*

**Summary**
Mobile IPV6 allows a mobile node to talk directly to its peers while retaining the ability to move around and change the currently used IP addresses. This mode of operation is called Route Optimization. In this method , the correspondent node learns a binding between the Mobile nodes permanent home address and its current temporary care-of-address. This introduces several security vulnerabilities to Mobile IP. Among them the most important one is the authentication and authorization of binding updates. This paper describes the Route optimization and the security threats created by the introduction of mobility. Based on an in-depth analysis of the security weaknesses existing in the previously proposed protocols, we suggest a high strength security protocol that provides more security than the route optimization.The protocol we suggested here decouples the internetworking layer from the higher layers by introducing a new addressing scheme. This is mainly done as the transport layer is coupled to the IP addresses which are used as locators and identifiers. This protocol makes use of a Diffie Hellman key exchange to provide mutual peer authentication

***Key words:***
*Authentication, Binding Update, Mobile IPV6, route optimization, Security*

## 1. Introduction

Mobile IPv6 is an IETF(Internet Engineering Task Force) standard communication protocol which allows nodes to remain reachable while moving around in the Internet. It is an IP-layer mobility protocol[1] for the IPv6 Internet. The design was based on the Mobile IP for IPv4.The mobile IPv4 protocol follows the design principles outlined first by Ioannidis[2].Mobility is implemented in the network layer in such a way that it is transparent to the higher layers , mobile hosts retain their IP addresses over location changes, and the non mobile hosts need not know about the mobility protocol. The main difference between Mobile IPv4 and Mobile IPv6 is that, in the latter, mobile hosts can perform mobility signaling directly with non mobile correspondents.

### I.1 Mobility Problem

Each mobile node is always identified by its home address, regardless of its current point of attachment. Each mobile node is associated with a home agent(HA)

and a home address (HoA). In mobile IPv6, a mobile node has two IP addresses:1)Home address is an address in the home network 2)a care-of-address is a temporary address in the visited network. The home address is constant but the care-of-address changes as the mobile node moves.

Mobile IP try to allow the transport layer sessions to continue even if the underlying hosts move and change their IP addresses. It also allows the mobile node to be reached through a static IP address, Home Address (HoA).

The rest of the paper is organized as follows. Section 2 describes the existing protocols in Mobile IPV6.In section 3 security vulnerabilities in the existing protocols are specified. Existing authentication methods for binding updates have been discussed in section 4.Our new security protocol for Mobile IPV6 is explained clearly in section 5.In section 6 performance analysis of the specified protocol is carried out based on an in depth study **.**

## 2. Existing Protocols in Mobile IPV6

### 2.1 Triangle Routing

In the basic Mobile IP protocol, IP packets destined to a mobile node that is outside its home network are routed through the home agent. However packets from the mobile node to the correspondent nodes are routed directly. This is known as triangle routing[3]. Figure 1 illustrates triangle routing.

This method is inefficient in many cases. Consider the case when the correspondent node and the mobile node are in the same network, but not in the home network of the mobile node. In this case the messages will experience unnecessary delay since they have to be first routed to the home agent that resides in the home network. One way to improve this is Route Optimization

Manuscript received March 18, 2009
Manuscript revised March 25, 2009

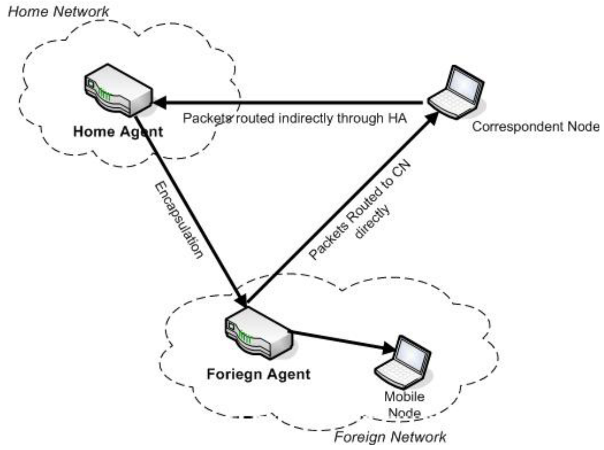


Fig 1: Triangle Routing

## 2.2 Route Optimization

Route Optimization[6] is an extension proposed to the basic Mobile IP protocol [4]. Here messages from the correspondent node are routed directly to the mobile node's care-of address without having to go through the home agent. Route Optimization provides four main operations. These are:

1. Updating binding caches,
2. Managing smooth handoffs between foreign agents,
3. Acquiring registration keys for smooth handoffs,
4. Using special tunnels.

**1. Updating binding caches:** Binding caches are maintained by correspondent nodes for associating the home address of a mobile node with its care-of address. A binding cache entry also has an associated lifetime after which the entry has to be deleted from the cache. If the correspondent node has no binding cache entry for a mobile node, it sends the message addressed to the mobile node's home address. When the home agent intercepts this message, it encapsulates it and sends it to the mobile node's care-of address. It then sends a Binding Update message to the correspondent node informing it of the current mobility binding.

**2. Managing smooth handoffs between foreign agents:** When a mobile node registers with a new foreign agent, the basic Mobile IP does not specify a method to inform the previous foreign agent. Thus the datagrams in flight which had already tunneled to the old care-of address of the mobile node are lost. This problem is solved in Route Optimization by introducing smooth handoffs. Smooth handoff provides a way to notify the previous foreign agent of the mobile node's new mobility binding.

If a foreign agent supports smooth handoffs, it indicates this in its Agent Advertisement message. When the mobile node moves to a new location, it requests the new foreign agent to inform its previous foreign agent about the new location as part of the registration procedure. The new foreign agent then constructs a Binding Update message and sends it to the previous foreign agent of the mobile node. Thus if the previous foreign agent receives packets from a correspondent node having an out-of-date binding, it forwards the packet to the mobile node's care-of address. It then sends a Binding Warning message to the mobile node's home agent. The home agent in turn sends a Binding Update message to the correspondent node. This notification also allows datagrams sent by correspondent nodes having out-of-date binding cache entries to be forwarded to the current care-of address. Finally this notification allows any resources consumed by the mobile node at the previous foreign agent to be released immediately, instead of waiting for the registration lifetime to expire.

**3. Acquiring registration keys for smooth handoffs:** For managing smooth handoffs, mobile nodes need to communicate with the previous foreign agent. This communication needs to be done securely as any careful foreign agent should require assurance that it is getting authentic handoff information and not arranging to forward in-flight datagrams to a bogus destination. For this purpose a registration key is established between a foreign agent and a mobile node during the registration process. The following methods for establishing registration keys have been proposed in the order of declining preference:

- If the home agent and the foreign agent share a security association, the home agent can choose the registration key.
- If the foreign agent has a public key, it can again use the home agent to supply the registration key.
- If the mobile node includes its public key in its Registration Request, the foreign agent can choose the new registration key.
- The mobile node and its foreign agent can execute the Diffie-Hellman key exchange protocol as part of the registration protocol.

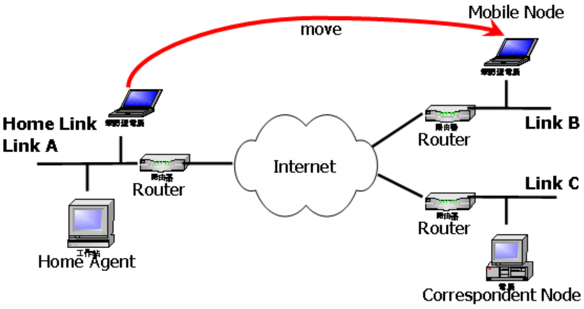
This registration key is used to form a security association between the mobile node and the foreign agent.

**4. Using special tunnels:** When a foreign agent receives a tunneled datagram for which it has no visitor list entry, it concludes that the node sending the tunneled datagram has an out-of-date binding cache entry for the mobile node. If the foreign agent has a binding cache entry for the mobile node, it should re-tunnel the datagram to the care-of address indicated in its binding cache entry. On the other hand, when a foreign agent receives a datagram for a mobile node for which it has no visitor list or binding cache entry, it constructs a special tunnel datagram. The special tunnel datagram is constructed by encapsulating the datagram and making the outer destination address equal to the inner destination address. This allows the home agent to see the address of the node that tunneled the datagram and prevent sending it to the same node. This avoids a possible routing loop that might have occured if the foreign agent crashed and lost its state information.

## 3. Vulnerabilities in Mobile IPV6

### 3.1 Home Address Option

When the Home Address Option (HAO) is used, the attacker can use it when he attacks by Denial of Service. HAO provides the method to hide the attacker's current location. An attacker chooses a victim and another addressable IPv6 nodes or node reflectors. He configures IPv6 packet header's source address and the destination address as his original address and reflector address, respectively. And then, in HAO, he puts victim's address, and sends the packet. The receiver, reflector, processes the packets and gets to know the packet has HAO, so he exchanges the source address with HAO. The reflector thinks the packet he has received is sent from victim, so he sends the packet to the victim. The victim receives the packet whose source address is reflector's, and he doesn't know the attacker's address, the original sender. Therefore, the reflector receives useless packets, and these packets consume the network resources. These packets can disturb the reflector in communication.

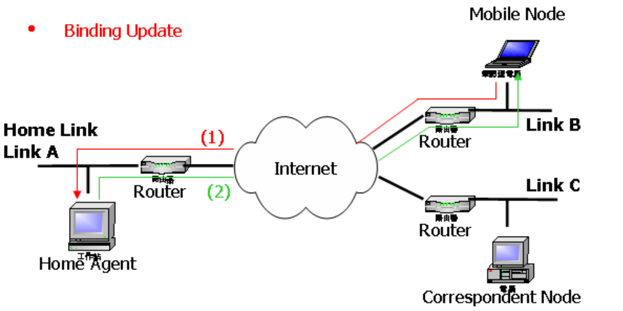


To solve this problem, IPsec[8] is used. When a correspondent node receives a packet with Home address option, it process that option only if there exist a binding information of IPsec SA (Security Association).

### 3.2. Routing Header

When send packets to the mobile node, a routing header is used to support the transparent communication for the upper layers. Also, the routing header is used for source routing, it is possible to choose ISP dynamically in traffic engineering or multi-homing environment. However, the type 0 routing header, which is defined in Mobile IPv6, has a problem: the routing header can be processed in both of hosts and router, and it can contain several addresses, so it can be used by reflection attack.

To solve this problem, it is recommended to use new type of Destination option, new extended header or routing header instead of using the ordinary routing header.



### 3.3 Binding Updates

When a mobile node sends a binding update message, an attacker can obtain the information about the mobile node's current location, and send a packet which has different address with the mobile node to the mobile node's home agent. Once a home agent receives the packet, the mobile node cannot receive the packets from its home agent.

The mobile node also uses the binding update to attack a host. It can send binding update message to its correspondent nodes with the false Care-of Address (victim's address). Once the correspondent nodes receive this packet, it sends packets to the false Care-of Address, not to the mobile node [9]. A mobile node can send a lot of binding update messages at once. The correspondent node receives the meaningless packets, and before it recognizes that the messages are invalid, it may consume its resources and cannot process the meaningful packets.

An attacker may replay the old binding update message. This replay attack leads the packets to the former location of mobile node, so the mobile node cannot receive its packets.

To protect these attacks, a mobile node uses IPsec ESP (Encapsulation Security Payload) when it sends binding update message to its home agent. When a mobile node sends binding update message to its correspondent node, it may uses RR(Return Routability) to check if the home address and the Care-of address are reachable.

## 4. Existing authentication methods and infrastructures

Various methods for protecting "binding information" from being exposed to attackers are suggested.

### 4.1 IKE (Internet Key Exchange)

The IKE (Internet Key Exchange) is a Key Distribution mechanism for Internet community. This is the common way to exchange keys in the conventional Internet, but it proved that this way is lack of extensibility and flexibility in mobile network. Basically, IKE provides strong security facilities, but in many case, the mobile nodes are portable, hand-held small terminals. It could be very hard for such devices that all incoming and outgoing packets are required to be processed with the cryptographic engine, which is very complex and power-consuming operation.

### 4.2 RR (Return Routability)

RR is a key distribution mechanism which is simplified the key distribution procedure, without depending on the existing infrastructure. In RR, a mobile node just requests the key distribution process. All the rest processes are in charge of correspondent node. It must create the keys and the keying materials, and distribute them. It is very simple and convenient for the mobile node, but it could lead the 'binding down' attack. Suppose an attacker is eavesdropping the security negotiation packets between mobile node and the correspondent node. All the procedures could be done by forging the negotiation packets as weak security level. And then, the peers (mobile node and correspondent node) agree to have weak security level, even though they can have more security.

### 4.3 Radius

RADIUS stands for Remote Authentication Dial-In User Service. Its purpose is to supply information and authentication for multiple dial-in servers. RADIUS works very well in the wired network. However, it is not suitable for the mobile network for the following reasons: it has too many messages to complete the authentication, and the number of Attribute-Value Pairs(AVPs), which define the authentication and authorization characteristics for their respective users and groups, is limited(the total item is 255).

### 4.4 Diameter

If binding information is embedded when the shared key between the mobile node and Attendant is not yet generated and the authentication is not completed, it is very easy for an attacker to obtain the current location of mobile node and the information about home network .

### 4.5 IPsec

IPsec is a protocol to provide a confidentiality and authentication service for IP level. The security services provided by IPsec are access control, confidentiality, connectionless integrity, anti-reply service, date origin authentication, and the limited flow confidentiality.

To overcome the security problem caused by the mobility between the home agent and the mobile node. IPsec is used. IPsec can authenticate the messages based on the SA's which is established between the home domain and the mobile node.

If the security mechanism about control traffic between a mobile node and home agent is not applied, these nodes are exposed easily to the Man-in-the-Middle attack, hijacking, confidentiality, impersonation, and the DoS attack. To protect these attacks and secure the control traffics, IPsec is used. These control traffics consist of various messages:

Binding update and reply message between mobile node and the home agent.

- RR messages from the home agent to the correspondent node.
- ICMPv6 message, to discovery prefix

Each node can also protect their payload traffics which are sent by home agent.

## 5. Secure Route Optimization Protocol

It is an end to end authentication and key establishment protocol. Each node in the network is assigned a tag value which is a unique bit pattern representing the public key. But this is not used for communication because of its varying size. A node can have more than one tag value. These tag values can be either public or unpublished. The public tag values are stored to DNS.

Each tag value is associated with an address, which is a 128 bit cryptographical hash of tag value. It is computationally hard to find a node that produces matching address. So address collision is very low.

Localized address is a 32-bit localized representation of the tag value. Localized address values are selected randomly by each node. Collisions may easily occur but can be neglected as it is used in the local scope. Localized addresses can be used as an address in the FTP command or in the socket call. Purpose of localized address is to facilitate the use of tag values in the existing protocols like ipv4 and API's.

It introduces a new namespace to overcome the drawbacks of the current IP address namespace and Domain Name namespace. Address assigned to a host that is calculated from the tag value separates the identity of the host from the location information that the IPaddress carries. This new namespace fills the gap between the IPaddresses and the DNS names by separating the IP addresses from the upper layer bindings.

It is a protocol for discovering and authenticating the bindings between public keys and IP addresses. Above layers are based on tag values but not on IP addresses. Binding of tag values to IP addresses is done dynamically.

SROP makes mobility transparent to the applications. Its main purpose is to provide authentication during the connection establishment and also to provide security association.

This protocol is used to authenticate the connection. It also establishes security associations for a secure connection with ESP by developing a SROP initial exchange.

## 5.1 SROP Initial Exchange

The initiator initiates the initial exchange by sending the packet I1.This packet contains the address of the initiator and the address of the responder is optional.

The second packet R1 sent by the responder starts the actual exchange. It contains cryptographic challenge that has to be answered by the initiator to start the exchange. It also consists of initial Diffie Hellman parameters and a signature.

Then initiator sends the packet I2 answering the question given by the responder. It also consists of the needed Diffie Hellman parameters and the signature. Then responder completes the exchange by signing the packet R2.The purpose of question in packet R1 is to protect the responder from DoS attacks. It does not protect from an attacker if he uses fixed addresses. The first 3 packets implement a standard Diffie Hellman exchange. The responder sends public DH key and its public authentication key i.e tag value of responder. Data packets start to flow after the packet R2.

## 5.2 End node Mobility

The actual payload traffic is protected with ESP and hence the ESP SPI acts as an index to the right host-to-host context.

When a node moves to another address , it notifies its peer of the new address by sending an SROP UPDATE packet containing a LOCATOR parameter. This packet is acknowledged by the peer. To ensure reliability UPDATE packet is sent again. the peer can authenticate the contents of the UPDATE packet based on the signature and keyed hash of the packet. The peer is not able to send the packets to these new addresses before it can reliably and securely update the set of addresses that they associate with the sending host. Also, mobility may change the path characteristics in such a way that reordering occurs and packets fall outside the ESP anti replay window for the security association,that requires rekeying.

Assume that the two nodes have completed a single SROP initial exchange with each other. Both of these have one incoming and one outgoing SA. Each SA uses the same pair of IP addresses , which are the ones used in the initial exchange.

The readdressing protocol is an asymmetric protocol where a mobile node informs a peer node about changes of IP addresses on affected SPIs. The readdressing exchange is designed to be piggybacked on existing SROP exchanges.

Consider a scenario between a mobile node and a peer node with out using any keys. Sometimes a mobile node can change its IP address that is bound to an interface. This can be due to a change in the advertised IPV6 prefixeson the link,a reconnected PPP link, a new DHCP lease or an actual movement to another subnet. To maintain the connection mobile node must inform its new IP address to its peer. This scenario assumes a single pair of SA's without any rekeying on the SAs. It is depicted in the figure as follows:

```
MOBILE NODE                PEER NODE

      UPDATE(ESP_INFO,LOCATOR,SEQ_NO)
      -------------------------------------->

    UPDATE(ESP_INFO,SEQ,ACK,ECHO-REQUEST)
      <--------------------------------------

          UPDATE(ACK,ECHO_RESPONSE)
       -------------------------------------->
```

Fig 5: Readdress with out rekeying

1.The mobile node is disconnected from its peer for a brief period of time while it switches from one IP address to another. Upon obtaining a new IP address, the mobile node sends a LOCATOR parameter to the peer host in an UPDATE message. This message also contains an ESP_INFO parameter Which contain the values of the old and new SPIs for a security association. In this case, the OLD SPI and NEW SPI parameters both are set to the value of the preexisting incoming SPI. ESP_INFO is included for possible parameter-inspecting middle boxes on the path. The LOCATOR parameter contains the new IP address and a locator lifetime. The mobile host waits for this UPDATE to be acknowledged, and retransmits if necessary.

2. The peer node receives the UPDATE, validates it, and updates any local bindings between the HIP association and the mobile host's destination address. The peer node performs an address verification by placing a nonce in the ECHO_REQUEST parameter of the UPDATE message sent back to the mobile node. It also includes an ESP_INFO parameter with the same contents as in step 1.It then sends this UPDATE with piggybacked acknowledgment to the mobile host at its new address. The peer uses the new address immediately, but it limits the amount of data it sends to the address until address verification completes.

3. The mobile node completes the readdress by processing the UPDATE ACK and echoing the nonce in an ECHO_RESPONSE. Once the peer node receives this ECHO_RESPONSE, it considers the new address to be verified and can put the address into full use. While the peer host is verifying the new address, the new address is marked as UNVERIFIED , and the old address is DEPRECATED. Once the peer host has received a correct reply to its UPDATE challenge, it marks the new address as ACTIVE and removes the old address. Next , consider a scenario between the mobile node and its peer which uses mobile initiated rekeying. The mobile host rekey the SAs at the same time that it notifies the peer of the new address. In this case, the above procedure described in Figure 3 is slightly modified. The UPDATE message sent from the mobile node includes an ESP_INFO with the OLD SPI set to the previous SPI, the NEW SPI set to the desired new SPI value for the incoming SA, and the KEYMAT Index desired. The host may also include a DIFFIE_HELLMAN parameter for a new Diffie- Hellman key. The peer completes the request for a rekey as is normally done for HIP rekeying, except that the new address is kept as UNVERIFIED until the UPDATE nonce challenge is received as described above. Figure 4 illustrates this scenario.

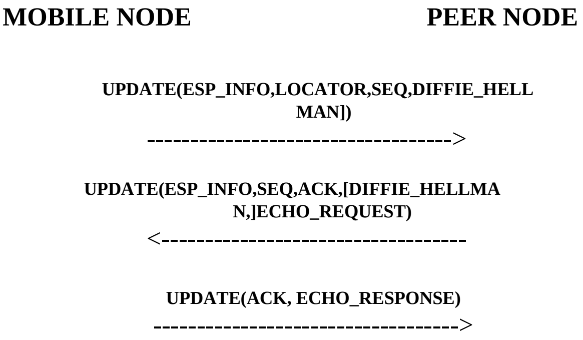


Fig 6: Readdress with Mobile-Initiated Rekey

## 6. Security and performance analysis of SROP

The performance of SROP can be assessed on theRound Trip Time (RTT) and Binding Cost (BC). RTT is defined as the elapsed time for transmitting data over a closed path. Let $RTT_{A,B}$ represent the RTT between Aand B. In Mobile IPv6, a handover requires a RR process and a SROP update, it takes $\max\{(RTT_{MN,HA}+RTT_{HA,CN}),RTT_{MN,CN}\}+ RTT_{MN,CN}$ to complete the process(Figure 5). It takes only 1.5 $RTT_{MN,CN}$ in SROP (Figure 6). The improvement is obvious.

BC is defined as the cost of handover handling which includes the SROP update packet transmission and the binding computation conducted in the nodes. Before we go to detailed discussion, some notions are defined in the following. Let

- BCx be the total binding cost for scheme X,
- PBCy be the binding cost incurred in process Y,
- CPi,A be the processing cost for process i at node A,
- CTi,A,B be the binding packet transmission cost in process i between node A and B.

The BC of Mobile IP is the sum of the cost of RR process and the cost of SROP Update. In the RR process, there are 4 different sub-processes, HoTI, CoTI, HoT and CoT. We can group HoTI and HoT into one combined sub-process (HT) and CoTI and CoT into another one (CT). MN sends a HoTI via HA to CN. CN will generate a home nonce after it receives it and send it back to MN via HA. MN will wait for the care-of nonce in CoT to create the SROP Update packet, so

$$PBC_{HT} = CT_{HoTI,HA,MN} + CP_{HoTI,HA} + CT_{HoTI,HA,CN} + CP_{HoTI,CN} + CT_{HoT,HA,CN} + \quad (1)$$

As the process HA only forwards the packets to MN and CN, so $CP_{HoTI,HA}$ is equal to $CP_{HoT,HA}$.

Similarly, the transmission cost of HoTI and HoT packets are almost equal, so the formula can be simplified as following:

$$PBC_{HT} = 2(CT_{HT,HA,MN} + CT_{HT,HA,CN}) + 2CP_{HT,HA} + CP_{HoTI,CN} \quad (2)$$

At the same time HoTI is sent out, MN sends a CoTI to CN directly. When CN receives the CoTI, it will generate a care-of nonce and sends it back to MN directly. After MN receives both HoT and CoT, it will use the home nonce and care-of nonce to create the Binding Update packet.

$$PBC_{CT} = CT_{CoTI,MN,CN} + CP_{CoTI,CN} + CT_{CoT,MN,CN} \quad (3)$$

Similar to HT process, the cost of CoTI and CoT packet transmission between MN and CN are close.
Therefore, the cost of CT can be simplified as following:

$$PBC_{CT} = 2CT_{CT,\ MN,CN} + CP_{\ CoTI\ ,CN} \quad (4)$$

The total cost of RR can be summarized as the sum of BCHT and BCCT. The cost of generation of home nonce and care-of nonce in CN are similar, so the total cost of RR is

$$PBC_{RR} = 2(CT_{HT,HA,MN} + CT_{HT,HA,CN} + CT_{CT,MH,CN}) + 2(CP_{HT,HA} + CP_{RR,CN}) \quad (5)$$

The cost of Binding Update process is the cost of generation of the Binding Update packet by home nonce and care-of nonce in MN. MS sends it to CN. CN checks the validation of the packet and replies MN.

$$PBC_{BU} = 2CT_{BU,MN,CN} + CP_{BU,MN} + CP_{BU,CN} \quad (6)$$

The cost of packet transmission between MN and CN are similar in both processes, so the BC of Mobile IPv6 handover process is the sum of PBCRR and PBCBU, that is:

$$BC_{MIP} = 2(CT_{MIP,HA,MN} + CT_{MIP,HA,CN}) + 4CT_{MIP,MH,CN} + 2(CP_{MIP,HA} + CP_{RR,CN}) + CP_{BU,CN} + CP_{MIP,MN} \quad (7)$$

The BC of SROP is less complex than Mobile IP. MN sends the Update Package with Locator parameter to the CN, CN replies MN and requests ACK for the address checking. MN replies an ACK to CN. As all processes are based on SA, so each node only processes the packet and replies with correct parameters. The BC of SROP is given below:

$$BC_{SROP} = 2CP_{SROP,CN} + CP_{SROP,MN} + 3CT_{SROP,MN,CN} \quad (8)$$

As shown in the equations (1) ~ (8), SROP requires less BC than Mobile IP. Furthermore, in the circumstance of frequent handover, the overhead of processing in nodes in Mobile IP will be even higher than that in SROP. In RR, to defend the messages from eavesdropping attack and time shifting attack, the key and state have a short life time. Binding update for a MN's frequent IP address changing has heavy processing cost. SROP relies on Sas and nodes do not need to do any extra computation when a MN is moving from one sub network to another until it requires the Readdress with re-keying in the SA. It is obvious that SROP requires less processing in binding update.

SROP is independent of HA/RVS. In Mobile IP RR, HoT and HoTI are processed via HA, that will slow the handover progress. The independence of HA/RVS in SROP leads to its shorter handover delay and lower binding cost.

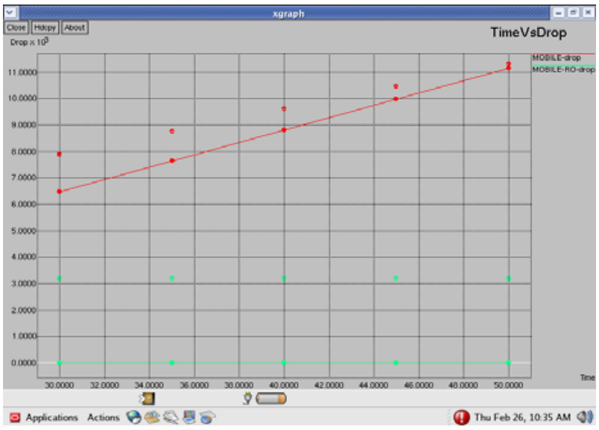
SROP's has stronger security as the connection between a MN and the CN is protected by ESP. In Mobile IP RR, a connection is protected by ESP only in HoT from HA to MN.

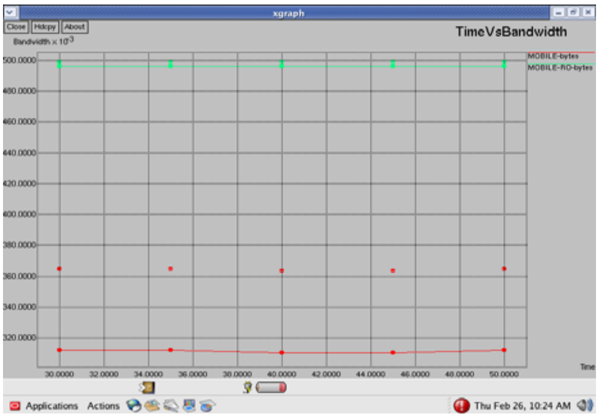
Another new feature of SROP is its support for multi homing., which is lacked in the current Mobile IP. By using the Update packet, the MN can notify the CN with more than one interface.

We have implemented SROP protocol and the results are generated as follows.

Following is a graph which shows Time Vs Drop in packets. Red and green line shows the results of basic Route Optimization protocol and Secure Route optimization protocol respectively.

Next graph results corresponds to Time Vs Bandwidth.





## 7. Conclusion

In this paper, we have discussed the mobility management in Mobile IP and the vulnerabilities in it. A new mobility management scheme SROP has been proposed. Our discussion and analysis have shown that the security and efficiency are improved in SROP when compared to Route Optimization in Mobile IPv6. In SROP, with out modifying the upper layer protocol it can still offer excellent features in mobility management by adopting the improved binding update process and the strengthened security. Its impact on the interconnection between IPv6 and IPv4 also needs to be further studied. Overall, SROP can be considered as an initial step in the migration from Mobile-IP-based networks to public-key based future networks.

## References

[1] David B Johnson ,Charles Perkins and Jari Arkko , Mobility support in IPv6,RFC 3775,IETF June 2004.

[2] John Ioannidis, Dan Duchamp and Gerald Q. Maguire. (1991). IP-based Protocols for Mobile Internetworking. , , 235-245.

[3] "Triangle routing in Mobile IP" Sohaib Mahmood

[4] "Mobile IP" Perkins, C.E.Communications Magazine, IEEE Volume 35, Issue 5, May 1997 Page(s):84 – 99

[5]Johnson,D. and Perkins,C. *Internet Draft - Mobility Support in IPv6*. http://www.ietf.org/internet-drafts/draft-ietf-mobileip-ipv6-12.txt. March

[6] Perkins,C. and Johnson,D. *Internet Draft - Route Optimization in Mobile IP*. http://www.ietf.org/internet-drafts/draft-ietf-mobileip-optim-09.txt. February 2000,

[7] **"**Mobile IPv6 Security" Tuomas Aura

[8] "Security Architecture for the Internet Protocol" S.Kent , R.Atkinson RFC 2401

[9] "Mobility Support in IPv6", Dave Johnson, Charles Perkins, Jari Arkko, 05-Jul-02.

[10] "Performance evaluation of Route Optimization Scheme in Mobile IPV6" In-Hye Shin , Gyung-Leen Park , Junghoon Lee, Jun Hwang , T.Jeong. Springer Berlin / Heidelberg Volume 4490/2007 Pages 586-589

[11] Dilip Antony Joseph , "Mobility Support n IPV6"

[12] Tuomas Aura , Michael Roe "Designing the Mobile IPV6 security protocol" Annuals of Tele Communications Vol. 61 March – April 2006

[13] Claude Castelluccia , Francis Dupont , Gabriel Montenegro "A Simple Privacy Extension for Mobile IPV6"

**D.Kavitha** obatained her B.Tech degree from Sri Krishna Devaraya University, Anantapur and M.Tech degree from Jawaharlal Nehru Technological University, Anantapur in the year 2001 and 2005 respectively. She is currently pursuing Ph.D from Sri Krishna Devaraya University, Anantapur, India. She is presently working as Associate Professor in the Department of Computer Science and Engineering at G. Pulla Reddy Engineering College, Kurnool, Andhra Pradesh, India. She has presented four research papers in national conferences so far Her research areas include Computer Networks and Network Security

.. **Dr. K.E. Sreenivasa Murthy** obtained B.Tech and M.Tech degrees in Electronics and Communication Engineering from Sri Venkateswara University, Tirupati, India in 1989 and 1992 respectively and Ph.D degree from Sri Krishna Devaraya University, Anantapur, India, in 1997. He presented more than 10 research papers in various national and international conferences and journals.He is at present working as principal at G. Pullaiah College of Engineering and Technology, Kurnool, India. His research interests include FPGA and DSP applications.

**S. Zahoor Ul Huq** obatained his M.E. degree from Anna University, Chennai he is currently pursuing his Ph.D from Sri Krishna Devaraya University, Anantapur, India. He is presently working as Associate Professor in the Department of Computer Science and Engineering at G. Pulla Reddy Engineering College, Kurnool, Andhra Pradesh, India. He has presented four research papers in national conferences so far. His research areas include Computer Networks and Databases and Object Oriented Programming.