CHAPTER 2

LITERATURE SURVEY

2.1 NEMO PROTOCOL OPERATION

The goal of MIPv6 protocol is to maintain the transparent mobility of the nodes in the subnetwork which is moving together, for example, a car that is traveling with four nodes (laptop, PDA, cell phone and a Bluetooth device) with a small subnetwork in it. The host mobility support must be enabled to the network so that the independent management of mobility can be accomplished. Host mobility support may not be possible to all the nodes in the network. A few nodes like wireless sensor and embedded devices might be having extremely limited capacity and it may not be possible to update the software to manage their mobility. A single device can be proposed to manage the mobility in such situations called as Mobile Router (Ernst and Lach 2007b). An MR duty is to maintain the transparent mobility support for the complete network. In such cases, other nodes in the network need not have any additional software for mobility support. An advantage of mobility support management by MR is that when the network starts roaming, signal exchanges for mobility support can be limited to only one device. The nodes or MR of the mobile network must be capable of attaching with any available access technology to connect with Internet. The MR may have UMTS (Universal Mobile Telecommunications Service), WiMAX (Worldwide Interoperability for Microwave Access) interfaces or any other related technology interfaces in order to connect with Internet. We cannot expect this facility to be available in all the devices in the network. If the MR has such
facility, then the network can maintain the connectivity through MR. This reduces the cost required to maintain the mobility support. A mobile network is shown in Figure 2.1.

![Figure 2.1 Mobile Network](image)

**Figure 2.1 Mobile Network**

NEMO is a protocol developed by IETF for managing the mobility when the network is on the move. Ernst (2007a) states that NEMO protocol will maintain the mobility support of the entire network, when the mobile network changes its attachment point through MR. The goal of mobile network is to maintain the seamless connectivity with its private network called as home network directly or through Internet. The mobile network can be single homed or multi homed, with a single MR or multiple MRs to maintain connectivity with Internet (Ernst 2004). In NEMO, the MR is the only device which is aware of the movement of the network; hence the network is movement transparent to the nodes in the network. Wakikawa et al. (2007) observed that each mobile network will have its HN where it resides, when it is not on the move.

In the home network, there will be a representative for the mobile network called as Home Agent (HA). HA is the only contact node for any communication to the nodes in the mobile network. When the mobile network (subnetwork) is moved out of its home, it maintains connectivity through the
foreign network called as Visited Network (VN) or Foreign Network (FN). Access Router (AR) is the node which provides connectivity to the mobile network. The connectivity between MR and AR accomplishes the mobility support. Qing et al. (2009) observe that, the external node that could maintain data session between any nodes in the mobile network is called as Correspondent Node (CN). A bi-directional tunnel between MR and HA is implemented by encapsulating the data. This will ensure the security of the data and preserve the continuity of the session when the network is on the move through private networks. Figure 2.2 shows a simple mobile network.

![Figure 2.2 Mobile Network](image)

When the mobile network visits a new network, it will obtain a new address called Care of Address (CoA). The CoA is the private address allocated by a visited network; hence it is NATed accordingly. This address identifies the current point of attachment of the mobile network. Hence the CoA must be updated to the HA. The process of updating the CoA to the HA is called as Binding Update (BU), which has been discussed by Hesham (2004). After acquiring the CoA from the visited network, it will send a BU to the HA through the AR. HA will send a Binding Acknowledgement (BA) after updating its current
point of contact. Thus, further communications with the mobile network through MR is going to be with the new CoA. This sequence of steps must be repeated whenever the MR changes the point of attachment by visiting a network. When the mobile node tries to join with a network, the network DMZ (Demilitarized Zone) may block the MN. In such scenarios, MN will search for a new network. Figure 2.3 illustrates a simple mobile network while on the move.

![Figure 2.3 Mobile Network](image)

The MN address is configured with the part of HN address block, as it is the subnetwork. This address is called as a topological perfect address (Gundavelli et al. (2009)). This common address block is known as Mobile Network Prefix (MNP). When CN sends a packet to any of the node in mobile network, it sends the predefined address of Mobile Network Node (MNN) with this MNP. This data will be forwarded to HA as its maintaining the CoA of the mobile network and HA will forward the packet to MR. This data transfer is tunneled by encapsulating the packet to ensure the security because it is going to pass through public and a few private networks. When the MR receives the packet it decapsulates the data and delivers to the destination MNN. Figure 2.4 shows a simple data exchange scenario between CN and MNN.
When there is a data exchange between the CN and the MNN, the following steps occur,

1. The CN sends an IP datagram for MNN with the MNP combined IPv6 address of MNN.

2. The IP datagram will be forwarded to the HN of MNN and the respective datagram will be acquired by the HA.

3. HA will encapsulate the respective datagram, and it will change the source as its address and destination as the CoA of the MR because MR is the only point of contact to MNN.

4. HA will forward the encapsulated data to CoA through the Internet. This datagram will reach MR through the AR of the visited network. With this encapsulated data a tunnel between HA and MR is established.

5. When the datagram is delivered to the MR it decapsulates the datagram and identifies the source and destination.
6. Then it will forward the original datagram to the MNN.

7. When an MNN sends a reply to the CN the operation is similar. The tunnel will be established from MR to HA.

The key points which leads to data encapsulation are,

1. To ensure the security as the data travels through Internet and a private network.

2. To avoid the problem while Ingress filtering, the router in the visited network will expect a topological perfect address in order to deliver the data to MR. Topological perfect address confirms that the MR is in visited network with CoA. It is impossible to deliver the datagram if we add the original destination. Hence the CoA must be updated as a destination address after encapsulating the datagram.

A sample encapsulation is shown in Figure 2.5, when data transfer is between CN and MNN.

![Encapsulation Diagram](image-url)
2.1.1 NEMO Node Types

There are three types of nodes as part of MN. They are Local Fixed Node (LFN), Local Mobile Node (LMN), and Visiting Mobile Node (VMN), as per the literature by KunChan et al. (2005). LFN is a fixed node in the mobile network. This node is not capable of moving hence it will not have mobility based software. LMN is a mobile node which works based on MIPv6. It can roam between MN, HN and some other foreign networks. A VMN is a mobile node based on MIPv6; it can also change the point of attachment. When a node visits a network then it is called as VMN. LMN and VMN are capable of maintaining mobility, when it is on the move.

The NEMO protocol is an extension of MIPv6 host mobility support protocol. MIPv6 follows three mechanisms to support the mobility of a node. They are Movement Detection, Location Registration and Traffic Tunneling. NEMO extends some of these mechanisms in order to provide the mobility support for the subnetwork.

2.1.1.1 Movement Detection

MIPv6 supports the host mobility with proper signaling flows and operations to discover the movement of the host. Router Advertisement (RA) message helps in finding the current attachment of the mobile host. RA can be volunteer message or a response from the AR to Router Solicitation (RS) message by the mobility host. In NEMO MR is responsible for mobility management for the mobile network. There is no change in movement detection mechanism in NEMO when compared to the MIPv6 protocol.
2.1.1.2 Location Registration

When the mobile host joins a new network it has to obtain a new address called as CoA through the AR. Once CoA is assigned, the mobile host will send a Binding Update (BU) with a new CoA to HA in order to maintain the connectivity. A Binding Acknowledgement (BA) will be a reply from HA to ensure the connectivity between the mobile host and HA. This role remains the same for the mobile router in NEMO and the following extensions are added in the binding update message as additional information.

1. Mobile Router Flag (R): This flag is used to identify whether the mobile node’s current role is a mobile router or not. If the flag is set, it will mean that the node is the Mobile Router for the concerned network. Hence the datagram for any node in the network can be forwarded to the MR. If the flag is unset it means that the node is not the MR. It is an individual mobile host so the respective datagram to the mobile host is forwarded from HA. This flag identifies the difference between the MR of the subnetwork and the individual host of the mobile network.

2. Mobile Network Prefix Option: This option updates the prefix information of the mobile network to the HA. Multiple MNP option is also possible if the MR maintains more than one IPv6 prefix in the mobile network.

2.1.1.3 Traffic Tunneling

After successful steps of movement detection and location registration in MIPv6, the HA and mobile node will go for an exchange of pending and current data. In NEMO, the same flow happens to the mobile network with the help of
MNP managed by MR. HA must be aware of the MNP list of the nodes in the mobile network in order to forward the datagram to the respective MNN. HA follows three mechanisms to identify the MNP in the mobile network under MR control, namely Explicit Mode, Implicit Mode, Intra Domain Dynamic Protocol.

1. Explicit Mode: An MR will explicitly update the MNP of the mobile network by including one or more MNP in the binding update.

2. Implicit Mode: The MR does not include MNP in the binding update; instead the HA must follow some other mechanism to determine the list of MNPs under MN control.

3. Intra Domain Dynamic Protocol: The MR and HA can run an intra domain dynamic protocol such as RIPng (Routing Information Protocol next generation) and OSPF (Open Shortest Path First Protocol) through the bidirectional tunnel to identify the list of MNPs.

When the traffic is from CN to MNN, the packets may be fragmented in HA as it is encapsulated between MR and HA. The MR is responsible for reassembling the fragmented packets and vice versa if the traffic is from MNN to CN.

2.1.2 Nested NEMO Operation

Mobile networks can also be nested. A mobile network is called as nested when it joins with another mobile network in order to maintain connectivity with its HN. For example when a user moves through a vehicle and joins his personal network with the mobile network in the vehicle then it is called as Nested NEMO. The mobile network 1 is the base network of vehicle. It will maintain
connectivity with the Internet and its HN, through the fixed infrastructure and foreign networks when it is on the move. The personal network (mobile network2) of the user who is traveling in the vehicle can maintain connectivity with its HN through the mobile network1. Figure 2.6 shows the Nested NEMO.

![Figure 2.6 Nested NEMO](image)

When CN sends a datagram to MNN of Mobile Network2 the following steps will occur,

1. The CN will create a datagram with the destination address of MNN in mobile network2 and send it.

2. As per the NEMO flow, the datagram will be captured by HA2 in home network2 which is representative for mobile network 2.

3. Mobile Network2 maintains connectivity with its home network through the mobile network1; hence the next hop for the datagram is HA1 in the home network1.

4. HA2 encapsulates the datagram and updates the source address as HA2 and destination address as HA1. This creates the first level of tunnel.
5. When the encapsulated datagram is delivered to HA1, it will again encapsulate the data and change the source address as HA1 and destination address as CoA of MR1. This creates the second level tunnel. The data size is increased as it is tunneled twice.

6. When the datagram is delivered to MR1, it decapsulates the packet and finds that the first level source is HA2 and destination is MR2. So it forwards the packet to MR2, which maintains connectivity with mobile network1.

7. The packet is delivered to MR2 and then it decapsulate the packet. It finds that the source is CN, and the destination is MNN.

8. When MNN replies to CN, the first level tunnel is established between MR2 and HA2. The second level tunnel is established between MR1 and HA1.

In nested NEMO, the packet size will increase based on the level of nesting. This leads the packet delay, additional overhead and some other issues as well.

2.1.3 Demerits of NEMO Protocol

2.1.3.1 Sub-Optimality with NEMO Basic Support

In NEMO basic support, all packets sent between an MNN and CN are forwarded through the MRHA tunnel. This results in a pinball route between the two nodes. The basic issues in NEMO protocol are shown in Figure 2.7.
Figure 2.7 Sub-Optimality with NEMO Protocol

Longer Route Leading to Increased Delay and Additional Infrastructure Load: As the packets must transit from a mobile network to the HA then to the CN, the transit time of the packet is usually longer than if the packet are to go straight from the mobile network to the CN. Some times the CN may be very near to the MN. However, when the mobile network and the CN are relatively near to each other, but far away from the HA on the Internet it creates a longer route. This longer route to reach the destination through HA will increase the delay. Applications such as real-time multimedia streaming may not be able to tolerate such increase in packet delay. In general, the increase in delay may also impact the performance of transport protocols such as TCP since the sending rate of TCP is determined by the Round Trip Time (RTT) perceived by the communication peers. Moreover, by using a longer route, the total resource utilization for the traffic would be much higher than if the packets are to follow a direct path between the MNN and CN. This would result in additional load in the infrastructure.
**Increased Packet Overhead:** The packet size of an outer header is increased due to the encapsulation of packets in the MRHA tunnel. This reduces the bandwidth efficiency as an IPv6 header can be quite substantial relative to the payload for applications such as voice samples. For instance, given a voice application using an 8 kbps algorithm (e.g., G.729) and taking a voice sample every 20 ms the packet transmission rate will be 50 packets per second. The voice packets added with additional IPv6 header for encapsulation. Each additional IPv6 header size of fixed 40 octets this leads to extra 320 bits per packet. The application uses 8 kbps algorithm to send the voice packets before encapsulation. As the packets are encapsulated, the payload is doubled. Thus the bandwidth is increased to 16 kbps. Carlos *et al.* (2007a) observed that this is twice the actual payload.

**Increased Processing Delay:** The encapsulation of packets in the MRHA tunnel also results in increased processing delay. Such increased processing time may include encryption or decryption, topological correctness verifications, Maximum Transfer Unit (MTU) computation, fragmentation, and reassembly.

**Increased Chances of Packet Fragmentation:** IPv6 routers will not fragment the packets. Packets exceeding the size of MTU of the destination link are dropped by signaling Packet too Big ICMPv6 type 2 message. The augmentation in packet size due to packet encapsulation may increase the chances of the packet being fragmented along the MRHA tunnel. This can occur if there is no prior path MTU discovery conducted, or if the MTU discovery mechanism did not take into account the encapsulation of packets. Packet fragmentation will result in a further increase in packet delays and decrease in bandwidth efficiency.

**Increased Susceptibility to Link Failure:** Under the assumption of that each link has the same probability of link failure; a longer routing path would be more susceptible to link failure. Thus, packets routed through the MRHA tunnel may be
subjected to a higher probability of being lost or delayed due to link failure, compared to packets that traverse directly between the MNN and its CN.

2.1.3.2 Bottleneck in the Home Network

Apart from the increase in packet delay and infrastructure load, forwarding the packets through the HA may also lead to either the HA or the home link becoming a bottleneck due to the aggregated traffic from or to all the MNNs. Congestion at home would lead to additional packet delay, or even packet loss. In addition, HA operations such as a security check, packet interception, and tunneling might not be as optimized in the HA software as basic packet forwarding. This could further limit the HA capacity for data traffic. Furthermore, as all the traffics are to pass through the home link, it becomes a single point of failure for the mobile network. Figure 2.8 illustrates the bottleneck in HA.

![Figure 2.8 Bottleneck in Home Agent](image)

Data packets are delayed or discarded due to congestion at the HN which would cause additional performance degradation to the applications. Signaling packets such as BU and BA messages are delayed or discarded due to
congestion at the HN. This may affect the establishment or update of bi-directional tunnels, causing disruption of all traffic flow through these tunnels. A NEMO route optimization mechanism that allows the MNNs to communicate with their CNs through the different path, by avoiding the HA may alleviate or even prevent the congestion at the HA or home link.

2.1.3.3 Amplified Sub-Optimality in Nested Mobile Networks

By allowing other mobile nodes to join with a mobile network, it is possible to form arbitrary levels of nesting of mobile networks. With such nesting, the NEMO basic support further amplifies the sub-optimality of routing. This amplifies the undesirable effects of a pinball route with NEMO basic support with each level of nesting of mobile networks. This is best illustrated in Figure 2.9.

![Figure 2.9 Nested NEMO](image)

Using NEMO basic support the flow of packets between an MNN and a CN would need to go through three separate tunnels. This leads to the following problems:
1. **Pinball Route:** Both inbound and outbound packets will flow via all the HA and MR on their paths with increased latency, less resilience, and more bandwidth usage.

2. **Increased Packet Size:** An extra IPv6 header is added for every level of nesting to all the packets. As per the literature by Ernst (2007a) the header compression cannot be applied because both the source and destination (the intermediate MR and its HA) are different between hop to hop. Nesting also amplifies the probability of congestion at the home network of the upstream MRs. In addition, the home link of each upstream MR will also be a single point of failure for the nested MR.

### 2.1.3.4 Sub-Optimality with Combined MIPv6 Route Optimization

![Figure 2.10 Sub-Optimality](image)

**Figure 2.10 Sub-Optimality**

When a MIPv6 host joins a mobile network (Figure 2.10), it becomes a VMN of the mobile network. Packets sent to and from the VMN will have to be routed not only via the HA of the VMN, but also via the HA of the MR of the
mobile network. This leads to the same amplification effect of nested mobile
to perform route optimization with its HA. This is because the route between
The route between the mobile host and its
CN is subjected to the sub-optimality introduced by the MRHA tunnel.

2.1.3.5 Security Policy Prohibiting Traffic from Visiting Nodes

NEMO basic support requires all traffic from visitors to be tunneled to
the MR's HA. Jean and Pekka et al. (2006) observed that this might represent a
breach in the security of the home network (some specific attacks against the
MR’s binding by unauthorized visitors have been documented). Administrators
might thus fear that malicious packets will be routed into the HN via the bi-
directional tunnel. As a consequence, it can be expected that in many deployment
scenarios, policies will be put in place to prevent unauthorized VMNs from
attaching to the MR. Figure 2.11 illustrates the same

Figure 2.11 Security Policy Prohibiting Traffic from Visiting Nodes
However, there are deployment scenarios where allowing unauthorized VMN is desirable. For instance, when MR maintains connectivity with its home network through other MR, it forms a nested NEMO. Both the nodes are depends on each other to reach the Internet. When MR have no prior knowledge of one another (no security association like Authentication, Authorization, and Accounting (AAA), Public Key Infrastructure (PKI)), it could still be acceptable to forward packets, provided the packets are not tunneled back to the home networks. A route optimization mechanism that allows traffic from MNN to bypass the bi-directional tunnel between an MR and its HA would be a necessary first step towards a tit for tat model. MRs would benefit from a reciprocal altruism based on anonymity and innocuousness to extend the Internet infrastructure dynamically.

2.1.4 QoS Analysis

Quality of Service (QoS) support for any Internet based application is the crucial part while using the MIPv6 protocol. Public transport vehicles will also work based on NEMO protocol for connectivity with its control station. This connectivity can also be extended as providing Internet service to the passengers. Due to the speed and huge service request, maintaining flawless session in public transport vehicles is highly challenging. Scalable QoS mechanisms specifically designed for such environments are required.

Zhigang et al. (2001) have pointed out that better QoS is an essential requirement for the real time applications such as video conferencing, VoIP (Voice over Internet Protocol) and business applications. George et al. (2009) have designed cost driven aggregation policy to provide better QoS. The mobile nodes may switch between heterogeneous access networks such as UMTS, 802.16 WiMAX and 802.11b WLAN (Wireless LAN). It is always crowded in this kind of wireless networks which leads to a bottleneck. The traffic has to be prioritized
to allocate the bandwidth based on the requirements. The existing QoS provisioning mechanisms for heterogeneous environment are discussed by Rafidah et al. (2011). The major QoS parameters are routing methodology, latency in handoff and the security level of the network. This part discusses the QoS requirements of NEMO protocol and status in the current scenario.

2.1.4.1 Routing

The routing mechanism of NEMO basic support protocol is well discussed already in the earlier part of this chapter (2.1). The bi-directional tunnel acts as the bridge between the CN and MNN; however, it has its own advantages and disadvantages.

**Merits:** In NEMO, the bi-directional tunnel has to be established between the HA and the MR before the communication to provide transparency between the CN and the MNN. That is either the CN or the MNN is aware of the intermediate nodes through which the packets passes. All communication between the CN and the MNN has to pass only through the MR-HA tunnel. This ensures the authentication such that only the secured nodes can send information to the nodes in the mobile network. NEMO uses the technique of ingress filtering which prohibits an attacker within the network. The attacker cannot launch a flooding attack using forged source addresses that do not confirm to ingress filtering rules. NEMO uses a strict traffic filtering routing that prohibits traffic which originates from outside the network. Another advantage of implementing this filtering is that it can easily trace the true source where the packet originated by using the MNP which provides authentication for the mobile networks (Jean and Romain 2006).

**Demerits:** A Nested NEMO network forms under specific circumstances. In Mobile Ad hoc Network (MANET), communication is predominantly supported in order to facilitate data transfers amongst the members. However in Nested NEMO
network, mobile networks are specifically trying to attain Internet connectivity (Pekka et al. 2006). Therefore, configuring an efficient default route to the Internet is the main characteristic that should be achieved by a solution for supporting the Nested NEMO. Supporting the efficient routing of packets to and from the Internet is of key importance but, consideration must be applied for the possibility that packet transfers may occur between two nodes in the same Nested NEMO. In this case, it is undesirable that any such packet transfer should first be routed out into the Internet, via any respective HA since a far more efficient, local route through the Nested NEMO may be available. In addition, to ensure that the packets traverse a direct optimized route when they are transmitted across a Nested NEMO, the route that packets follow in order to reach the entry point of the Nested NEMO (i.e. The Gateway-MR) must also be taken into consideration. This addresses the pinball routing problem and ensures that the packets are transmitted through the HA.

2.1.4.2 Handoff

Whenever an MR moves from one access network to another access network, it has to obtain a new CoA from the AR and register this CoA with its HA. RA and RS control messages are used to solve this. In both methods the MR eventually receives a new CoA from the new AR. The MRs new CoA must be registered with the HA. In order to register, a registration request message is sent by the MR to the HA after which the HA replies with a registration reply message. A bi-directional tunnel is established after this binding. The process of dealing with the movement of the MR to a new access network is called a handoff. To support the mobility of nodes NEMO has implemented a handoff mechanism.

Latency: The delay that occurs during handoff is called handoff latency. This latency is made up of several factors. The handoff latency is the sum of the registration latency and the binding latency. Ignacio et al. (2009) observed that the
registration latency is the time taken to detect the movement of MR and the time taken to obtain a new CoA from the access network. The binding latency represents the time taken to send the binding update message to the HA and to get the binding acknowledgement from the HA.

*Throughput and Bandwidth:* In communication networks throughput is referred to as the average rate of successful message delivery over a designated channel. It is measured as data packets per time slot usually in bits per second. Bandwidth is referred to as the amount of data carried from one device to another device in a given period of time. It is usually measured as bits per second (bps) or bytes per second (Bps). However, it represents the capacity of data that can be carried in a link. NEMO poses a few restrictions over bandwidth since in wireless networks it is difficult to send large packets over time. This bandwidth is limited by the bi-directional tunnel which does not admit larger data to be transmitted (Ignacio et al. 2009). In the case of NEMO throughput depends on source processing delay, transmission delay, packet processing delay and the limited bandwidth of the network.

*Error Rate:* In digital transmission bit error rate is defined as the number of received bits that have been altered due to noise or distortion to the total number of bits transferred during the given time interval. It is also the number of incorrectly transferred data packet to the total number of packets transferred. Error rate defines the degree of errors encountered during a communication. When the error rate is high the communication becomes less reliable. In NEMO errors usually occur during handoffs where there are chances for packet loss, which is stated by Jean and Romain (2006). Some handoff mechanisms like fast handoff and simultaneous binding allows the same packet to be buffered in several routers leading to multiple delivery of the same packet. This results in error leading to inefficiency of NEMO.
**Jitter:** The term jitter refers to the measurement of variability over a time of the packet latency across a network. It is defined as the deviation from the network mean latency known as Packet Delay Variation (PDV). The main cause of jitter is due to large packet overhead leading to delay in packet processing and delivery. In the case of nested NEMO an MR contacts another MR to access Internet leading to the establishment of several tunnels and numerous encapsulations for a single packet delivery. Fayza (2006) points that this type of packet encapsulation in MR-HA tunnels adds to packet overload since each encapsulation adds 40 bytes of the header to the original datagram leading to inefficient usage of bandwidth. In the case of simple voice application like VoIP which takes a voice sample for every 20 milliseconds, each encapsulation adds 320 bits per packet which is thrice the actual payload. This increases the processing delay for each packet leading to the occurrence of jitters.

### 2.1.4.3 Security Threats

In NEMO security mechanisms are needed to ensure secured packet transmission between the CN and MNN. Timo (2004) and Khaled and Mohamed (2007) ensured that, the BU provides authenticity and integrity to the packets as incorrect BU can lead to malicious attacks such as traffic hijacking or denial of service. IPsec (Internet Protocol Security) Encapsulating Security Payload (ESP) is used to protect the BU messages between HA and MN/MR. IPsec provides strong cryptographic components under its architecture. Mobile IP and NEMO are network layer protocols which are built on top of the security strength of IPsec. IPsec itself provides a network layer security service between two network entities, and it nicely integrates a number of strong cryptographic components under its architecture. Due to this strong fact of IPsec security, many Internet protocols, especially in the network layer, have been built on top of the security strength of IPsec. Some of those protocols are OSPFv6 (Open Shortest Path First
version 6), TRIP (Telephony Routing over IP, under the IP Telephony working group), RSVP/NSIS (Next Step in Signaling), L3VPN, PANA (Protocol for Authentication and Network Access), Mobile IP and NEMO. While IPsec itself is indeed quite secure, the security of the protocols using IPsec might still be very questionable. The IPsec architecture itself does not specify its relationship with other functional components such as packet forwarding, ingress filtering, IP-in-IP tunnel, or application interface in the same router. Therefore, IPsec by itself is indeed doing its job securely, but the component putting packets into the IPsec module might not. Hence the IPsec is quite secure, but it is not properly glued with the rest of the system such that the whole system can be easily attacked by the attackers. The components putting packets into the IPsec module may not be secure. The security aspects of NEMO are further discussed in detail in Chapter 8.

2.2 PERFORMANCE ANALYSIS OF VARIOUS MIPv6 PROTOCOLS

Mobility of the nodes requires them to detach themselves from one network and attach to another network in order to receive service during its mobility. This change occurs from one domain to another. It requires that the old IP connections be terminated and new connections to be established. Each mobile node is assigned an address from its HN. MIPv6 and NEMO protocols support the movement of a complete network that changes its point of attachment to the fixed infrastructure. There are various MIPv6 protocols and each one follows a different or enhanced mechanism when compared to each other. This chapter analyzes various MIPv6 protocols with three basic parameters. The various MIPv6 protocols considered for discussion are

1. Simple Mobile IPv6 (SMIPv6)
2. Hierarchical Mobile IPv6 (HMIPv6)
3. Fast handoff Mobile IPv6 (FMIPv6)
4. Fast handoff for Hierarchical Mobile IPv6 (F-HMIPv6)
5. Simultaneous Binding Mobile IPv6 (SBMIPv6)

2.2.1 Performance Metrics

The basic parameters considered for the study and analysis the protocol’s are handoff latency, packet loss and bandwidth usage.

1. **Handoff latency**: The term handoff or handoff refers to the process of transferring an ongoing call or data session from one network to another network. The time taken for implementation of the above process is called handoff latency (Fakrulradzi and Sharafah 2008). During handoff, the ongoing session may be affected, hence the higher the handoff latency, lower will be the performance of the network.

2. **Packet loss**: It is the amount of packet dropped or lost or corrupted during transfer. The performance will decrease if the packet loss is high.

3. **Bandwidth Usage**: The amount of data a node can put on a link for transfer at a given time is called as bandwidth. The network is considered as effective if the bandwidth is high.

A common topology is created for each protocol. The mobility is given to the nodes, and a data flow is initiated between the mobile node and any one of the external nodes. The handoff is implemented during the data transfer between the control nodes. Data flow is used to identify the packet loss and bandwidth usage efficiency. Handoff latency can be figured out with the help of handoff
message transfer between the control nodes. This simulation is implemented and tested in NS2 tool (NSNAM). The trace files are generated from the simulation. The graph is plotted using Gnu plot by giving the trace file as input. A bar graph is also generated to compare the results for analysis of various MIPv6 protocols. Various MIPv6 protocols performance metrics are analyzed with simulation results in the forthcoming parts of this Chapter.

2.2.2 Simple MIPv6

IPv6 (Internet Protocol version 6) is an enhancement for IPv4 (Internet Protocol version 4) by IETF. MIPv6 facilitates the transparent routing of IPv6 packets to mobile nodes. Home address assigned to the mobile node is the only identification for the external nodes in MIPv6 for each mobile node. CoA is associated with the mobile node when it is away from its home IP subnet to identify its present location. MIPv6 facilitates any mobile node to discover and store the CoA associated with its visited network. A simple data transfer scenario with a handoff is simulated. The result shows that the handoff latency of MIPv6 for the scenario is 17 seconds. The result is shown in Figure 2.12.

![Figure 2.12 MIPv6 Handoff Latency](image)

Figure 2.12 MIPv6 Handoff Latency
The packet loss percentage is identified by implementing the data transfer between CN to MN through HA, AR and MR. It is assumed as the payload of the packet is 1280 bits (160 octets). The fixed overhead of IP is 40 octets and Ethernet is 38. Hence the simulation environment considers that the total size of the packet is 238 octets. There are 9,414 packets transferred between CN and MN in 50 seconds, out of which 3259 was dropped. The packet loss percentage of the MIPv6 protocol is around 34%. The delay in handoff leads to huge packet loss. Figure 2.13 illustrates the packet loss during the packet transfer in MIPv6.

Figure 2.13 Packet Loss of MIPv6

The simulation result shows that the bandwidth usage of SMIPv6 is 15MB. Figure 2.14 illustrates the bandwidth usage of MIPv6.
2.2.3 Hierarchical MIPv6

The Mobile node sends a frequent binding update to the HA every time its AR changes. The Mobile node can send a packet at any time to the respective HA. However the HA cannot send a data to its mobile node until it gets a BU from the appropriate node. This increases the delay before the packets are forwarded, and the delay is amplified more as the mobile node may wait for the BA. These delays will undoubtedly increase the handoff latency. If we reduce these delays there will be an enormous reduction in handoff latency.

HMIPv6 introduces a local anchor point which is a solution for MIPv6 to reduce the mobility signaling and latency issues with its HA. A new MIPv6 node called the Mobile Anchor Point (MAP) is placed between the AR and the HA. This protocol is designed in such a way that the mobile node sends a BU to the MAP rather than to its HA, which is discussed by Harini and Ramanaiah (2008). MAP will update the details to HA and forward the data to HA. This creates a local and global mobility between these nodes. Local mobility involves

Figure 2.14 Bandwidth Usage of MIPv6
frequent handoffs and updates which will be in the MAP’s control area. Global mobility is a handoff occurrence of a mobile node from one MAP’s control domain area to another MAP’s domain area. Xavier et al. (2003) and Chen et al. (2011) have pointed out that the MAP reduces the handoff latency because local MAP can be updated quicker than the remote HA. HMIPv6 reduces the additional traffic involved in signaling as the MAP takes care of the registration process. The cost involved in MIPv6 and HMIPv6 location update has been discussed by Brahmtjit (2008).

The MAP handles the local handoff as intra-domain and global as inter-domain with the help of an on link address and regional address respectively. Mobile Nodes register with the MAP and the MAP collects the packets on behalf of Mobile Nodes and redirects it to the Mobile Node. The basic structure of an HMIPv6 is shown in Figure 2.15.

![Figure 2.15 HMIPv6](image)

When a mobile node enters into an MAP domain it will receive an RA message. This will have information about the local MAP. The MN will update its current location called as on-link CoA with its address to the MAP. MAP is always considered as a local HA for the mapped mobile nodes. MAP will receive
all packets on behalf of the mapped MN and forward the data to HA. If the mobile
node changes its location, it will be updated to MAP rather than HA. Mobile nodes
are aware of HMIPv6 implementation and based on the situation MN can choose
to use the MAP. In some cases, MN may also prefer to use SMIPv6. Soliman et al.
(2008) state that if MN moves to a new network, where HA is close to it, MN may
prefer to avoid HMIPv6. When the mobile node is on the move from AR1 to AR2,
MAP will provide seamless mobility to maintain its connectivity. One or more
MAP can be there in the operator network as multi level hierarchy is not required
for a higher handoff performance.

Once an MN visits a new network the discovery phase starts. It will find
out the global address of the MAP through the RA message from the AR. When
mobile node moves from one subnet to other, it will continue the process of the
MAP discovery. For every movement before the MAP discovery, the MN will
ensure that it is in the same MAP domain. Through RA Neighbor Discovery
mobile node will also have an update of MAP domain connectivity or coverage.
Mobile node will have seamless service as longer as its mobility is within the
MAP domain. Any address change in the MAP will be updated immediately by
the mobile node to its HA and to the CNs.

The MAP discovery will not be performed if the mobile node is not
aware of the HMIPv6, which results in the mobile node using the simple MIPv6
protocol for its mobility management. If the mobile node is HMIPv6-aware, it
chooses to use its HMIPv6 implementation. Then, the mobile node will first
register with an MAP by sending it a BU containing its home address and a on-
link address (LCoA). In order to carry out an optimized route, the mobile needs to
be aware of the original sender. Hence the MAP will not modify any details of the
original packet. A mobile node may go for multiple MAP registration
simultaneously for an efficient bandwidth usage. It may use a single MAP address for a set of CNs.

The HMIPv6 simulation result shows that the Handoff latency is 1.3 seconds which is updated in Figure 2.16.

![Figure 2.16 Handoff Latency of HMIPv6](image)

It has been tried to verify packet loss percentage of HMIPv6 by sending 2799 packets of data in 6 seconds, and found that 144 packets are dropped. The result shows that the packet loss percentage is around 5.1%. Figure 2.17 reflects the packet loss of HMIPv6.
Figure 2.17 Packet Loss of HMIPv6

The Bandwidth efficiency of HMIPv6 is found by simulation result as 8 MB. Figure 2.18 shows the bandwidth efficiency graph of HMIPv6.

Figure 2.18 Bandwidth Efficiency of HMIPv6
2.2.4 Fast Handoff MIPv6

Fast Handoff is an extended version of MIPv6, which reduces the latency in movement detection, IP address configuration and location update in MIPv6. MN identifies its movement between the new router referred to as New Access Router (NAR) and current router called Present Access Router (PAR). ‘Router Solicitation for Proxy Advertisement’ (RtSolPr) and ‘Proxy Router Advertisement’ (PrRtAdv) are the control messages used to maintain the connectivity by preparing a new CoA before the MR leaves the PAR (Kwon et al. 2008). Through these control messages, MN is able to invent the new CoA (nCoA) even if its in PAR’s control when its ready for handoff. Thus, the latency associated with the prefix discovery and handoff is avoided. Moreover, when the mobile node performs handoff the address can immediately be used once it is attached with the NAR. It will get a Fast Binding Acknowledgement (FBAck) control message prior to its movement. If the MN starts moving without ‘FBAck’ control message, it can still use ‘nCoA’ by intimating its joining to NAR through a ‘Fast Neighbor Advertisement’ (FNA) control message. If there is any modification in the nCoA, the NAR will respond to the FNA with the new address.

Fast handoff mechanism consists of three phases: Handoff Initiation (HI), tunnel establishment and packet forwarding.

2.2.4.1 Phase I – Handoff Initiation

The Mobile host sends the RtSolPr message to the PAR to initiate the handoff. From the NAR’s beacon message, the RtSolPr obtains the link layer address of new the point of attachment. The PAR will reply with the PrRtAdv message indicating that the NAR is unknown or known but connected through same address. It may also be known to specify the new prefix that the mobile node should use. Ernst (2007a) quotes that the new Care-of Address is used by the MN
to send the Fast Binding Update (FBU) to the PAR. After successful binding of MN, PAR sends FBAck message. The first phase is shown in Figure 2.19

2.2.4.2 Phase II – Tunnel Establishment

The Tunneling phase creates a tunnel between NAR and PAR. To establish a tunnel, PAR sends an HI message to the NAR. As a response to the HI message, NAR sends the Handoff Acknowledgement (HAck) message to PAR (Koodli 2005). After an exchange of these two messages, a tunnel will be established between the two access routers so that the pending data can be transferred. The steps are demonstrated in Figure 2.20

2.2.4.3 Phase III – Packet Forwarding

After the tunnel is established, the packets must be forwarded. Forwarding packets between PAR and NAR is based on anticipated timing interval, so it is difficult and may lead to massive packet loss (Parveen et al.
2011). When the MN completes its transition to the new location it sends an F-NA to initiate packet flow from NAR to itself, which is shown in Figure 2.21.

![Figure 2.21 Packet Forwarding in Fast handoff Mechanism](image)

**Figure 2.21 Packet Forwarding in Fast handoff Mechanism**

Sequence diagram in Figure 2.22 explains the steps involved between MNN, PAR and NAR for fast handoff mechanism.

![Figure 2.22 Sequence Diagram of Fast Handoff Mechanism](image)

**Figure 2.22 Sequence Diagram of Fast Handoff Mechanism**

Simulation results show that the handoff latency of FMIPv6 is 1.2 seconds as shown in Figure 2.23.
Figure 2.23 Handoff Latency of FMIPv6

The packet loss is evaluated by sending 4235 packets between CN and MNN in 7.5 seconds and it is found that 39 packets (0.9%) are lost. Figure 2.24 illustrates the packet loss in FMIPv6.

Figure 2.24 Packet Loss in FMIPv6
The bandwidth usage of FMIPv6 is 24 MB shown in figure 2.25.

![FMIPv6 Bandwidth Usage](image)

**Figure 2.25 Bandwidth Usage of FMIPv6**

### 2.2.5 Fast Handoff for Hierarchical MIPv6

For improving the handoff performance of MIPv6, two typical extended schemes HMIPv6 and FMIPv6 are being standardized by IETF. Both FMIPv6 and HMIPv6 have so far been designed in their own ways so as to enhance the MIPv6 in the signaling and handoff aspects. HMIPv6 facilitates a reduction in the signaling overhead and delay concerned with the BU using the MAP in hierarchical architecture. On the other hand, FMIPv6 exploits various L2 triggers to prepare for a new CoA at the new router in advance and a bidirectional tunnel is established between PAR and NAR to minimize any service disruption during the handoff. It is noted that HMIPv6 does not touch the fast handoff support described in FMIPv6. This means that we still need a certain fast handoff scheme in HMIPv6 based networks. The data transfer of HMIPv6 works based on the tunneling from the MAP to MNN, whereas FMIPv6 uses the tunneling between the PAR and NAR for fast handoff.
In F-HMIPv6, the tunnel is established between the MAP and NAR, rather than between PAR and NAR and it is discussed by HeeYoung et al. (2005). For this purpose, the MN exchanges the signaling messages for the handoff with MAP and not PAR. F-HMIPv6 makes use of the FMIPv6 control messages for handoff support without any additional definition of any new messages (Li and Samuel 2008). The procedure of F-HMIPv6 is illustrated in Figure 2.26. It is assumed that an MN is trying to move from PAR to NAR in the MAP region, and the MAP already has information on the link-layer address (or identifier) and network prefix of each AR in the region. It is also assumed that the layer 2 triggers indicating events on layer 2 are informed to the MN. F-HMIPv6 defines no additional messages to the existing FMIPv6 messages, except for changing the source and or destination IP addresses of the messages. When the MN knows its movement toward NAR by using the layer 2 pre handoff trigger that includes the link layer address of NAR, it sends a router solicitation for the proxy to request the information of NAR and a new LCoA. On receiving this request the MAP replies with a proxy router advertisement that contains the network prefix of NAR.

![Figure 2.26 Sequence Diagram of F-HMIPv6](image-url)
The MN configures the new CoA by using the prefix information. The MN then requests a FBU to the MAP with the new LCoA. On reception of the FBU, the MAP starts the fast handoff procedure by sending a HI message to NAR. This HI message includes the request for verification of the new LCoA and for the establishment of a bi-directional tunnel between the MAP and NAR. In response to the HI, the NAR performs the duplicated address detection process and then responds with a HAck to the MAP. After receiving the HAck, the MAP sends the result to the MN by using FBAck. Li Jung (2008) ensures that, when the MN gets the connection to NAR, it sends a router solicitation message including a FNA option in order to inform its presence. Then, the NAR will deliver packets to the MN. As described earlier, F-HMIPv6 does not need a new message except the messages already defined in FMIPv6 and HMIPv6. However, the following extensions of existing messages are needed.

A new flag is defined in the HMIPv6 MAP option so as to indicate whether or not the MAP supports the F-HMIPv6 within the HMIPv6 domain. Some of the FMIPv6 messages have a different IP source and destination addresses in the respective IP fields. In particular, the MAP address is used instead of the PAR address.

It has been found that the handoff latency of F-HMIPv6 is 2.5 seconds, which is updated as a graph in Figure 2.27.

![Figure 2.27 – Handoff latency of F-HMIPv6](image)
5551 packets are transferred between CN and MNN in 9 seconds through F-HMIPv6 protocol. The trace file shows that 232 packets are dropped, which is of around 4.1%. Figure 2.28 shows the packet loss details of F-HMIPv6.

![Figure 2.28 Packet Loss in F-HMIPv6](image1)

**Figure 2.28 Packet Loss in F-HMIPv6**

The bandwidth efficiency of F-HMIPv6 is 15 MB. The total bandwidth is extracted from the trace file. The trace file output is shown as graph in Figure 2.29 graph.

![Figure 2.29 Bandwidth Usage in F-HMIPv6](image2)

**Figure 2.29 Bandwidth Usage in F-HMIPv6**
2.2.6 Simultaneous Binding MIPv6

It is highly impossible to find out when an MN will detach from the existing connectivity from AR and join with the new AR. Hence resolving the time to start sending the pending packets between PAR and NAR is not easy. A few wireless technologies use layer 2 control messages to instruct the mobile node to perform handoff instantly. In addition, it may use movement detection algorithms to recognize the mobile nodes detachment and attachment state. Even for these operations and after finding the detachment and attachment state, to tunnel the packets certain time will be taken by the respective nodes. Normal layer 2 handoff time ranges between 10 to 100 ms.

Simultaneous Binding proposes a solution to this issue. Shariq and Ahmad (2008) observed that, SBMIPv6 proposes to bi-cast or n-cast the packets for a short time from PAR to one or more guessed potential access routers of the mobile node based on its movement before the mobile nodes handoff. Hence the mobile node is capable of receiving the traffic autonomously. The operation of SBMIPv6 is analogous to FMIPv6 protocol excluding FBU and Simultaneous Binding flag set is introduced in SBMIPv6. A small modification in the mobile node packet is proposed by adding two BU lifetime values. The bi-casting life time and new CoA life time are added in simultaneous binding sub option and BA option respectively. The CoA lifetime starts once the bi-casting life time ends. Rarely MN may get more than a copy of the same packet due to mispromise of delivery of a data to a node. However, TCP congestion avoidance implementations will react negatively to the reception of 3 duplicate acknowledgements (HeeYoung et al. 2008). Hence these problems can be resolved with the help of the algorithms designed to manage multiple copy detection and deletion.

Simulation result shows that the handoff latency of SBMIPv6 is just 0.5 seconds. Figure 2.30 shows the handoff latency of SBMIPv6.
Figure 2.30 Handoff Latency of SBMIPv6

A data transfer is implemented between CN and MNN with 3862 packets in 7.5 seconds through SBMIPv6 protocol. It shows that 23 packets are dropped which is around 0.5% of total packets. Figure 2.31 shows the packet flow.

Figure 2.31 Packet loss in SBMIPv6

It has been found the bandwidth usage of SBMIPv6 is high which is of 27 MB. Figure 2.32 illustrates the bandwidth usage of SBMIPv6.
2.2.7 Performance Analysis

The analysis of various MIPv6 protocols has been implemented to judge the performance of each. MIPv6, HMIPv6, FMIPv6, F-HMIPv6 and SBMIPv6 are the protocols simulated with simple data transfer scenario. The data transfer scenario is implemented with considerable count of packets in a certain period. There will be a handoff during the data transfer to measure the handoff latency of the protocol. Handoff latency, packet loss and bandwidth usage are the parameters considered to examine those protocols. The result of every simulation is logged as trace file. The output of the trace file is plotted as graph.

The MIPv6 protocol provides support to the mobile networks, when they are on the move. The data transfer is initiated from CN to MN through HA, MR tunnel. There are 9414 packets transferred in 50 seconds for MIPv6 protocols. In the simulated environment, it took 17 seconds for a simple handoff in MIPv6 protocol. Since MIPv6 protocol takes more time for handoff, 3259 packets are dropped during the data transfer. This dropped packet count is around 34% of the total packets. The bandwidth usage of MIPv6 protocol is 15 MB during the data...
transfer. This analysis proves that the MIPv6 protocol lack successful packet transfer.

HMIPv6 protocol creates a hierarchical structure in the network and introduces the MAP node. This MAP node acts as a local home agent for the mobile network. Through HMIPv6 protocol, the packet transfer is simulated between CN and MN. 2799 packets are transferred in 6 seconds with handoff. It has been measured that 1.3 seconds were taken for handoff. 144 packets are lost during the transfer, which is 5.1% of the total. However, the bandwidth usage of the protocol is just 8 MB.

FMIPv6 protocol concentrates on reducing the handoff latency. Three phases of handoff are implemented during the packet transfer in simulation environment. There are 4235 packets transferred in 7.5 seconds. The handoff latency of FMIPv6 is just 1.2 seconds. It is identified that 39 packets are lost, which is of 0.9% of the total packet count. The bandwidth usage of FMIPv6 protocol is 24 MB. This simulation conveys that the FMIPv6 protocol is comparatively better than MIPv6 and HMIPv6 protocols.

Applying FMIPv6 mechanism in hierarchical (HMIPv6) environment is called as F-HMIPv6 protocol. The packet transfer was implemented for 9 seconds with 5551 packets. It has been found that 232 packets are lost. This lost packet count is 4.1% of the total packets. The bandwidth usage of F-HMIPv6 protocol is 15 MB.

Simultaneous Binding MIPv6 is the concept of bi-casting and n-casting of the packets to the current and future locations of the MN. 3862 packets are transferred between CN and MN in 7.5 seconds. It took 0.5 seconds only for handoff. It has been recognized that just 0.5% of the total packets, which is 23 are
lost. This packet loss count is very less when we compare with other MIPv6 protocols. The bandwidth usage of the protocol is 27 MB.

The implementation of various MIPv6 protocols shows that SBMIPv6 performs better for all the above said parameters. SBMIPv6 protocol has lowest handoff latency among other protocols because it multicast the packets early to the NAR. SBMIPv6 protocol has the lowest packet loss as it makes sure that a successful handoff is achieved. In case of bandwidth usage, the SBMIPv6 protocol has the highest bandwidth usage. FMIPv6 is the next best protocol if SBMIPv6 protocol is not used for mobile networks. The Table 2.1 lists the comparative performance results.

**Table 2.1 Performance Results of Various MIPv6 Protocols**

<table>
<thead>
<tr>
<th>MIPv6 Protocols</th>
<th>Handoff Latency (S)</th>
<th>Packet Loss Percentage</th>
<th>Bandwidth Usage (MB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMIPv6</td>
<td>17</td>
<td>34 %</td>
<td>15</td>
</tr>
<tr>
<td>HMIPv6</td>
<td>1.3</td>
<td>5.1 %</td>
<td>8</td>
</tr>
<tr>
<td>FMIPv6</td>
<td>1.2</td>
<td>0.9 %</td>
<td>24</td>
</tr>
<tr>
<td>F-HMIPv6</td>
<td>4.7</td>
<td>4.1 %</td>
<td>15</td>
</tr>
<tr>
<td>SBMIPv6</td>
<td>0.5</td>
<td>0.5 %</td>
<td>27</td>
</tr>
</tbody>
</table>

Performance results of various MIPv6 protocols in terms of bar graph, with the basic parameters is shown in Figure 2.33.
2.3 SUMMARY

MIPv6 is a key protocol for movable networks. There are good numbers of enhanced MIPv6 protocols proposed, and still the work is in progress. In this chapter the MIPv6, HMIPv6, FMIPv6, F-HMIPv6 and SBMIPv6 protocols are analyzed. Handoff latency, packet loss and bandwidth usage are the parameters considered to measure the performance of these protocols. The analysis results show that SBMIPv6 protocol performs well. FMIPv6 also provides reasonable performance next to SBMIPv6.

Handoff is the vital operation of any MIPv6 protocol because handoff latency causes the packet loss and delays and bandwidth usage. Hence new optimized handoff mechanism to reduce the handoff latency and other parameters is proposed in the next chapter.