Abstract: the Mobile IPv6 protocol allows an IPv6 host to leave its home subnet while transparently maintaining all of its present connections and remaining reachable to the rest of the Internet. This is essentially realized by assigning a static home address and a dynamic Care-of-address which keeps on changing as the mobile node moves from one subnet to another. Essentially, the mobile node keeps on notifying its home agent about its current care-of-address, and the home agent intercepts packets addressed to the mobile nodes home address and tunnels them to the mobile nodes current subnet. One of the major issues regarding the basic Mobile IPv6 protocol is related to the handover management of a mobile node. Whenever a mobile node performs a handover from its current subnet to the new subnet, then the whole handover process results in non-trivial latency and packet loss. In this work, three scenarios for Handover are simulated. These scenarios are Normal Handover Mobile IP, Anticipated Fast Handover Mobile IP, and Buffering Handover Mobile IP. This work evaluates the performance of these scenarios. The work shows how the Buffering Handover protocol for Mobile IP can result in a more efficient handover mechanism for Mobile IPv6.

1. INTRODUCTION

Internet Protocol (IPv4 and IPv6) is considered as the universal routing solution in wireline and wireless networks, it can be used on the top of all radio access technologies. That make the introduction of mobility management mechanisms on IP the perfect solution to keep application sessions and manage efficiency and transparently mobile node movement through different access points to the network, regardless of their radio access technologies. In The Internet-based core network, such as radio access points are under the control of special IP routers for signaling and data transmission, named IP access routers. Each access router manages the application access to one or more radio cells. One of the most important metrics in IP based mobility protocol is the handover management. An IP handover is the global process that shifts the management of mobile node IP connection to the network, from an IP old access router to a new one. Such process introduces (Mobile Node) MN disconnection, the delay D of global mobile node IP disconnection, as shows Figure 1, is the delay needed by the mobile to perform the wireless handover (D) and the IP additional delay (t), where t is the necessary latency to detect the handover in IP layer, obtain a new IP address and finally register its new address within the network. This disconnection delay can introduce packet loss, retransmission, additional end-to-end transmission delays and jitters for the current communication session.

In this work, main solutions to manage mobility in Internet protocol are introduced. Mobile IPv6 is the natural evolution of Mobile IP [3, 4]. It supports many improvements of Mobile IP and exploits advanced features of IPv6, as described in part I. In mobile IPv6, each MN is able to create quickly its own care of address using IPv6 automatic address configuration or stateless address auto configuration mechanism, so foreign agents are not needed. Larger range of address is also available for mobile node in IPv6, which eliminate the problem of address shortage in IPv4 [6]. One of the main evolutions of mobile IPv6 compare to mobile IPv6 is the introduction of native mechanisms to fix the triangular routing anomaly in mobile IP, by the introduction of an additional registration message. When performing a mobile IPv6 handover, the MN can send directly the binding update, with its new CoA, to its corresponding nodes in addition to the HA. Thus, they can learn and create locally a binding entry between the new MN’s CoA and its Home address. They send packets directly to the new MN location, without additional routing through the home network, which fix triangular routing problem as shows Figure 2.
In this work, three scenarios for Handover are simulated. These scenarios are Normal Handover Mobile IP, Anticipated Fast Handover Mobile IP [8], and Buffering Handover Mobile IP. The details descriptions are given in the next subsections [7].

2. NORMAL HANDOVER MOBILE IP:

The home agent receives the packets on behalf of the mobile node and then tunnels the packets to the current access router (oAR) of the mobile node at its current care-of address (CoA1). The mobile node is moving constantly from Subnet I to Subnet II, for Normal Handover [1]. The network system was also used for simulating the basic Mobile IPv6 handover situation. A step-by-step description of the handover which takes place in the depicted network system is given next:

1. When the mobile node detects that it is moving to a new subnet, it sends a Router Solicitation for Proxy (RtSolPr) message to the its current access router(shown as oAR in figure 3).

2. The old access router (oAR) receives the RtSolPr message from the mobile node and initiates the handover process with the new access router (nAR). The depicted network system assumes that the old access router has information about the new access router (nAR), and its point of attachment is known to the old access router.

3. The oAR should send a Proxy Router Advertisement (PrRtAdv) back to the mobile node. The PrRtAdv should provide the mobile node with information about the new subnet, such as the subnet prefix or the new care-of address which the mobile node is supposed to use in the new subnet. In order to get a valid new care-of address for the mobile node, the old access router sends the new access router exchanges messages with the new access router. First, it sends a Handover Initiation (HI) message to the new access router. The modeled network system assumes that the new access router uses stateful address auto-configuration, to discover a valid new care-of address. Therefore, the HI message sent by the old access router contains the old care-of address of the mobile node.

4. The new access router receives the HI message from the old access router, and allocates a new care-of address with the help of stateful address auto-configuration. This new care-of address is returned to the old access router in a Handover Acknowledgement (HACK) message.

5. The old access router receives the HACK message and then constructs a Proxy Router Advertisement (PrRtAdv) message containing the new care-of address and sends it to the mobile node.

6. As soon as the mobile node receives confirmation of a pending layer 3 handover through the PrRtAdv (sent by the oAR) with a new care-of address (nCoA) in it, the mobile node confirms its movement into the new subnet by sending a Fast Binding Update (F-BU) message to the oAR. The F-BU is supposed to be the last message sent by the mobile node before the layer 2 handover is executed. On receipt of the F-BU, the oAR responds with a Fast Binding Acknowledgement (F-BACK), which is sent to the mobile node both at the new and old care-of addresses, as the oAR is not sure about where the exact location of the mobile node is.

7. As the HACK message sent by the nAR indicated a valid new care-of address for the mobile node, the oAR starts forwarding any packets addressed to the mobile node old care-of address (CoA1), to the new care-of address (CoA2), via the nAR. The nAR takes care of delivering packets to the mobile node, once it establishes a solid link at the new subnet. But the oAR starts forwarding the packets only after it receives an F-BU message from the mobile node, confirming the handover.

8. When the mobile node arrives on the new subnet (Subnet II in figure 4), it tries to set up a solid link with the nAR. When successful in setting up a layer 2 link in the new subnet, it sends a Fast Neighbour Advertisement (F-NA) to signal the nAR that it has arrived on the new subnet. This triggers packet delivery to the mobile node on the new subnet.

9. The mobile node finally settles down on the new subnet and sends a Binding Update to its home agent (HA), to register its new care-of address (CoA2).

Figure 3 The selected random path for Normal Handover in MIPv6

Figure 4 Normal Handover in MIPv6 (Proxy (RtSolPr) from Mobile Node to oAR (old Access Router “current access router”)
3. ANTICIPATED FAST HANDOVER MOBILE IP:
The mobile node is moving constantly from Subnet I to Subnet II, which involves an Anticipated Fast Handover [2]. A step-by-step description of the handover which takes place in the depicted network system is given next.

1. When the mobile node detects that it is moving to a new subnet, it sends a Router Solicitation for Proxy (RtSolPr) message to its current access router.
2. In Anticipated Fast Handover, the Mobile Node start sending and receiving messages while it is still with the old access router so from the motion toward the new subnet (the displacement vector close to a new subnet).
3. The old access router (oAR) receives the RtSolPr message from the mobile node and initiates the handover process with the new access router (nAR). The depicted network system assumes that the old access router has information about the new access router (nAR), and its point of attachment is known to the old access router.
4. According to the Anticipated Fast Handover Protocol, the oAR should send a Proxy Router Advertisement (PrRtAdv) back to the mobile node. The PrRtAdv should provide the mobile node with information about the new subnet, such as the subnet prefix or thenew care-of address which the mobile node is supposed to use in the new subnet. In order to get a valid new care-of address for the mobile node, the old access router exchanges messages with the new access router. First, it sends a Handover Initiation (HI) message to the new access router. The modeled network system assumes that the new access router uses stateful address auto-configuration, to discover a valid new care-of address. Therefore, the HI message sent by the old access router contains the old care-of address of the mobile node.
5. The new access router receives the HI message from the old access router, and allocates anew care-of address with the help of stateful address auto-configuration. This new care-of address is returned to the old access router in a Handover Acknowledgment (HACK) message.
6. The old access router receives the HACK message and then constructs a Proxy Router Advertisement (PrRtAdv) message containing the new care-of address and sends it to the mobile node.
7. As soon as the mobile node received confirmation of a pending layer 3 handover through the PrRtAdv (sent by the oAR) with a new care-of address (nCoA) in it, the mobile node confirms its movement into the new subnet by sending a Fast Binding Update (F-BU) message to the oAR. The F-BU is supposed to be the last message sent by the mobile node before the layer 2 handover is executed. On receipt of the F-BU, the oAR responds with a Fast Binding Acknowledgement (F-BACK), which is sent to the mobile node both the new and old care-of addresses, as the oAR is not sure about where the exact location of the mobile node is.
8. As the HACK message sent by the nAR indicated a valid care-of address to the mobile node, the oAR starts forwarding any packets addressed to the mobile node old care-of address (CoA1), to the new care-of address (CoA2), via the nAR. The nAR takes care of delivering packets to the mobile node, once it establishes a solid link at the new subnet. But the oAR starts forwarding the packets only after it receives an F-BU message from the mobile node, confirming the handover.
9. When the mobile node arrives on the new subnet (Subnet II in figure), instead of setting up a solid link with the nAR, it suddenly changes its direction of movement and ventures back into its old subnet.
10. The mobile node finally reaches its old subnet. Meanwhile, the old access router (oAR) does not know about the mobile nodes erratic movement and keeps on forwarding packets to the mobile node new care-of address. Upon regaining solid link with the old subnet, the mobile node sends a fast binding update (F-BU) to the old access router (oAR), notifying it about its return to the old subnet.
11. The mobile node finally settles down on the old subnet. As its care-of address has not changed, even though it moved and changed its point of attachment twice, while moving to the new subnet and coming back to the old subnet during the erratic movement, the home agent (HA) does not need to be notified about this. This is because the HA still has the binding with the mobile node old care-of address (CoA1).

4. BUFFERING HANDBEY MOBILE IP
The Buffering Extension In order to add the buffering function to the described network system, the following additions are done in the steps described below [2]:
1) As discussed before, the mobile node in the network system is moving in an erratic manner. Therefore, the buffers on both the old access router (oAR) and the new access router (nAR) will be utilized to reduce packet loss. The buffer on the oAR will be initiated when the mobile node sends the F-BU to the oAR, Confirming its movement into the new subnet (as in step 6). The buffer on the nAR will be initiated when the old access router (oAR) sends a Handover Initiation (HI) message to the new access router with the U bit set (as described in step 3).
2) The oAR starts temporarily storing packets addressed to the mobile node. Similarly, the nAR starts temporarily storing packets in its buffer.
3) When the mobile node returns back to the old subnet and sets up a solid link in the old subnet (as described in step 9), the old access router (nAR) should send the buffered packets to the mobile node,
once it receives a fast binding update (F-BU) message from the mobile node.

4) As the MN settles in the new subnet, the buffer space can be released by both the access routers. The time when the buffer space is released will depend on the mobility pattern and a pre-determined timeout period. In a real implementation, the buffer space may not be released and could be reserved for handovers in the future, if need be (especially, when the mobile node is performing an erratic movement between the two subnets).

5. EXPERIMENTS:

Two different paths for the mobile node had been simulated, first linear (straight line), and random U turn path for the three protocols, namely normal, fast, and buffered handover in Mobile IP. The packets are sent from the HA to the MN 1 packet every 500 ms. The first three experiments are done for linear steady trajectory as shown in figure 5 for the normal handover.

In this protocol the signaling for handover starts when the mobile node leaves Subnet I and enters Subnet II (already in the intersection region as shown in figure. Note that the packet loss during handover is 12 packets as shown in figure 6. Figure 6 depicts the sending time for each packet versus the delay time of arrival to the mobile node (arrival time). Figure 7 shows the linear steady trajectory for the mobile node for fast anticipated handover. In this protocol the signaling for handover starts early. The displacement vector give a prior information about the predicted position of the mobile node. The handover starts when the mobile node reaches the second subnet although it is still linked with the first subnet. The packet loss analysis is shown in figure 8, total number of packet loss is reduced to be 7 lost packets as shown in this figure.

The previous three experiments are repeated for the three protocols but with different mobile node trajectory (U turn shape). The packet loss is almost doubled because it
changes the subnet regions two times. Figure 11 illustrate the random path for normal handover analysis in Mobile Internet protocol version 6. The packet loss analysis is shown in figure 12, 24 packets are lost.

Figure 11 Random Path (U turn) Normal Handover MIPv6

Figure 12 Packet Analysis Random Path (U turn) Normal Handover MIPv6 (24 packet loss)

Figure 13 Random Path (U turn) Fast Handover MIPv6

Figure 13 describe the selected trajectory for fast handover is shown (U turn). Again the packet loss is reduced to be 14 packets as shown in figure 14.

The last experiment trajectory is shown in figure 15 for Buffering handover. Also the packet loss analysis is shown in figure 16. Table 1 summarizes these results.

Figure 14 Packet Analysis, Random Path (U turn) Fast Handover MIPv6 (14 packet loss)

Figure 15 Random Path (U turn) Buffering Handover MIPv6 (24 packet loss)

Figure 16 Random Path (U turn) Buffering Handover MIPv6 (zero packet loss)

Table 1: The results of the experiments

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Number of Packet loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal Handover (linear path)</td>
<td>12</td>
</tr>
<tr>
<td>Anticipated Fast Handover (linear path)</td>
<td>7</td>
</tr>
<tr>
<td>Buffering Handover (linear path)</td>
<td>Zero</td>
</tr>
<tr>
<td>Normal Handover (random path “U turn”)</td>
<td>24</td>
</tr>
<tr>
<td>Anticipated Fast Handover (random path “U turn”)</td>
<td>14</td>
</tr>
<tr>
<td>Buffering Handover (random path “U turn”)</td>
<td>Zero</td>
</tr>
</tbody>
</table>

6. CONCLUSION

This work studies three scenarios for Handover. These scenarios are Normal Handover Mobile IP, Anticipated Fast Handover Mobile IP, and Buffering Handover Mobile IP. The analysis of these protocols is done using Matlab. The results of the simulation model showed that the Buffering Handover protocol increased the performance of the handover process. The handover process was more efficient when this protocol was used. There are actually some other possible scenarios which further need testing and simulation. This could be one of the future directions for research. Also, as the simulation results showed that the buffering function resulted in a more efficient
handover process, future research may be aimed at incorporating a buffering function in other MIPv6 handover protocols like Tunnel Based Fast Handover or Hierarchical Mobile IPv6 handover protocol. Addition of a buffering function with these handover protocols may result in a more efficient handover mechanism.

REFERENCES:


AUTHOR

Bella S. Tawfik received his B.Sc. in Electrical engineering from the Military Technical Collage, Cairo in 1986. He received his M. Sc. in Computer Engineering from the Military Technical Collage, Cairo in 1991. He received his Ph. D. in Electrical Engineering from Colorado State University in August 1999. He got his Post Doctor in Computer Engineering from Colorado State University in October 2006.

Mohammed A. El-Shrkawey received his B.Sc. in Electrical engineering from the Military Technical Collage, Cairo in 1987. He received his M. Sc. in Computer Engineering from Faculty of Engineering, Al Azhar University, Cairo in 2002. He received his Ph. D. in Network Security from Faculty of Computers & Informatics, Cairo University in June 2007. He is currently a lecturer in Faculty of Computers & Informatics, Suez Canal University, Ismailia, Egypt. His current research interests are Networks, Modeling, simulation, and Image Processing.