A Comparative Analysis of MIFAv6, HAWAII and MIP

Ali Diab, Andreas Mitschele-Thiel
Integrated HW/SW Systems Group
Ilmenau University of Technology
Ilmenau, Germany
{ali.diab|mitsch}@tu-ilmenau.de

Christian Kellner
Integrated HW/SW Systems Group
Ilmenau University of Technology
Ilmenau, Germany
christian.kellner@stud.tu-ilmenau.de

Abstract—The research in the field of wireless communication networks focuses nowadays on the development of the 4th Generation (4G) networks. The key features of this new generation is that the 4G capabilities should be integrated with all existing mobile technologies through a common IP core. These networks are termed, therefore, as “All-IP” networks and are expected to offer any type of service- anytime, anywhere and anyhow under dynamic network conditions. However, many challenges should be faced when developing such networks. One of the main challenges is how to manage the mobility between the cells connecting by means of an IP core in a way that satisfies the real-time requirements. In order to face this challenge, several approaches have been proposed. These solutions still suffer, however, from many drawbacks making them inadequate for the future “All-IP” networks. Mobile IP Fast Authentication protocol (MIFAv6) is a mobility framework for IPv6 and developed to avoid the problems of previous solutions and to support the requirements of real-time applications. This paper evaluates this protocol compared to Handoff-Aware Wireless Access Internet Infrastructure (HAWAII) and Mobile IP (MIP). The evaluation is performed by means of simulations using the network simulator 2 (ns2) and comprises the studying of the handoff latency and the number of dropped packets on up- and downlink. The simulation results have shown that MIFAv6 outperforms HAWAII and MIP under all conditions. On uplink, the average number of the dropped packets experienced by MIFAv6 is about 90% less than that dropped by MIP and HAWAII. On downlink, MIFAv6 drops about 46% and 62% lower than that dropped by HAWAII and MIP respectively. MIFAv6 achieves fast and smooth handoffs even in high loaded networks.

Keywords-component; Mobility management; Mobile IP; fast handoff

I. INTRODUCTION

Wireless communication networks have experienced an exponential growth and are widely deployed in the recent years. They have seen a tremendous development and a wide variety of new applications such as Internet browsing, e-banking…etc. Nowadays, the research focuses on development of the 4 Generation (4G). Accessing information anywhere and anytime with a seamless connection to a wide range of information and services are the key features of these networks. 4G can be defined as a set of heterogeneous networks that inter-connects different existing and future communication networks through a common IP core. 4G is termed, therefore, as “All-IP” and is expected to serve stationary as well as mobile subscribers and offer any type of service- anytime, anywhere and anyhow under dynamic network conditions. Development of “All-IP” networks requires, however, facing many new challenges such as how to manage the mobility between the cells connecting by means of an IP core, how to reserve bandwidth and guarantee QoS for the users…etc.

MIP [1], [2] presents the well known IETF standard used to support mobility in IP networks. It introduces two new entities, which are Home Agent (HA) and Foreign Agent / Access Router (FA / AR). Each Mobile Node (MN) has a fixed IP address, a home address, acting as identity for the MN. When a MN is away from its home network, it obtains a temporary IP address called Care of Address (CoA). The CoA can be assigned to a certain interface of a MN, referred to as co-located CoA, or can be provided by a local router serving the visited sub-network, such as FA. In this case the CoA is called a FA-CoA. Changing a CoA necessitates a re-registration with the HA. This registration enables the HA to intercept the MN’s data packets, encapsulate and forward them to the new CoA. However, informing the HA about each change in the CoA produces a considerable latency especially if the HA is far away. This latency makes MIP not adequate for delay sensitive applications and forces the development of new mobility management solutions that are able to satisfy the requirements of real-time applications.

The rest of this paper this is organized as follows: Section (II) highlights the state of the art. MIFAv6 is discussed in section (III). Section (IV) presents the simulation environment and discusses the obtained results. Section (V) concludes this paper with the main results and the future work.

II. STATE OF THE ART

In order to satisfy the real-time requirements, several approaches have been proposed. These approaches can be broadly classified in four main categories. The first one aims to support a global mobility in the Internet and is referred to as macro mobility management approaches. A well known example is MIP. The second category speeds up the handoff by
Reducing the time required to register with the network. This is achieved by processing the handoff procedure inside an administrative domain locally. The solutions of this category are termed as micro mobility management solutions. The third category attempts to reduce the address resolution time are termed as micro mobility management solutions. The third category can be further classified into two main groups, Proxy Agent Architecture (PAA) and Localized Enhanced Routing Scheme (LERS) [3].

PAA-based approaches, referred to as tunnel based schemes too, extend MIP principle to process the mobility locally. Regional Registration for MIPv4 (MIPRR) [4] and Hierarchical Mobile IPv6 (HMIPv6) [5] are examples for these approaches.

With MIPRR and HMIPv6 the HA is not aware of every change in the point of attachment. This is because the handoff is processed locally by a special node, e.g. a Gateway Foreign Agent (GFA) or a Mobility Anchor Point (MAP), while moving inside an administrative domain. Thus, the communication with the HA is restricted only to the movements between different domains. The both approaches require, however, a hierarchical network topology and introduce new intermediate nodes to the network. A well known problem of these approaches is the single point of failure.

LERSs, termed as routing based schemes too, introduce normally a new layer 3 dynamic routing protocol in a localized area and distribute a specialized path setup protocol and a location database (routing cache) in the routers existing in a certain domain. A well known approach is HAWAII [6].

HAWAII does not try to replace IP. Its domain is controlled by a certain Gateway called domain root router (DRR). Each router and BS in the domain maintains a routing cache that is updated using special control packets and used to forward the data packets hop by hop towards the MN. The routing caches are updated when the MN moves inside the domain. There are four schemes for a path setup after the movement in a HAWAII domain. They can be classified into two types based on the way, through which the packets are delivered to the MN during the handoff. In the first type, the packets are forwarded from the old BS to the new one. Multiple Stream Forwarding (MSF) and Single Stream Forwarding (SSF) are the schemes proposed in this type. In the second type, the packets are delivered at the crossover router to the new BS. Unicast Non-Forwarding (UNF) and Multicast Non-Forwarding (MNF) scheme are the schemes of this type.

B. Accelerating Layer3 Mobility Management Using Layer2 Information

These solutions suppose that the MN is able to receive some information from layer2, referred to as layer2 triggers, to help in accelerating the layer3 handoff. Seamless MIP (S-MIP) [7] and Fast MIPv6 [8] (FMIPv6) are well known examples of such solutions. S-MIP deploys a hierarchical network topology and exploits the layer2 information to accelerate the layer3 handoff. S-MIP introduces a new entity called Decision Engine (DE) to control the handoff process. When the MN reaches the boundary of a cell, it informs the current AR about the probable movement and about the addresses of the newly discovered ARs. The current AR informs the DE and the new ARs. Following this, the MN’s movement is tracked by the DE to decide accurately to which AR the MN will move. When the DE determines the new AR, it informs the old AR and the other participating ones about the decision. After that, the data packets are forwarded to the old and the new AR until the DE is informed by the new AR that the handoff is finished.

FMIPv6 functions as follows: When the MN notices that it has to make a handoff, it informs the old AR, which in turn exchanges the necessary control messages with the new AR and forwards the MN’s packets to it. The MN receives its packets after the handoff directly from the new AR. Updating the MN’s binding at the HA is necessary after the handoff.

C. Network-based Mobility Management

As written above, the solutions of this category try to support the mobility without involving the MNs. Proxy MIPv6 [9] is the well known example for network-based mobility. When the MN finishes the layer2 handoff, the current Mobile Access Gateway (MAG), acting as a FA/AR, exchanges a proxy binding update and a proxy binding acknowledgement with the Local Mobility Anchor (LMA), acting as a HA. After that, the MAG emulates the MN’s home subnet. As a result, the MN thinks that it still remains in its home subnet and starts resuming communication.

III. MOBILE IP FAST AUTHENTICATION PROTOCOL (MIFAv6)

MIFAv6 [10] is proposed to fulfill the requirements of the future “All-IP” networks by supporting smooth handoffs without making restrictions on the network topology and without introducing any new entities more than that currently known from MIPv6. The basic idea is motivated from the fact that the MNs restrict their movements always to a neighbor AR, which has normally a short distance to the old one with respect to the number of hops. By utilizing this fact, the HA can delegate the authentication to the ARs. As a result, the MN requires only contacting the new AR to resume the communication on uplink. On downlink, the new AR relies on the old AR to obtain the MN’s data packets until the HA / CN is informed. The operation of MIFAv6 is presented in figure 1.

The local authentication relies on groups of neighbor ARs called Layer 3 Frequent Handoff Regions (L3-FHRs). Each AR
builds its own L3-FHR, which is composed of a set of neighboring ARs, to which the MN is likely to move. L3-FHRs can be built either statically by means of a certain algorithm such as neighboring graph [11] or dynamically using neighbor discovery protocol of IPv6 [12] or by tracking the MNs movements. Of course, there must be Security Associations (SAs) between the ARs in each L3-FHR. These SAs can be established using AAA infrastructure [13], IKE [14], or any other key distributing mechanism.

A. Initial Registration

As soon as the MN switches on, it uses the same procedures of MIPv6. Binding Updates (BUs) are sent to the CN as well as to the HA. The MN informs the current AR and the HA that MIFAv6 is preferred for the next registrations. This is achieved by setting one of the reserved bits in the BU message sent to the HA, referred to as “MI” flag. Similar “MI” flag should be set in the Router Advertisement (RA) message to indicate the support of MIFAv6. The BU sent to the CN is built according to MIPv6 specifications.

When the HA receives the BU message, it sends a Binding Acknowledgement (BA) message containing two SAs. One is between the HA itself and the current AR, while the other is between the MN and the current AR. Upon the current AR receives the BA message, it extracts the SAs, generates two random variables $R1$, $R2$. In addition, another SA is generated to be used between the MN and the ARs in the L3-FHR of the current AR. The new generated data is sent to the MN in suitable extensions to the BA message.

B. Initial Authentication Procedure

After the initial registration, Movement Probability Notification (MPN) and Movement Probability Acknowledgement (MPAck) messages are exchanged between the current AR and the HA. MPN message contains the generated random variables and a new SA to be used to secure the control messages between the HA and the next new AR, which will be one of the ARs existing in the current L3-FHR. MPAck message contains the information required for the new AR to be able to authenticate the MN during the next movement. The key idea is that the HA generates two hash values ($auth1$ and $auth2$) using the two generated random variables and some other data related to the MN, such as MAC address, home address...etc. These hashes are sent with the MPAck message. $auth1$ presents the authentication value the MN should generate, while $auth2$ expresses the value the HA should generate as a response to $auth1$.

After that, the current AR distributes the data received with the MPAck message to the all ARs locating in the current L3-FHR. This is done by sending another MPN message to each neighbor AR. This data is recorded in a soft state and will be used by one AR in the future and deleted from the others.

C. Handoff Procedure

When the MN moves to another AR, it sends a BU message to the new AR and a BU message to the CN. The BU message sent to the CN is built according to MIPv6 specifications, while the BU sent to the new AR should be modified. Additional to setting the “MI” flag, the first hash value ($auth1$) calculated by the MN should be added in a suitable extension to the BU too. The new AR authenticates the MN and compares the values of ($auth1$) calculated by the MN with that received from the HA. Afterwards, the new AR checks if the HA can satisfy the MN’s requirements. This is achieved by checking the data distributed from the old AR.

If the check is successful, the new AR sends three messages, a Handoff Notification (HNot) to the old AR, a BA to the MN and a BU message to the HA, see figure 1.

![Figure 1. Operation of MIFAv6](image-url)

The BA contains two new random variables and a new SA to be used for the next registration with the next new AR. The value of $auth2$, generated by the HA, is sent with the BA message as well. The MN generates a hash value using $R2$ and compares it with the value of $auth2$. After a successful authentication, the MN resumes its uplink communication. When the old AR receives the HNot message, it responds by sending a Handoff Acknowledgement (HACK) to the new AR and starting the packets forwarding to the new CoA.

The BU message sent to the HA is intended to inform it about the new CoA and to send it the new generated random variables and a new SA to be used between it and the next new AR. The HA sends a BA message to the new AR and forwards the MN’s packets to the new CoA in case of triangular routing. This BA message contains the information required to authenticate the MN in the next registration. Upon the new AR receives this BA message it distributes the received data to the ARs in the current L3-FHR with MPN messages.

D. Security Considerations

Similar to MIPv6, it is highly recommended that the security between the current AR and the MN as well as between the current AR and the HA should be granted by means of ESP [15] in transport mode. The required SAs can be
generated by means of an AAA infrastructure or any other key distribution method. The data sent from the old AR to the ARs of the current L3-FHR should be secured using ESP in transport mode too. However, ESP depends here on the SAs established between these ARs and is the same for all MNs. The control messages exchanged between the old and the new AR should be authenticated using the SAs established between the ARs of the current L3-FHR, while the control messages exchanged between the MN and the new AR or between the new AR and the HA should be authenticated using the generated SAs during the handovers. The security consideration regarding the control messages exchanged between the MN and the HA / CN are the same as by MIPv6.

IV. SIMULATION RESULTS

A. Network Topology

In order to evaluate MIFAv6 compared to MIP and HAWAII (UNF scheme), ns2 [16] is used. The protocols are evaluated in a hierarchical topology, see figure 2.

Figure 2. The used network topology

A domain of 4 sub-domains that has the same structure is used. Each sub-domain contains 4 ARs. A GW interconnects the domain with the other nodes. The HA is situated outside the domain. There are 160 MNs in the domain. The active MNs communicate with 6 CNs. The distance between each two neighbour ARs is 198 m. The distance between the GW and each AR is 4 hops. The delay on a link between each two hops in the domain is 5 msec. The delay between the HA and the GW is 25 msec, while the delay between the GW and CN0, CN1, CN2, CN4, CN5 and CN6 is 27, 23, 28, 27, 23 and 28 msec respectively. All links have a bandwidth of 100 Mbit/s. During the simulation a certain MN is observed. This MN moves from AR0 to AR15 (in sub-domain D) at a speed of 40 km/h. The simulation is repeated 10 times, which results in 150 handoffs for each measurement.

B. Performance Evaluation under Dynamic Network Conditions

As known, the load in real networks as well as the speed of the idle and the active MNs changes randomly. In order to evaluate the above listed protocols under these situations, a down- and an uplink constant bit rate UDP stream with a packet length of 500 bytes between CN0 and the observed MN are used. The time interval between each two packets from these two streams is 20 msec. 59 other MNs are made active, while the other 100 still remain in idle mode. The active MNs communicate with the other CNs. UDP traffic is used too. All MNs except the observed one move randomly in the network and start sending and receiving data packets at random times and with a random time interval for each UDP stream.

Figure 3 presents the distribution function of the handoff latency experienced when deploying MIP, HAWAII and MIFAv6. The handoff latency on up- and downlink is defined as the time duration, after which the MN resumes its communication on up- and downlink respectively.

From this figure it can be seen that the handoff latency on uplink differs from that on downlink deploying MIFAv6. This is not the case for MIP and HAWAII. This can be interpreted through the definition of the handoff latency. The MN receives a BA from the new AR indicating the end of the handoff from the MN's point of view, while the handoff in the reality has not been finished. It can be clearly noticed that MIFAv6 outperforms the other both protocols with respect to the handoff latency. On uplink, about 50 % of the all handoffs by MIFAv6 are lower than 10 msec. This is because MIFAv6 requires only contacting the new AR to be able to resume its uplink communication. In addition, the uplink handoff latency experienced by MIFAv6 does not exceed 50 msec under all network conditions. Neither MIP nor HAWAII can achieve such a fast handoff.

Let now the downlink handoff latency be taken into account. Only about 2% of all handoffs experienced by MIFAv6 and HAWAII are comparable to each other. In all other situations MIFAv6 performs better. About 78% from all
handoffs can be finished in time duration lower than 70 msec by MIFAv6, while only 6% from the all handoffs can be finished in this duration deploying HAWAII. Compared to MIP, about 80% from all handoffs can be finished in a time duration that is less than 80 msec by MIFAv6, while all handoffs by MIP need more than 80 msec to be finished. From figure 3 it can be noticed too that 60% from the handoffs deploying HAWAII outperform their counterparts deploying MIP. In the rest 40%, which stand mainly for high loaded scenarios, HAWAII is outperformed by MIP. This can be interpreted through the fact that the control messages in HAWAII should be processed in the all routers on the way to the old AR, which makes the impacts of the load more than the impact by the other both protocols, which process the control messages only in the end nodes.

Our results have shown that the average handoff latency experienced by MIFAv6 in up- and downlink is only about 10% and 40% from the latency experienced by MIP and HAWAII respectively.

C. Impact of Network Load

In order to study the impact of the network load on the performance of MIFAv6, HAWAII and MIP, the number of the active MNs is selected to be 1, 10 30 and 60 active MNs in each scenario. The load in the network is not changed during the simulation. The other assumptions stay the same. Figure 5 presents the average number of the dropped packets per a handoff under different network loads.

From this figure it can be seen that there is a significant increase in the average number of the dropped packets when increasing the network load. Let the packets dropped on downlink be taken firstly into account, HAWAII functions well in low loads. However, its performance is worst in high loaded networks. The impact of the load on MIP is lower than on HAWAII. However, MIP remains outperformed by HAWAII. The minimum load’s impact is experienced by MIFAv6. Even under high loads, MIFAv6 functions very well and even comparable to HAWAII under low loads. On uplink, MIFAv6 is very efficient compared to the other both protocols. Even in high loaded networks, MIFAv6 remains better than the other both protocols in low loaded networks. The main conclusion resulting from figure 5 is that the load has a minimum impact on the performance of MIFAv6. Even under high loads, MIFAv6 still be able to achieve fast and seamless handoffs.

V. Conclusion

In this paper we have evaluated MIFAv6 compared to HAWAII (UNF scheme) and MIP. The evaluation comprises the studying of the performance under dynamic network conditions and the analysis of the network load impact. The evaluation is performed in a hierarchical topology by means of ns2. The main obtained results can be summarized as follows: MIFAv6 presents a mobility framework that can satisfy the requirements of the future “All-IP” networks. It achieves fast and smooth handoffs without making restrictions on the network topology and without introducing new intermediate nodes. MIFAv6 clearly outperforms HAWAII and MIP with respect to the handoff latency under dynamic network conditions. In contrasts to HAWAII and MIP, which drop on uplink more than on downlink, MIFAv6 drops on uplink less than on downlink. The load has a minimum impact on MIFAv6 performance on up- as well as on downlink. In addition, MIFAv6 achieves smooth handoffs even in high loaded networks.

Currently, we are studying the impact of the network load on TCP throughput and the impact of the speed on the performance using UDP as well as TCP traffic.

REFERENCES

[16] Network simulator ns-2, URL: http://www.isi.edu/nsnam/ns/