A Cross-layer Mechanism Based on Dynamic Host Configuration Protocol for Service Continuity of Real-Time Applications

Luis Rojas Cardenas
Universidad Autonoma Metropolitana
Vicentina DF, Mexico
e-mail: lmrc@xanum.uam.mx

Mohammed BOUTABIA
dept. wireless networks and multimedia services
Telecom Sudparis
Evry, France
e-mail: Mohamed.boutabia@it-sudparis.eu

Hossam AFIFI
dept. wireless networks and multimedia services
Telecom Sudparis
Evry, France
e-mail: Hossam.afifi@it-sudparis.eu

*Abstract***—Most important frameworks supporting mobile communications are not capable of meeting real-time application requirements because of the service degradation appearing during the handover process. Such degradation is mainly noticed as an excessive blocking time and a non-negligible packet loss rate. This is due to slow procedures for address allocation, too much packets exchanged by signaling procedures, and the delay required to establish a new end-to-end delivery path. Although these problems have been widely analyzed, and a number of solutions have been proposed, better handover performances are still needed. In this paper, we propose the introduction of some functionalities into access point equipments to improve the handover performances. These functionalities are based on the reduction of both the address allocation delay and the number of exchanged signaling packets, as well as the parallel execution of certain procedures. Our approach is implemented over the signaling mechanism of Dynamic Host Configuration Protocol (DHCP), from which extended options are used to convey information related to each procedure allowing mobile communication to be maintained.**

Keywords-component; mobility; cross-layer; real-time; DHCP;

I. INTRODUCTION

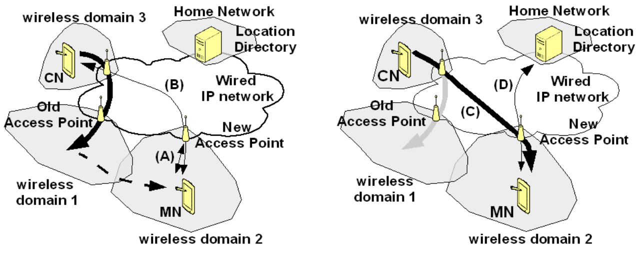
All As new wireless technologies are deployed and *Mobile Nodes* (MN) such as mobile phones, PDA, Internet tablets etc. acquire more hardware capabilities in terms of processing speed, communication and storage space, it is expected that wireless communications will be more heterogeneous and commonly based on IP protocol. However, to operate in such scenario, mobile nodes must be equipped with multiple wireless cards such as WIFI, WIMAX (*Worldwide Interoperability for Microwave Access*), UMTS (*Universal Mobile Telecommunications System*), etc. and special communication protocols able to cope with mobility. These capabilities will allow Mobile Nodes not only to communicate through different network technologies, but also to choose the most convenient one in case of several available networks; this latter characteristic is known now as ABC (*Always Best Connected*) capability.

In this context, it seems that Internet Protocol will play an important role in this world of heterogeneity and mobility in spite of the fact that it was not designed to handle mobility. Indeed, Internet protocols are not suitable for supporting mobile communications because of its principles for handling addressing and routing. They establish that any host address must be derived from the network address where it is physically attached as well as they do not consider that a host can change its attachment address at the middle of a session. Under such scheme, when a MN moves from its original network to a *Foreign Network* (FN), it will experience at least the following problems: 1) when it reaches a new network, any communication becomes impossible. Given that its address is not valid in the context of the foreign network, it can not be accepted neither by foreign nodes nor corresponding routers. Obtaining a new valid address from the foreign network is then necessary. 2) The ongoing communication associations are lost due to address inconsistency i.e. at operating system level each communicating system represents a communication association by means of a 5-tuple {*protocol*, *local-address*, *local-process*, *foreign-address*, *foreign-process*} [13]. If one of these elements becomes inconsistent, for example when a mobile node reaches a foreign network and a new *local address* is obtained, ongoing communications are lost. Nevertheless, informing the corresponding node about the new local address can help to recover the lost communication. 3) Mobile hosts disappear from the global network. Normally, hosts are found in the network by means of the *Location Directory* (LD). It is a distributed database containing the host name and its corresponding IP address which is known in the Internet world as DNS (*Directory Name System*). If one of the elements of this association changes without informing the LD, nobody in the network will be able to reach that host. That is what happens when a MN goes from one network to the other and MN changes its IP address. To keep in touch with the global net, MN must inform the LD each time it acquires a new IP address.

In order to cope with IP limitations in mobile communications, a number of approaches have been proposed. Although they tackle the problem from different perspectives [3][4][5], they agree on the way iit must be handled. Indeed, the main approaches relay on a number of procedures that can be classified on: 1) *network discovery and address allocation*, 2) *preservation of the ongoing communications* and 3) *update of the global location directory*. These three procedures and the problems they address are analysed in more detail in the following paragraphs.

First of all, when a node reaches a new network and discovers it by means of low level mechanisms, an *address allocation* phase starts. We consider that the MN starts this phase by sending an address request message to the FN. This phase finishes when the corresponding access point informs the MN about the allocated address by means of an acknowledge message (see label A in Figure 1.a).

In the second phase, as soon as MN obtains a new address and in order to maintain the ongoing communications, MN notifies the *correspondent node* (CN) about the new acquired address (Label B). Then, the CN immediately redirects the data flow to the new address (see Figure 1.b, label C). These two phases are the most critical ones. Actually they form what is known as *handover process*. In the third phase, the location tracking procedure is achieved to maintain the reachability of the MN at global network level. This is a less critical operation and it is achieved by updating the Location Directory (LD) with the new acquired address (see Figure 1.b, label D).



a) address allocation b) location tracking process

Fig. 1. Handover process

In this paper, we propose the introduction of new functionalities into access point equipments to improve the handover performances. Specifically, blocking times are minimized by reducing both the address allocation delay and the number of exchanged signaling packets. Additionally, parallel execution of certain procedures contributes to obtain a performance gain.

The remainder of this article is organized as follows. In Section II, we speak about the related work. The architecture of our approach is described in Section III and the corresponding performance analysis is presented in Section IV. Section V discusses security issues of our solution. The conclusion and future work are discussed in Section VI.

II. Related Work

By tacking into account the classification of procedure stated above, we analyse the most representative approaches for handling node mobility, in particular Mobile IP and SIP. The global performances around the handover process are especially important for this analysis.

A. Network Layer Perspective: Mobile IP

The main goal of *Mobile IP* (MIP) is to avoid upper layers to be worried about address changing due to node mobility. The principle is as follows: when the CN sends packets to the MN, it employs the home address of the MN so that packets arriving to the home network are intercepted by the *Home Agent* (HA) and sent to the Care-of-Address (CoA) via a tunnel. As this latter is associated to the FA, it receives the packets and redirects them to the MN. This mechanism allows a transparent application operation. Recent standards of IETF propose more sophisticated mobility schemes like MIPv6 [9] and Fast MIPv6 [10] but these standards cannot be widely deployed and have to wait the transition to IPv6.

Address Allocation

The mechanism for CoA acquisition relies on the services of the new FA, which periodically broadcasts a *Router Advertisement* message containing CoA related information. This mechanism has a drawback: the minimum broadcast period is one second [3]. A faster mechanism is based on *Router Solicitation* message which explicitly requests a *Router Advertisement*. This operation takes $2t_s$ and corresponds to the round-trip time between the MN and FA (see Figure 2).

Preservation of the ongoing communication

When the new CoA is obtained, the MN must inform its HA about the obtained CoA by sending a REGISTRATION message. After this registration, the HA can forward the packets (originally sent by the CN to MN's home address) to the FA by tunneling and then to the MN. This scheme generates what is known as *triangle routing*, which is characterized by the introduction of additional end-to-end delay. To reduce this delay the *Route Optimization* (RO) [8] can be used so the CN encapsulates packets directly to the current CoA without passing through the HA. This procedure is described in Figure 2.

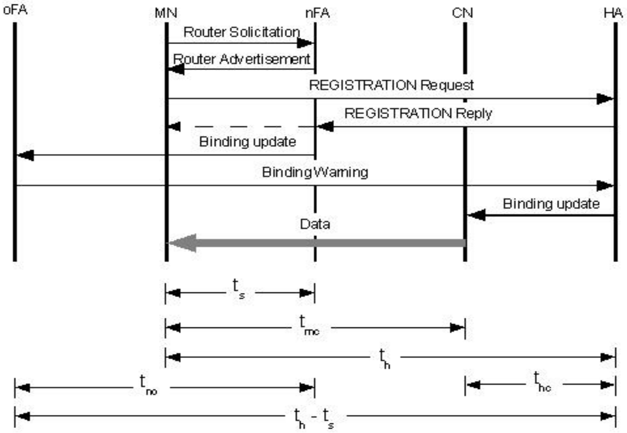


Fig. 2. Handover process in Mobile IP with RO.

The HA sends to the MN a REGISTRATION Reply message which is intercepted by the *new FA* (nFA) and then sent to the *old FA* (oFA) which sends a Binding Warning message to the HA. Finally the HA send a Binding update to the CN which starts sending data directly to the MN. Smooth Handoff [4] is an additional functionality that reduces the packet loss generated during the handover by means of a Binding Update between the nFA and the oFA. In accordance with [7], during the handover process, the service disruption time under MIP with RO is:

$$T_{mip\_inter} = t_{no} + 3t_h + t_{hc} + t_{mc} \tag{1}$$

Where t_{no} denotes the delay of a message between the new FA and the old FA, t_h is the delay between the MN and the HA, t_{hc} is the delay between the home network and CN, finally t_{mc} is the time that data takes to arrive from the CN to MN.

The smooth handoff starts after a delay of :

$$T_{mip\_smooth} = 2t_s + 2t_h + 2t_{no} \tag{2}$$

The Smooth Handoff avoids packets to be lost by redirecting packets from the old FA to the new FA before a handoff process is completely achieved. A tunnel created between these FAs undertakes this task.

Maintaining the global location tracking

There is no need to a global tracking registration in MIP since the HA is updated with the new CoA and the future CNs will use the original home address to reach the MN.

B. *Application Layer Perspective: S IP*

Handling mobility at transport and network layer requires considerable changes in the MN kernel. This is the main motivation for developing upper layers solutions, such as *Session Initiation Protocol* (SIP). SIP is capable of supporting terminal mobility, session mobility, personal mobility, and service mobility. Moreover, SIP has been widely accepted as the signaling protocol in emerging wireless networks. Therefore, SIP seems to be an attractive candidate for an application-layer mobility management protocol for heterogeneous all-IP wireless networks. However, SIP entails application-layer processing of messages, which may introduce considerable delay.

Address Allocation

After a MN discovers a new network by means of low level procedures, an address allocation phase starts. The procedure commonly used in this context is DHCP. Although this TCP/IP-based protocol was not designed to operate in mobile contexts, it is widely employed to support address allocation in access networks. This protocol relies on four different DHCP messages: DHCP Discover, DHCP Offer, DHCP Request, and DHCP Acknowledge, which are all UDP packets. DHCP satisfies most of non real-time applications but it appears to be unsuitable when it deals with real-time ones. The main problem here is related to the number of packets and the long delay that DHCP takes for address allocation. This latter is mainly caused by the address conflict checking mechanism based on ICMP Echo request and reply. A DHCP server has to send out an ICMP Echo Request to the address in question before responding to a Discover message. If nobody responds with an ICMP Echo Reply within a typical interval of 1 to 3 seconds, the DHCP server will send the Offer message. As far as the client is concerned, it performs a similar checking. In order to improve the performances of DHCP, there are some proposals to reduce the number of packets, from four to only two [2]. Others works suggest to remove the address conflict checking [17]. And finally, there are proposals to use new protocols for supporting address allocation more suitable for mobile applications, in particular, Dynamic Registration and Configuration Protocol (DRCP) [12].

Preservation of the ongoing communication

The procedure allowing MN to preserve its ongoing communications is known as *mid-call* procedure. The principle is the following: when the MN reaches a new network and a new address has been acquired, the MN sends a re-INVITE request to the CN. This operation is accomplished without intervention of any intermediate SIP proxies. This INVITE request contains an updated session description with the new IP address. The CN starts sending data to the MN's new location as soon as it gets the re-INVITE message.

In accordance with [6], the total handover delay in SIP must consider: the DHCP and ARP resolution delay, the updating delay of the LD or Home Registrar (HR), and the time the INVITE message takes from the MN to the CN and the time CN data take to reach the new MN location.

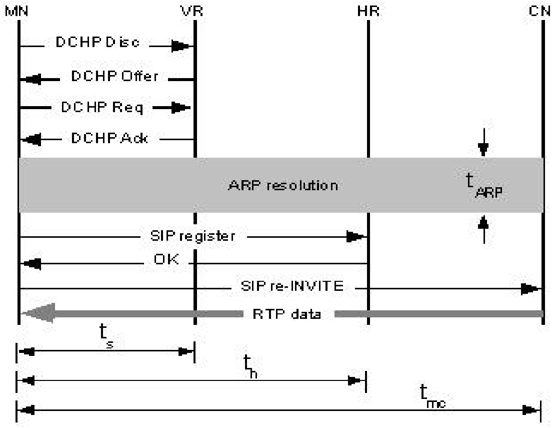


Fig. 3. Handover process in SIP

This total time T_{sip_inter} is given by:

$$T_{sip\_inter} = 4t_s + t_{arp} + 2t_h + 2t_{mc}. \quad (3)$$

Where $4t_s$ corresponds to the four messages exchanged by DHCP, t_{arp} is the time of address conflict checking, $2t_h$ is the time to update the HR and $2t_{mc}$ corresponds to the time the INVITE message takes, in addition to time for redirecting data from the CN to the new MN location.

One drawback of this approach is the packet loss rate during the handover process; which can also be seen as a period of disruption. While MIP solves this issue by implementing a smooth handoff, SIP lacks such a mechanism. Consequently all the packets transmitted during $2t_s + 2t_h + 2t_{no}$ will be lost.

Maintaining the global location tracking

The location tracking procedure is achieved by sending an update message to the home registrar which update the current location of the user agent allowing the future clients to reach the MN with the same URI.

III. The Fast Cross-Layer Handoff

In this section, we describe our proposal called *Fast Cross-Layer Handoff* (FCLH) [12], which is capable of improving the performances of mobile communication with respect to the approach described above [6]. The handoff improvement is obtained by following these three operations: i) the reduction of the address allocation delay, ii) the minimization of the number of exchanged signaling packets, and iii) parallel execution of certain procedures. These operations are accomplished in order to support the quality of service requirements imposed by voice over IP (VoIP) applications type. We integrate FCLH scheme to SIP mobility which is the most convenient mobility protocol for real-time applications as it was proven in [14], but it can be integrated to other application level mobility protocols.

A. *Overview*

Our approach is based on the idea that the three main procedures required to support mobile communications (see section I) can be achieved in parallel and started by only one message. Parallel processing is possible because it relies on three different entities: the Correspondent Node, the Location Directory and the two access points involved in the handover process. More specifically, CN is involved in the *preservation of the ongoing communication* (POC), The LD supports the *maintaining of the global location tracking* (MGLT) and the APs are responsible of the *address allocation* (AA) service and the smooth handoff procedure (SHP). In principle, these tasks are more or less independent, so they can be achieved in parallel. The only condition for doing so is breaking the classical layered protocol stack. In fact, this operation is commonly called cross-layer which opens up the possibility to introduce parallelism on the different tasks to maintain ongoing communications while speeding up the global performance of the handover process. In order to explain this principle, consider a MN reaching a new network. To obtain a new address, it exchanges DHCP messages with the visited network and then informs its home registrar about the new location using a SIP-register message. In Figure 4.a, we can see that DHCP and SIP can only operate in a sequential way because SIP cannot start updating its home registrar without knowing the new allocated address. This update is possible only after receiving the DHCP ACK message. In contrast, a cross-layer approach has less restriction; therefore the MN achieves two different transactions with only one DHCP message as shown in Figure 4.b; It not only negotiates a new address but also informs the HR about the new location.

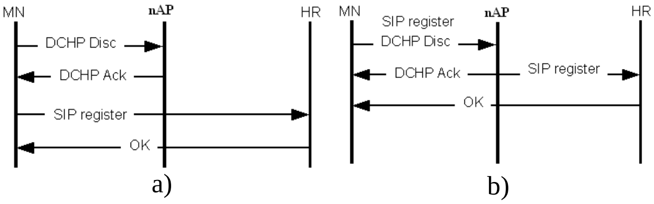


Fig 4. Classical vs Cross-layer protocol transactions.

Two advantages can be obtained from this approach: the number of exchanged messages is minimized and the handover delay is reduced. But this approach is possible at the expense of implementing some SIP functionalities in the different entities participating in the handoff process. In Figure 4.b, a SIP register message is built by MN and included in discovery message. The nAP completes the received SIP message with the missing information which is the new acquired address. At this level, some questions must be asked: Does DHCP allow to convey such information? Is the DHCP payload capacity enough to carry messages like SIP-messages? The answers are: First, DHCP has the option fields which have been created to convey vendor-independent options between client and server, so we can use these fields to convey SIP-messages. Second, the payload capacity of a DHCP message depends on the Maximum Transfer Unit (MTU) of the visited network. For WiFi networks, the MTU is 1492 bytes. So, there is no problem with SIP messages, for example, a re-INVITE message is more or less 140 byte long [6]. Following the principle stated above, Figure 5 proposes the FCLH mechanism and the interaction between the different entities.

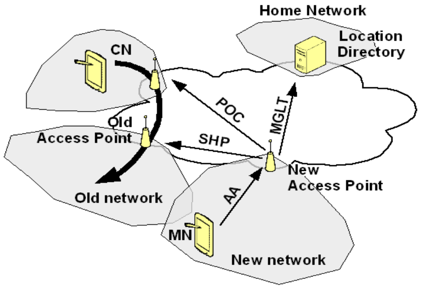


Fig. 5. A single message starts in parallel all the procedures required for handling mobility.

It should be noted that the cross-layer capacity is mainly supported by some functionalities installed on access points. The procedure is achieved as follows. Access points receive classical Discovery DHCP messages, which contain upper level information. The DHCP server installed on access points process and ask under the standard protocol but upper layer information contained in DHCP extended options is extracted and completed with the MN's new allocated address. Upper layer information corresponds to MGLT, SHP and POC procedures.

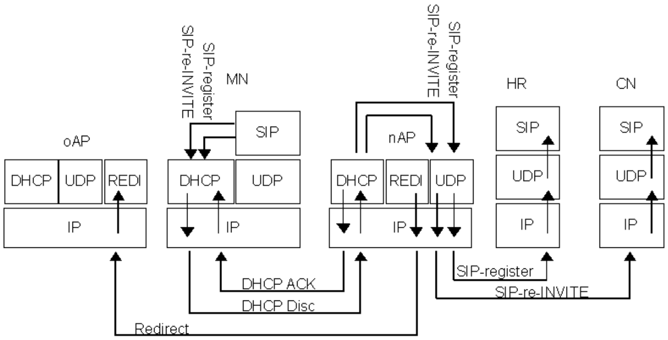


Fig 6, layered protocol stack.

A special procedure recovers this information and generates at least three data packets, which are sent to the corresponding network entities (see Figure 5 and Figure 6). As far as correspondent node and location directory are concerned, their protocol stack is not modified. Figure 6 represents the layered protocol stack of access point as well as the interaction with the MN and the other elements.

It should be noted that the cross-layer operation is mainly supported by MN and access points. Indeed, CN and LD do not require additional components or modifications to operate with FCLH. Moreover, a MN equipped with our approach can operate on networks that are not equipped with FCLH. In this case, MN can distinguish the absence of the FCLH infrastructure in the new visited network by means of the options included in DHCP ACK packets. In a similar way, a network equipped with FCLH can operate with any standard DHCP client.

Now, as in our approach a handover process is started by sending only one packet from MN to the discovered access point, this packet must to convey information corresponding to the POC, the MGLT and the SHP processes. The POC process is started by a SIP re-INVITE message, whereas the MGLT process requires a SIP register message. As far as SHP process is concerned, it is not related to SIP. It is an optimization mechanism similar to that proposed in low latency handoffs in MIPv4 [15]. It supports smooth handover by creating a tunnel between old and new access routers. This tunnel is used to convey the packets that were intended for MN when it was unreachable during the physical handover. The information that should be known to previous access router to perform an SHP is the new access router address so that the tunnel can be initiated. As far as the AA process is concerned, it is essentially supported by a DHCP procedure. The protocol stack of a MN with FCLH capacities is represented in Figure 7.

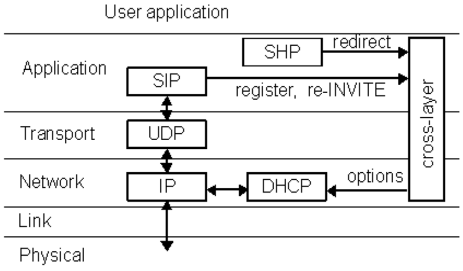


Fig 7. Protocol Stack at Mobile Node.

SHP and SIP modules insert the necessary information allowing the handover process to be started. This information is inserted in the DHCP-DISCOVER message by means of the cross-layer. All the information related to MGLT, POC and SHP processes are sent in a single packet. However, in the downlink, responses related to those procedures are processed normally and sent directly to the MN.

Figure 8 represents the protocol stack of the access point. This stack is responsible for dispatching the information contained in the DHCP-DISCOVER message, and then it rebuilds each message by filling the destination address with the new allocated IP address. Finally, the nAP sends all the messages to the appropriate correspondent modules at once.

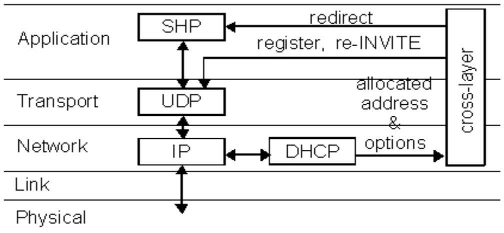


Fig 8. Protocol stack at Access Point.

Address allocation

After MN discovers a new network by means of low level procedures, an address allocation phase starts. In the context of FCLH, the protocol used is DHCP as proposed in [2]. This document proposes to reduce, from four to two, the number of messages required to allocate an IP address by DHCP server. To eliminate *duplicate address detection* (DAD) delay we implement a scheme of address reservation in advance. Under this scheme, a process running in the access point reserves a number of addresses and keeps them alive by running the DAD in the background. Moreover, our proposal is a full compatible approach: a MN with our solution can operate in classical DHCP context. A node can distinguish between a FCLH context and a classical context by the options contained in the DHCP ACK. If the MN realizes that DHCP ACK does not include the options it waits for, then it starts a classical procedure. On the other hand, when a classical DHCP server receives DHCP messages with extended options, it just drops the options it does not know and continues a classical procedure. Figure 9 shows the AA procedure in FLCH.

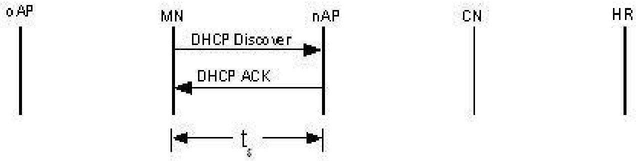


Fig. 9. Address allocation with DHCP-FCLH.

Under this address allocation scheme, an address can be obtained from the *new access point* (nAP) in only $2t_s$, where t_s is the delay of the channel connecting the MN and the access point.

Preservation of the ongoing communication

At the same time, the DHCP ACK message is sent to the MN, SIP re-invite message is sent to the CN. Indeed, the access point builds a SIP message by using the information contained in the extended option of the DHCP Discover message. To send this message, the AP acts as a router and emulates the SIP re-INVITE message as if it was sent by the MN. This is possible because the access point decides which address will be allocated to the MN, from the list of reserved addresses. Once the SIP re-INVITE message has been accepted by the CN, it finally sends an OK response to the MN. The different events of the handover process are described in Figure 10. It should be noted that this approach is cross-layer because in this case, a link layer message generates a SIP re-INVITE message without respecting the classical sequence of events neither the hierarchy of the protocol layers.

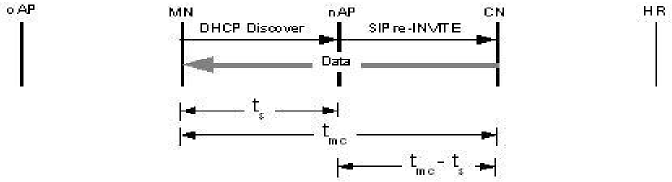


Fig. 10. Preservation of the ongoing communication: the handover process.

The service disruption time during the handover process is as follows:

$$T_{fclh\_inter} = t_s + (t_{mc} - t_s) + t_{mc}$$
$$T_{fclh\_inter} = 2t_{mc} \quad (5)$$

The Smooth handoff in FCLH is achieved by redirecting the data packets received by oAP to the nAP before the CN knows that MN has changed its network attachment point. The nAP requests this service to oAP by means of a special message which contains both the old and the new address of the MN. In contrast to MIP, our approach does not require the establishment of a tunnel and the encapsulation of the original data flow. This method improves the procedure performance and simplifies the implementation.

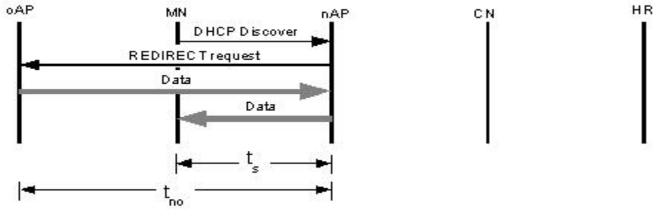


Fig. 11. Smooth handoff in FCLH.

More specifically, the access point has to change only the IP header of the packets, recalculate the CRC (Cyclic Redundancy Check) and finally redirect the data flow to the new MN address (Figure 11). The time required to obtain the smooth handoff is calculated as follows:

$$T_{fclh\_smooth} = t_s + t_{no} + (t_{no} + t_s)$$
$$T_{fclh\_ smooth} = 2t_s + 2t_{no} \quad (6)$$

Maintaining the global location tracking

Once again, the SIP Register message is generated by the access point after the reception of the message DCHP

Discover. The Information contained in this message as well as the address chosen by the access point are used to generate a SIP Register message. The MGLT process is described in Figure 12.

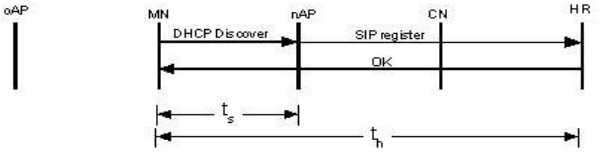


Fig. 12. Maintaining the global location tracking.

The delay required to update the LD, or HR in the context of SIP, is only t_h.

IV. Performance evaluation

In this section, our discussion is based on the above analysis. More precisely, this work compares the performances of MIP and SIP for an application of voice over IP (VoIP). So, the test conditions used here are the same as those considered in [6]. We assume t_s = 10 ms which corresponds to a relative low bandwidth for the wireless channel. For the wired network connecting wireless access points, we consider a more important bandwidth, then a smaller delay t_{no} = 5 ms. On the other hand, we suppose that processing time of the different entities is negligible.

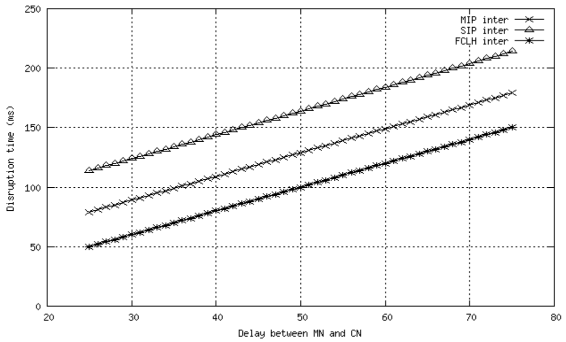


Fig 13. Disruption time vs. delay between MN and CN.

We take three different configurations. In the first one, the MN is connected to the network via a wireless channel and the distance of the CN varies. In the second configuration, the CN and the MN are close but the distance from the MN's home network varies. Finally, in the last configuration the delay of the wireless channel varies. In Figure 13, we can see that the disruption time increases as the delay t_{mc} between the MN and CN increases. In Figure 14, t_h increases, t_{mc} = 25 ms, and the wireless link delay is equal to 10 ms. Observe that the disruption time associated to SIP becomes smaller than MIP as the delay between MN and its home network increases. MIP disruption time increases because the handover delay depends on the registration within the HR. As far as our approach is concerned, the handover process depends on the delay between the CN and the MN only. That explains why the disruption time is constant.

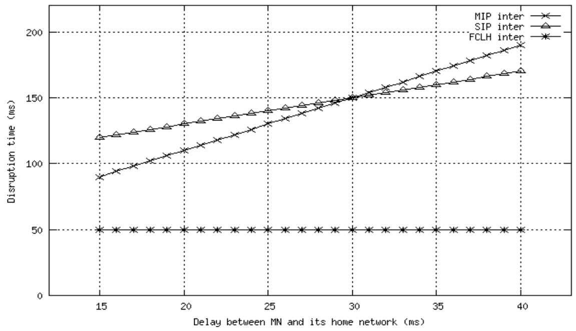


Fig 14. Disruption time vs delay between the MN and its home network.

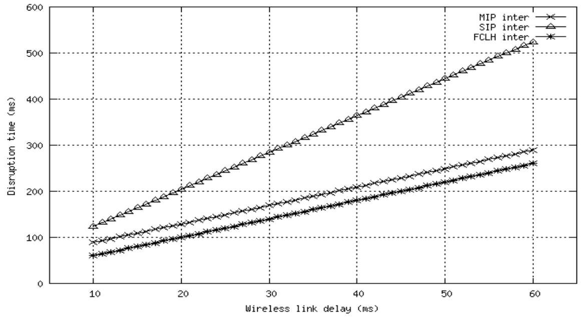


Fig. 15. Disruption time vs. wireless link delay.

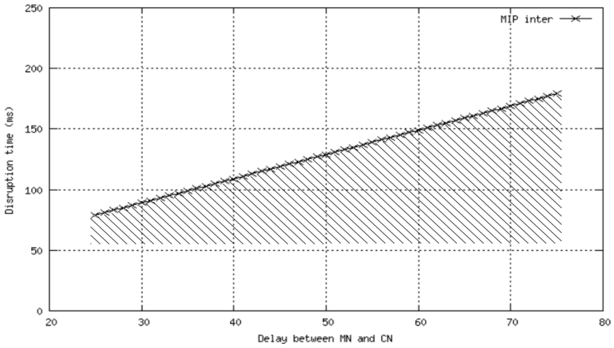


Fig. 16. Smooth handoff area for MIP.

Finally, the last scenario demonstrates the impact of the wireless delay on disruption time (see Figure 15). We can see that the impact of this parameter is limited on the total handoff delay in the case of FLCH. This result is due to minimization of signaling packet exchange over the wireless channel during the hand over.

As far as smooth handoff is concerned, MIP takes advantage over SIP which lacks this mechanism. By taking into account t_{mip_smooth}=2t_s+2t_h+2t_{no}, the MN in MIP starts receiving data packets before the handover is accomplished. This period can be calculated as being T_{mip_inter}–T_{mip_smooth}=T_{mip_inte} –54 ms (see Figure 16). In our approach $T_{fclh\_handoff}$ = 2t_s + 2t_{no}, therefore the MN receives forwarded packets for a period of time equal to T_{fclh_inter} -$T_{fclh\_handoff}$ = $T_{fclh\_inter} - 30$ ms (see Figure 17).

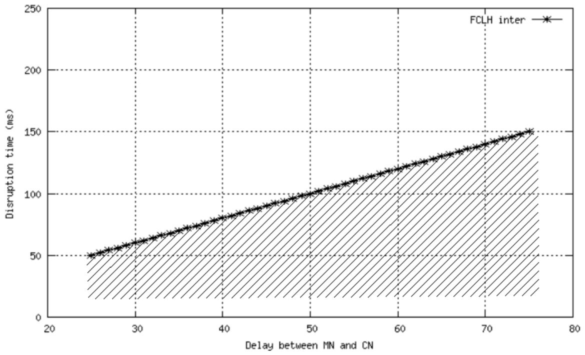


Fig. 17. Smooth handoff area for FCLH.

The smooth handoff period starts earlier in our approach than in MIP, that is to say, we can recover packets earlier and for more time before the handover is accomplished. On the one hand, the smooth handoff should start as soon as possible in order to avoid damaging the user perception. On the other hand, the faster the smooth handoff occurs the smaller the buffer size allocated to packet collection before redirection in the AP is.

V. Security Considerations

Since our scheme rely on DHCP, it is mandatory to secure the access to DHCP service by authenticating the clients and encrypting the payload witch contains parameters related to the current session. Malicious client can generate a lot of address requests to prevent the legitimate users from acquiring their IP addresses. The second attack is when a malicious DHCP server in the network answers to client requests and provides bogus configuration that prevent them from using network resources normally. As we talk about mobility in wireless networks, the first thing that should be carefully secured is the physical medium with adequate authentication and encryption protocols so that only authorized client can access physically the network. To overcome DHCP weakness, IETF proposed an authentication option [11] for DHCP messages. This option allows only authorized client to request for address configuration and allows for the clients to authenticate the server identity. Moreover, the threat can still come from classical DHCP users since the critical point is maintaining a pool of addresses ready for use by mobile hosts. We propose to reduce the lease for these addresses compared to addresses intended for non mobile nodes. We also have to encrypt the DHCP option containing information related to the different operations to prevent man-in-the-middle attacks.

VI. Conclusion

In this paper, we proposed the introduction, into access point equipments, of some functionalities to improve the handover performances. These functionalities are based on the reduction of the address allocation delay, the number of exchanged signaling packets as well as the parallel execution of certain procedures. Our approach is implemented over the signaling mechanism of DHCP in such a way that the proposed functionalities can be used by means of extended options. The obtained results indicate that our approach can reduce the handover delay with respect to most popular and already improved approaches such as MIP with Route Optimization as well as SIP. Moreover, our proposal does not require the introduction of additional entities in the network neither modifications in the current protocol stack, and in contrary to certain approaches, which do not consider the address allocation delay in the calculation of their results, we consider this problem and solve it. Finally, we presented the main attacks that threaten our system, and proposed some methods to make it more secure. Future research will be orientated to the simulation of this approach and its study in more heterogeneous context.

References

[1] L. Rojas-Cardenas, M. Boutabia, and H. Afifi "an infrastructure-based approach for fast and seamless handover", 3rd International Conference in Digital Telecommunications ICDT 2008, Bucharest, 29 June -6 July 2008.

[2] Park, S., Kim, P., and Volz, B., "Rapid Commit Option for the Dynamic Host Configuration Protocol version 4 (DHCPv4)," RFC4039, IETF, March 2005.

[3] M. Handley, H. Schulzrinne, E. Schooler, and J. Rosenberg. SIP: Session Initiation Protocol. rfc 2543, IETF, March 1999.

[4] C. Perkins, "IP Mobility Support", RFC 2002, Internet Engineering Task Force, October 1996

[5] A. C. Snoeren and H. Balakrishnan, "An End-to-End Approach to Host Mobility", 6th IEEE/ACM Mobicon 2000. Boston, August 2000.

[6] N. Banerjee, W. Wu, and S. K. Das,"Mobility Support in Wireless Internet", IEEE Wireless Communications, October 2003.

[7] T. T. Kwon, M. Gerla, S. Das, S. Das, "Mobility Management for VoIP Service: Mobile IP vs. SIP", IEEE Wireless Communications, October 2002.

[8] Nen-Chung Wang and Yi-Jung Wu, "A Route Optimization Scheme for Mobile IP with IP Header Extension", IWCMC'06, Canada, July 3-6, 2006.

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

[10] R. Koodli, "Fast Handovers for Mobile IPv6", RFC 5268, IETF, June 2008

[11] R. Droms, W. Arbaugh, "Authentication for DHCP Messages", RFC 3118, IETF, June 2001.

[12] A. McAuley et al., "Dynamic Registration and Configuration Protocol (DRCP) for Mobile Hosts," Internet draft, draft-itsumo-drcp-01.txt, July 2000, work in progress.

[13] W. Stevens. UNIX Network programming. Prentice Hall

[14] S. Mohanty, F. Akyildiz "Performance Analysis of Handoff Techniques Based on Mobile IP, TCP Migrate, and SIP", IEEE Transactions on Mobile Computing, VOL.6, NO.7, July 2007.

[15] K. El Malki "Low-latency Handoffs in Mobile IPv4", RFC 4881, IETF, June 2007.