A Low-Cost and Low-Latency Approach for Inter-domain Mobility Management

Nivia Cruz Quental and Paulo André da Silva Gonçalves
Department of Computer Science, Centro de Informática (CIn)
Universidade Federal de Pernambuco (UFPE)
Recife, Brazil
Email: ncq@cin.ufpe.br, pasg@cin.ufpe.br

***Abstract*—Providing an inter-domain handover solution for PMIPv6 that achieves a low signaling overhead and a low handover latency remains a major challenge. In this paper, we respond to this challenge by proposing the Clustered Inter-domain PMIPv6 (CI-PMIPv6). CI-PMIPv6 takes advantage of the following: the use of Peer-to-Peer (P2P) techniques; the use of a clustering technique; and the execution of inter-domain handover-related operations in parallel with the execution of intra-domain handover-related operations. By doing so, CI-PMIPv6 allows the fast spread of Mobile Node (MN) information among Local Mobility Anchors (LMAs) from different domains during intra-domain handovers, thereby avoiding the need for extra signaling to request and obtain such information during inter-domain handovers. CI-PMIPv6 boosts the performance of inter-domain handovers. We support this statement by providing a comparative study of the performance of CI-PMIPv6 and related work. Additionally, we apply the design concepts of CI-PMIPv6 to Fast handovers for Proxy Mobile IPv6 (FPMIPv6). This results in a new proposed protocol, namely CI-FPMIPv6 (Clustered Inter-domain FPMIPv6), which also achieves a notable performance.**

Keywords–CI-PMIPv6; CI-FPMIPv6; P2P; Mobility; Inter-domain.

I. INTRODUCTION

The Proxy Mobile Internet Protocol version 6 (PMIPv6) is an IETF standard for network-based mobility management. PMIPv6 is mainly designed to overcome issues encountered in Mobile IPv6 (MIPv6) related to energy consumption of the Mobile Node (MN) and the latency incurred in intra-domain handovers. PMIPv6 introduces two types of network entities: the Mobile Access Gateway (MAG), which tracks the current location of the MN; and the Local Mobility Anchor (LMA), which plays a similar role as the MIP's Home Agent in a local domain. Signaling between MAG and LMA is responsible for updating the binding of the MN. A downside of PMIPv6 is that it has no support for inter-domain mobility. This occurs because it relies on a non-mobile entity to keep track of the MN.

There have been many contributions to the problem of giving inter-domain mobility support to PMIPv6 (e.g., [1],[2],[3],[4],[5]). Recently, the Clustered Inter-domain PMIPv6 (CI-PMIPv6) [1] has emerged as a low cost and a low latency intra- and inter-domain handover solution. CI-PMIPv6 makes an inter-domain handover possible because it spreads information on MNs among LMAs from different domains. However, the information spreading is anticipated and happens during intra-domain handovers. In this manner, this information will be rapidly available to those LMAs in subsequent inter-domain handovers. This, in turn, greatly saves inter-domain handover costs and latency. The main characteristics of CI-PMIPv6 are:

- **Distributed mobility management** - LMAs from each domain form a cluster, which is a Kademlia-based DHT [6] so as to spread information efficiently; this avoids the use of global entities and, thus, avoids creating single points of failure and performance bottlenecks;
- **Network-based handover** - CI-PMIPv6 maintains the PMIPv6 advantage of reducing MNs' consumption of energy by avoiding host-based handover signaling and processing overheads;
- **Reuse of existing PMIPv6 entities to exchange inter-domain information** - the compatibility with PMIPv6 legacy systems is achieved; no new entity needs to be added to the system;
- **Anticipation of MN information for future handovers** - during the MN's ongoing handover, its current LMA proactively spreads the MN information to neighbor LMAs in the cluster; this information is needed for future inter-domain handovers and is rapidly available to neighbor LMAs, thereby avoiding wasting time during such handovers due to the extra signaling needed to request and obtain such information.

Previous research in inter-domain support for PMIPv6 focuses on different strategies. Joe *et al.* [2] propose modifying the MAG function at the boundary region between two domains to reduce inter-domain signaling overhead. In the proposal of Neumann *et al.* [3], the LMA continues to manage the MN until the end of the session, even if the MN visits a new domain and relies on a centralized entity to keep track of the location of the MN. Zhong *et al.* [4] propose a solution that relies on a centralized entity to store and update the information of the MNs while they visit other domains. Park *et al.* [5] present a scheme that forwards all PMIPv6 signaling messages from a LMA in the local domain to an LMA in another domain in order to accomplish inter-domain handover. These proposals exhibit one or more issues such as: a high cost of signaling; the lacking of inter-working capability with legacy systems; high handover latency; and the use of centralized entities. CI-PMIPv6 is designed to add inter-domain handover capability to PMIPv6 and overcome these issues.

This paper is an extended version of the study presented in [1]. We present the CI-PMIPv6 protocol in a more detailed

fashion. In particular, our motivation for using a Kademlia-based protocol for cluster management is discussed and a more detailed description of the cluster behavior is provided. We also apply the concepts of CI-PMIPv6 to Fast handover for Proxy Mobile IPv6 (FPMIPv6). This allows us to introduce a new protocol, namely Clustered Inter-domain FPMIPv6 (CI-FPMIPv6). We also improve the study presented in [1] to include a performance evaluation of CI-FPMIPv6. The remainder of this paper is organized as follows: Section II presents the PMIPv6 protocol and some of its most known extensions. Section III presents the state of the art on inter-domain mobility in PMIPv6-based networks. Section IV presents in detail the CI-PMIPv6 and CI-FPMIPv6. Section V presents a theoretical comparison among CI-PMIPv6, CI-FPMIPv6 and other solutions found in the literature. Section VI compares the performance of both CI-PMIPv6 and CI-FPMIPv6 with that of other proposals. Section VII presents the conclusions of this paper. Future research is presented in Section VIII.

II. *Proxy Mobile* IPv6 (PMIPv6) AND EXTENSIONS

One of the main challenges in IP mobility management is to achieve seamless and low-latency inter-domain handover. Mobile IP (MIP) is the best-known IP mobility standard ever released by IETF, in which an MN maintains its original IP address while it moves beyond its *Home Network*. MIP has versions for IPv4 and IPv6. Since MIP assumes that MNs must have the MIP protocol implemented in their operational systems and communicate with the *Home Network* whenever a handover occurs, high energy consumption and high latency are noteworthy issues.

PMIPv6 is mainly conceived by IETF in order to surmount these issues. PMIPv6 introduces two local entities: a MAG and an LMA. Signaling exchanged between the MAG and the LMA is responsible for the binding update of the MN. Thus, the LMAs and MAGs from the corresponding domain are responsible for mobility management instead of the MNs. Figure 1 presents the PMIPv6 architecture. The MAG tracks the current MN location. The LMA is responsible for the binding updates and assigns IP prefixes to the MNs in its domain.

Figure 2 presents the signaling flow for a PMIPv6 handover. When the MN moves away from an area managed by a previous MAG (PMAG) and enters an area managed by a new MAG (NMAG), a handover in the IP layer takes place. The MN sends the `Rtr Sol` message, which comes from the Internet Control Message Protocol (ICMP), to ask the closest NMAG for a route to the external network. The NMAG sends a *Proxy Binding Update* (`PBU`) message to its LMA that sends the *Proxy Binding Acknowledgment* `PBA` message to the PMAG. Finally, the NMAG announce a new route sending the ICMP message `Rtr Adv` to the MN.

The *Fast handovers for Proxy Mobile IPv6* (FPMIPv6) [7] protocol is an extension for PMIPv6 that aims to reduce packet loss. It adds a buffering scheme and a tunnel set up between the PMAG and the NMAG while signaling is exchanged. FPMIPv6 can operate in two modes: reactive or predictive. Figure 3 presents the reactive mode. After the MN enters in the new network, the NMAG and the PMAG send, respectively, the `HI` (*Handover Indication*) and `HACK` (*Handover Acknowledgment*) messages to set up a tunnel. The packets stored in the NMAG's buffer must be forwarded to the

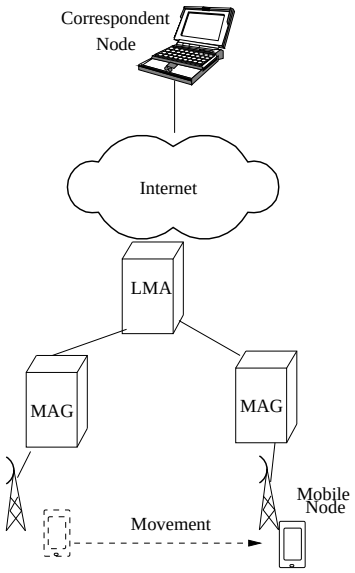

Figure 1. Architecture of PMIPv6.

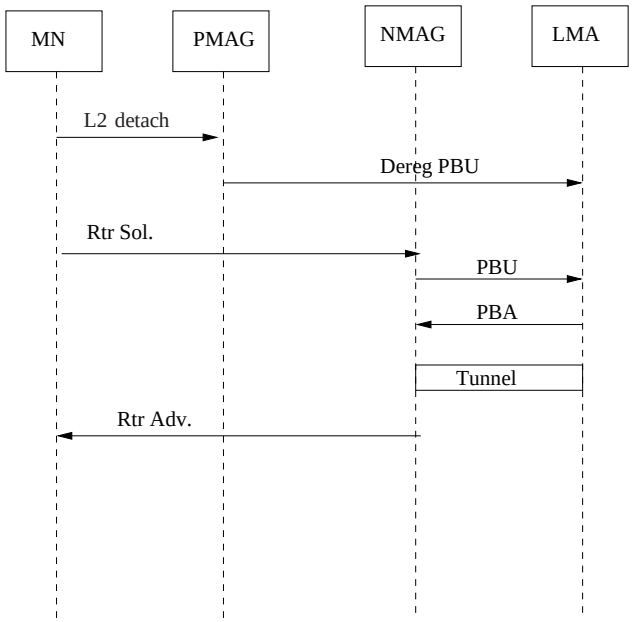

Figure 2. Signaling flow for PMIPv6.

MN when the handover is complete. Then, the NMAG and the LMA exchange the `PBU` and `PBA` messages as in PMIPv6.

In the predictive mode of the FPMIPv6, the tunnel between the PMAG and the NMAG is set up before the MN enters the new network as depicted in Figure 4. In that case, the PMAG sends the `HI` message to initiate a tunnel set up. Then, the NMAG responds with the `HACK` message. The PMAG can locate the chosen NMAG using a table that maps the address of Points of Attachment (PoA) - provided by the MN - to the corresponding MAG. The rest of the signaling is similar to that of the PMIPv6.

According to the RFC 5949 [7], the FPMIPv6 is designed to minimize packet loss during handover in comparison to PMIPv6. However, because of the increase of the signaling

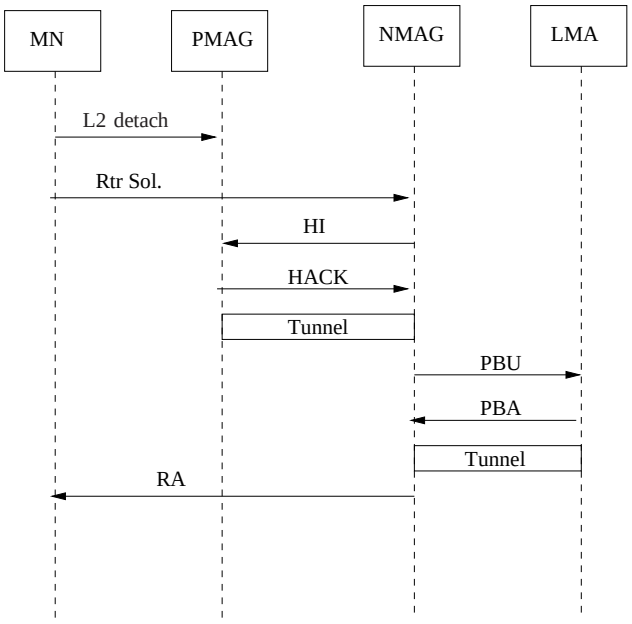

Figure 3. Signaling flow for the FPMIPv6 in the reactive mode.

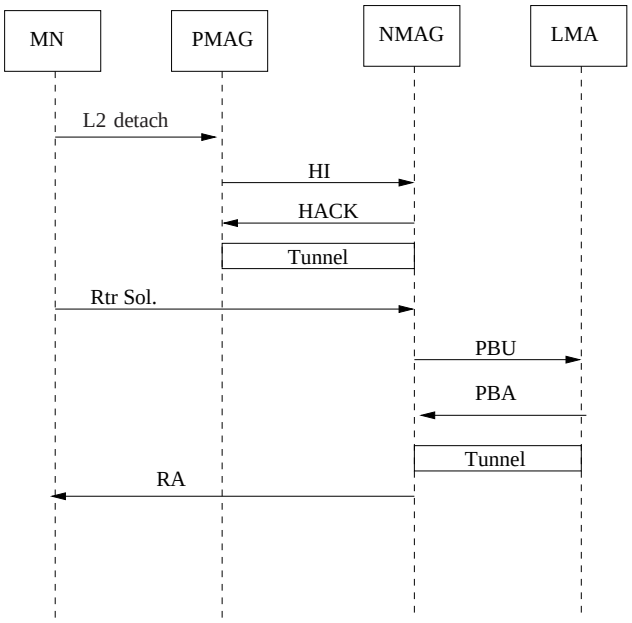

Figure 4. Signaling flow for the FPMIPv6 in the predictive mode.

overhead, the handover latency may become greater. The main advantage of the reactive mode is that it is not necessary to get the PoA information, since the handover in the link layer has already happened. On the other hand, the predictive mode can lead to a lower packet loss.

III. State of the Art on Inter-domain mobility

A wireless domain can be defined as the logical representation of a wireless access network [8]. It is related to a coverage area where the same company controls the authentication and reliability of the network entities. Unlike MIPv6, PMIPv6 and its extensions do not have knowledge about other networks outside their domains, as a MIP's Home Agent would. The MIP's Home Agent can access other domains thanks to the MN, which informs about its new location to its home network. In PMIPv6 the MN does not have this responsibility, thus, it is not possible to keep track of the node outside its domain. Providing inter-domain mobility for PMIPv6-based systems has been the object of ongoing research. In the following sections, the main approaches for inter-domain mobility are presented.

A. Decentralized approach

Park *et al.* [5] present a scheme where the LMA from a domain forwards the handover signaling to the LMA in another domain to achieve inter-domain handover. There are neither protocol modifications nor additional entities. Figure 5 shows the signaling flow. The MN is responsible for requesting the authentication. Each domain has its own Authentication, Authorization, and Account (AAA) service. There must be an extra tunnel between those LMAs. The signaling messages of PMIPv6 are replicated in communication with PLMA, NLMA, and AAA serves, which increases signaling cost. Additionally, the extra header in IP-in-IP tunneling increases the packet delivery overhead.

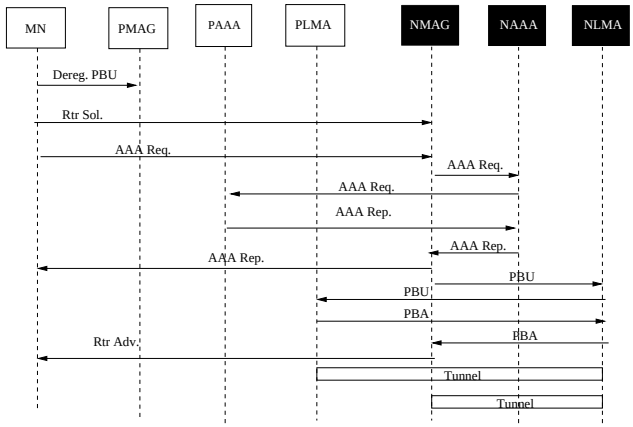

Figure 5. Inter-domain handover in the decentralized approach.

Simulations with QualNET [9] evaluate packet loss and latency in comparison with those of a scheme in which PMIPv6/MIPv6 inter-works. The authors state that the proposal is better suited for scenarios where handover is frequent.

B. LMA as session anchor

In I-PMIP [3], the original LMA keeps managing the node until the end of the session and exchanges signaling with the MAG in the new domain during inter-domain handover. That LMA is called the Session Mobility Anchor (SMA). It is assumed that LMAs from different domains already know each other and are physically close to each other. To locate the MAG in the new domain, the original LMA relies on a centralized entity called the Virtual Mobility Anchor (VMA), which undertakes location updates whenever a handover takes place. Hence, that solution faces a single point of failure issue. The authors state that I-PMIP sees to it that the policies of different domains remain transparent since there is no direct connection between MAGs from different domains.

Figure 6 presents the signaling flow for I-PMIP. When a MN moves to a new domain, the NMAG detects its presence and sends a PBU message to the new LMA. Then, the new LMA forwards the request to the VMA, which is updated whenever a MN moves to a new domain. The SMA forwards the data to the new LMA, which creates a tunnel to the new MAG.

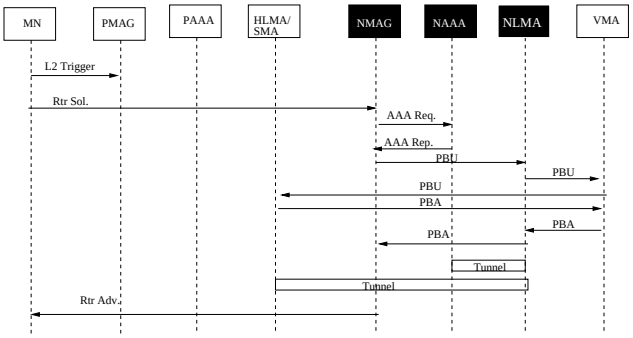

Figure 6. Inter-domain handover in I-PMIP.

The authors evaluate the performance of I-PMIP through a theoretical analysis that compares the latency of I-PMIP with that of MIP, PMIP and a hierarchical approach that uses MIP. According to [3], I-PMIP has proven to be more efficient in the scenarios studied. In addition, the authors state that I-PMIP has lower handover latency. However, we should take into consideration that the VMA introduces a single point of failure and an additional tunnel increases the packet delivery overhead. Nyguyen and Bonnet propose a similar solution in [10] focusing on routing optimizations.

C. Centralized entity

Zhong *et al.* propose the Enabling Inter PMIPv6 Domain Handover (EIPMH) [4]. The authors introduce the Traffic Distributor (TD), which is an entity that redirects data to the LMA while the MN is out of the original domain. The TDs are statically configured and have knowledge about other TDs, their IP prefixes, and mapping to the LMAs. In that proposal, the TD is responsible for assigning prefixes to its MNs instead of the LMA. The NLMA must send a query PBU_Forwarding to the PLMA to find additional information about the MN and the TD responsible for communicating with the Internet. The TD also creates a tunnel to the NLMA. Also, there are tunnels between LMAs and between the NLMA and the MAG. The authors acknowledge that there may be more than one distributor, each of which is responsible for a coverage area. Nevertheless, the handover between distributors is not covered by the authors.

Figure 7 presents the signaling flow for EIPMH. After the NMAG registers the MN using the PBU message, the NLMA queries the previous LMA using a PBU_Forwading message in order to get additional information about the MN and the TD that connects the network to the Internet. The PLMA replies with a PBA message. Then, the NLMA forwards the received MN information to the NMAG. A tunnel is set up between the TD and the NLMA. Another tunnel is set up between the PLMA and the NLMA.

The NS-2 simulation tool is used to evaluate performance. Latency and throughput are compared to those of I-PMIP.

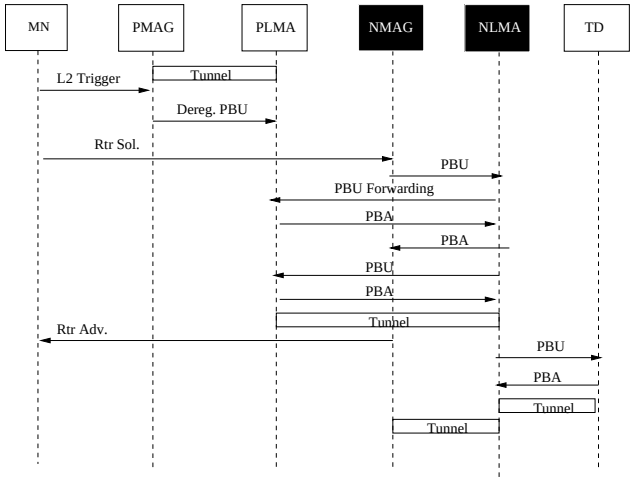

Figure 7. Inter-domain hanover in the EIMHP scheme.

However, the evaluation does not consider the extra overhead derived from the tunnel between the TD and the NLMA. The process of finding the PLMA, the lookup for the NLMA, and the change of MAGs are not considered.

Since EIPMH introduces two extra tunnels to the PMIPv6, it is expected an increase in the packet delivery overhead. A similar proposal can be found in [11], in which the solution is called GPMIP.

D. MAG Specialization

Joe *et al.* [2] present an inter-domain approach based on an architecture that considers special types of MAG: the Boundary and Overlapping MAG (BMAG and OMAG, respectively). The BMAG is associated with only one LMA, while the OMAG is associated with more than one domain. Both are found in regions where a domain ends and another domain begins. Also, only one authentication entity for all domains is considered. The presence of a gateway guarantees maintenance of the IP address. The authors propose two solutions: Reactive and No-Gap. In the Reactive solution, a path is created between CN and PLMA and NLMA. The BMAG discovers a NLMA by geographically locating it. The authors do not specify how the lookup is done. The functionality of the BMAG is shared with edge routers. A tunnel must be created between the gateway and the NLMA, between LMAs, and between the PLMA and the NMAG. In the No-Gap approach, the OMAG has information from both domains and creates two simultaneous paths as the MN enters its area. Thus, the MN receives redundant information from both LMAs. Besides the PMIPv6 messages, extra signaling is exchanged between the NLMA and the gateway to confirm and obtain additional information about the MN. Additionally, the NLMA must authenticate the MN. A tunnel must be created between the gateway and the NLMA, and between the NLMA and the OMAG. The No-Gap approach requires changes in legacy border routers and generates redundant data packets in the same MAG, coming from different LMAs.

Figure 8 presents the signaling flow for the *no-gap* approach. Beside the traditional PMIPv6 signaling, the messages FBD and FBDA are exchanged between the NLMA and the gateway to request and retrieve additional information about

the MN. Additionally, the NLMA is responsible for requesting the authentication on behalf of the MN. A tunnel between the gateway and the NLMA is set up in addition to the tunnel between the NLMA and the OMAG. It is worth to notice that the same OMAG is shared by both the previous and the new domains.

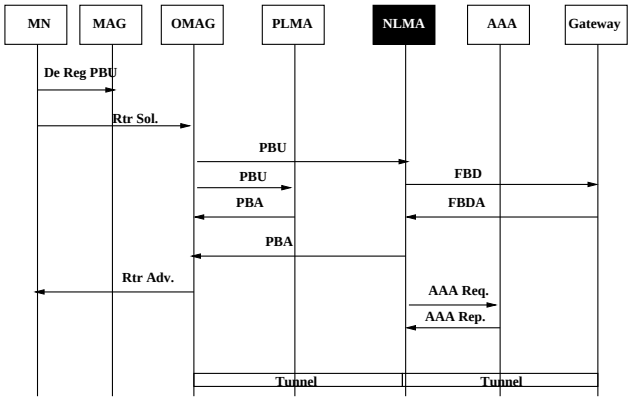

Figure 8. Inter-domain handover in the No-Gap scheme.

The evaluation of the performance compares the solution with MIPv6, Fast Handovers for MIPv6, I.PMIPv6, and EIPMH by measuring handover latency. What may well be noticed is that the Reactive mode leads to greater overheads because of an additional tunnel in comparison to the No-Gap model. According to the authors, the No-Gap model is the most efficient model. This is why this paper gives more focus to the No-Gap solution, which has a counterpart in [12].

IV. CI-PMIPv6 Overview

The architecture of CI-PIMIPv6 is depicted in Figure 9. This architecture makes the communication among LMAs from different domains possible. CI-PMIPv6 organizes LMAs in a structure called *cluster*, which is a P2P network. The data structures shared in the cluster represent the up-to-date information of the MNs. This allows LMAs to know the previous location of the MNs before the next handover takes place. This is possible since the cluster is updated at the moment of the MN registration and the execution of intra and inter-domain handovers.

The P2P protocol, which is used for the communication among LMAs, is Kademlia [13]. In the following sections, the Kademlia standard, the *cluster* management, and the main signaling flows of CI-PMIPv6 are described in detail.

A. Kademlia

Kademlia is a fault-tolerant Distributed Hash Table (DHT) with a logarithmic performance in lookup procedures. DHTs are the latest generation of P2P networks, in which resources are available through a relation between <key,value> pairs and the peers where they are stored. In a DHT, each peer has a unique identifier, namely *nodeID*. The resources are stored in the peers whose *nodeIDs* have a mapping function to their corresponding keys. Among the most widely known DHTs [14] [15] [16] [17], Kademlia [13] distinguishes itself because of its arrival/departure process of peers, and its performance in the access of keys, values, and routing table entries. A <key,value> pair is stored in peers whose *nodeID* is the

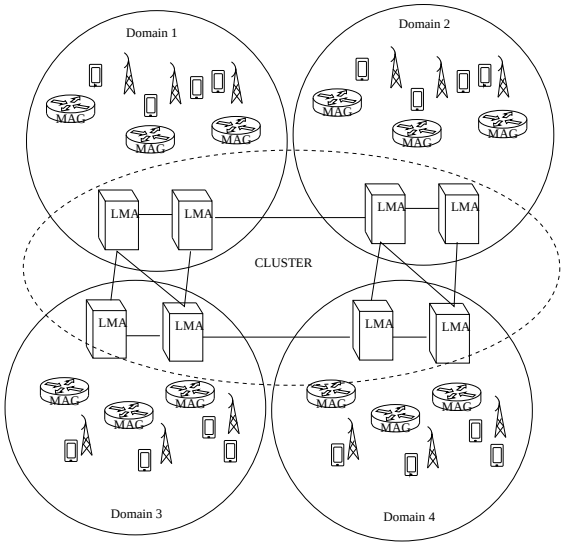

Figure 9. Domains in CI-PMIPv6.

TABLE I. Example of a routing table for the peer "110" using 3 k-buckets.

Peers dist. $1(2^0)$ to 2 (2^1)	[(IP, port,"111")]
Peers dist. (2^1) to (2^2)	[(IP, port,"100"),(IP, port,"101")]
Peers dist. (2^2) to (2^3)	[(IP, port,"000"), (IP, port,"001"), (IP, port,"010")]

closest to that key. The XOR operation is used for distance measurement between a key and a *nodeID*. The use of XOR simplifies the formal analysis due to its simple arithmetic. Figure 10 shows an example of a Kademlia-based network. In this example, the distance between the peers "110" and "100" is 2 ("10" in binary), which is the result of the XOR operation between their *nodeIDs*. Thus, for a given key, it is possible to find in the Kademlia routing table which peer has that particular key and its corresponding value by checking the peers with the smallest "distance". By default, keys and *nodeIDs* are in the 160-bit space. When a peer enters a Kademlia network, its *nodeID* is generated. Each peer has its own routing table with a set of 160 *k-buckets* (the same value of the key/*nodeID* size in bits), where *k* is a parameter that represents the maximum size of what is considered a "neighborhood". Depending on the distributions of the *nodeIDs* in the network, a *k-bucket* may never be entirely filled. Table I shows an example of a routing table in Kademlia. For simplification purposes, a 3-bit space is considered. The peer "011" does not appear in the table because it is not in the network at the moment. Each entry in a *bucket* is a <IP address, UDP port, *nodeID*> tuple. As new peers enter the Kademlia network, they are added to the respective *buckets*. A peer is added to the *bucket i* of another peer if the distance between them is between 2^i and 2^{i+1}, where $0 < i < \#buckets$.

Kademlia has four main primitives:

- `PING` - to check if a peer is online;
- `STORE` - instructs a peer to store a <key, value> pair;
- `FIND_NODE` - receives a 160-bit *nodeID* as parameter. The recipient must send a list of the k closest peers to the *nodeID* in the format <IP, UDP port, ID>;

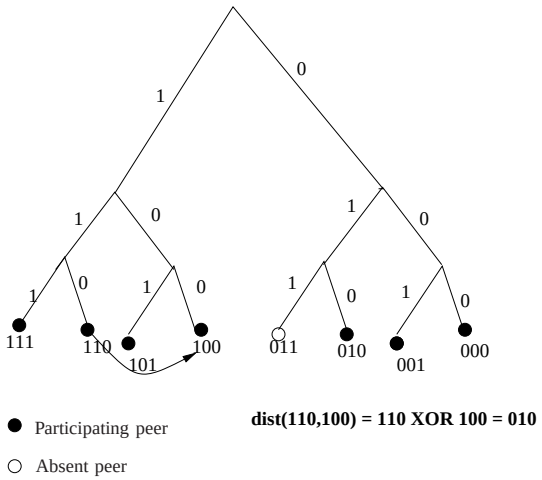

Figure 10. Example of a Kademlia network with a 3-bit key space

.

- FIND_VALUE - returns a similar result to FIND_NODE, however, the parameter is a 160-bit key. If the recipient peer has the key, then it responds with the corresponding value, otherwise, it returns the k closest peers in a list of tuples <IP, UDP port, ID>.

A very important operation in Kademlia is the *lookup*. This operation is used whenever a peer needs to find the *k* closest peers to a key or to another peer (represented by its *nodeID*). The search begins when the seeker peer selects α peers from its closest *k-bucket* and sends them a request of the type FIND_NODE or FIND_VALUE, depending on the context of the search. The α parameter is a parallelism parameter and its default value is 3. When these α peers respond to their requests, the seeker peer updates its *k-buckets* with the information that came in the responses. The seeker peer selects α more peers and continues doing so until its *k-buckets* stop growing. The bootstrap process of a peer involves a *lookup* operation in which the peer searches for itself. To enter the network, at least one neighbor must be known. This helps the new peer to discover the other neighbors and, therefore, fill its *k-buckets*. The Kademlia standard states that peers must republish their keys every hour and seeder peers must republish their keys every 24 hours. A peer is considered expired if it has not done any operation in the previous 24 hours. These peers may be removed from *k-buckets* and will be replaced by other peers.

B. Cluster Management

In the context of the CI-PMIPv6, the *cluster* is a Kademlia-based network where the peers are the LMAs from the different existing domains. The <key, value> pairs are stored in the *cluster* following the same logic as in Kademlia, where:

- The key is the prefix of the MN's IP address in its original domain;
- The value is a data structure containing the corresponding MAG's IP address, the current LMA's address, an identifier for the MN in its original network, an identifier of the link between the MN and its original network, and the prefix of the MN's IP address in its original domain, the International Mobile Subscriber Identity (IMSI) when applicable, and the list of all MAC addresses of the MN;
- The *nodeID* of an LMA in the *cluster* is its IP address;
- Keys and *nodeIDs* are in the 128-bit key space since it is the size of an IPv6 address instead of the 160-bit key space from the Kademlia standard.

TABLE II. KADEMLIA'S ROUTING TABLE FOR AN LMA - 128 K-BUCKETS.

Peers with distance $1(2^0)$ to 2 (2^1)	List of *k* LMAs
...	...
Peers with distance (2^x) to (2^{x+1})	List of *k* LMAs
Peers with distance (2^{127}) to (2^{128})	List of *k* LMAs

Following the logic in the Kademlia's original implementation, the <key, value> pairs are stored in the LMAs with the IPs closest to the MN's original IP prefix. Each LMA must have a local storage for its *k-buckets*. Each *bucket* has the IP addresses of the *k* LMAs whose distance to it is *n*, where *n* varies from 1 to 128. Table II presents an example of a Kademlia routing table for 128 *k-buckets*.

The PING, STORE, FIND_NODE, and FIND_VALUE primitives and the *lookup* procedure work in the same way as in the original implementation of Kademlia. An LMA in the *cluster* is registered during the deploy process of the CI-PMIPv6, following agreements among the related telecommunication companies. LMAs are not mobile entities and the departure of an LMA from the *cluster* during a call would be a very unlikely event. Therefore, the *cluster* can be considered a trusted area and the authentication services of the original PMIPv6 implementation remains unchanged.

The benefits of a solution based on a P2P architecture include:

- LMAs can communicate without there being a hierarchy among them;
- Mobility management is accomplished without centralized entities, which reduces the probability of bottlenecks in the network;
- MAGs can ignore the existence of the *cluster*, and therefore be out of the path of the core network;
- The spread of the STORE message during *handover* makes it unnecessary further communication to obtain the MN information in the next handover; in case of an eventual failure in *cluster* communication, the *lookup* process could be done in $\log(n)$ steps, where n is the size of the *cluster*.

CI-PMIPv6 introduces the new primitives UPDATE and DELETE to, respectively, update and remove keys during MNs handover and de-registration. These primitives follow the same logic as in STORE.

C. CI-PMIPv6 signaling

CI-PMIPv6 allows intra- and inter-domain handover with minor changes in the signaling flow of PMIPv6. For this purpose, CI-PMIPv6 assumes that:

- MAGs are physically reachable from a nearby LMA of another domain;

- LMAs work as Internet *gateways* - as in PMIPv6;
- Each domain has its own Authentication, Authorization and Accounting (AAA) service - as in PMIPv6.

Figure 11 shows the signaling flow for the MN registration in its original domain. The MN sends the `Rtr Sol` message to request the nearest MAG for a route to the external network. Initially, the MAG authenticates the MN with the corresponding AAA service of its domain. After authorization, the MAG sends a `PBU` message to its LMA. Until this point, the flow is exactly the same as in PMIPv6. Then, the LMA sends the `STORE` asynchronous message to the *cluster* according to its Kademlia routing table. The other LMAs in the *cluster* receive the MN information. Since the `STORE` message is asynchronous, the LMA does not have to wait for the responses from the LMAs in the *cluster* to proceed with the handover. The LMA sends the `PBA` message to the MAG. The MN is then registered and the MAG announces a new route sending to the MN the `Rtr Adv` ICMP message.

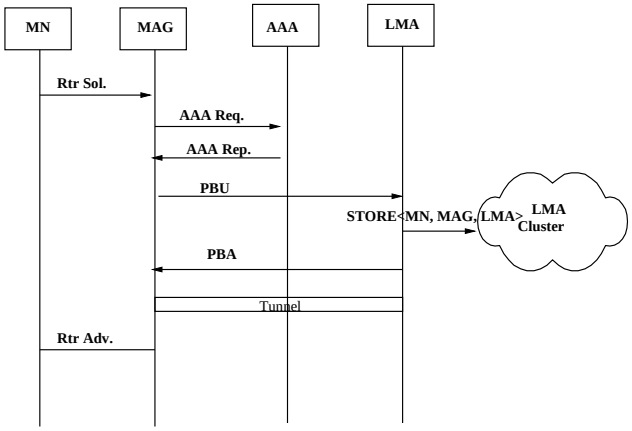

Figure 11. Registration of an MN in CI-PMIPv6.

Figure 12 presents the de-registration process for an MN. Initially, the signaling is the same as in PMIPv6. After detecting the MN's detachment event, the MAG sends the `PBU` message to the LMA. The LMA waits for a fixed amount of time named `INITIAL_BINDACK_TIMEOUT` [18] before deleting the MN information from its records. Then, the LMA sends the `DELETE` message to the *cluster*. As for the `STORE` message, the `DELETE` message is sent in an asynchronous manner. The LMA sends the `PBA` message to the MAG and finishs the de-registration process.

Figure 13 presents the signaling flow for the intra-domain handover. It is similar to that of the PMIPv6, except for the addition of the `UPDATE` message to update the *cluster* after the LMA acknowledges that the MN is associated to the new MAG. We assume that the LMA runs both the update operation and the rest of the intra-domain handover operation in parallel, e.g., the LMA runs both of the operations simultaneously on different cores. These two operations do not block each other. This is possible since the spread of binding information in the cluster is not useful for concluding the current intra-domain handover. MAGs do not need to interact with the cluster and may proceed with the handover normally. We further assume to be negligible the amount of time spent performing a system call for starting the update operation during intra-domain handovers. We also assume that traffic from the LMA to the cluster and traffic from the LMA to the MAGs can be kept isolated from each other. For instance, each LMA might have exclusive network interfaces and paths for communicating with MAGs. In this manner, update messages flowing from the LMA to the cluster during intra-domain handovers cannot block (e.g., head-of-the-line blocking in network interfaces) or affect (e.g., increasing queuing delay) messages flowing to the MAGs. The MN information is proactively spread in the cluster. The information will be necessary if there is ever an inter-domain handover executed by the MN. The MN information is rapidly available to neighbors LMAs in the cluster, thereby avoiding the need for the extra signaling to request and obtain such information during inter-domain handovers. Notice that CI-PMIPv6 takes advantage of the execution of inter-domain handover-related operations in parallel with the execution of intra-domain handover-related operations.

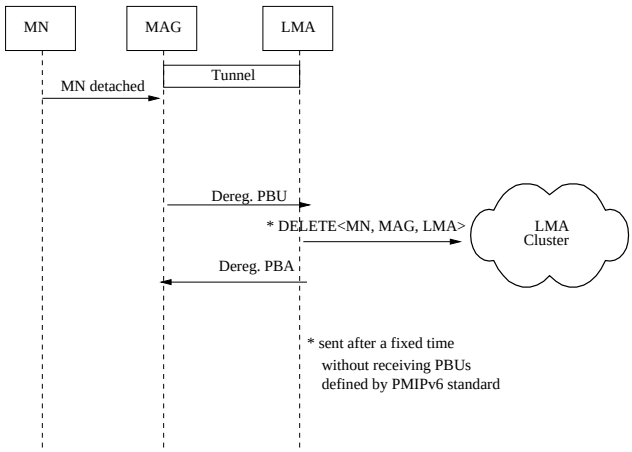

Figure 12. De-registration in CI-PMIPv6.

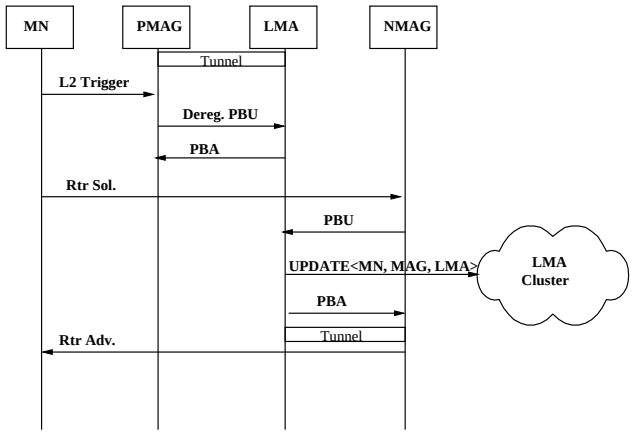

Figure 13. Intra-domain handover in CI-PMIPv6.

Figure 14 presents the signaling for the inter-domain handover. The PMAG sends the `PBU` to the previous LMA (PLMA) as the MN is about to leave the network. When the MN enters a new domain and requests the NMAG for a new route (`Rtr Sol`), the NMAG sends the `PBUNoProf` message to the new LMA (NLMA). This is because the NMAG cannot identify the MN in its records. The NLMA

finds the MN's IP address in its records, which came from previous interactions with the *cluster*. The NLMA sends the PLMA the `PBUInter` message in order to inform it that the MN is doing an inter-domain handover. It is important to notice that the PLMA must receive this message before the `INITIAL_BINDACK_TIMEOUT` expires, so that it does not remove the MN record. The value of `INITIAL_BINDACK_TIMEOUT` must be adjusted depending on the network conditions so as to avoid the unnecessary removal of MN records. The PLMA sends the `UPDATE` asynchronous message to the *cluster* and, in parallel, sends the `PBAinter-domain` message to the NLMA. Finally, the NLMA sends the `PBAProf` message to the NMAG with the MN information, so that a tunnel between the NMAG and the PLMA can be set up. The PLMA remains responsible for the data delivery until the end of the session.

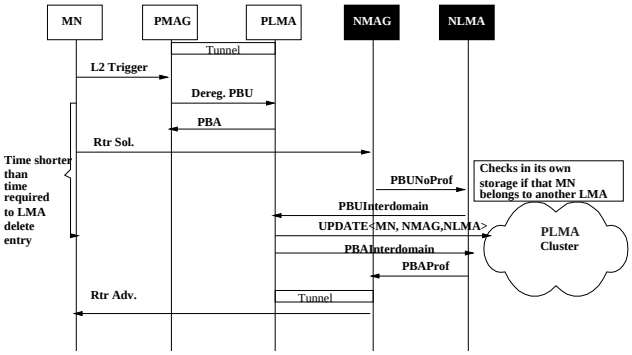

Figure 14. Inter-domain handover in CI-PMIPv6.

The greatest benefit of our approach to manage inter-domain handovers comes from the fact that LMAs have anticipated knowledge of MNs information. It is not necessary to wait for responses for messages sent to the *cluster* in order to finish the current handover since messages are asynchronous. Additionally, the messages exchanged in the *cluster* do not add signaling costs to the current intra-handover. It is important to notice that our approach does not remove any behavior from the original implementation of PMIPv6. Thus, a CI-PMIPv6 network can co-exist with legacy PMIPv6 networks. In such a case, the legacy LMA would not belong to any cluster and would manage only intra-domain handovers as is expected in PMIPv6.

D. CI-FPMIPv6

The design concepts of CI-PMIPv6 are generic and can be applied to other variants of PMIPv6 that has no support to inter-domain handover such as FPMIPv6. In this paper, we apply these concepts to FPMIPv6 as another case study. This results in a new proposed protocol, namely CI-FPMIPv6 (Clustered Inter-domain FPMIPv6). The inter-domain handover of the CI-FPMIPv6 in the reactive mode is straightforward and is depicted in Figure 15. As soon as the MN arrives in the new domain, the NMAG sends the `PBUNoProf` message to the NLMA in order to request the MN information. After receiving the `PBAProf` response, the NMAG sets up the tunnel and the buffer with the PMAG using the FPMIPv6 `HI` and `HACK` messages. After that, the NMAG sends a `PBU` message to inform the NLMA that the handover is happening and the NLMA informs the PLMA about the ongoing inter-domain handover. To do this, the PLMA sends the `PBUinter-domain` message. The PLMA, then, updates the *cluster* with the `UPDATE` asynchronous message and responds to the NLMA with the `PBAinter-domain` message. Thus, the data tunnel is created between the NMAG and the PLMA.

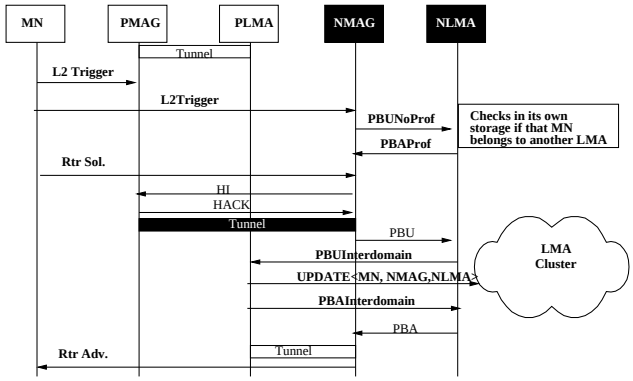

Figure 15. Inter-domain handover in CI-FPMIPv6 using the reactive mode.

In order to accomplish the inter-domain handover by considering the predictive mode of FPMIPv6, a new piece of information needs to be added to the tuple stored in the cluster: the IP address of the latest PoA associated to the MN. This information is important for the predictive mode since it is the only way a PLMA can find the NMAG that manages this PoA and then, it gives to its PMAG the NMAG address so that they can exchange tunnel information before the IP handover takes place. The `UPDATE` asynchronous message must now be sent not only during every intra-domain handover but also during every intra-MAG handover (when the MN changes the PoA without changing the MAG). This is important for the LMA to feed the mapping between PoAs and their corresponding MAGs. Figure 16 presents the signaling flow for an inter-domain handover considering the predictive mode in CI-FPMIPv6. After the link-layer handover, the PMAG sends the `FindNMAG` message to the PLMA since it could not find in its internal entries the NMAG that manages the new PoA. The PLMA, which has this information thanks to the *cluster* messages exchanged in previous handovers, replies with the `NMAGInfo` message. The PMAG then exchanges with the NMAG the `HI` and `HACK` messages. Thus the tunnel and buffering are initiated. When the MN finally arrives at the new network, the NMAG does not know that node, and, therefore, must send the `PBUNoProf` message to the NLMA. The NLMA checks for its records fed by the interactions with the *cluster* and informs the PLMA that an inter-domain handover is taking place by sending the `PBUinter-domain` message. The PLMA sends the `UPDATE` asynchronous message to the cluster and replies with the `PBAinter-domain` message. Finally, the NLMA sends the `PBAProf` message to the NMAG and the data tunnel is created between the NMAG and the PLMA.

E. CI-PMIPv6 and CI-FPMIPv6 Messages Format

In this section, the signaling messages used by CI-PMIPv6 and CI-FPMIPv6 are detailed. Some of the messages are inherited from PMIPv6 and FPMIPv6 protocols, respectively. Tables III to XIX show the fields of each signaling message.

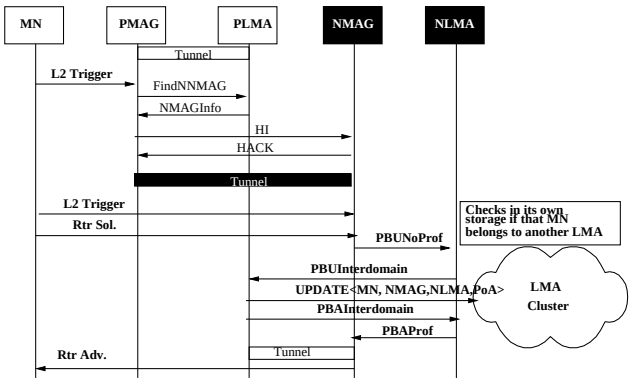

Figure 16. Inter-domain handover in CI-FPMIPv6 using the predictive mode.

Tables III to XIX shows the fields of each signaling message.

V. Preliminary analysis

Table XX summarizes the differences among CI-PMIPv6, CI-FPMIPv6, and other inter-domain solutions. The extra signaling during an intra-domain handover is calculated in comparison with the original implementation of PMIPv6. FPMIPv6 has 2 more signaling messages than PMIPv6. Thus, CI-FPMIPv6 introduces 2 signaling messages with respect to FPMIPv6 but has 4+2 additional signaling messages with respect to PMIPv6. Notice that it is not the fault of our approach since it inherits the 2 extra signaling messages from FPMIPv6. The decentralized approach [5] has one of the greatest increase in extra signaling in comparison with the other approaches. Additionally, there might be an overhead related to the addition of one more IP header because of the need for the extra tunnel. It is expected that these factors cause a noteworthy increase in latency during the inter-domain handover.

CI-PMIPv6 and CI-FPMIPv6 appear as the best solutions. The reason is as follows: the extra signaling needed for inter-domain handover is one of the lowest; they do not require extra tunnels; and they can inter-work with legacy systems. The cluster messages do not add extra signaling costs to the ongoing handover because they are asynchronous and are necessary only in future inter-domain handovers. Thus, it is expected CI-PMIPv6 and CI-FPMIPv6 to exhibit a smaller handover cost, lower latency - as a consequence, less packet loss - and a higher useful traffic rate than the other proposals.

VI. Performance Evaluation and Results

In this section, the performance of the CI-PMIPv6 and CI-FPMIPv6 are compared to that of the decentralized, No-Gap, I-PMIP, and EIPMH solutions. The evaluation is based on the analytical modeling presented in [8] [23] [24]. This allows the cost of handover signaling in a session, latency and the packet loss of one handover, and the goodput in a session to be measured. It is considered that mobile devices are attached to vehicles in a highway during a voice call (e.g., Skype). Inter-domain handover takes place as the MN arrives at a new domain. The mobility pattern follows the Fluid-Flow model [25]. That model considers average velocity (v), the subnet and domain coverage areas (A_M and A_D,

TABLE III. PBU Format [19].

Field name	Field size (bytes)	Data type	Comments
Sequence	2	integer	Identify the order of signaling messages
A	1	bool	Asks for an acknowledgment (from MIP [18])
H	1	bool	Home registration (from MIP [18])
L	1	bool	Link-Local Address Compatibility (from MIP [18])
K	1	bool	Key Management Mobility Capability (from MIP [18])
M	1	bool	Register to a Mobility Anchor Point (from Hierarchical MIP [20])
R	1	bool	Mobile Router (from NEMO Basic Support Protocol [21])
P	1	bool	Indicates that it is a proxy in behalf of the MN
Reserved	2	byte	
Lifetime	2	integer	The granted lifetime (from MIP [18])
Mobility Options	variable	byte	Optional information about prefix, handover, among others

TABLE IV. PBA Format [19].

Field name	Field size (bytes)	Data type	Comments
Status	1	integer	Indicates the disposition of the binding update (from MIP [18])
K	1	bool	Key Management Mobility Capability (from MIP [18])
R	1	bool	Mobile Router (from NEMO Basic Support Protocol [21])
Reserved	2	byte	
Sequence	2	integer	Same value as in PBU
Lifetime	2	integer	The granted lifetime (from MIP [18])

TABLE V. PBU No Profile Format.

Field name	Field size (bytes)	Data type	Comments
Same fields from PBU	-	-	-
Mac address	6	byte	Indicates the MN's MAC address came from L2 handover-if it is using Wi-Fi
Imsi	8	byte	Indicates the MN's IMSI - if it is using 3GPP

TABLE VI. PBA Profile Format.

Field name	Field size (bytes)	Data type	Comments
Same fields from PBA	-	-	-
Value	variable	byte	The information about the MN queried (see SectionIV-B)

TABLE VII. PBU INTERDOMAIN FORMAT.

Field name	Field size (bytes)	Data type	Comments
Same fields from PBU	-	-	- -

TABLE VIII. PBA INTERDOMAIN FORMAT.

Field name	Field size (bytes)	Data type	Comments
Same Same fields from PBA	-	-	-

TABLE IX. HI FORMAT [7].

Field name	Field size (bytes)	Data type	Comments
Sequence	2	integer	Identify the order of signaling messages (from PMIPv6 [19])
S	1	bool	Assigned address configuration flag (from Fast Handovers for MIP [22])
U	1	bool	Buffer flag (from Fast Handovers for MIP [22])
P	1	bool	Proxy flag (from PMIPv6 [19])
F	1	bool	Request to forward the packets for the mobile node
Reserved	-	-	
Code	1	bool	May indicate completion of forwarding, or context transferred (from Fast Handovers for MIP [22])
Mobility options	variable	byte	May indicate an alternative CoA or binding authorization data(from MIP [18])

TABLE X. HACK FORMAT [7].

Field name	Field size (bytes)	Data type	Comments
Sequence	2	integer	Identify the order of signaling messages (from PMIPv6 [19])
U	1	bool	Buffer flag (from Fast Handovers for MIP [22])
P	1	bool	Proxy flag (from PMIPv6 [19])
F	1	bool	Request to forward the packets for the mobile node
Reserved	-	-	
Code	1	byte	May indicate handover status - success, or failure
Mobility options	variable	byte	May indicate an alternative CoA or binding authorization data (from MIP [18])

TABLE XI. FIND NMAG FORMAT.

Field name	Field size (bytes)	Data type	Comments
PoA address	16	byte	IP address of the target PoA in the MN's handover

TABLE XII. NMAGINFO FORMAT.

Field name	Field size (bytes)	Data type	Comments
NMAG address	16	byte	IP address of the NMAG corresponding to the target PoA in the MN's handover

TABLE XIII. STORE FORMAT.

Field name	Field size (bytes)	Data type	Comments
Sender ID	16	byte	Node ID of Sender
Key	16	byte	Key for the content
Value	variable	byte	Information about the MN to be stored (see SectionIV-B)

TABLE XIV. UPDATE FORMAT.

Field name	Field size (bytes)	Data type	Comments
Sender ID	16	byte	Node ID of Sender
Key	16	byte	Key for the content
Value	variable	byte	Information about the MN to be stored (see SectionIV-B)

TABLE XV. DELETE FORMAT.

Field name	Field size (bytes)	Data type	Comments
Key	16	byte	Key for the content

TABLE XVI. FIND NODE FORMAT.

Field name	Field size (bytes)	Data type	Comments
Sender ID	16	byte	Node ID of Sender
Node ID	16	byte	The Node ID to be searched
Lookup	1	bool	Identifies if it is a lookup operation

TABLE XVII. FIND NODE RESPONSE FORMAT.

Field name	Field size (bytes)	Data type	Comments
Closest peers	variable	byte	A list of the closest peers to the key

TABLE XVIII. FIND VALUE FORMAT.

Field name	Field size (bytes)	Data type	Comments
Sender ID	16	byte	Node ID of Sender
Key	16	byte	Key for the content

TABLE XIX. FIND VALUE RESPONSE FORMAT.

Field name	Field size (bytes)	Data type	Comments
Key	16	byte	Key for the content
Found	1	bool	Tells if the search was successful
Value	variable	byte	The tuple of information about the MN in case of success (see SectionIV-B)
Closest peers	variable	byte	A list of the closest peers to the key in case of failure in search

TABLE XX. COMPARISON OF THE DIFFERENT PROPOSALS.

Solution	# extra messages in inter-domain handover	# extra tunnels	Infrastructure maintenance	Compatibility with legacy systems
decentralized [5]	8	1	Yes	Yes
EIPMH [4]	6	2	No	No
I-PMIP [3]	6	1	No	No
No-Gap [2]	4	1	No	Yes
CI-PMIPv6	2	0	Yes	Yes
CI-FPMIPv6 reac.	4+2	0	Yes	Yes
CI-FPMIPv6 pred.	4+2	0	Yes	Yes

respectively) and the subnet and domain perimeters (L_M and L_D, respectively) as parameters. The direction of movement is uniformly distributed in a range of 0 to 2π. Since this experiment is interested in a vehicular scenario, the choice of this model is very appropriate.

Two variables determine the dynamics of the MN: the domain crossing rate (μ_D) and the subnet crossing rate (μ_M). The former is the rate at which the node switches from one domain to another. It is equivalent to the inter-domain handover rate (Ng). The latter is the rate at which the node switches from one subnet to another. The intra-domain handover rate (Nl) considers a subnet crossing when this does not imply a domain crossing. That is, Nl is the difference between μ_M and μ_D. Their equations are as follows [8] [24]:

$$\mu_M = \frac{vL_M}{\pi A_M}, \tag{1}$$

$$Ng = \mu_D = \frac{vL_D}{\pi A_D}, \tag{2}$$

$$Nl = \mu_M - \mu_D. \tag{3}$$

Another important parameter to describe mobility of a node is the Session-to-Mobility Ratio (SMR), which relates session arrival rate and the subnet crossing rate as follows [8]:

$$SMR = \frac{\lambda_S}{\mu_M}. \tag{4}$$

If SMR is near zero, this means that the node has high mobility. The higher the SMR, the more static the node.

The signaling cost is the number of handover signaling messages, taking into consideration the distance in hops between two entities x and y, namely $H_{(x-y)}$, the underlying media, and the processing cost. For each protocol message sent, the signaling cost is (see [8])

$$C_{x-y} = \alpha(H_{(x-y)}) - \beta + PC_y, \tag{5}$$

$$PC_y = \varsigma \log N^y_{MN}, \tag{6}$$

where the parameters α and β represent the coefficients of unity transmission costs (in messages/hop) in wired and wireless links, respectively. The cost of processing at one end is represented by PC_y. It is measured based on a logarithmic search in a data structure with the size of the number of MN entries and a normalizing constant ς equivalent to the bandwidth allocation. If the reception of a message at one end does not imply searching a local storage, PC_y is considered zero. Additionally, if the node that sends or receives the message is not an MN, the β factor is excluded. The handover signaling cost is the sum of the cost of all messages exchanged during a handover. The average cost is measured as a weighted sum of the intra-domain and inter-domain counterparts. It depends on Ng and Nl rates. The average cost [8] is presented as

$$cost = \frac{intraDHO\ cost \times Nl + interDHO\ cost \times Ng}{Nl + Ng}. \tag{7}$$

The inter-domain signaling cost for a session is the cost of one inter-domain handover multiplied by both Ng and the session duration:

$$cost\ in\ session = interDHO\ cost \times Ng \times session\ duration. \tag{8}$$

Handover latency is measured as the handover duration, i.e., the time a node spends without effective communication. The latency equation for a message exchanged between two nodes *x* and *y* is (see [24])

$$T_{x-y} = \frac{1+q}{1-q}\left(\frac{M_{size}}{B_{wl}} + L_{wl}\right) + H_{x-y}\left(\frac{M_{size}}{B_w} + L_w + T_q\right). \tag{9}$$

The first part of the sum is the wireless overhead and it must be excluded if neither *x* nor *y* is a wireless device. The second part is the overhead in the wired medium. The parameter *q* is the probability of failure of the wireless link, M_{size} is the average length of a message, and B_{wl} and B_w are the wireless and wired bandwidths, respectively. The propagation delay in wireless and wired media are L_{wl} and L_w, respectively. The average queuing delay in each router is represented by T_q. Handover latency is the sum of the latency of all signaling messages exchanged during a handover, plus the link-layer handover latency. In the case of CI-PMIPv6 predictive mode, the link-layer handover latency is not considered, since it occurs nearly in parallel with the handover in the network layer. As in the signaling cost, the average latency is measured as a weighted sum of the intra-domain and inter-domain counterparts as follows [8]:

$$latency = \frac{intraDHO\ lat \times Nl + interDHO\ lat \times Ng}{Nl + Ng}. \tag{10}$$

The average packet loss in a handover is the average number of packages not sent/received during handover. The packet loss (PL) is the product of the handover latency (T) and the packet arrival rate (λ_p) [8], i.e.,

$$PL = T\lambda_p. \tag{11}$$

For the case of FPMIPv6-based protocols, the Equation (11) must be adapted to consider the packet buffering during handover. In the reactive mode, the average packet loss (PL_{reac}) is the average number of packets not sent/received during both the link-layer handover and the exchange of the `HI` and `HACK` messages (cf. [24]), i.e.,

$$PL_{reac} = (T_{L2} + T_{HI} + T_{HACK}) \times \lambda_p. \quad (12)$$

In the predictive mode, the link-layer handover starts nearly in parallel with the network-layer handover. Thus, we assume that in this mode the average packet loss is the average number of packets not sent/received during the tunnel setup, excluding the time interval ($T_{L2trig-L2HOexec}$) while link-layer handover has triggered but not yet executed (cf. [24]). In this manner, the packet loss under the preditive mode is defined as

$$PL_{pred} = ((T_{HI} + T_{HACK}) - (T_{L2trig-L2HOexec})) \times \lambda_p. \quad (13)$$

Finally, the goodput is a measure that relates the useful data traffic during a session and the total traffic (TOT), which is the total number of bytes transmitted during a session. The goodput is determined as follows (cf. [8]):

$$Goodput = \frac{TOT - (P_{size} \times PL_{session} + TOT \times PD)}{session\ duration}, \quad (14)$$

$$TOT = session\ duration \times \lambda_p \times P_{size}, \quad (15)$$

$$PD = \frac{40 \times H_{tunnel}}{(40 + P_{size}) \times H_{MN-CN}}. \quad (16)$$

Goodput additionally depends on the packet loss and the packet delivery (PD) overhead. PD overhead is the cost of tunneling the IP-in-IP extra 40-byte header along the path between an MN and its correspondent node (H_{MN-CN}). Packet size (P_{size}) and the PMIPv6 tunnel size in hops (H_{tunnel}) are parameters for the PD.

Now, let us turn our attention to the evaluation of the performance of CI-PMIPv6. The signaling cost in a session is measured as a function of SMR. Latency and packet loss in one handover are measured as a function of the probability of failure of the link in the wireless network. The goodput in a session is measured as a function of SMR.

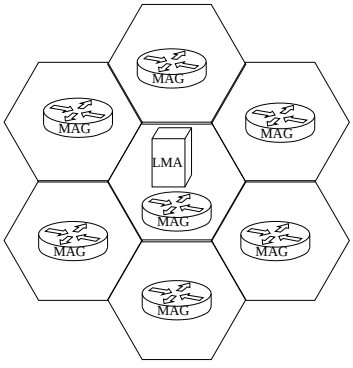

Figure 17. A domain with 7 subnets.

In these evaluations, a domain has 7 subnets. Each subnet follows a hexagonal model, has one PoA and one MAG. There is a central subnet that is managed by a single LMA. The other subnets surround the central subnet. The coverage area of each subnet is equal to 1.87 km^2 and the perimeter is equal to 5 km.

TABLE XXI. EVALUATION PARAMETERS.

Parameter	Default value
Number of subnets per domain	7
Coverage area of each subnet (A_M)	1.87 km^2
Kademlia's constant (k)	10
MN velocity (v)	15 m/s
Prob. of failure of the wireless link (q)	0.5 (range 0-0.8)
Coefficient of cost in wired medium (α)	1 message/hop
Coefficient of cost in wireless medium (β)	10 messages/hop
Normalizing constant (ς)	0.01
Queuing time (T_q)	5 ms
Subnet residency time ($1/\mu_M$)	300 s
Prop. delay (wired link) (L_w)	0.75 μs
Prop. delay (wireless link) (L_{wl})	10 ms
Packet arrival rate (λ_p)	38 packets/s (100 kbps)
Session arrival rate (λ_S)	0.001 sessions/s
Average data packet size (P_{size})	300 bytes
Average signaling packet size (M_{size})	160 bytes
Link-layer handover latency (T_{L2})	50 ms

Table XXI summarizes the values of the parameters used for performance evaluation. The Kademlia parameter *k* used in CI-PMIPv6, which represents the size of the neighborhood, is set to 10. This value is chosen based on a scenario where nodes have an average speed of 15 m/s (60 km/h) and may cross 10 domains during a session. The probability of failure of the wireless link ranges from 0 to 0.8 in experiments to consider the radio channel under different quality conditions during handover. The greater this probability is, the more link-layer retransmissions are necessary. The value of α is equal to 1 message/hop and β is equal to 10 messages/hop, since wireless links tend to cost more than wired links. The average queue time is a typical value of 5 ms. The average residency time of an MN is considered equal to 300 s, which corresponds to a mean speed of 15 m/s. The theoretical latency across a 4G LTE interface is in the order of 10 ms. It is assumed that the wireless link has a propagation delay of 10 ms in order to capture such behavior. The propagation delay of wired links are assumed to be a typical value for Fast Ethernet. The arrival rate of packets corresponds to a voice call (e.g., Skype) and the session arrival rate allows consecutive voice calls that are 13 minutes long each. The average data packet size considered is 300 bytes long [26]. The average packet size used for handover signaling is 160 bytes long. In our evaluation of the CI-FPMIPv6 operating in the predictive mode, we consider the contribution of the term $T_{L2trig-L2HOexec}$ in Equation (13) to be negligible.

Figure 18 presents the influence of SMR on the overall cost during a session. If SMR is near zero, there is a high mobility scenario. If SMR is high, this means that the network mobility is low. Therefore, the cost tends to be lower with higher values of SMR for all proposals. When SMR tends to zero, there is a high number of handovers during a session. In this case, the number of messages exchanged during handover plays an important role in the overall cost. Additionally, the presence of a cluster that exchanges proactively domain information and in parallel with the current binding update simplifies communication during future inter-domain handovers, which require less interaction between core network entities. CI-

PMIPv6 has a cost 20% lower than the cost in No-Gap when the SMR is equal to 0.01. The decentralized scheme has the worst performance. CI-PMIPv6 always exhibits the lowest cost since it requires fewer messages to accomplish handover, as shown in Table XX. CI-FPMIPv6 follows as the second best in performance along with the No-Gap solution. Both the predictive and reactive modes have the same number of additional messages. Although the same can be said about I-PMIPv6, it has a greater cost due to the signaling of de-registration between the MN and the previous domain, which is not necessary in FPMIPv6-based protocols.

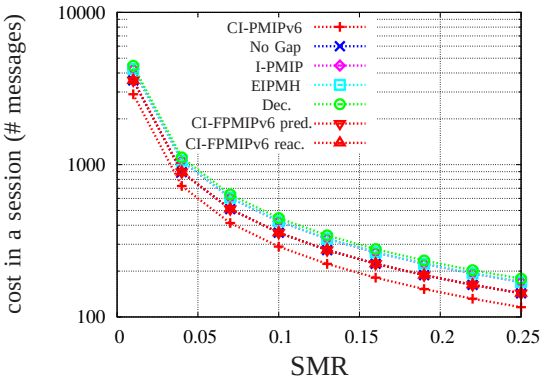

Figure 18. Overall cost *versus* SMR.

Figure 19 presents the average handover latency as a function of the probability of failure of the wireless link. This probability represents the reliability of the wireless channel and may degrade performance due to retransmissions in the link layer. The EIPMH results are influenced by the high number of interactions in the core network. It has the highest latency until the probability of failure reaches 0.65. From this point on, the decentralized scheme has greater latency. This is due to the fact that it has more messages involving the MN, thus making the scheme more sensitive to the wireless media. I-PMIP presents results with values close to the those of No Gap. It is important to notice that CI-PMIPv6 and CI-FPMIPv6 (predictive) present the smallest results for latency. In particular, CI-PMIPv6 latency is 16% smaller than the latency in I-PMIP when the probability of failure is 0.8. CI-PMIPv6 performs better because unnecessary interactions in both the core network and the wireless network were eliminated. CI-FPMIPv6 (predictive) performs similar because although it has 2 additional signaling messages than CI-PMIPv6, the handover starts as soon as the link-layer triggers the handover, which contributes to reduce the overall latency. The reactive mode of CI-FPMIPv6 has bigger latency than the predictive mode, despite having the same number of signaling messages in the inter-domain handover. Nevertheless, since the buffer setup is done after the handover in the link layer, the reactive mode of CI-FPMIPv6 finishes the overall process later than the predictive mode.

Figure 20 presents the number of lost packets based on the probability of failure of the wireless link. For those schemes that does not involve buffering, the packet loss is directly related to the handover latency. Considering that in this scenario the arrival rate is 38 packets/s, there is a significant loss of quality in the worst case. The number of lost data

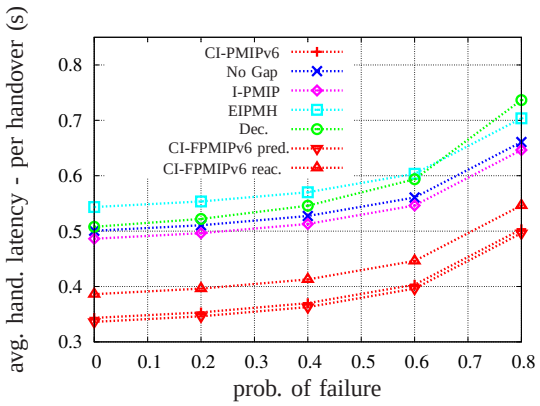

Figure 19. Overall latency *versus* prob. of failure of the wireless link.

packets for CI-FPMIPv6 (predictive) is the smallest, in all cases studied, and followed by CI-FPMIPv6 (reactive). This is due to the FPMIPv6's buffering of packets while the handover takes place. These packets are preserved and sent after the handover is finished, which reduces the packet loss during this process. CI-PMIPv6 loses a smaller number of packets in comparison to the other non-buffering schemes since the interval of time when handover takes place and the data path is "broken" is smaller. In particular, it is 16% smaller than the value observed for No-Gap when the failure probability is 0.8.

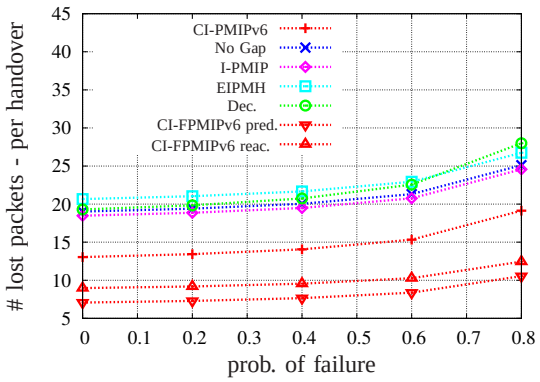

Figure 20. Packet loss *versus* prob. of failure of the wireless link.

Figure 21 presents the goodput *versus* the SMR. If SMR is high, it means that the network mobility is low. Thus, goodput tends to be more stable as SMR grows. CI-PMIPv6 and CI-FPMIPv6 have the highest goodput for all SMR values. This means that our approach makes both protocols capable of sending more useful data during a session. They maintain the same number of tunnels created in PMIPv6. This avoids the PD overhead due to headers in IP-in-IP tunneling. For a small SMR, the CI-FPMIPv6 in the predictive mode has slightly greater values, followed by CI-FPMIPv6 in reactive mode and CI-PMIPv6. This is due to the predictive CI-FPMIPv6's lower packet loss. When the SMR is greater, there is less mobility and less handovers. Thus, in this case, the difference in the goodput values among them is negligible. EIPMH has the worst goodput because it requires the creation of two extra tunnels, besides the pre-existing PMIPv6 tunnel. The

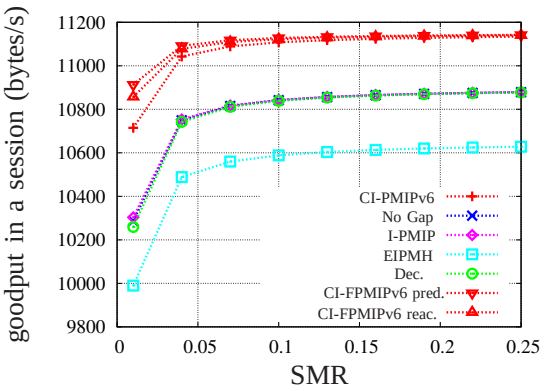

Figure 21. Goodput *versus* SMR.

decentralized solution as weel as I-PMIP and No-Gap have similar results, since they introduce just one extra tunnel in comparison to PMIPv6.

VII. Conclusion

This paper presented CI-PMIPv6 as distributed solutions for inter-domain IP mobility in PMIPv6-based systems. CI-PMIPv6 has a distributed design, which organizes LMAs from different domains in a cluster as Kademlia peers. In the cluster, information on MNs is spread proactively and in parallel with the current binding update, thereby simplifying future inter-domain handover processes. We have shown that CI-PMIPv6 significantly boosts the performance of inter-domain handovers. The design concepts of CI-PMIPv6 are generic and can be applied to other variants of PMIPv6 that have no support to inter-domain handover such as FPMIPv6. We applied these concepts to FPMIPv6 as another case study and showed that the performance can also be significantly boosted. Plain CI-PMIPv6 and its reactive and predictive modes were compared to several inter-domain approaches and results have shown that when CI-PMIPv6 is used, the cost, the latency, and the packet loss in the studied scenario are lower. Additionally, the goodput reaches higher values.

VIII. Future Work

CI-PMIPv6 network uses a P2P-based architecture. Thus, a study of the network scalability will be done. Scalability tests can verify the behavior of the CI-PMIPv6 network as a function of the domain size and under high mobility scenarios. We will also evaluate the robustness of the CI-PMIPv6 network in the presence of faulty LMAs. Another future step will be the use of the cluster as a load balancer in order to provide high availability for all domains [27]. In future studies, CI-PMIPv6 will be extended to support churn, ie., peers entering and leaving the cluster. In such a case, security aspects [28] and consistency of the information shared among entities need to be considered. Further, the application of localized routing techniques [29] may be applied to enhance the CI-PMIPv6 performance in high mobility scenarios.

References

[1] N. C. Quental and P. A. S.Gonçalves, “CI-PMIPv6: An Approach for Inter-domain Network-based Mobility Management,” in Proc. of the 16th International Conference on Networks, Venice, 2017, pp. 111–117.

[2] I. Joe and H. Lee, “An efficient inter-domain handover scheme with minimized latency for PMIPv6,” in Proc. International Conference on Computing, Networking and Communications, Maui, 2012, pp. 332 – 336.

[3] N. Neumann, J. Lei, X. Fu, and G. Zhang, “I-PMIP: an inter-domain mobility extension for proxy-mobile IP,” in Proc. International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly, Leipzig, 2009, pp. 994–999.

[4] F. Zhong, S. Yang, C. K. Yeo, and B. S. Lee, “Enabling inter-PMIPv6-domain handover with traffic distributors,” in Proc. 7th IEEE CCNC, Las Vegas, 2010, pp. 1–5.

[5] S. Park, E. Lee, F. Yu, S. Noh, and S.-H. Kim, “Inter-domain roaming mechanism transparent to IPv6-node among PMIPv6 networks,” in Proc. of the IEEE 71st Vehicular Technology Conference, Taipei, 2010, pp. 1–5.

[6] N. Neumann, J. Lei, X. Fu, and G. Zhang, “Kademlia with consistency checks as a foundation of borderless collaboration in open science services,” in Proc. of the 5th International Young Scientist Conference on Computational Science, Krakow, 2016, pp. 304–312.

[7] H. Yokota, K. Chowdhury, R. Koodli, B. Patil, and F. Xia, “Fast Handovers for Proxy Mobile IPv6,” RFC 5949, september 2011. [Online]. Available: http://tools.ietf.org/html/rfc5949

[8] A. Taghizadeh, T.-C. Wan, R. Budiarto, F. T. Yap, and A. Osman, “A performance evaluation framework for network-based IP mobility solutions,” International Journal of Innovative, Computing, Information and Control, vol. 8, no. 10, 2012, pp. 7263–7288.

[9] QualNet, “QualNet - Scalable Network Technologies,” 2017, Acessed: 11–18–2017. [Online]. Available: http://web.scalable-networks.com/content/qualnet

[10] T. T. Nguyen and C. Bonnet, “DMM-based inter-domain mobility support for proxy mobile IPv6.” in Proc. IEEE WCNC, Shanghai, 2013, pp. 1998–2003.

[11] H. Zhou, H. Zhang, Y. Qin, H. Wang, and H. Chao, “A Proxy Mobile IPv6 based global mobility management architecture and protocol,” Mobile Networks and Applications, vol. 15, no. 4, 2010, pp. 530–542.

[12] K.-W. L. et al., “Inter-domain handover scheme using an intermediate mobile access gateway for seamless service in vehicular networks,” International Journal of Communication Systems, vol. 23, no. 9–10, 2009, pp. 1127–1144.

[13] P. Maymounkov and D. Mazires, “Kademlia: A Peer-to-Peer Information System Based on the XOR Metric,” in Proc. of the First International Workshop on Peer-to-Peer Systems, 2002, pp. 53–65.

[14] I. Stoica, R. Morris, D. Liben-Nowell, D. R. Karger, F. F. Kaashoek, F. Dabek, and H. Balakrishnan, “Chord: A Scalable Peer-to-Peer Lookup Protocol for Internet Applications,” IEEE/ACM Transactions Networking, vol. 11, no. 1, February 2003, pp. 17–32. [Online]. Available: http://portal.acm.org/citation.cfm?id=638336

[15] A. I. T. Rowstron and P. Druschel, “Pastry: Scalable, Decentralized Object Location, and Routing for Large-Scale Peer-to-Peer Systems,” in Proceedings of the IFIP/ACM International Conference on Distributed Systems Platforms Heidelberg (Middleware ’01). London: Springer-Verlag, 2001, pp. 329–350.

[16] B. Zhao, L. Huang, J. Stribling, S. C. Rhea, A. D. Joseph, and J. Kubiatowicz, “Tapestry: a resilient global-scale overlay for service deployment,” IEEE Journal on Selected Areas in Communications, vol. 22, no. 1, 2004, pp. 41–53.

[17] D. Malkhi, M. Naor, and D. Ratajczak, “Viceroy: a Scalable and Dynamic Emulation of the Butterfly,” in Proceedings of the twenty-first annual symposium on Principles of distributed computing, Monterey, 2002, pp. 183–192.

[18] D. Johnson, C. Perkins, and J. Arkko, “Mobility Support in IPv6,” RFC 3775, june 2004. [Online]. Available: http://tools.ietf.org/html/rfc3775

[19] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, “Proxy Mobile IPv6,” RFC 5213, aug 2008. [Online]. Available: http://tools.ietf.org/html/rfc5213

[20] H. Soliman, C. Castelluccia, K. E. Malki, and L. Bellier, “Hierarchical Mobile IPv6 Mobility Management (HMIPv6),” RFC 4041, aug 2005. [Online]. Available: http://tools.ietf.org/html/rfc4041

[21] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert, “Network

Mobility (NEMO) Basic Support Protocol," RFC 3963, jan 2005. [Online]. Available: http://tools.ietf.org/html/rfc3963

[22] E. R. Koodli, "Mobile IPv6 Fast Handovers," RFC 5568, july 2009. [Online]. Available: http://tools.ietf.org/html/rfc5568

[23] J. McNair, I. Akyildiz, and M. D. Bender, "Handoffs for real-time traffic in mobile IP version 6 networks ," in Proc. First Global Telecommunications Conference, San Antonio, 2001, pp. 3463–3467.

[24] C. Makaya and S. Pierre, "An analytical framework for performance evaluation of IPv6-based mobility management protocols," IEEE Transactions on Wireless Communications, vol. 7, no. 3, 2008, p. 7.

[25] A. Salehan, M. Robatmili, M. Abrishami, and A. Movaghar, "A comparison of various routing protocols in mobile ad-hoc networks (MANETs) with the use of fluid flow simulation method," in Proc. 4th International Conference on Wireless and Mobile Communications, Athens, 2008, pp. 260–267.

[26] S. Molnár and M. Perényi, "On the identification and analysis of Skype traffic," International Journal of Communication Systems, vol. 24, no. 1, 2011, pp. 94–117.

[27] A. J. Jabir, "A comprehensive survey of the current trends and extensions for the proxy mobile ipv6 protocol," IEEE Systems Journal, vol. PP, no. 99, 2015, pp. 1–17.

[28] Y. Lee, H. Koo, S. Choi, B. hee Roh, and C. Lee, "Advanced Node Insertion Attack with Availability Falsification in Kademlia-based P2P Networks," in Proceedings of the 14th International Conference on Advanced Communication Technology (ICACT), PyeongChang, 2012, pp. 73–76.

[29] A. Rasem, C. Makaya, and M. St-Hilaire, "O-PMIPv6: Efficient Handover with Route Optimization in Proxy Mobile IPv6 Domain," in Proc. of the IEEE 8th International Conference on Wireless and Mobile Computing, Networking and Communications, Barcelona, 2012, pp. 47–54.