

H-SIP Inter-Domain SIP Mobility: Design

Joud S. Khoury *

Henry N. Jerez[†]

Chaouki T. Abdallah*

*School of Electrical and Computer Engineering, 1 University of New Mexico, Albuquerque, NM 87131-0001
{jkhoury, chaouki}@ece.unm.edu

[†]Corporation for National Research Initiatives, Reston, VA 20191
hjerez@cnri.reston.va.us

Abstract—Supporting mobility in IP networks is a crucial step towards satisfying the nomadic communication paradigms on the current Internet. The Session Initiation Protocol (SIP) presents one approach towards supporting IP mobility and is increasingly gaining in popularity as the next generation multimedia signaling and session establishment protocol. In this paper, we explore the design of an efficient approach to inter-domain SIP mobility in an attempt to improve personal and terminal mobility schemes. We apply a persistent identification framework to application level SIP addressing by introducing a level of indirection on top of the traditional SIP architecture. We show how this approach helps achieve efficient inter-domain authentication and call routing towards providing inter-domain mobility. This paper presents the design of H-SIP, while its implementation is described in a companion paper.

I. INTRODUCTION

Low cost, broader data services and deployment of high speed access networks are major drivers pushing service providers and enterprises to adopt packet switched multimedia communication as opposed to current circuit switched and Cellular alternatives. The industry has recently witnessed a rapid increase in the popularity and deployment of Voice over IP services. Enterprises and mobile operators are currently promoting simultaneous Cellphone/Wi-Fi access by introducing dual-mode phones that can switch between the cellular network and the IP packet switched network. Identity persistence issues become obvious and need to be addressed in this context. The Session Initiation Protocol (SIP) [1] and H.323 [2] are among the most widely adopted protocols for IP telephony. We focus in this paper on SIP, due to its simpler implementation and open collaboration. Additionally, SIP has been accepted by 3GPP as a signaling protocol and has been adopted by service providers like Verizon and Sprint to provide IP telephony, instant messaging and other data services. The widespread deployment of SIP is the premise of this paper, as we will leverage this idea to propose an efficient inter-domain mobility scheme for SIP environments.

The session initiation protocol (SIP) [1] is a signaling and control protocol for handling multimedia sessions, allowing the establishment and termination of media streams between two or more participants. The SIP architecture is proposed as an efficient candidate that can be reused to provide personal, terminal and session mobility [3], [4], [5], [6] with a readily available infrastructure. This avoids the redundancy introduced by simultaneous deployment with Mobile IP [7]. The successful reuse of SIP to support both multimedia communications

and mobility simultaneously leverages the issues emanating from SIP users *roaming* across multiple SIP domains. SIP handles user location through the use of a Proxy/Location server that accepts user registration requests and updates the respective user location in a location repository. The protocol inherently implements location independence through the use of the uniform resource identifiers (URI) [8], which directly offers personal mobility. A URI acts as a location independent identifier abstracting the actual physical location of a user with respect to the system. So, SIP allows for personal mobility whether through the use of a Proxy that sets up the session between the calling parties or through the use of redirection servers. However, the protocol defines a user only within the domain boundaries of the service provider. A user must associate with a specific proxy server that handles user authentication as well as initial traffic routing. The proxy maintains a unique account for the user, who in turn, is expected to coordinate with that same proxy irrespective of his location. This requirement translates into undue loads on the SIP server and on a particular domain. Additionally, it complicates the coordination of *roaming* users who must communicate with a central proxy server while roaming. Despite the possible presence of Firewalls and other network restrictions on the foreign domain, roaming users are required to use the central home server instead of using the available local servers. Consequently, while URIs solve the location binding issue, they introduce the domain binding issue. Inefficient traffic routing is a direct consequence of such binding. Besides, the URI identification translates into users needing to be aware of each others' current domain associations. It also brings up the complexity of satisfying calls when initiated from regular keypad terminals.

This paper addresses the inter-domain mobility issue by introducing an abstraction framework based on a unique and persistent identification mechanism. As far the paper is concerned, it only provides an approach that can enhance personal and terminal mobility [5] in current SIP architectures. As to session mobility, the readily available approaches like mid-call mobility [4] or enhancements to that [9] can be used. The framework we propose, referred to as the Handle-SIP or H-SIP, can seamlessly fit within the current SIP architecture allowing SIP users to transparently roam across different SIP domains. H-SIP may thus be gradually deployed.

User location and association are abstracted through the use of globally unique and persistent identifiers called *handles*

which are part of the Handle System [10], [11], [12], [13]. The Handle System is a distributed system extensively used as an indirection layer for the management of persistent Identifiers. Using the Handle System as an intermediate layer on top of multiple distributed SIP implementations allows us to implement seamless multi-domain authentication and call routing.

The rest of the paper details our proposed approach. Section 2 shows how H-SIP is efficiently used to enhance inter-domain SIP mobility. In this section we present a detailed explanation of the proposed inter-domain authentication, registration and call routing mechanisms. In section 3, we describe our conclusions.

II. SIP INTER-DOMAIN MOBILITY

A. Sessions and Mobility

We present an example to clarify the SIP inter-domain mobility problem. Recall that SIP defines a user as an entity that associates with a particular domain. Figure 1 depicts a simple scenario of a roaming user r_user who has a valid association with his home domain $hdomain$ but is currently present in a foreign domain $fdomain$. SIP signaling traffic originating from (REGISTER) or terminating at (arrows 1,2,3: arbitrary SIP user trying to INVITE the roaming user) r_user must inefficiently pass through his home proxy server. Figure 1 identifies this traffic as traditional traffic flow. There are several

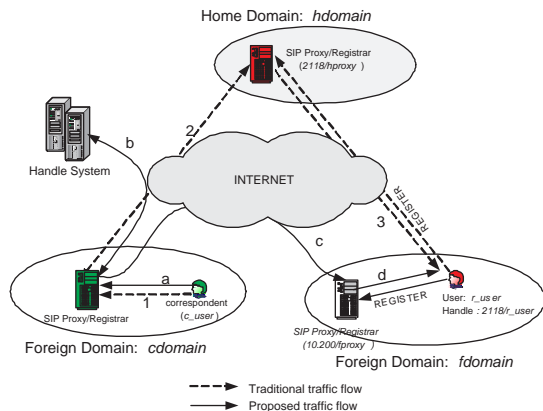


Fig. 1. A Reference inter-domain roaming scenario

ways in which roaming issues can be addressed, depending on whether the SIP architecture is roaming-unaware or modified to become roaming-aware. We study these issues and we present our approach by showing a typical flow for INVITE and REGISTER requests. We also compare the different approaches and illustrate the different scenarios in Figure 2.

- The first scenario shows how SIP naturally handles a call flow for a roaming user. A data flow is presented in Figure 2.A. In this case, no roaming logic is injected into the system (system is roaming-unaware). All requests to/from the roaming user must go through the central home proxy server. The home proxy thus treats both roaming and non-roaming users equally and portrays a

roaming user as merely a home domain user registering with a foreign contact address. Clearly, if the user is present in another country, his traffic would still have to go through his central home proxy (triangle routing) as depicted in Figure 2.A, despite the availability of a local proxy server in the foreign domain (Foreign Server). This results into significant delays that are not accepted for time sensitive applications. Even with SIP mobility management (SIPMM) [3], [4] support (personal, terminal and session mobility) enabled, the same scenario occurs. SIP Mobility allows a user to roam between subnets and domains maintaining accessibility and session continuation using pre-call and mid-call mobility signaling. With pre-call signaling, the mobile user will re-REGISTER with the home proxy anytime his IP address changes. With mid-call signaling, the mobile user will negotiate an address change with the correspondent user while the session is in progress using re-INVITE messages. Mid-call mobility assumes a session is already in progress between the calling parties. Inefficient pre-call traffic routing, and service centralization, are obvious limitations that users roaming in these traditional and Mobile SIP environments have to suffer from. This is the same case also for Mobile IP with Location Registers (MIP-LR) [14], [15], whereas here the SIP proxy servers are replaced with location registers. We argue that our proposed approach to roaming and inter-domain mobility in general, can significantly enhance the SIP personal and terminal mobility performance. Additionally since our approach addresses SIP personal and terminal mobility, we can improve the pre-call portion of any SIP session mobility scheme while other features like mid-call mobility can remain unchanged. For mid-call mobility, current proposals like MIP-LR, SIPMM, or a combination of these two [16]) can be used. These approaches implement mid-call mobility by sending binding updates directly to correspondent nodes without going through Home Agents. Mobile IP (MIP) [7], however, uses Home Agents to forward traffic which creates triangular routing issues. An enhanced version of MIP is MIPv6 [17] that avoids triangular routing and implements route optimization. As to the simultaneous mobility issue, discussed lately in [18], it is left for a future paper to offer a secure framework for simultaneous mobility in the context of H-SIP.

- A second scenario is that of a SIP roaming-aware approach such as the one proposed by Double User Agent Servers [19], that mimics the roaming solution employed in the telecommunication environments. In other words, a user who is roaming outside his home domain, registers with a foreign server. The latter consults the user's home server for redirection, authentication and billing, and proceeds to process the user's transactions. Correspondent users trying to communicate with the roaming user will have to go through his home proxy server which in turn redirects them to the foreign proxy where the

user is currently located. Hence, significant signaling overhead results primarily due to the nature of the SIP URI. The URI is composed of a domain part, like in $r_user@hdomain$, thus forcing the calls directed to this user to go through the $hdomain$ proxy server first. The data flow for this scenario is presented in Figure 2.B. We argue that this approach is inefficient as it introduces unnecessary overhead and load on the original server .

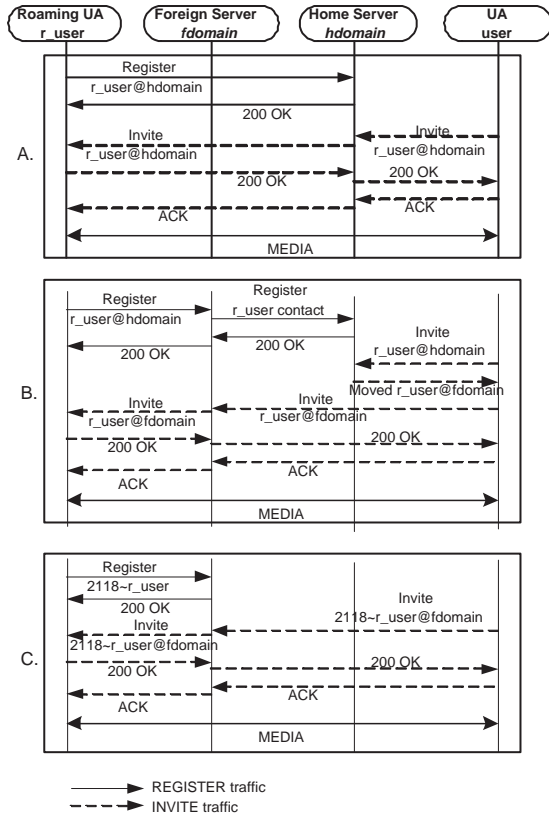


Fig. 2. SIP traffic flow A. With no roaming logic B. With traditional roaming logic C. With proposed roaming logic

In the two scenarios above, the use of URIs to identify users and the inherent dependence of the URI on a particular domain, complicates message routing. One solution is to abstract the actual identifier eliminating per-call coordination to minimize the signaling traffic in highly mobile environments.

B. H-SIP: Abstraction layer

Our proposed approach uses *handles* as globally unique identifiers to locate and identify SIP architectural elements. This abstraction allows the system to route calls independent of user location and domain association. We refer to the modified SIP framework as the Handle-SIP or H-SIP. Note that we have also exploited this abstraction approach at the level of network devices and services in [20], [21]. Briefly, the Handle System [10], [11], [12], [13] is intended to be a means of universal basic access to registered digital objects [22]. It provides a distributed, secure and global name service for administration and resolution of *handles* over the Internet. A

handle is a persistent name that can be associated with a set of attributes. Some of these attributes can describe location, permissions, administrators and state. The fact that *handles* are defined independently of any of the attributes or public keys of the underlying objects, makes them persistent identifiers [23]. These identifiers are managed and resolved using a secure global name service that guarantees the association of the identifier with its respective attributes over distributed communication.

Security is a crucial property of the Handle System. The system acts as a certification authority assuring that attributes of the name/reference are securely transferred between the communicating ends. Hence, the Handle System allows for secure name resolution and administration in a distributed fashion making it highly scalable and suitable to operate in mobile environments. In our approach, elements of the SIP architecture, SIP users and proxy servers, are identified with *handles* abstracting any domain binding. Users will identify each other, and identify the SIP servers they associate with using *handles* instead of URIs and domain names respectively. In Figure 1, the roaming user r_user will have his own *handle* $2118/r_user$ with the necessary administrative privileges over the *handle*. Additionally, the home proxy server has a *handle* $2118/hproxy$, and the foreign proxy server has a *handle* $10.200/fproxy$. Note that a *handle* has the form "*prefix/suffix*". The prefix represents the naming authority (NA) while the suffix represents a unique local name under the NA namespace [10], thus rendering the *handle* globally unique. A possible realization of the *handle* $2118/r_user$ inside the Handle System is depicted in Figure 3. The *handle* has several

handle	Field Type:index	Value
2118/r_user	HS_ADMIN:100	nwr:0.NA/2118:300
	HS_ADMIN:101	nwr:2118/r_user:200
	HS_VLIST:200	nwr:2118/r_user:300
		nwr:2118/hproxy:300
		nwr:10.200/fproxy:300
SIP_URL:250	sip:2118.r_user@x.y.z.w	
SIP_PWD:251	password	
HS_PUBKEY:300	00BE0034.....	

Fig. 3. Sample user *handle* structure

fields. The HS_ADMIN and HS_VLIST fields determine the administrators of the *handle* who are the naming authority ($0.NA/2118$), the *handle* itself ($2118/r_user$) and the two proxy servers in the HS_VLIST field. Any of these administrators has the privilege to modify the fields inside the *handle* provided the administrator succeeds to authenticate with the Handle System using his private key.

C. Authentication and Registration

Currently, the most common authentication mechanism employed by SIP is the digest authentication [24] used by HTTP. When a user associates with a domain proxy server, he obtains an account on that server with a username and password which

he uses to authenticate himself to the server if asked to. The digest authentication depicted here is domain dependant i.e. the user's credentials are valid for a particular domain. Briefly, digest authentication proceeds as follows:

- 1) User sends a REGISTER request to a SIP proxy/registrar server.
- 2) The server replies with a 401 unauthorized response message challenging the user to authenticate himself for the requested service (realm) through a user and password prompt.
- 3) The user sends back a message digest of his credentials, which include his username, password etc.
- 4) The same message digest is computed internally using the server's internal user information and compared to the one sent by the user.
- 5) Authentication is granted if the two digests match.
- 6) User registers with the SIP proxy/registrar server.

In our approach, we still use digest authentication for the SIP users due to its wide support by current SIP servers and user agents, although a better authentication mechanism can be designed that would leverage the inherent security that *handles* expose.

Access to the authentication information is controlled inside the Handle System by the users. Recall that each user owns and administers his own *handle*. As part of this process, the user specifies in the HS_VLIST field, the set of *handles* that have administrative rights over his *handle*. Among these *handles*, the user should include *handles* of any SIP proxy server that he wishes to register with, which could be any foreign server(s) that he trusts.

Two approaches can be exploited to implement the logic needed by the current SIP architecture for supporting *handle* authentication and registration. The first is to modify the actual SIP servers by extending their functionality through a server plug-in. This approach requires absolutely no changes to the current User Agent devices whether hardphones or softphones. The devices will adapt seamlessly to the system. Alternatively, a second approach would be to modify the User Agent devices instead, which is a more cumbersome task that would require software upgrades for all existing User Agents.

This paper implements the first approach that deals with extending the functionality of the proxy/registrar servers. We present the proposed solution in light of the reference example of Figure 1. In Figure 3, the roaming user *2118/r_user* has granted both SIP proxy servers *2118/hproxy* and *10.200/fproxy* administrative rights over his *handle*. Note that the VLIST could refer to another *handle* containing a list of globally trusted servers. For the roaming user *r_user* present in the foreign domain *fdomain*, the authentication/registration process with the foreign proxy server *10.200/fproxy*, depicted in Figure 2.C and Figure 1 (proposed traffic flow, arrows a,b,c,d), proceeds as follows:

- 1) *r_user*, after including the *handle 10.200/fproxy* in his *handle* HS_VLIST field, sends a REGISTER request to *fproxy*.

- 2) *fproxy* challenges *r_user* to authenticate himself.
- 3) *r_user* uses same digest authentication with username as the *handle 2118/r_user* and password as the value of the SIP_PWD field that he created in his *handle* as shown in Figure 3.
- 4) *fproxy* uses the Handle Protocol [12] to resolve the *handle 2118/r_user* into the SIP_PWD field. The server then computes a message digest over the obtained credentials.
- 5) Authentication is granted if the two digests match.
- 6) After authenticating *2118/r_user*, the foreign proxy *fproxy* proceeds to create an internal account for *r_user* to be able to use the SIP services on *fproxy*. The internal user account will have a username identical to the *handle* of the registering user with the '~' replaced by '.' i.e *2118.r_user* in this case.
- 7) Registration of the user follows. This requires that *fproxy* modifies the *handle 2118/r_user* updating the field SIP_URL to point to the internal account, *2118.r_user@x.y.z.w* in this case, as shown in Figure 3. This means that *r_user* is currently associated with *fproxy*.

Obviously, our modified authentication algorithm is domain independent. In other words, the user's credentials are valid for all realms provided the correct administrative privileges are set in the Handle System. This property is essential, as it allows a particular authenticated SIP message to traverse multiple domains instead of requiring re-authentication for each domain on the path of the message. Since all communication between the Proxy and the Handle System is secure [12], the proxy can be reasonably certain that the roaming user is indeed who he claims to be by validating his credentials against the secure *handle*. Internally, the proxy server monitors the user accounts created and removes an account (also updating the *handle*) due to unregister requests or account expiration. A sample *handle* for the foreign proxy is shown in Figure 4. Devices,

handle	Field Type:index	Value
10.200/fproxy	HS_ADMIN:100	nwr:0.NA/10.200:300
	HS_ADMIN:101	nwr:10.200/fproxy:300
	INET_HOST:240	x.y.z.w
	HS_PUBKEY:300	00BE00445.....

Fig. 4. Sample proxy *handle* structure

whether hardphones and softphones are treated similarly. This depends on the ability of the device owner to present the SIP proxy with a username (could be the *handle*) and password for authentication. With this approach, a user does not need to register with a home proxy server as would otherwise be required by pre-call mobility [4]. After registering with the foreign server, the user's handle-to-URI mapping remains fresh allowing correspondent users to reach him simply by addressing his *handle* as we will show in the section II-D.

D. Routing

After abstracting any domain binding from users and allowing seamless authentication and registration with local proxy

servers, the next step is to permit the user to initiate and receive calls by addressing a particular *handle* with no explicit reference to domain bindings (URIs). In this sense, a SIP user can INVITE any other SIP user provided he knows the latter's *handle*. From the perspective of a user, all other users seem to belong to one local domain and abstraction is complete. To explain how the call routing is achieved, we will go through the steps where an arbitrary SIP user *c_user* (caller) tries to INVITE the roaming user *r_user* (callee) using the latter's *handle* *2118/r_user* as shown in Figure 1. The call routing process, presented in Figure 2.C, proceeds as follows:

- 1) Caller *c_user* sends an INVITE request to *r_user*. The invite request reaches the caller's SIP proxy/registrar containing the following header fields:

```
INVITE sip:2118~r_user@somedomain SIP/2.0
To:<sip:2118~r_user@somedomain> .....
```

Note that in this message, the domain *somedomain* is irrelevant to our approach. We are only concerned with the *handle* part of the Request-URI. To distinguish between *handle* and non-*handle* requests, we resort to the '~' character¹ in the host name.

- 2) Proxy checks if the *handle* *2118~r_user* is a locally registered user. If not, the server resolves the *handle* into the SIP_URL field which is *2118.r_user@x.y.z.w* in this case as shown in Figure 3.
- 3) The server then rewrites the target URI of the message to the resolved URI.
- 4) From this point on, the natural SIP call flow is leveraged and the traditional SIP architecture [1] is utilized for efficient call routing. Note that other proxy servers on the call path treat the request as a normal request i.e. no *handle* resolution is required.

Again, with our approach, correspondent users trying to communicate with the mobile user need not go through a home proxy for session setup or redirection. This renders the call route more efficient eliminating unnecessary overhead and significant round-trip times. One last point worth mentioning is the ability of a user to register with multiple servers from different devices simultaneously using the same *handle*. In our implementation, the *SIP_URL* field of a particular *handle* can contain a list of bindings (URIs) to enable this attractive property. Exploiting this property is left for future papers.

III. CONCLUSIONS

In this paper, we have outlined the use of an indirection architecture based on the Handle System to address SIP inter-domain mobility. Our approach not only enables roaming controlled by the users rather than organizations, but also provides a faster implementation than traditional approaches currently deployed. Throughout our work, users are able to dynamically enable their own mobility and benefit from the advantages of a secure distributed persistent identifier network. By disassociating users from DNS domains, while still providing the means to interact with traditional SIP systems, we

¹Since Internet hostnames can not contain the '~' character [25] ascii (0x2F) (essential character in the *handle* Namespace [10]), we replaced it with the '~' ascii (0x7E) character in the examples above for implementation purposes. We also allow the '#' ascii (0x23) character for compatibility with hard IP phones.

provide a scalable interchangeable enhancement to the SIP infrastructure. In part II [26], we describe the implementation details of our architecture.

REFERENCES

- [1] J. Rosenberg, H. Schulzrinne, and etal., "Sip: Session initiation protocol," RFC 3261, June 2002.
- [2] "H.323 : Packet-based multimedia communications systems," <http://www.itu.int/rec/T-REC-H.323-200307-1/en>.
- [3] E. Wedlund and H. Schulzrinne, "Mobility support using sip," 2nd ACM/IEEE International Conference on Wireless and Mobile Multimedia, Seattle, WA, August 1999.
- [4] H. Schulzrinne and E. Wedlund, "Application-layer mobility using sip," in *Service Portability and Virtual Customer Environments*. IEEE, December 2000, pp. 29–36.
- [5] R. Pandya, "Emerging mobile and personal communication systems," *IEEE Communications Magazine*, vol. 33, pp. 44–52, June 1995.
- [6] A. Dutta, F. Vakil, J. Chen, M. Tauli, S. Baba, N. Nakajima, and H. Schulzrinne, "Application layer mobility management scheme for wireless internet," 2001.
- [7] C. E. Perkins, "Ip mobility support for ipv4," RF 3220, January 2002.
- [8] T. Berners-Lee, R. Fielding, and L. Masinter, "Uniform resource identifiers (uri): Generic syntax," RFC 2396, August 1998.
- [9] N. Banerjee, S. K. Das, and A. Acharya, "Sip-based mobility architecture for next generation wireless networks," in *Pervasive Computing and Communications*, PerCom 2005. Third IEEE International Conference, March 2005, pp. 181–190.
- [10] S. Sun, L. Lannom, and B. Boesch, "Handle system namespace and service definition," RFC 3651, November 2003.
- [11] S. Sun, L. Lannom, and B.Boesch, "Handle system overview," RFC 3650, November 2003.
- [12] S. Sun, S. Reilly, L. Lannom, and J. Petrone, "Handle system protocol (ver2.1) specification," RFC 3652, November 2003.
- [13] "The handle system," <http://www.handle.net>.
- [14] R. Jain, T. Raleigh, D. Yang, L.-F. Chang, C. Graff, M. Bereschinsky, and M. Patel, "Enhancing survivability of mobile internet access using mobile IP with location registers," in *INFOCOM*, 1999, pp. 3–11.
- [15] R. Jain, T. Raleigh, C. Graff, M. Bereschinsky, and M. Patel, "Mobile internet access and qos guarantees using mobile ip and rsvp with location registers," vol. 3. ICC International Conference on Communications, June 1998, pp. 1690 – 1695.
- [16] K. Wong, A. Dutta, J. Burns, R. Jain, K. Young, and H. Schulzrinne, "A multilayered mobility management scheme for auto-configured wireless ip networks," *Wireless Communications*, vol. 10, no. 5, pp. 62–69, October 2003.
- [17] D. Johnson, C. Perkins, and J. Arkko, "Mobility support in ipv6," IETF RFC 3775, June 2004.
- [18] K. Wong, A. Dutta, H. Schulzrinne, and K. Young, "Simultaneous mobility: analytical framework, theorems, and solutions," *Wireless Communication and Mobile Computing*, June 2006.
- [19] C. Hongtao, Y. Fangchun, and X. Peng, "Analysis on sip mobility of double user agent servers," in *Communications and Information Technology*, vol. 1, ISCIT. IEEE, October 2005, pp. 87–90.
- [20] H. Jerez, C. Abdallah, and J. Khoury, "A mobile transient network architecture," 2006, pre-print available at <https://dSPACE.istec.org/handle/1812/55>.
- [21] J. Khoury, H. Jerez, N. Nehme, and C. Abdallah, "An application of the mobile transient network architecture: Ip mobility and inter-operability," 2006, pre-print available at <https://dSPACE.istec.org/handle/1812/54>.
- [22] R. Kahn and R. Wilensky, "A framework for distributed digital object services," Internet Whitepaper <http://www.cnri.reston.va.us/k-w.html>, January 1995.
- [23] S. Sun, "Establishing persistent identity using the handle system," Tenth International World Wide Web Conference, May 2001.
- [24] J. Franks, P. Hallam-Baker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen, and L. Stewart, "Http authentication: Basic and digest access authentication," RFC 2617, June 1999.
- [25] K. H. etal., "Dod internet host table specification," RFC 952, October 1985.
- [26] J. Khoury, H. Jerez, and C. Abdallah, "H-sip inter-domain sip mobility: Implementation," pre-print available at http://hdl.handle.net/2118/sip_impl.