Thierry Ernst
Hong-Yon Lach
Claude Castelluccia
Motorola Labs and INRIA Planete, France

13 July 2001

"Network Mobility Support in IPv6: Problem Statement and Requirements"

draft-ernst-mobileip-monetv6-00.txt

Status of This Memo

Abstract

This draft addresses the problems of routing datagrams to nodes located in an IPv6 mobile network. A mobile network is one or more IP-subnets attached to a mobile router and mobile as a unit. The mobile router dynamically changes its point of attachment. Applications of mobile networks include networks attached to people (PANs) and networks of sensors deployed in an aircraft, a boat, or a car.

This draft defines a terminology and presents a number of specific issues faced by mobility of an entire network. An explicit mobility support scheme is required, what we call "network mobility support" in contrast with "host mobility support". We have listed a number of requirements that need to be addressed by network mobility support.

Contents

Introduction

This document addresses the question of routing datagrams to nodes located in an IPv6 mobile network, i.e. network mobility support. We define a mobile network as an entire network that dynamically changes its point of attachment in the Internet and thus its reachability in the Internet.

The first section gives the motivations for network mobility support. We then describe mobile networks and we define a new terminology used throughout this study (section 1.2). There may exist various kind of mobile networks and they obviously have specific characteristics as depicted in section 1.3. Section 1.4 explains what this study tries to achieve. Section 1.6 concludes this section with a number of issues faced by network mobility support.

Network mobility support in wide-area IPv6 networks has to comply with a number of constraints and requirements. Constraints limit the implementation and the deployment of a potentially and ideally good solution, and solutions need to fulfill a number of requirements. Some requirements must be solved whereas other should be solved whenever possible. Constraints and requirements for network mobility support are discussed in the second section. Most constraints and requirements that we have listed are equally applicable to host mobility support and network mobility support. Some of them have been debated in the literature as far as host mobility support was concerned; we have extended this list to include those related to mobile networks.

1. Definitions and Problem Statement

1.1. Motivations

The purpose of traditional mobility support is to provide continuous Internet connectivity to mobile hosts (host mobility support). There are situations where an entire network might move and attach to different locations in the Internet topology. In this paper, we refer to a network as a set of nodes that share the same IP prefix and that are attached to the Internet through a border router. We refer to a mobile network as a network whose border router is a mobile router which dynamically changes its point of attachment to the Internet and thus its reachability in the Internet.

Cases of mobile networks include networks attached to people (Personal Area Network or PAN) and networks deployed in aircrafts, boats, cars, trains, etc. An Ad-hoc network as defined in manet is not to be confused with a mobile network; however it may become a mobile network when its border router changes its point of attachment

to the Internet. As an example of a mobile network, we could think of an airline company that provides permanent on-board Internet connectivity. This allows all passengers to use their laptops to connect to remote hosts, download music or video from any provider, or browse the web. The Internet could also be used to exchange information between the aircraft and air traffic control stations. This scenario has already been investigated by Eurocontrol (European Organization for the Safety of Air Navigation [8]). During the flight, the aircraft changes its point of attachment to the Internet and is reachable by different care-of addresses over time, most likely owned by distinct Internet service providers. This scenario justifies that mobile networks may be of a big size, containing hundreds of hosts and several routers and may attach to very distant parts of the Internet topology. Moreover, it shows that we face two distinct levels of mobility, node mobility and network mobility, since laptops owned by passengers are themselves mobile nodes visiting the aircraft mobile network. However, this paper does not address the specific issues involved when mobile nodes visit the mobile network. We are focusing on the general case.

1.2. Terminology

We mostly adopt the terminology already defined in the IPv6 [5] and Mobile IPv6 [6] specifications. We also introduce the following new terms relevant to mobile networks. A mobile network attaches to the rest of the Internet through its border routers which we refer to as the mobile routers (MRs). A mobile router has at least two interfaces, the first attached to the home link or the foreign link, and the other attached to an internal link of the mobile network. We call mobile network node (MNN) any host or router located within the mobile network, either permanently or temporarily.

All MNNs located in the same mobile network share a common and permanent IP prefix that we call the Mobile Network Prefix. The Mobile Network Prefix is a bit string that consists of some number of initial bits which identifies the set of subnetworks that compose the mobile network. It also identifies the topological location of the mobile network when the mobile router is attached to its home link. In addition, we call correspondent node (CN) any node external to the mobile network that is communicating with one or more MNNs. The terminology is summarized in fig.1.

Mobile Network

A set of nodes which are mobile, as a unit, with respect to the rest of the Internet, i.e. a mobile router and all its attached nodes. The mobile router changes dynamically its point of attachment to the Internet and thus its reachability in the Internet. All nodes in the mobile network share the same IP

prefix: the Mobile Network Prefix. Note that a mobile network may be composed by one or more IP-subnets.

```
    ____
   |    |
   | CN |
   |____|
  ___|____________________
 |                        |
 |                        |
 |       Internet         |
 |                        |
 |________________________|
    __|_            __|_
   |    |  Access  |    |
   | AR |  Router  | AR |
   |____|          |____|
______|__ foreign   __|_____________ home
          link               __|_    link
                            |    |
                            | MR | Mobile Router
                            |____|
                      _________|_______  internal
                       __|__     __|__   link
                      |     |   |     |
                      | LFN |   | LFN | Local Fixed Nodes
                      |_____|   |_____|
```

Figure 1: Terminology

Mobile IP-subnet

A mobile network that is composed of a single IP-subnet.

Mobile Router (MR)

The border router of a mobile network which attaches the mobile network to the rest of the Internet. The mobile router has at least two interfaces, an external interface, and an internal interface. The mobile router maintains the Internet connectivity for the mobile network. It is used as a gateway to route packets between the mobile network and the fixed Internet.

External Interface of a Mobile Router

The external interface of a mobile router is attached to the home link if the mobile network is at home, or is attached to a foreign link if the mobile network is in a foreign network.

Internal Interface of a Mobile Router

The internal interface of a mobile router is attached to an internal link within the mobile network. This interface is configured with the Mobile Network Prefix (see definition below) for all the MNNs inside the mobile network.

Local Fixed Node (LFN)

Any host or router permanently located within the mobile network and that does not change its point of attachment.

Local Mobile Node (LMN)

A mobile node that belongs to the mobile network and that changes it's point of attachment. The home link of the LMN is a link within the mobile network. The LMN may attach to any link within the mobile network, or to any link outside the mobile network.

Visiting Mobile Node (VMN)

A mobile node that does not belong to the mobile network and that changes it's point of attachment. The home link of the VMN is not a link within the mobile network. A VMN may attach to a link within the mobile network and obtain a careof address on this link.

Mobile Network Node (MNN)

Any host or router located within the mobile network, either permanently or temporarily. A MNN could be any of a MR, LFN, VMN, or LMN.

Node behind the MR

A synonym for a mobile network node (MNN). See corresponding definition.

Correspondent Node (CN)

Any node located outside the mobile network that corresponds with any of the MNNs. By extension, we say that CNs corresponding with MNNs of a mobile network are CNs of this mobile network.

Access Router

Any subsequent point of attachment of the mobile network at the network layer. Basically, a router on the home link or the foreign

link.

Home subnet prefix

A bit string that consists of some number of initial bits of an IP address which identifies the home link within the Internet topology. (i.e. the IP subnet prefix corresponding to the mobile node's home address, as defined in [6]).

Foreign subnet prefix

A bit string that consists of some number of initial bits of an IP address which identifies a foreign link within the Internet topology.

Mobile Network Prefix

The network prefix that is common to all IP addresses in the mobile network when the mobile router is attached to the home link. For a mobile network containing only one subnet, the Mobile Network Prefix is the prefix of this subnet ("home subnet prefix" as defined in [6]). Note that the Mobile Network Prefix may not be the home prefix.

1.3. Characteristics

Structure of the mobile network

The internal structure of a mobile network is preserved while it is moving. As a result of the mobility of the mobile network, MNNs do not change their point of attachment; however, MNNs move from the point of view of their CNs. From a routing perspective, a mobile network may therefore be virtually perceived as a single node (the MR) with a topologically correct address or prefix. The topological location of a MNN being dependent of the location of the MR, the knowledge of the topological location of the MR is sufficient for routing datagrams from a CN towards a MNN.

Mobile Router is a transit point

All packets sent from any CN to a MNN necessarily transit through the MR. As a result, providing the CN with the current location of the MR in the Internet topology may be sufficient for optimally routing packets intended to a MNN.

Size of the mobile network

A mobile network may comprise one or more subnetworks. Its size

could scale from a sole subnetwork with a few IP devices, such as in the case of a PAN, to a collection of subnets with hundreds of IP devices, such as in a train.

Large number of CNs

A mobile network may have a very large number of CNs. For instance, each passenger in a train may be considered a MNN. Each of them may be communicating with a few CNs. As a result, the total number of CNs would be several times as large as the number of MNNs and could scale up to a few thousands.

Nested mobility

A mobile network may comprise mobile nodes (local mobile nodes or visiting mobile nodes) and even other mobile networks. For instance, a bus is a mobile network whereas passengers are mobile nodes or even mobile networks themselves if they carry a PAN.

Various mobility frequencies

Mobile networks may not move with the same speed and frequency. For instance, a PAN connected to the Internet via a WLAN, or a car connected to the Internet via GSM are likely to change their point of attachment very quickly, while an aircraft or a boat may be connected to the Internet via the same satellite link for a couple of hours. Obviously, mobile networks may not move at all for a large amount of time.

Multi-homing

A mobile network may be multi-homed. By multi-homing, we mean that the MR may have two or more active interfaces connected to distinct parts of the Internet, or the mobile network may be connected to the Internet via tow or more MRs. In the first case, we could think of a unique device used to connect a car both to the cellular phone network and to a navigation satellite. In the second case, we may think of a PAN where the GSM is used to connect the PAN to the cellular phone network whereas a PDA is used to collect bus timetables from the city bus network.

Routers in the mobile network

All routers in the Internet are considered to run a number of protocols such as a routing protocol, Neighbor Discovery, ICMP, and others. This also applies to any router in the mobile network, including the mobile router.

Ad-hoc network

An ad-hoc network that changes its point of attachment to the Internet may be seen as a mobile network.

Idle Mobile Network

A mobile network that does not engage in any communication outside the network may be considered as idle from the point of view of the fixed Internet, although there may be internal traffic between any two MNNs.

Idle Mobile Network Node

A MNN that does not engage in any communication.

1.4. Aim of network mobility support

The purpose of network mobility support is to provide MNNs with an uninterrupt Internet connectivity and to route datagrams between CNs and MNNs by the most optimal path in both directions.

1.5. Assumption

We limit the scope of our study to mobile networks that are stub networks, i.e. the mobile network does not forward traffic not intended to itself.

1.6 Issues

Mobility of networks has an impact on routing, addressing, and a number of network protocols.

1.6.1. Routing Issues

All packets sent to a MNN must transit through the current AR of the mobile network and the MR itself. As a result of mobility, the path to the mobile network is varying according to the AR to which the MR is currently attached. We have to investigate how this path could be determined in order to route packets via the most optimal path. Particularly, we need to examine if this is best solved by routing protocols or by some transient means as this is done for mobile hosts. We need to investigate:

o if there is a need for a CN to determine that the node it is corresponding with is in a mobile network.

o if there is a need to determine the topological location of

the mobile network or the mobile network node.

o if there is a need to determine the AR where the mobile network is currently attached.

o if correspondent nodes should be aware of the topological location of the mobile network or the mobile network node or if this should this be transparent to them

o if forwarding should be established from a former AR to a latter one.

1.6.2. Addressing Issues

o Impact on MR

Following existing IPv6 specifications, any host is in theory required to obtain a topologically correct address on the link on which it is currently attached to. We must investigate if this can alternatively be done for a single host or for a router and for a mobile network. If yes, this means that the external interface of the mobile network is configured with the foreign prefix. We also have to investigate if the configuration of the MR's interface with a new address has an impact on the MNNs.

o Impact on MNNs

As for MNNs, they don't actually change their own point of attachment, then it is very questionable whether MNNs should also get a topologically correct address that actually reflects their topological [and hierarchical] location in the Internet. If we conclude that mobile network nodes should get a topologically correct address, we have to determine how this could be performed internally in the mobile network. If we renumber, we have to investigate how to maintain connections and how and where to advertise the new address; if we do not renumber, we have to investigate how to perform optimal routing between CNs and MNNs.

1.6.3. Network Protocols Issues

As seen in section 1.3, all routers in a mobile network are routers like the others and have to run a number of protocols. Following the existing IPv6 specifications, they particularly should run at least an instance of a routing protocol, and other protocols like Neighbor Discovery, etc. We therefore have to investigate how the network protocols running in the mobile

network must interact with the network protocols running in each subsequent visited network and how the mobile router is going to interact with the ARs it attaches to. This raises a number of issues for each network protocol, as listed in the following sections.

o Impact on Neighbor Discovery

One task of Neighbor Discovery is to send Router Advertisements and Router Solicitations. When the mobile router is attached to some AR in a visited network, it should receive such Router Advertisements from its current AR. We have to investigate how those Router Advertisements should be processed by the mobile router and how the mobile router should interact with this instance of the protocol running at the AR. We also have to investigate what is the impact on this protocol when the mobile network leaves its point of attachment.

o Impact on the Visited Network

We have to investigate if the subsequent ARs and the other routers in the visited network should be aware that the visiting mobile node is a router and not a host. In addition, we have to examine if it is necessary to let them know that there is an entire network behind the mobile router. In such a case, a network route may have to be propagated in the visited network and this raises an additional number of issues as discussed in the section about routing protocols.

o Impact on Routing Protocols

We have to investigate how the mobile router interacts with the routing protocols running at each of its subsequent ARs. The impact may not be the same whether the mobile network is limited to a single IP-subnet or a number of IP-subnets. Indeed, a single mobile IP-subnet may not need to run an instance of a routing protocol whereas a mobile network comprising more than one router may. We have to evaluate what kind of routing protocols may run in a mobile network and how it interacts with the routing protocol running at each of its subsequent ARs.

oo In case the mobile network is running the same routing protocol as its ARs, it is questionable whether the mobile network should participate or not in the routing protocol running in the visited network. If it does, the mobile network can be seen as a partition of the local network. The topology computed by the routing protocol becomes more

dynamic and we have to evaluate how existing protocols are able to handle this case. Moreover, mobility may cause a routing table partition.

oo In case the mobile network doesn't participate in the routing protocol running in the visited network, the mobile network can be seen as a kind of Autonomous System that is running an instance of an Internal Gateway Protocol.

routing protocol running in the mobile network and the routing protocol running in the visited network. In addition, we must determine what routing protocol is suitable within the mobile network. We also have to evaluate the impact on routing protocols when the mobile router is multi-homed, when the mobile network comprises more than one mobile router, and when the mobile network itself receives another mobile network.

1.6.4. Security Issues

All security concerns that usually apply to host mobility support also apply to network mobility support. We may face a number of additional ones that complement the addressing issues, network protocols issues, and routing issues depicted in the previous sections.

2. Constraints and Requirements

2.1. Constraints

2.1.1. Host Mobility Support constraints

LMNs and VMNs that operate Mobile IPv6 must still be able to use the same protocol once located in a mobile network. If needed, the solution to support mobile networks has to provide the necessary Mobile IPv6 extensions.

2.1.2. Addressing constraints

The network part of IP addresses is used for routing and identifying the subnetwork in the topology. Every interface attached to a subnetwork must have a unique address with the network part identifying the subnetwork.

2.1.3. IPv6 constraints

In order not to re-invent the wheel, any solution has to be based on IPv6 protocols. It is also desirable that it becomes an integral part of the existing protocol suite. It is desirable to introduce new features as extensions to the existing protocols with minimum modifications.

2.1.4. Security constraints

Any solution must comply with IPv6 security policies.

2.2. Requirements

Requirements relative to mobility of hosts are discussed in most published papers in the field of mobile networking as found in [1] and also [7, 4]. [OTHERS]. Most of them are equally applicable to network mobility support, with some additions.

2.2.2. Wide-Area mobility support

A truly worldwide mobility support requires international standards in order to move between heterogeneous networks, i.e. wide-area mobility. A lack of international standardization would prevent from this. We must avoid a situation where distinct Internet Service Provider would develop distinct network mobility support schemes which are unable to inter-operate with each other. Not only standard between countries and organizations is required, but also between networks in which different policies may apply. Indeed, nothing but administrative and security policies should prevent a mobile network to attach anywhere in the Internet. For doing so, we need a mobility support scheme that fits well into the existing standards, that is easy to deploy and that does not require too much additional services in the network.

2.2.3. Security

Unlike fixed nodes, MNNs are more exposed to security issues and identity usurpation. Mobility support must provide MNNs and their CNs with at least as good security as for fixed nodes and single mobile nodes. In practice, network mobility support signalling must be exchanged in a secure manner and must ensure the following:

o Confidentiality

Mobility support must ensure confidentiality of all control datagrams transmitted between MNNs and CNs in any direction to insure MNNs' confidentiality. If requested, only the recipient must be able to decrypt the content of the datagram.

o Authentication   All control messages must be authenticated by recipients in order to prevent intruders to usurp the identity of a MNN. Mobility support shouldn't leave more room for intruders to usurp an identify nor to perpetrate any kind of attack against MNNs or CNs.

o Authorization

Mobility support must ensure that a node which performs a mobility management operation is effectively authorized to perform such an operation.

o Location Privacy

Mobility support has to provide means for to keep the location of MNNs secret to any third party. It shouldn't be possible to determine the topological location of a mobile network and its MNNs by monitoring control messages exchanged between any two nodes. In practice, MNNs may wish to hide their location to some or all of their CNs. The network administrator may also wish to hide the location of the mobile network to all CNs without discrimination between MNNs.

2.2.4. Transparency

o Mobility Transparency

With respect to the layer separation of the Internet protocol suite, handover of IP sessions should be transparent at layers above the network layer. At least, there shouldn't be an abrupt interruption of the IP sessions. This means that a mobile network is always reachable regardless of its point of attachment. Particularly, mechanism have to be added so that transiting datagrams are forwarded to the current location of the mobile network.

o Operational Transparency

From an application's point of view, continuous access to the Internet must be maintained regardless of the location of the mobile network. Moreover, it is required that the application does not need to perform any action to remain connected. This means that mobility support should be performed at the network layer. It is the responsibility of the network protocols to support connectivity of the network in an absolute transparent manner to the applications.

o Mobility management transparency for MNNs

We have seen that MNNs appear to move from the point of view of their CNs although do not change their point of attachment within the mobile network. Mobility management of a mobile network is therefore better seen as MR's responsibility and should be transparent to MNNs. MNNs should have no responsibility in network mobility management. They should only be concerned about managing their own mobility if they

themselves appear to change their point of attachment. However, MNNs may encounter variable delays of transmission and loss with their respective CNs as the network is moving.

o Performance Transparency

Network mobility support should exhibit low latency, incur little or no data loss, minimum delays, scale to a large internetwork, incur minimum signalling load, bandwidth consumption for datagrams delivery and memory requirements, as seen in [3]. The solution is termed "efficient" provided mobility is supported without performance degradation of the Internet. Loss and delays should indeed range into those experimented for communication flows between two fixed nodes. Moreover, both local-area mobility and wide-area mobility need to be handled as efficiently. At last, the addition of network mobility support shouldn't impact the performance of upper layers. In order to limit losses during hand-offs and to avoid degradation of performance at the upper layers, it may be necessary to perform seamless handovers.

o Layers Independence

Support of mobility is best managed at the network layer. A change of topological location therefore shouldn't have any repercussion at other layers of the TCP/IP reference model. If this is respected, compatibility with existing transport and application layers is maintained. Support of mobility in transport and application protocols is not the focus of this study.

2.2.5. Optimal routing

The amount of traffic intended for the mobile network is understandably more significant than in the case of a single mobile node. Non-optimal routing therefore becomes an even more important issue that it was already for mobile nodes. Avoiding triangle routing reduces bandwidth consumption and transmission delays.

2.2.6. Minimum signalling overload

Routing packets efficiently from a CN to the current location of the mobile network may be performed at the cost of control traffic. The cost of this control traffic has to be balanced against the expected gain of optimal routing. Minimizing the amount of control traffic has always been an important concern for host mobility support. Due to a potentially large number of CNs,

this becomes an even more important concern for network mobility support.

2.2.7. Scalability

Scalability has always been an important concern in the design of new protocols. As far as host mobility is concerned, mobility support has to take into consideration a growing number of mobile hosts and should even assume that a major part of the nodes composing the Internet are mobile in the near future. This means that signalling load and memory consumption should scale to an important number of mobile nodes. Network mobility support has to address scalability in two ways:

o Large number of mobile networks Scaling to a large number of mobile networks as hosts mobility support is required to scale to a large number of mobile nodes.

o Large number of correspondent nodes Scaling to the size of large mobile networks comprising hundreds of MNNs communicating with an important number of CNs.

In other words, mobile network support must be able to support large mobile networks containing hundreds of nodes like a train and corresponding with thousands of CNs, and a very large number of small mobile networks such as PANs comprising a few IP devices. Scaling to a large number of CNs indeed deserves more consideration than scaling to a large number of mobile networks.

2.2.8. Nested mobility

Network mobility support must allow VMNs to visit the mobile network and LMNs to leave it. Basically, a VMN should be able to operate Mobile IPv6 or any forthcoming standard. Network mobility support should therefore consider both mobile networks and mobile nodes, otherwise it may hardly interact with host mobility support. In practice, it should handle visiting mobile nodes as optimally as if networks where fixed. It is also advisable to consider the special case where the correspondent node is itself mobile or located in a mobile network.

2.2.9. Backward compatibility

Backward compatibility corresponds to the ability to leave the actual protocol suite unchanged. This was an important issue for IPv4 since it is not possible to require all hosts to implement new features in order to manage mobility. On the other hand, the emergence of IPv6 is an opportunity for making the necessary

changes. Backward compatibility is not an issue at the time being although IPv6 itself has to interwork with IPv4. Indeed, IPv6 offers the possibility to add new features until the IPv6 specification is fully ratified. There is still scope for adding new capabilities if needed.

2.2.10. Minimum Impact on Existing Protocols

In order to provide a deployable solution and to allow wide-area mobility, a good solution should better make use of the existing protocols whenever possible and impose minimum changes or extensions on the existing ones.

References

[1] Pravin Bhagwat, Satish Tripathi, and Charles Perkins. Network Layer Mobility: an Architecture and Survey. IEEE Personal Communications, 3(3):54, June 1996.

[2] Editor R. Braden. Requirements for Internet Hosts - Communication Layers. Request For Comments 1122, Internet Engineering Task Force (IETF), October 1989.

[3] Ramon Caceres and Venkata N. Padmanabhan. "fast and scalable handoffs for wireles internetworks". In Proc. of the Second ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom), Rye, New York, USA, November 1996. Bell Laboratories and University of California at Berkeley.

[4] Claude Castelluccia. A Hierarchical Mobility Management Scheme for IPv6. Third Symposium on Computers and Communications (ISCC'98), Athens, Greece, June 1998. http://sirac.inrialpes.fr/planete

[5] S. Deering and R. Hinden. Internet Protocol Version 6 (IPv6) Specification. Request For Comments 2460, Internet Engineering Task Force (IETF), December 1998.

[6] David B. Johnson and C. Perkins. Mobility Support in IPv6. Internet Draft draft-ietf-mobileip-ipv6-14.txt, Internet Engineering Task Force (IETF), July 2001. Work in progress.

[7] Andrew Myles and David Skellern. Comparing Four IP Based Mobile Host Protocols. In Joint- European Networking Conference. Macquarie University, Sydney, Australia, May 1993.

[8] Thomas Quinot. An IPv6 architecture for Aeronautical Telecommunication Network. Master's thesis, Ecole Nationale Sup'erieure des T'el'ecommunications Paris, EUROCONTROL - European Organization for the Safety of Air Navigation - ISA project (IPv6, Satellite communication and ATMode for ATN), 1998. http://www.eurocontrol.fr/.

Author's Addresses

Questions about this document can be directed to the authors:

Thierry Ernst
Motorola Labs Paris and INRIA - PLANETE team Grenoble
ZIRST - 655 avenue de l'Europe
38330 Montbonnot Saint Martin, France
http://www.inrialpes.fr/planete/
Phone: +33 4 76 61 52 69
Email: Thierry.Ernst@inrialpes.fr

Hong-Yon Lach
Motorola Labs Paris, Lab Manager,
Networking and Applications Lab (NAL)
Espace Technologique - Saint Aubin
91193 Gif-sur-Yvette Cedex, France
Phone: +33 1 69 35 25 36
Email: Hong-Yon.Lach@crm.mot.com

Claude Castelluccia
INRIA - PLANETE team Grenoble
ZIRST - 655 avenue de l'Europe
38330 Montbonnot Saint Martin, France
Phone: +33 4 76 61 52 15
Email: Claude.Castelluccia@inrialpes.fr