IETF Seamoby Working Group
INTERNET-DRAFT
draft-ietf-seamoby-cardiscovery-issues-04.txt
16 October, 2002

Dirk Trossen
Govind Krishnamurthi
Hemant Chaskar
Nokia
James Kempf
DoCoMo

Issues in candidate access router discovery for seamless IP-level handoffs

Status of this Memo

Copyright notice

Abstract

Handoff in IP mobility protocols involves moving a mobile node's Layer 3 routing reachability point from one access router to another, before or after the mobile node has established a Layer 2 connection with the radio access point that is covered by the new access router. In addition, other context information about the mobile node's IP service may be transferred from the old access router to the new one, in order to minimize the service disruption during the handoff process. While the exact details of how this is accomplished vary depending on the IP mobility and seamless handoff protocols, one common thread required for IP-level handoffs is discovering the candidate access routers for the mobile node's handoff. Discovering the candidate access router involves identifying its IP address as well as its capabilities that the mobile node might be interested in. At the time of IP-level handoff, if a collection of candidates is identified, an algorithm is run to determine the target access router for the mobile node's handoff. This document describes the problem of candidate access router discovery. The document does not discuss the algorithm by which the

actual target access router is selected, nor how the handoff to the target is achieved.

Table of Content

1. INTRODUCTION.....3
1.1. Seamless Handoff Protocols.....3
1.2. Choice for Handoff.....3
2. TERMINOLOGY.....4
3. MOTIVATION FOR CAR DISCOVERY.....4
4. THE CAR DISCOVERY PROBLEM.....6
4.1. CAR IP Address Discovery.....6
4.2. Identifying Capabilities of CAR.....7
5. SECURITY CONSIDERATIONS.....7
6. ACKNOWLEDGEMENTS.....7
7. REFERENCES.....7
8. AUTHORS' ADDRESSES.....8

1. INTRODUCTION

IP mobility protocols enable mobile nodes (MNs) to change the access routers (ARs) by which they obtain the Layer 3 connectivity to the Internet, while communicating with another node over the Internet. An AR providing Internet connectivity to the MN changes when there is a change (usually as a result of movement of the MN) in the access point (AP) through which the MN communicates with the wired network, such that the AR serving the new AP is in a new subnet. There are existing solutions [1, 2] that enable MNs to execute IP-level handoffs between the ARs.

1.1. Seamless Handoff Protocols

Additionally, work is underway [3, 4, 5, 6, 7], to define protocols that would allow seamless, meaning low latency and low packet loss, handoffs of MNs between the ARs. These seamless handoff solutions assume that the (wireless) link protocol is capable of delivering a Layer 2 identifier for the new AP or the radio interface of new AR [8] to the current AR or to the MN, and require that the current AR be able to translate this Layer 2 identifier to the IP address of the new AR in order to facilitate the seamless handoff. In addition to simply providing the Layer 2 to IP address mapping, the AR needs some way to determine if the Layer 2 identifier is that of a legitimate AP or AR or whether it is an imposter. Some link layers provide Layer 2 security mechanisms for this purpose.

1.2. Choice for Handoff

In future mobile networks, there will be cases when MN has a choice of performing IP-level handoff to a different AR. For example, an MN having network interface cards supporting two or more wireless access technologies (such as, 3G and wireless LAN) and communicating over one of them, may wish to switch to a different access network if it feels that the IP service offered by the latter better suits its requirements. A generalization of this case is when the MN has a choice of different APs (of possibly different media and access technologies) connected to different ARs, for the sake of maintaining Internet connectivity. These different ARs may have different capabilities (different service providers, different load conditions, different wired QoS availability, etc.). The MN requires some means of obtaining information about the capabilities of these ARs so that the best decision about the handoff target can be made. Note that there might be scenarios when a handoff is essential to at least one of these ARs (old connection is fading fast) as well as those when MN may live without performing a handoff to any of these ARs (coverage of new AR is subsumed within that of the current AR). Further, depending upon the handoff scenario, seamless handoff

protocols may or may not be used.

The two problems are linked in the sense that they both involve determining the information about a new AR (IP address and capabilities) that is a candidate for the next handoff. In this document, we discuss the problem of Candidate Access Router (CAR) discovery.

2. TERMINOLOGY

Access Point (AP)

A radio transceiver by which an MN obtains Layer 2 connectivity with the wired network.

Access Router (AR)

An IP router residing in an access network and connected to one or more APs. An AR offers IP connectivity to MN.

Capability of AR

A characteristic of the IP service offered by an AR that may be of interest to an MN when the AR is being considered as a handoff candidate.

Candidate AR (CAR)

An AR to which MN has a choice of performing IP-level handoff. This means that MN has the right radio interface to connect to an AP that is served by this AR, as well as the coverage of this AR overlaps with that of the AR to which MN is currently attached to.

Target AR (TAR)

An AR with which the procedures for the MN's IP-level handoff are initiated. TAR is selected after running a TAR Selection Algorithm that takes into account the capabilities of CARs, preferences of MN and any local policies.

3. MOTIVATION FOR CAR DISCOVERY

This section describes some features that can be implemented with the help of CAR discovery protocol.

Scenario 1: Load balancing

Consider an AR to which an MN is currently attached. This AR is denoted by AR1. Further, assume that AR1 is heavily loaded. Suppose

there is another AR, denoted by AR2, that is reachable from the

attached MN and is not heavily loaded. Then, MN may decide to undergo handoff to AR2. Such load balancing can be achieved using the capability information about AR2 obtained via CAR discovery protocol.

Scenario 2: Resource intensive applications

Consider an MN running a streaming video application, which might be an important application for the future mobile networks. These applications require high bandwidth and possibly other QoS support to be available at the AR serving the MN. When this MN moves into the coverage area of a new AR, it is possible that the new AR does not have the capability to support the MN's application. The MN can then be informed about this fact when it is still connected to the current AR. This information might be used to alert the user about possible service degradation when moving. If the MN does have choices in what AR might be used for connectivity after moving, i.e., because of overlapping coverage areas, these choices might be presented to the user or the running application might make choices based on certain preferences. Clearly for this, it is necessary to have the knowledge of the capabilities of the neighboring ARs, and this can be obtained using the CAR discovery protocol.

Scenario 3: Least-cost phone call

Consider the preference expressed by the MN to prioritize handoffs to an AR with minimal cost of access for phone call (``least cost policy"). The ``cost of access" capability of an AR can be obtained using CAR discovery protocol.

Scenario 4: Adaptability to change in the coverage topology

Consider a situation in which ARs may be temporarily introduced in hot-spots to cater to the existing traffic demand. In such a case, a static configuration of the neighborhood information in ARs is not feasible as the operators may not inform each other of temporary changes. A protocol is therefore needed in such cases for the MN to automatically identify any change in the coverage topology and identify the capabilities of the neighboring ARs. This can be facilitated by the CAR discovery protocol.

Scenario 5: Inter-technology handoff

Consider the case in which an MN has a variety of wireless access network media available to it, and also possibly a wired interface. Theoretically, the MN could bring up each interface and solicit a Router Advertisement on it, but as the number of interfaces becomes larger, such a procedure results in a larger and larger drain on power. An alternative would be if the MN could solicit for

alternative AR choices on an active interface, and use this information to choose handoff target.

4. THE CAR DISCOVERY PROBLEM

There are two basic problems associated with CAR discovery:

1) Mapping from a Layer 2 identifier for an AP to the IP address of the CAR

2) Identifying the capabilities of CAR

The two problems are related in that both are concerned with obtaining IP-level information about a CAR for the purposes of determination of the target access router for handoff.
We discuss these two problems in the following subsections.

4.1. CAR IP Address Discovery

The seamless handoff protocols defined in [3, 4, 5, 6, 7] require a certain amount of IP level signaling between a MN's current AR and the target AR to which the MN will undergo handoff or has undergone handoff. For [3] and [4], the signaling is required to rearrange routing for a Mobile IP handoff when the MN's link moves to the target AR. For [5], [6], and [7], the signaling is required so that the current AR can transfer IP service context to the target AR. IP service context may include QoS state, AAA state, etc. Being able to quickly set up IP service context on the target AR is important because it determines how quickly the MN will receive the same level of IP service on the target AR as it received on the old. In order for the IP level signaling to occur, the current AR requires the IP address of the target AR.

Typically, the seamless handoff protocols assume that the MN knows a Layer 2 identifier for the wireless AP or AR to which it may undergo a handoff. The Layer 2 identifier might be obtained when the MN has Layer 2 beacon contact with the AP. It is now the task of the CAR discovery protocol is to enable mapping from the Layer 2 identifier to the IP address of the CAR that serves this AP.

This problem is not dissimilar to reverse address resolution [9] or to the use of DHCP [10] to obtain the address of a host based on its MAC address. In the current case, however, the reverse address translation is occuring across subnets for ARs rather than between a host and a server. Another added twist is that the actual L2 identifier may be for the new wireless AP and not for the new AR, whereas the current AR requires the new AR IP address. Any solution to this problem must provide for dynamic autoconfiguration of reverse address resolution, so that ARs and APs that are added and removed can be quickly discovered without requiring much, if any, human intervention.

4.2. Identifying Capabilities of CAR

Although not common now, future generation mobile networks may consist of ARs that offer coverage in the same geographical area but are heterogeneous in capabilities. The basic functionality shared by all IP routers is that of packet forwarding. In that respect, all ARs are similar. However, heterogeneity may arise among different ARs due to factors such as additional functions performed by ARs (seamless handoff support, security functions, wireless performance enhancing functions, etc.), administrative and business aspects of providing service to MN (service provider, cost of access, etc.), availability of certain type of resources with AR (QoS availability) etc. A solution is needed that will allow the MN to learn the capabilities of CARs that it might be interested in. CAR discovery protocol enables this.

However, since the complexity of the process might grow, in particular with growing number of capabilities, limitations in the scope of CAR discovery with respect to, for instance, the number of supported capabilities or the final decision making, might be necessary to cope with this complexity issue.

5. SECURITY CONSIDERATIONS

CAR discovery may allow other nodes to learn information about an AR, including its IP address and capabilities. Malicious nodes may use this kind of information to launch DoS attacks and/or service hijacking.

Information about the capabilities of a CAR often needs to be digitally signed. Otherwise, intentional or accidental APs can capture traffic, to the detriment of the MN. Such captures can result in black holes, and/or can facilitate eavesdropping and active attacks. Attacks like these have already occurred on 802.11 networks.

The need for digital signatures can cause other problems. MNs MUST be preprovisioned with information that lets them ascertain the authorization of any CAR. Digital signatures are expensive to compute and verify; this can translate into increased computational load on the CARs and on the MNs, and increased power consumption on the MNs.

Therefore, the following topics should be covered in any solution developed for CAR discovery:

- Authentication of nodes
- Security associations between nodes
- Message/payload encryption.
- Encryption of CAR capabilities
- Additional load on CARs and MN due to additional security measures

6. ACKNOWLEDGEMENTS

Special thanks are due to John Loughney (Nokia) and Hesham Soliman (Ericsson) for their input during the preparation of this document. Steve Deering's thoughts about how to involve the mobile node in CAR discovery were instrumental in achieving more focus to the problem statement.

7. REFERENCES

1. "IP Mobility Support", C. Perkins (Editor), RFC 2002, October 1996.

2. "Mobility Support in IPv6", D. Johnson, C. Perkins, and Jari Arkko, draft-ietf-mobileip-ipv6-17.txt, work in progress, May 2002.

3. "Low Latency Handoffs in Mobile IPv4", MIPv4 Handoffs Design Team, draft-ietf-mobileip-lowlatency-handoffs-v4-00.txt, work in progress, February 2001.

4. "Fast handoffs for Mobile IPv6", MIPv6 handoff Design Team, draft-ietf-mobileip-fast-mipv6-01.txt, work in progress, April 2001.

5. "Problem Description: Reasons For Performing Context Transfers Between Nodes in an IP Access Network", O. H. Levkowetz, et. al., draft-ietf-seamoby-context-transfer-problem-stat-01.doc, work in progress, May 2001.

6. "General requirements for a context transfer framework", H. Sayed, et. al., draft-ietf-seamoby-ct-reqs-00.txt, work in progress, May 2001.

7. "Buffer Management for Smooth handoffs in Mobile IPv6", G. Krishnamurthi, R. Chalmers, and C. Perkins, draft-krishnamurthi-mobileip-buffer6-01.txt, work in progress, March 2001.

8. "Supporting Optimized Handover for IP Mobility - Requirements for Underlying Systems", J. Kempf, et. al., draft-manyfolks-l2-mobilereq-02.txt, work in progress, November 2001.

9. "A Reverse Address Resolution Protocol", R. Finlayson, et. al. RFC 903, June 1984

10. "Dynamic Host Configuration Protocol", R. Droms, RFC 1531, October 1993.

8. AUTHORS' ADDRSSES

Dirk Trossen

Communication Systems Laboratory
Nokia Research Center
5 Wayside Road
Burlington, MA 01803, USA
Phone: +1 781 993 3605
Fax: +1 781 993 1907
E-mail: dirk.trossen@nokia.com

Govind Krishnamurthi

Communication Systems Laboratory
Nokia Research Center
5 Wayside Road
Burlington, MA 01803, USA
Phone: +1 781 993 3627
Fax: +1 781 993 1907
E-mail: govind.krishnamurthi@nokia.com

Hemant Chaskar

Communication Systems Laboratory
Nokia Research Center
5 Wayside Road
Burlington, MA 01803, USA
Phone: +1 781 993 3785
Fax: +1 781 993 1907
E-mail: hemant.chaskar@nokia.com

James Kempf

DoCoMo Communication Laboratories, USA
181 Metro Drive, Suite 300
San Jose, CA 95110, USA
Phone: +1 408 451 4711
Email: kempf@docomolabs-usa.com