Available online at www.sciencedirect.com
SCIENCE DIRECT®

Computer Networks 50 (2006) 1860–1871

Computer Networks

www.elsevier.com/locate/comnet

A soft-handoff transport protocol for media flows in heterogeneous mobile networks

Antonios Argyriou *, Vijay Madisetti

School of Electrical and Computer Engineering, Georgia Institute of Technology, 777 Atlantic Drive, Atlanta, GA 30332, United States

Received 20 July 2004; received in revised form 21 July 2005; accepted 9 August 2005
Available online 12 September 2005

Responsible Editor: W. Wang

Abstract

In this paper we introduce a protocol for end-to-end handoff management in heterogeneous wireless IP-based networks. The protocol is based on the stream control transmission protocol (SCTP), and employs a soft-handoff mechanism that uses end-to-end semantics for signaling handoffs and for transmitting control messages. The objective of this protocol is first to reduce the home registration delay, and second, to eliminate the tunneling cost that exist in the current IP-based handoff management protocols. While the multihoming feature of SCTP has been suggested as way to realize soft-handoffs, our study is the first one the presents the relative merits of this handoff approach through an analytical methodology. After our theoretical analysis, we evaluate the performance the soft-handoff mobile-SCTP protocol, when media flows with stringent QoS requirements are employed. Our objective is to evaluate whether the soft-handoff mechanism employed by the protocol, can efficiently support media flows in terms of jitter and throughput. We present simulation results that show performance improvements for several vertical handoff scenarios in current and emerging mobile networks.

Keywords: Wireless LAN; SCTP; Mobile IP; Handoff management; Real-time flows

1. Introduction

A high quality of service (QoS) is possible for mobile communications over wireless networks, if it were possible to provide higher bandwidth and tighter control over path delay, jitter, and packet loss. Mobile IP, and its various derivatives [1,2], were designed in order to provide a scalable solution that facilitates handoff between IP-based subnets using encapsulation and tunneling. Its basic functionality is based on three features: Advertising a "care-of address", registering the current location of the mobile host, and tunneling. Agent advertisements, sent by specialized routers called foreign agents (FAs), are used to discover available links within a subnet. However, these mechanisms incur significant overheads like increased handoff delay, triangular routing, and IP encapsulation. All these

* Corresponding author. Tel.: +1 404 4838328.
E-mail addresses: anargyr@ece.gatech.edu (A. Argyriou), vkm@ece.gatech.edu (V. Madisetti).

1389-1286/$ - see front matter © 2005 Published by Elsevier B.V.
doi:10.1016/j.comnet.2005.08.002

issues constitute important performance bottlenecks that must be resolved prior to the widespread acceptability of Mobile IP. Even though a number of optimizations have been reported [2,3], the fundamental overhead in tunneling is unavoidable, while new problems appear mainly related to security [4].

While Mobile IP targets mobility at a macro-level, a number of supplementary mobility management schemes have been developed in order to optimize for the case of frequent handoffs due to increased localized mobility of a host (micro-mobility). Hierarchical Mobile IP [2], Hawaii [5], Cellular IP [6], are some of the approaches that fall into this category. Hierarchical Mobile IP (HMIP) [2] is an extension to the base Mobile IP that allows the creation of a localized and scalable architecture. HMIP solves the problem of excessive signalling delay when the current visited network is far away from the home network. HMIP defines a way of localizing registrations to the visited network so that they do not have to traverse through the home network. This local architecture is realized through an entity called the gateway foreign agent (GFA). The mobile host uses regional registrations to the GFA in order to reduce the number of signaling messages to the home network. Moreover, for frequent intra-domain moves, the signaling delay is reduced since the related signaling messages have only localized significance. However, while reducing some signalling costs, these localized Mobile IP-based approaches share a common overhead—tunneling costs. Moreover, the implied dependence on specialized routing agents (FA/GFA) creates points of failure in the network. Mobile IP with route optimization [3], is used in order to route all the packets destined to a mobile host (MH) directly to its current location and not through its home agent (HA). The authors propose protocol extensions to Mobile IP, so that the correspondent host (CH) can cache the current binding of the MH, and then tunnels the packets for the MH directly to its care-of address, bypassing thus the MH's HA. The authors also propose a mechanism that allow packets in flight to a MH that moves, and packets sent based on an out-of-date cached binding, to be able to forwarded directly to the MH's new address binding. Another approach that shares some features with the proposed one in this paper, is homeless mobile IPv6 [7]. Homeless MIPv6 is basically intended for mobile hosts that do not need to or want to use any explicit home agent. The authors propose a number of modifications to mobile IPv6 so that it does not require, nor assume, any explicit home addresses or agents. One major drawback is that is based on IPv6, making it thus impractical for the current Internet. Moreover, it operates at the network layer and so TCP cannot handle the IP address changes. Finally, this protocol also requires the support of IPSec which incurs significant overhead and adds to the registration delay.

The first approach to handle mobility at the transport layer was TCP-Migrate [8], which is based in extensions of TCP. Location management is implemented with DNS [9] updates sent to the home network notifying it about the new IP address of the mobile host. In the meantime the TCP connection is suspended until the DNS update has taken place. If the delay is large (which is highly probable since the updates are sent to the home network), TCP might suffer from timeouts and so performance will be degraded. Another major handicap is the need for IPSec (which is penalized by a high overhead) every time the IP address is changing. Finally, additional performance degradation is attributed to the increased number of packets being lost during handoffs, because of TCP's inability to accept new socket parameters while in an existing session. Some recent works use the stream control transmission protocol (SCTP) [10] for mobility management [11–13]. These approaches simply state the observation that SCTP can handle changes in IP address, and exploit that for demonstrating a simple handoff. However, neither a detailed analysis of the benefits of such a solution nor a comparative study with current mobility management solutions are presented.

We argue that handoff management would be best handled by a protocol that operates over IP while still being able to inter-operate with network layer mechanisms (i.e. mobile IP). The protocol works at the transport layer and is implemented as extensions to the IETF's standard, the stream control transmission protocol (SCTP). The proposed handoff management protocol is general enough in that since it operates over generalized IP-based connectionless networks (Internet). This feature, will be even more important in the near future, since new incompatible wireless access technologies are emerging, while old ones are changing and evolved.

2. The handoff protocol

Primary design goal of the mobile-SCTP protocol is to operate under various wireless access