Available online at www.sciencedirect.com
SCIENCE DIRECT®
Computer Networks 50 (2006) 128–144
Computer Networks
www.elsevier.com/locate/comnet

A performance analysis of context transfer protocols for QoS enabled internet services

N. Bartolini [a,*], E. Casalicchio [b]

[a] Department of Computer Science, University of Rome "La Sapienza", Via Salaria 113, Rome 00198, Italy
[b] Department of Computer Science, University of Rome "Tor Vergata", Rome 00133, Italy

Received 10 January 2005; received in revised form 10 January 2005; accepted 17 February 2005
Available online 5 July 2005

Responsible Editor: Dr. G. Morabito

Abstract

In nowadays wireless networks, mobile users frequently access Internet services that are often based on information concerning the application context and service status. In presence of mobility, the procedure of service handover, may require a restart of the ongoing service, if the necessary context information is not properly transferred to the new point of access. Context transfer procedures introduce additional overheads to handovers possibly affecting the quality of service perceived by mobile users and making handovers very critical. In this paper the need for efficient protocols for transferring service context and profile related information is pointed out with reference to many mobile internet services, and the possible scenarios are differentiated on the basis of the handover triggering mechanisms. A performance model to compare these mechanisms, when context transfer protocols run on top of IPv6 with fast handover, is proposed. Numerical results point out the necessity to adapt the triggering mechanism to the size of the context data.

Keywords: Context transfer protocol; IPv6; Fast handover; Performance analysis

1. Introduction

The introduction of several multimedia services in new generation of wireless networks, brought about the need to develop efficient methods to manage the mobility of users. Nowadays internet services are often session oriented, delay bounded (or real-time) and context sensitive. Just to

* Corresponding author. Tel.: +39 06 49918357; fax: +39 068541842.
E-mail addresses: novella@dsi.uniroma1.it (N. Bartolini), casalicchio@ing.uniroma2.it (E. Casalicchio).

1389-1286/$ - see front matter © 2005 Elsevier B.V. All rights reserved.
doi:10.1016/j.comnet.2005.02.009

mention some, VoIP, multimedia streaming, on-line games, on-line transactions and many Content Delivery Networks (CDN) related services are often session oriented, delay bounded and context sensitive. In wired networks, the use of broadband technologies has a significant impact on the user's perceived Quality of Service (QoS) making Service Level Agreements (SLA) achievable. On the contrary, in wireless networks the introduction of broadband wireless connectivity is not sufficient to guarantee the fulfillment of QoS requirements mostly due to users movement across the network coverage areas managed by different access routers (AR). Handover requests may be issued during critical service phases for which the avoidance of service disruption is mandatory, and the connection must be seamlessly handed off from a point of access to another. The fast handover mechanism, introduced to reduce the packet losses during handovers, needs to be enhanced with proper mechanisms to preserve the service continuity. In context and session based services, the realization of a handover is not only a matter of keeping a connection alive during users movements, but also of transferring the necessary information to avoid the re-establishment of a service session every time the user reaches a new point of access. The re-establishment of a service session causes the repetition of the service protocol message flow from scratch and is necessary if the information to keep the service alive is unavailable when a handover to a new point of access occurs. Thence service continuity and context transfer during handover procedures are very critical for delay sensitive and context dependent applications.

The IETF SeaMoby working group identifies general motivations for Context Transfer [13] and defines a Context Transfer Protocol (CTP) [14]. In Section 2, we consider critical scenarios like the one of Content Delivery Networks (CDN) supporting mobile users, in which context-aware handovers are of significant impact on quality of service. In Section 3, we show the interaction between CTP and Mobile IPv6 protocol, with fast handover mechanisms to reduce packet losses. Since understanding how and when the context transfer can be activated by a mobile node or access router is fundamental to give a performance model and evaluation of the CTP, in Section 4 we describe the CTP message flow in tree different cases: dummy (post-handoff) context transfer, mobile initiated context transfer and access router initiated context transfer.

A performance model of the CTP is given in Section 5, where performance is evaluated in terms of bandwidth occupation, packet loss, percentage of packets that violate the SLA, context transfer time and completion time of the protocol message flow. Section 6 concludes the paper.

2. Motivation for context transfer

All the information needed to negotiate, establish and manage network services may be considered part of the context to be transferred when a Mobile Node (MN) issues a handover request during an ongoing service.

The context data include:

- authentication, authorization, and accounting information [13] needed to permit the re-authentication of the mobile host and the mobile host's authorization to access the network service from a new subnet;
- header compression [13] information that is necessary to avoid the repetition of messages between the last hop router and the mobile host;
- network QoS information to avoid the re-negotiation and re-establishment of QoS agreements between the mobile node and routers;
- application level QoS parameters, e.g. maximum end-to-end perceived latency, level of image resolution (e.g. high-level resolution for laptop and low-level resolution for enlarged mobile phone/palmtop), maximum/minimum bit-rate for streaming sessions, security specification (e.g. which suite of encryption algorithms is allowed/used), service authentication (e.g. certificate, list of certification authorities, list of trusted servers);
- session state information, e.g. the list of items in the basket or the phase that most likely will be entered next, for an e-commerce session or the next chunk of data needed in a streaming