Improving the Performance, Availability, and Security of Data Access for Opportunistic Mobile Computing

Steve Smaldone
Rutgers University

11/18/2010 at 10:00 am
CoRE A (Room 301)

Abstract

A new model of mobile computing is presently emerging where users are no longer burdened by the need to carry "heavy-weight" hardware with them, in order to interact with their personal computing environments wherever they go. Influenced by pervasive computing concepts, and fostered by the increasing availability of local PC hardware, the near ubiquity of powerful compact handhelds and smart phones, and modern trends in virtualization and cloud computing, this new opportunistic mobile computing model is reducing the size, weight, and energy demand of what must be carried to be effective on the go. As the burden of carrying PC hardware is being retired, a new set of burdens, centered on mobile user data access, arises due to this new model. Essentially, mobile users cannot simply borrow their data in an equally opportunistic fashion as they do for the PC hardware. Instead, they require safe and efficient access to their data, from whatever PC or device they are currently using, wherever they may be. These requirements expose several new challenges to the performance, availability, and security of user data access under opportunistic mobile computing conditions.

In this dissertation, we identify limitations to user data access within the opportunistic mobile computing model, present novel solutions to them, and demonstrate the effectiveness of these approaches through extensive experimentation. To improve the performance of data access for opportunistic mobile computing, we introduce the concept of safe borrowing of local storage, which we prototyped as the TransPart system. To improve the availability of data for opportunistic mobile computing, we introduce the concept of a mobile self-cleaning cache, which we prototyped as the Horatio system. To improve the security of remote data access for opportunistic mobile computing, we introduce the Working Set-Based Access Control (WSBAC) scheme, which applies the concept of the working set to network file system access control.