Chapter 3
Cloudlet-Based Cyber-Foraging in Resource-Limited Environments

Grace A. Lewis
Carnegie Mellon Software Engineering Institute, USA

Sebastián Echeverría
Carnegie Mellon Software Engineering Institute, USA

Soumya Simanta
Carnegie Mellon Software Engineering Institute, USA

James Root
Carnegie Mellon Software Engineering Institute, USA

Ben Bradshaw
Carnegie Mellon Software Engineering Institute, USA

ABSTRACT

First responders and others operating in crisis environments increasingly make use of handheld devices to help with tasks such as face recognition, language translation, decision making, and mission planning. These resource-limited environments are characterized by dynamic context, limited computing resources, high levels of stress, and intermittent network connectivity. Cyber-foraging is the leverage of external resource-rich surrogates to augment the capabilities of resource-limited devices. In cloudlet-based cyber-foraging, resource-intensive computation is offloaded to cloudlets: discoverable, generic servers located in single-hop proximity of mobile devices. This chapter presents several mechanisms for cloudlet-based cyber-foraging that consider a tradeoff space beyond energy, performance, and fidelity of results. It demonstrates that cyber-foraging in resource-limited environments can greatly benefit from moving cloud computing concepts and technologies closer to the edge so that surrogates, even if disconnected from the enterprise, can provide offload capabilities that enhance the computing power of mobile devices.

DOI: 10.4018/978-1-4666-8213-9.ch003
1. INTRODUCTION

Mobile applications are increasingly used by first responders and others operating in crisis and hostile environments in support of their missions. These environments are not only at the edge of the network infrastructure, but are also resource limited due to dynamic context, limited computing resources, intermittent network connectivity, and high levels of stress. Applications that are useful to field personnel include speech and image recognition, natural language processing, and situational awareness. These are all computation-intensive tasks that take a heavy toll on the device’s battery power and computing resources.

Cyber-foraging is the leverage of external resource-rich surrogates to augment the capabilities of resource-limited mobile devices (Satyanarayanan, Bahl, Caceres, & Davies, 2009). Most existing cyber-foraging solutions rely on conventional Internet for connectivity to the cloud or strategies that tightly couple mobile clients with servers at deployment time. These solutions are not appropriate for resource-limited environments because of their dependence on multi-hop networks to the cloud and static deployment. Cloudlet-based cyber-foraging relies on discoverable, generic, stateless servers located in single-hop proximity of mobile devices. These characteristics make cloudlets a good match for the characteristics of resource-limited environments. However, most cyber-foraging solutions identified in the literature do not address the challenges of “being at the edge.”

The goal of this chapter is to propose cloudlet-based cyber-foraging as a solution for supporting mobile systems in resource-limited environments. Section 2 presents a summary of related work in cyber-foraging. Section 3 describes cloudlet-based cyber-foraging. Section 4 describes cloudlet discovery. Section 5 presents five mechanisms for cloudlet provisioning. Section 6 describes the generic process for mobile application execution. Section 7 presents experimental data that shows the pros and cons of each cloudlet provisioning mechanism. Section 8 presents future research directions. Finally, Section 9 concludes the chapter.

2. RELATED WORK

Multiple cyber-foraging systems have been developed that differ in terms of the strategy that they use to leverage remote resources — where to offload, when to offload, and what to offload.

Where to offload varies between remote clouds (Kosta, Aucinas, Hui, Mortier, & Zhang, 2012), local servers located in proximity of mobile devices (often called surrogates; Satyanarayanan et al., 2009), or local servers that are connected to remote clouds for provisioning (Xiao, Simoens, Pillai, Ha, & Satyanarayanan, 2013) or as intermediaries to the cloud (Rahimi, Venkatasubramanian, Mehrotra, & Vasilakos, 2012).

When to offload varies between a runtime decision or an “always offload” strategy. To support runtime offload decisions, one strategy is to manually or automatically partition code into portions that either run on the mobile device or on a remote machine. At runtime an optimization engine — typically targeted at optimizing energy efficiency, performance, or network usage — decides whether the code should execute locally or be offloaded to a remote machine. An example of such a cyber-foraging system is MAUI (Cuervo et al., 2010). CloneCloud (Chun, Ihm, Maniatis, Naik, & Patti, 2011) follows the same code partitioning principle but automatically partitions code at the process level without the need for manual code annotation. Other cyber-foraging solutions assume that the computation-intensive code exists in a remote machine and the cyber-foraging task therefore becomes one of service discovery and composition. ThinAV (Jarabek, Barrera, & Aycock, 2012) is an example of this “always offload” strategy.