Measuring Energy Consumption of Privacy-Preserving Protocols for Fun and Profit

Daniel Hugenroth*
University of Cambridge, dh623@cam.ac.uk

Abstract Many protocols for anonymous communication have been designed without smartphones in mind. For example, we do not know whether protocols using cover traffic are practical with the limited energy provided by a smartphone battery. In this talk I summarise existing literature on mobile energy consumption and present results from literature and measurements that I have performed. These results then help identify challenges and solutions for such protocols on mobile devices.

For many people smartphones are their main device for Internet access. However, many protocols grew up in a time when stationary computers and wired Internet connections were the norm. This informed assumptions on continuous connectivity, low latency, and uninterrupted availability. In contrast, Smartphones are frequently offline and they need to carefully manage available battery power.

In my research I am studying protocols for privacy preserving and anonymous communication. Many of the newer designs explicitly address the sporadic connectivity of mobile devices. However, little attention has been paid to the energy aspects of running such services on a smartphone. For example, many protocols send packets at regular intervals (cover traffic) to hide communication patterns. Doing so every few seconds raises the question of whether this is actually practical with the energy stored in a typical battery.

My presentation starts with a brief summary of the literature on mobile energy consumption over the last 15 years. In particular, it discusses the relative strengths of direct measurements using power meters and model-based approaches. I then describe a low-cost and simple setup for direct measurements that I plan to open-source.

Most of the talk is dedicated to the discussion of results from both literature and my measurements. I believe that many of them are counterintuitive and challenge common assumptions. For example, cryptographic operations are negligible and benefit from CPUs with higher core frequency. On the other hand, the energy costs of radio communication are more influenced by traffic patterns than by the total amount transmitted.

Finally, I will present some ideas on how the battery efficiency of protocols can be improved. I am looking forward to learning from the audience about more application areas and interesting experiments to pursue.

*Daniel Hugenroth is a PhD student at the University of Cambridge where he studies the practicalities of strong metadata-privacy for mobile devices and group communication. Before returning to academia he worked at Facebook on mobile performance and image formats with a particular focus on emerging markets where cheap devices and limited connectivity pose challenges for modern applications.