CCIT REPORT #715 January 2009

Discouraging Selfishness in Lossy Peer-to-Peer Networks

Alex Friedman and Idit Keidar*

January 2009

Abstract

We present *Loss-Tolerant Selfishness Monitor (LTSM)*, a generic service for detecting selfish behavior in various P2P applications, such as MANET routing and multicast. Unlike most previous selfishness-resistant protocols, LTSM can be used in networks subject to message loss, where selfish behavior detection is particularly challenging. One of our main contributions is mathematically analyzing the impact of various system parameters on the incentives for cooperation, and showing how to choose these parameters so as to ensure full cooperation at a minimal cost. We illustrate the applicability of LTSM in two exemplar contexts: multicast and MANET routing.

1 Introduction

Peer-to-Peer (P2P) protocols are used in numerous different settings, e.g., mobile-ad-hoc networks (MANETs), P2P multicast systems, and file sharing networks. The underlying networks used by many such P2P systems are lossy. For example, wireless networks, such as MANETs, inherently suffer from high packet loss rates. Furthermore, multicast systems for streaming video or audio typically use unreliable transport like UDP, since it is acceptable for some of the data to be lost.

Resources in P2P systems are provided by the participating peer nodes themselves; each node has to contribute memory, CPU power, bandwidth, and energy. Since most nodes in a MANET are battery-powered, energy is a scarce resource in such an environment. In commercial P2P applications, nodes may exhibit selfish behavior by tampering with the P2P protocol in order to lower their cost [3, 6, 18]. Consequently, it is important for such protocols to work well even when users are equipped with a selfish version of the protocol.

In recent years, much research has been dedicated to tackling selfish behavior in various P2P applications (e.g., MANET routing, multicast, and file sharing – see Section 2). Many challenging issues, however, remain open. Previous work, for instance, has not exposed and leveraged the similarity among different P2P protocols. Rather, each previous work has focused on one specific protocol, in one specific setting. Another challenge largely overlooked in previous work is lossy networks (with the exception of [26, 27] – see Section 2). Selfish behavior detection becomes much more challenging when one has to cope with unpredictable packet loss. Conventional detectors, such as those used in [2, 4, 18, 19], would wrongfully accuse cooperating nodes for not sending lost packets. Finally, previous work has not mathematically quantified the relationship that needs to hold among system parameters such as a cooperating node's cost, the penalty for lack of cooperation, and the decision when to punish a node, in order to achieve full cooperation at a minimal cost.

In this paper, we address the three open issues above. We leverage the similarity among many different P2P protocols in order to define a common monitoring abstraction suitable for detecting selfish behavior in various such protocols (Section 3). Our abstraction's interface enables each peer node to monitor other nodes, and to determine when to punish a node for alleged misbehavior. We then present a

*Department of Electrical Engineering, Technion, Haifa, 32000, Israel. {ghost@tx, idish@ee}.technion.ac.il