Distributed Management Architecture
for Cooperative Detection and Reaction to DDOS Attacks

Georgios Koutepas, Fotis Stamatelopoulos, and Basil Maglaris

Network Management and Optimal Design Laboratory,
Electrical and Computer Engineering Department,
National Technical University of Athens,
Zografou, GR 157 80, Athens, Greece.
E-mail: {gkoutep, fotis, maglaris}@netmode.ntua.gr

Abstract
We propose a cooperative intrusion detection framework focused on countering Distributed Denial
of Service (DDoS) attacks through the introduction of a distributed overlay early-warning network.
Our goal is to minimize the detection and reaction time and automate responses, while involving as
many networks as possible along the attack path. The proposed approach relies on building a
"community" of trusted partners that will cooperate by exchanging security information so that
inclusion in the attack path is detected locally and without traceback procedures. The main building
block is the Cooperative anti-DDoS Entity, a modular software system deployed in each
participating network domain that supports secure message exchanges and local responses tailored
to individual sites' policies. We discuss the operation and the implementation of a prototype, and we
provide a survey of the methodologies against DDoS and compare our approach to related work.

Keywords: DDoS, Network security, distributed management, inter-domain, multicast, automated
reaction