Available online at www.sciencedirect.com
ScienceDirect
European Journal of Operational Research 176 (2007) 1283–1292
EUROPEAN JOURNAL OF OPERATIONAL RESEARCH
www.elsevier.com/locate/ejor

O.R. Applications

A packet filter placement problem with application to defense against spoofed denial of service attacks

Benjamin Armbruster [a], J. Cole Smith [b,*], Kihong Park [c]

[a] Department of Mathematics, The University of Arizona, Tucson, AZ 85721, United States
[b] Department of Systems and Industrial Engineering, The University of Arizona, Tucson, AZ 85721, United States
[c] Department of Computer Sciences, Purdue University, West Lafayette, IN 47907, United States

Received 4 November 2004; accepted 23 September 2005
Available online 27 December 2005

Abstract

We analyze a problem in computer network security, wherein packet filters are deployed to defend a network against spoofed denial of service attacks. Information on the Internet is transmitted by the exchange of IP packets, which must declare their origin and destination addresses. A route-based packet filter verifies whether the purported origin of a packet is correct with respect to the current route map. We examine the optimization problem of finding a minimum cardinality set of nodes to filter in the network such that no spoofed packet can reach its destination. We prove that this problem is NP-hard, and derive properties that explicitly relate the filter placement problem to the vertex cover problem. We identify topologies and routing policies for which a polynomial-time solution to the minimum filter placement problem exists, and prove that under certain routing conditions a greedy heuristic for the filter placement problem yields an optimal solution.

Keywords: Combinatorial optimization; Internet; Route-based packet filtering; Spoofed denial of service attack; Vertex cover

1. Introduction

Given the vulnerability of communication networks to a wide array of security attacks, a number of network security measures have been proposed to counter these attacks [1,4,10,18]. One of the pressing problems facing the global Internet is distributed denial of service (DDoS) attacks, wherein a set of compromised hosts

* Corresponding author. Tel.: +1 352 392 1464x2020; fax: +1 352 392 3537.
E-mail addresses: barmbrus@stanford.edu (B. Armbruster), cole@sie.arizona.edu, cole@ise.ufl.edu (J.C. Smith), park@cs.purdue.edu (K. Park).

0377-2217/$ - see front matter
doi:10.1016/j.ejor.2005.09.031

concurrently send large amounts of traffic targeted at a server, gateway, or network [3,8]. The aim of the attack is to disrupt normal operation of the targeted network system by depleting its resources. Many DDoS attacks disguise their true origin by inscribing bogus information in the source address field of the IP (Internet Protocol) packet header, referred to as IP source address spoofing. This causes recovery to take on the order of hours and days, at which point damage has already been done. IP traceback—the problem of locating the attack source—has been an active area of research [15,17].

Whereas most DDoS defenses are reactive in nature, a proactive approach called route-based distributed packet filtering [16] is aimed at preventing spoofed DDoS packets from reaching their targets in the first place. Route-based filtering uses route constraints in transportation networks to determine whether a packet, given its source and destination address, is misrepresenting its true origin. In semi-maximal route-based filtering, only the source address is utilized to affect filtering, which enables the linear filter table size required for implementation in resource-bounded routers. Distributed route-based packet filtering applies this action at select transit nodes in the network so that with a small deployment at "checkpoints," effective discarding of spoofed packets is achieved. Although the scope of scenarios to which this filtering concept applies is broader than Internet DDoS attacks—e.g., distributed intrusion detection and sensor networks in physical transportation systems—DDoS network security is the focus area of this paper.

Consider a communication network whose connectivity is represented as a graph. The fields of a packet header, in particular, its source and destination addresses, are inscribed by the originating node. Node o can "attack" another node d by forging the source address of a sequence of packets as node s and sending them to d. The role of route-based packet filters is to identify and remove packets from the network whose source addresses can be ascertained to be spoofed, before they can aggregate and impart harm at their target. They must do so without violating the requirement of *safety*: a packet whose source address is not spoofed must not be discarded. We study the following optimal filter placement problem: Given a network and its routing, find a minimum cardinality set of nodes where route-based filters are placed such that no packet with a falsely reported origin is permitted to reach its destination.

The feasibility criterion is called *perfect security*, a special case of more relaxed security measures studied in [16] where certain triplets (o, s, d) are allowed through. The optimization criterion examined in this paper, minimizing the size of the filter node subset, is not the only meaningful criterion. For example, one may consider the number of edges as the cost function, or a notion of processing overhead that varies depending on the traffic load a node encounters. In the global inter-domain Internet context where a single node represents an entire domain, deployment of cooperative security solutions is hindered by policy barriers across different administrative boundaries. Bilateral agreements require significant effort to establish, and multilateral agreements are that much harder to come by. This provides a practical motivation, from a deployment perspective, for considering the number of filter nodes as the optimization criterion. The "processing overhead" of a node with many edges—likely a large ISP (Internet Service Provider) that provides transit service to other domains—is not localized to a single physical router since the ISP will have entry/exit/switching stations, called POPs (points-of-presence), at major cities where it interfaces with other domains. Route-based filters would need to be installed only on border routers that connect to other domains. In the intra-domain context, high-degree nodes correspond to routers with many links, and processing overhead is amplified proportionally to the number of edges.

We assume that route-based filters have access to routing information to determine if a packet with source address s destined to d is spoofed, subject to safety. In the global inter-domain Internet, route asymmetry—the path from o to d is not the same as from d to o—is common, which makes maintaining accurate route-based filter tables a nontrivial challenge. The focus of this paper is on studying an optimal filter placement problem