Computer Communications 35 (2012) 554–564

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

Intra-domain IP traceback using OSPF

André Castelucio [a], Antônio Tadeu A. Gomes [a], Artur Ziviani [a,*], Ronaldo M. Salles [b]

[a] LNCC – National Laboratory for Scientific Computing, Av.Getúlio Vargas, 333 – 25651-075 – Petrópolis, RJ, Brazil
[b] IME – Military Institute of Engineering, Praça General Tibúrcio, 80 – 22290-270 – Rio de Janeiro, RJ, Brazil

ARTICLE INFO

Article history:
Received 23 December 2009
Received in revised form 26 August 2010
Accepted 27 August 2010
Available online 8 September 2010

Keywords:
Bloom filter
Overlay network
DDoS attacks
Performance evaluation

ABSTRACT

Denial of service (DoS) attacks are a serious threat to the appropriate operation of services within network domains. In this paper, we propose a system called OsTraS (OSPF-based Traceback System) that helps network operators to deal with this threat by creating an overlay network for intra-domain IP traceback. The main contribution of our proposal with respect to previous work is its ability to provide partial and progressive deployment of the traceback system throughout a monitored network domain. The OsTraS system builds its overlay network using the OSPF routing protocol through the definition of an Opaque LSA (Link State Advertisement) specially conceived for this purpose. We investigate and evaluate the performance of partial and progressive deployment of the proposed system, showing its suitability even for large network domains.

1. Introduction

Currently, denial of service (DoS) and distributed denial of service (DDoS) attacks are common in the Internet [1–4]. Such attacks aim to make a network or a service provided by the network unavailable to requests coming from legitimate users. This typically happens when an attacker sends packets at a rate higher than the victim can process; and modern DDoS attacks occur with multiple distributed attacking sources simultaneously sending packets against a target victim.

The defense against (D)DoS attacks comprises three main different steps: (i) the detection of the attack, which is usually performed by intrusion detection and prevention systems [5]; (ii) the identification of the route(s) taken by attacking packets, which can be provided by IP traceback systems [6–8]; and (iii) the mechanism to block attacking packets at key points along the route(s) taken by them.

This paper focuses on the second step above, *i.e.*, on the identification (at least partially) of the route(s) taken by attacking packets. Identifying such route(s) is a challenging task, for several reasons: (i) IP routing is solely based on the destination IP address carried by each packet; (ii) due to scalability restrictions, no information about packet forwarding is normally kept at the intermediate routers; (iii) attackers can be behind a firewall or protected by a private IP address, thus even if the network keeps track of the routes taken by attacking packets, such routes will usually point to network middleboxes as the sources of attacking packets; (iv) IP packets are not authenticated at the moment they are forwarded, allowing spoofed source IP addresses to be used in (D)DoS attacks [9,10]; and (v) zombie hosts—remotely controlled by an attacker—are used for sending attacking packets and, in this case, their owners are unaware they are taking part in a DDoS attack.

Previous work on IP traceback systems typically requires complete deployment of the system over the network, *i.e.*, the system must operate on all routers in the network to properly traceback an ongoing (D)DoS attack. We believe this constraint limits the possibility of such IP traceback systems to be used in larger networks.

Our main contribution in this paper when compared with related work on IP traceback (see Section 4 for a detailed discussion on related work) is the proposal of an *intra-domain* IP traceback system,[1] called OsTraS (OSPF-based Traceback System), that can be *partially* and *progressively* deployed on networks taking part of an Autonomous System (AS).[2] The main motivation to develop an intra-domain IP traceback system with such characteristics stems from the fact that the decision of its deployment within a domain can be

[1] This paper is an extended version of [11], providing a more in-depth analysis of the basic mechanisms, new analytic results about the trade-off between the false positive rate and the amount of traceback information conveyed by the packets, and new simulation results concerning topologies based on real network traces.

[2] An Autonomous System is a collection of networks which are under the same administrative authority. Such collection may comprise different routing domains; for simplicity, however, we consider in this paper an AS as comprising a single routing domain, so the terms *domain* and *AS* are used interchangeably throughout the remainder of this paper.

* Corresponding author. Tel.: +55 24 2233 6199.
E-mail addresses: castelucio@lncc.br (A. Castelucio), atagomes@lncc.br (A.T.A. Gomes), ziviani@lncc.br (A. Ziviani), salles@ime.eb.br (R.M. Salles).

0140-3664/$ - see front matter © 2010 Elsevier B.V. All rights reserved.
doi:10.1016/j.comcom.2010.08.010

based on a trade-off between the intended system performance and the required investment to be done by the administrative authority depending on the size of the domain. We evaluate this trade-off through simulations, showing the feasibility of deploying OsTraS in large domains. We demonstrate that an efficient traceback implementation can be achieved even with a relative small portion of routers in the domain having the system deployed.

The remainder of this paper is organized as follows. The OsTraS system is presented in Section 2. In Section 3, we evaluate our approach through simulations. In Section 4, we discuss related work. Finally, in Section 5 we present conclusions and some pointers to future work.

2. Intra-domain overlay network for IP traceback

In this section, we present the architecture of OsTraS and its mechanisms: (i) the use of the OSPF protocol to disseminate information about OsTraS; (ii) the overlay network to traceback attacking packets at the router level; (iii) the packet marking procedure; (iv) the reconstruction of the route(s) taken by attacking packets.

2.1. OsTraS architecture

All routers inside an AS that are candidates to have the OsTraS system deployed should be associated with the same OSPF domain. An example of an OSPF domain is presented in Fig. 1. In this figure, each router represented by a double border box participates in the proposed IP traceback system, thus being capable of marking packets and, as a consequence, taking part in the overlay network built to traceback packets. Each one of these routers has an associated traceback agent (TBA). A TBA could be a computer running any operating system executing an open source version of OSPF—*e.g.*, a Linux box with Quagga [12]. TBAs are in charge of triggering the process of marking packets in the associated router—*e.g.*, using management procedures through SNMP (Simple Network Management Protocol) or CLI (Command Line Interface) automation—and also are in charge of tracebacking the route(s) taken by attacking packets. In addition, a TBA participates in the OSPF message exchanging, but in a passive way regarding the propagation of routes within the domain. The main purpose of this structure is to allow TBAs to have knowledge of the complete domain topology, thus allowing the construction of an intra-domain overlay network for IP traceback, as we describe in Section 2.3.

It is important to mention that a TBA could be associated with more than one router in the network domain. In an extreme case, just one TBA could be working in the domain; such a case, however, constitutes a centralized approach causing the system to be more vulnerable to attacks and failures. Therefore, we recommend TBAs to be deployed in a distributed way. To achieve this, TBAs must exchange information concerning their associated routers among each other. This functionality is performed by the OSPF protocol, as described in Section 2.2.

2.2. Using OSPF Opaque LSAs

OSPF routers periodically exchange information about the network domain topology using advertisement messages called LSAs (Link State Advertisement). The OsTraS system uses a special type of LSA, called Opaque LSA, to exchange information about the traceback overlay network, *i.e.*, to identify which routers in the network domain have the OsTraS deployed.

Opaque LSAs have the goal to give more flexibility to the OSPF protocol and have been previously used with different purposes in the literature [14–16]. Opaque LSAs are of three different types and indicate how far the advertisement should be propagated within the domain: (i) type 9, which is not distributed to external routers in a local network; (ii) type 10, which is not distributed to routers outside of an OSPF area; (iii) type 11, which is distributed throughout the whole OSPF domain. (One exception is when stub areas are used within the OSPF domain, as discussed in Section 5.)

In OsTraS, we propose the creation of a new Type-11 Opaque LSA, called IP Traceback Opaque LSA, which is generated only by TBAs. Each TBA advertises an IP Traceback Opaque LSA comprising information about which routers are associated to the TBA. This feature allows that, after the OSPF protocol converges, each TBA knows all other TBAs present in the domain, as well as all their associated routers, allowing each TBA to build an overlay network for intra-domain traceback, as detailed in Section 2.3. We highlight that the distribution of IP Traceback Opaque LSAs does not rely on a legacy router having knowledge about their purpose, since OSPF

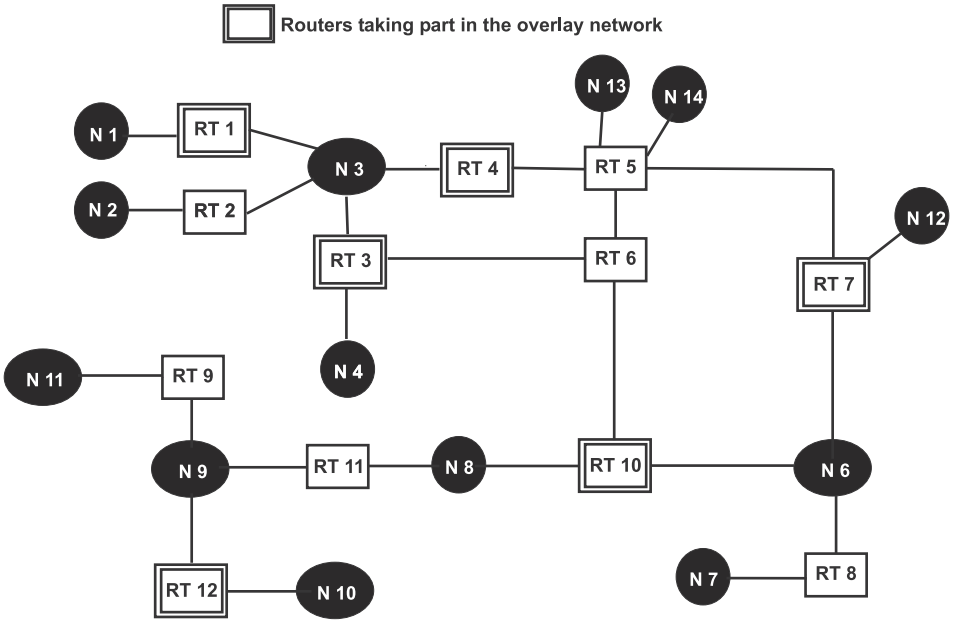

Fig. 1. Example of OSPF domain (adapted from Moy [13]).