Computer Networks 108 (2016) 40–54

Contents lists available at ScienceDirect

Computer Networks

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

An incentive-compatible and trust-aware multi-provider path computation element (PCE)

Molka Gharbaoui[a,*], Barbara Martini[b], Carol.J. Fung[c], Francesco Paolucci[a], Alessio Giorgetti[a], Piero Castoldi[a]

[a] Scuola Superiore Sant'Anna, Pisa, Italy
[b] CNIT, Pisa Research Unit, Pisa, Italy
[c] Computer Science Department, Virginia Commonwealth University, Richmond, Virginia, USA

ARTICLE INFO

Article history:
Received 2 September 2015
Revised 26 February 2016
Accepted 25 July 2016
Available online 2 August 2016

Keywords:
Trust
Multi-domain
Multi-provider
Traffic engineering
PCE
Confidentiality
Security

ABSTRACT

In multi-domain backbone networks, the Path Computation Element (PCE) architecture provides effective traffic engineering while limiting the exposure of intra-domain information. However, returned path computations may still reveal confidential intra-domain information, if artfully correlated by a malicious PCE. In such cases, the cooperation among PCEs should consider not only the capability of providing feasible paths but also the likelihood of security breaches (e.g., confidentiality risk exposure). In fact, a PCE might have the interest to block a request if it is arriving from a malicious or a competitor provider. In this scenario, the PCEs cooperation could benefit from a trust management model that accounts for the quality of the past interactions in terms of security violations while avoiding abuse of path computation services.

This work introduces the concepts of Trust Ranking and Quality of Interaction in PCE-based multi-domain backbone networks and elaborates a Bayes trust model to regulate the cooperation among PCEs. Specifically, the proposed trust management model aims at creating a common interest for the PCEs in contributing to effective traffic engineering while avoiding misuse of path computation services. Accordingly, we further propose a trust-aware PCE architecture and an incentive-compatible decision model that stimulate the behaviors of PCEs towards an effective cooperation.

Simulation results show that the proposed trust model provides effective incentive-compatible service differentiation to collaborating domains and is effective in detecting malicious PCE behaviors thereby tuning the amount of information returned in the path computation replies.

1. Introduction

Traffic engineering (TE) in multi-domain backbone networks has been demonstrated to achieve end-to-end Quality of Service (QoS) while improving network capacity utilization with respect to standard Border Gateway Protocol (BGP) techniques [1]. However, for an effective employment of TE solutions, intra-domain information is required to be shared among domain providers, e.g., bandwidth availability [2–4]. Therefore, in multi-provider networks, where each domain is typically administrated by a different Network Service Provider (NSP), TE solutions might be prohibited in order to preserve confidentiality.

In order to provide effective TE implementations in multi-provider networks while restricting intra-domain information exposure, the Path Computation Element (PCE) architecture has been proposed within IETF for generic multi-domain backbone networks, e.g., Multiprotocol Label Switching (MPLS) and Generalized Multiprotocol Label Switching (GMPLS) networks [1,5,6]. A centralized node, i.e., a PCE, is deployed in each network domain to elaborate path computation requests aiming at the set-up of virtual circuits, referred to as Label Switched Paths (LSPs) crossing domain's nodes. The path computation requests are issued by Path Computation Clients (PCCs) operating within the same domain, i.e., local PCCs, or by PCEs operating in adjacent domains, i.e., peer PCEs. Each domain PCE considers the intra-domain resource availability to perform local path computations. In the case of inter-domain connection requests, the end-to-end paths are computed through a concatenation of intra-domain path segments resulting from cascaded request-response interactions among PCEs using the PCE Protocol (PCEP) [6]. Due to the centralization of path computation functions, the PCE architecture allows a significant reduction on intra-domain information that need to be shared among domains

* Corresponding author.
E-mail address: m.gharbaoui@sssup.it (M. Gharbaoui).

http://dx.doi.org/10.1016/j.comnet.2016.07.013
1389-1286/

while providing effective TE [1,7,8]. However, despite implemented authentication, authorization and encryption mechanisms, confidential intra-domain information still might be discovered. In fact, the results of the returned path computations might reveal intra-domain resource availability if artfully correlated by a malicious PCE, which falls under the *inference attacks* category. For instance, a malicious peer PCE might submit multiple requests to a PCE with the same destination node and different values of requested bandwidth while using the obtained replies to derive possible bandwidth bottlenecks towards the considered destination [9,10].

Such a misuse of the path computation services might prevent a beneficial cooperation among PCEs belonging to different domains and compromise the dynamic provision of end-to-end LSPs. In fact, a PCE might not have an interest in processing a request if it is arriving from a competitor provider or if some security threat is perceived that is likely to cause any operational or economic damage.

We claim that in order to enable operative service deployments in Future Internet scenarios and effective TE solutions, the selection of the sequence of domains participating in a multi-domain path should be based not only on the capability of neighbor PCEs to address path computations demands, but should be also based on business-oriented criteria (e.g., expected revenues) or security-related aspects (e.g., risk exposure) [9,11]. Therefore, the PCE cooperation should be enhanced with trust-based mechanisms and incentives to discourage the misuse of path computation services while stimulating effective interactions among PCEs.

In this work, we propose a trust-based PCE cooperation model which aims at incentivizing PCEs to avoid malicious usage of computation services through interactions regulated by pair-wise trust rankings. The trust ranking is based on the evaluation of interactions between PCEs through a Bayesian trust management model. In the proposed PCE cooperation, malicious PCEs that abuse of path computation services collect low trust rankings that, eventually, results in low quality path computation services from adjacent domains in terms of traffic performance (e.g., high latency of data transfers). Definitely, this paper proposes an incentive-compatible PCE cooperation design to strategically select differentiated path computation services based on the behavior of PCE clients.

The use of differentiated path computation services achieves a twofold goal. First it gives incentives (i.e., reserved bandwidth at low latency) to high-trusted PCEs and, similarly, it gives penalties (i.e., not guaranteed bandwidth at high latencies and, possibly, at a higher price) to low-trusted PCEs. Thus, virtuous inter-domain TE is encouraged, while malicious behaviors are discouraged. Second, it triggers a defensive reaction towards low-trusted PCEs by making intra-domain resources practically undiscoverable, thus preserving confidentiality.

Trust management for collaborative systems is a widely investigated topic in the information technology area, e.g., models have been proposed for peer-to-peer systems [12], intrusion detection systems [13] and multi-agent systems in e-market platforms [14]. Conversely, this is an emerging topic in the communication technology area where the most noteworthy works consider access control in multi-domain networks [15–17]. However, the aforementioned works mainly focus on authorization mechanisms and on trust management regulating the grant of resource access rights. To the best of our knowledge, none of them addresses the rating of trustworthiness among PCEs or creates an incentive for beneficial multi-provider cooperation.

The major contribution of this work can be summarized as follows. 1) we introduce the concepts of *Quality of Interaction* (QoI) and *Trust Ranking* (TR) in multi-domain PCE environment. 2) we propose a novel *trust-aware PCE architecture* as metrics that differentiates the quality of the offered path computation services based on the TR of interacting PCEs. 3) we define a Bayesian inference *trust management* model for the computation of QoI and TR. Specifically, this work extends our previous work [18] by refining the trust-aware PCE architecture, providing a novel incentive-compatible PCE cooperation design, and extensively evaluating the trust module performance under different scenarios and network load conditions.

The rest of this paper is organized as follows. Section 2 gives an overview of related research works in the literature. Section 3 presents the security breaches in the current PCE interactions and the benefits of a trust-aware PCE cooperation. Section 4 describes the trust-aware PCE architectural design and an incentive-compatible decision model. Section 5 describes the design of the Bayesian trust model. Section 6 presents simulation design and results. Finally, Section 7 provides the concluding remarks for this paper.

2. Related works

Security issues in multi-domain networks have been widely investigated in different IP-based environments, e.g., pervasive networks [19], all-IP network integrating wireless and wired technologies [20], IP-based VPN management [21], IP Multimedia Systems [16,22]. Overall, the proposed solutions in most of these works address Authentication, Authorization of users and devices, Accounting (AAA) and trust management models for information exchange among different administrative domains.

In the context of network control plane, [23] identifies a number of security breaches against routing protocols such as deliberate exposure, sniffing, traffic analysis, spoofing, falsification, interference and overload. Such attacks are typically carried out by exploiting vulnerabilities of protocol interaction schemes. In multi-domain networks the most critical security issues are related to BGP [24]. In fact, as inter-domain routing protocol, BGP is exposed to the lack of effective security as a result of the routing infrastructure vulnerabilities of today's Internet. In this regard, a number of solutions have been proposed, that are mainly related to securing the operation of BGP [25,26] as well as securing the integrity of the BGP data [27,28]. As far as our knowledge, confidentiality issues are not explicitly addressed in BGP because confidentiality is inherently pursued by hiding intra-domain information details (e.g., topology, operational status) for scalability issues. However, this is achieved at the cost of traffic performance degradation of effective protocol operation (e.g., acceptable protocol convergence time) or along the chosen path (e.g., selection of congested end-to-end paths due to lack of knowledge about neighboring domains) [29].

Focusing on (G)MPLS-based networks, [30] describes possible threats to control plane protocols resulting from the breaches of single protocol procedures. Among the considered protocols, PCEP is cited as vulnerable to attacks such as Denial of Service (DoS) and blind spoofing. However, a limited number of works address security issues in the PCE architecture. Specifically, such works mainly focus on the access control regulating path resource reservation [15,17]. Typically, confidentiality is considered as a constraint to effectively achieve either TE or monitoring solutions on end-to-end basis while preserving the provider's confidential information during the exchange of network status information [31,32]. Confidentiality as a breach is only tackled by [33] where the issue of preserving the disclosure of internal network topology information is considered in multi-domain path computation. Nonetheless, this work considers the use of the path-key mechanism and ignores the risk resulting from malicious activities.

The confidentiality issue in PCE activities has been introduced in our recent works. In particular, [9] is focused on specific network scenarios (e.g., WSON) and proposes ad-hoc detection heuristics based on signature-based statistical approach. In the most recent work [10], malicious PCEP activity is detected through a