Guaranteeing Confidentiality in Multi-domain Networks: the PCE Anomaly Detector (PAD)

M. Gharbaoui, F. Paolucci, A. Giorgetti, P. Castoldi
TeCIP Institute, Scuola Superiore Sant'Anna
Pisa, Italy
Email: {m.gharbaoui, fr.paolucci, a.giorgetti, castoldi}@sssup.it

B. Martini
CNIT
Pisa, Italy
Email: barbara.martini@cnit.it

Abstract—**Traffic Engineering (TE) is currently required in multi-domain multi-provider networks to effectively exploit network resources. The Path Computation Element (PCE) architecture has been recently proposed for actually enabling TE in the aforementioned scenario. However, it might be exposed to several confidentiality leaks among network providers. Numerous research works in the context of multi-domain networks recently focused on authentication, authorization, and encryption mechanisms to mitigate the PCE architecture confidentiality leaks. With respect to such works, this paper tackles confidentiality issues from a different perspective, i.e., the detection of malicious utilization of path computation services aiming at inferring salient intra-domain information of other providers.**

This paper proposes the PCE Anomaly Detector (PAD) for detecting malicious PCE using a statistical anomaly-based approach. The novel statistical model used by the PAD is accurately described and PAD building blocks are presented. Simulation results show the effectiveness of the proposed approach that achieves an effective trade-off between the false alarms probability and the detection delay.

Keywords*—*Internet, Multi-domain, Multi-provider, Traffic Engineering, PCE, Confidentiality, Security, Sequential Hypothesis Testing.

I. Introduction

Due to scalability and manageability reasons, the Internet is organized in separate domains managed by different providers. In this multi-domain multi-provider architecture, the need of providing end-to-end connectivity services with Quality of Service (QoS) constraints requires the deployment of effective Traffic Engineering (TE), e.g., lambda services [1], MPLS-based services [2]. However, with respect to the canonical Border Gateway Protocol (BGP), where just summarized reachability information is exchanged, the implementation of effective TE implies the advertisement of significant amount of intra-domain information among providers [3], [4].

The Path Computation Element (PCE) architecture has been proposed within IETF for enabling the effective implementation of TE in multi-domain networks while trying to guarantee an acceptable level of intra-domain information exposure [5]. In the PCE architecture, a PCE is used in each domain for elaborating path computation requests issued by Path Computation Clients (PCC) using the Path Computation Element Protocol (PCEP) [6], [7]. In particular, path computation requests from PCC to PCE are enclosed in PCEP `PCReq` messages, while path computation replies from PCE to PCC are enclosed in PCEP `PCRep` messages. PCCs might be located in the same domain, e.g., a local node, or might be other PCEs located in adjacent domains requesting for an inter-domain path. In the latter case, the end-to-end inter-domain path is computed by concatenating intra-domain path segments resulting from cascaded PCE-to-PCE communications, with each PCE playing in turn PCC role with respect to PCE of an adjacent domain. Alternatively, inter-domain path computation may be performed by resorting to the Hierarchical PCE architecture, however this solution is preferably adopted in multi-domain single-provider networks [8], [9].

However, the utilization of the PCE architecture alone does not guarantee the required level of confidentiality. Typically adopted countermeasures are based on policies established as Service Level Agreements (SLAs) between providers to prevent disclosure of confidential information (e.g., allowing a limited number of path computation requests from other PCEs) [10]. Moreover, authentication and authorization mechanisms are deployed for avoiding PCEP abuse, e.g., impersonation of trusted PCE [11]–[13]. Finally, PCEs and PCCs encrypt each path exchanged during the inter-domain path computation (i.e., path-key [14]). Nonetheless, the deployment of the aforementioned countermeasures does not completely avoid confidentiality issues, since malicious PCEP activity can be carried out during inter-domain path computation through licit protocol utilization [5], [15]. Indeed, issuing a path computation request does not constrain to trigger the signaling for actually establishing the connectivity service. Therefore, as an example, a sequence of licit path computation requests with the same destination node and different values of requested bandwidth could be submitted to a PCE; instead of establishing the connectivity services, the obtained replies can be used to derive the intra-domain bandwidth bottleneck toward the specified destination. This represents a critical security leak that could be exploited by malicious providers for obtaining valuable advantages on the competitors.

Several recent works on multi-domain networks focus on authentication, authorization, and encryption mechanisms [16]–[19]. In these works, confidentiality is considered as a constraint in the design of TE solutions [20], conversely, in our approach confidentiality is an issue to be addressed without affecting TE operation. In [21], we have introduced a signature-based approach employing pre-configured attack patterns for detecting malicious utilization of path computation services in IP/MPLS and GMPLS multi-domain networks. In this work, an anomaly-based scheme, i.e., the *PCE Anomaly Detector* (PAD), is proposed using Sequential Hypothesis

978-3-901882-50-0 ©2013 IFIP

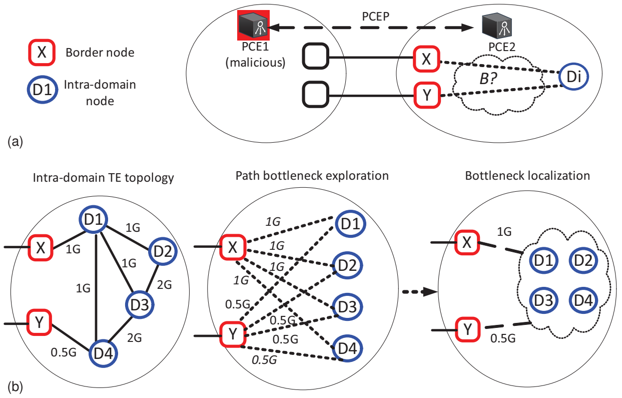

Fig. 1. PCE malicious activity: bottleneck exploration and localization.

Testing (SHT) [22] for detecting any misuse of PCE services aimed at breaking confidentiality. With respect to similar approaches [23], [24], the proposed PAD scheme is novel in the multi-dimensional elaboration of path computation requests arriving at the PCE. Moreover, the applied detection method employs an innovative double-step formulation, that extends and refines the preliminary single-step formulation of our preliminary work [25]. Simulation results show the PAD effectiveness in terms of detection and responsiveness under several attack scenarios. In particular, the double-step multi-feature SHT formulation assures a trade-off between accuracy and detection delay.

II. Malicious PCE and detection strategies

A *malicious PCE* is defined as a PCE aiming at discovering confidential intra-domain information of adjacent domains through a licit sequence of PCReq messages. The malicious activity can be carried out during the normal issuing of path computation requests for the actual provisioning of inter-domain connectivity services (i.e., MPLS Label Switched Paths, LSPs). This case is defined as *smart attack*, and can be particularly challenging to be revealed.

The following example demonstrates the security leak of the PCE-based inter-domain path computation mechanism using the PCE-based Per-Domain procedure [5]. In Fig. 1(a), the malicious PCE1 sends several PCReq messages to PCE2 with the same destination node (i.e., D_n), different source node (i.e., X and Y) and different bandwidth values. The standard procedure for preserving confidentiality is assumed (i.e., computed paths are returned in form of path-keys). The goal of PCE1 is, first, to identify the bandwidth bottleneck between border nodes X and Y and each intra-domain node D_n; second, to infer portions of the the intra-domain topology. The former procedure is hereafter referred to as *path bottleneck exploration*, the latter *bottleneck localization and topology discovery*.

1) Path bottleneck exploration: This procedure progressively reduces the uncertainty on the bottleneck B, defined as the maximum value of available reservable bandwidth along the set of paths between a given border node and the destination node. For instance, in Fig. 1(b) not more than 0.5 Gb/s is available between node Y and nodes D_n; this is a confidential intra-domain information that should not be revealed to other domains since it could be used for hostile purposes, e.g., discourage future LSP requests.

Returned PCRep messages containing a path-key (i.e., a path is available) define the estimated lower bound, while NO-PATH replies (i.e., no path is available) identify the higher bound. If a constant bottleneck value is assumed during the procedure, by performing an adequate sequence of requests the bounds converge to B. The procedure is iterated for any pair of border node and intra-domain node, thus obtaining a weighted virtual meshed topology connecting borders and intra-domain nodes (see Fig. 1(b)). While NO-PATH replies do not imply any subsequent expected action, PCRep messages enclosing path-keys are usually followed by the RSVP-TE (Resource Reservation Protocol with Traffic Engineering, [26]) signaling in order to establish the LSP. In the case of positive PCRep the malicious PCE is here assumed to not trigger the signaling.

2) Bottleneck localization and topology discovery: The virtual topology is used by PCE1 to localize bottlenecks and infer the intra-domain topology by employing off-line topology discovery algorithms [27]. Fig. 1(b) shows the actual intra-domain topology, the virtual topology, and the topology inferred by the bottleneck localization procedure. Bottlenecks are located within the intra-domain links connecting border nodes X and Y with intra-domain nodes, i.e. links $(X, D1)$ and $(Y, D4)$. The retrieved confidential information is that intra-domain destination nodes are connected to X and Y trough 1 Gb/s and 500 Mb/s bottlenecks, respectively, while they are part of a single topological area, i.e., island, with internal connectivity ≥ 1 Gb/s.

A. Relevant information for Attack Detection

To characterize the key events used for the detection of confidentiality attacks, the statistical analysis detailed in Sec. III resorts on two relevant event outcomes and on a set of salient PCReq parameters.

The relevant event outcomes are related to the two main stages of the LSP provisioning, i.e., the return of the path computation reply and the subsequent triggering of the RSVP-TE signaling. i.e., the *path computation outcome* and the *signaling trigger outcome*, respectively.

The path computation outcome is defined as follows:

- Positive path computation reply (i.e., path-key);
- Negative path computation reply (i.e., NO-PATH).

As explained in Sec. II-1, both positive and negative path computation replies represent a source of information for a malicious PCE. Negative replies disclose bandwidth bottlenecks, conversely, positive replies reveal bandwidth availability.

The signaling trigger outcome is considered after a positive path computation reply and is defined as follows:

- LSP is signaled (i.e., setup);
- LSP is not signaled within a timer (i.e., timeout).

Timeout events may be a sign of confidentiality attacks making clear that the PCE has no interest in establishing LSPs.

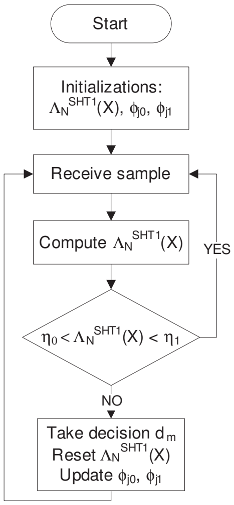
Start
Initializations:
$\Lambda_N^{SHT1}(X)$, ϕ_{j0}, ϕ_{j1}
Receive sample
Compute $\Lambda_N^{SHT1}(X)$
YES
$\eta_0 < \Lambda_N^{SHT1}(X) < \eta_1$
NO
Take decision d_m
Reset $\Lambda_N^{SHT1}(X)$
Update ϕ_{j0}, ϕ_{j1}

Fig. 2. SHT1 flowchart.

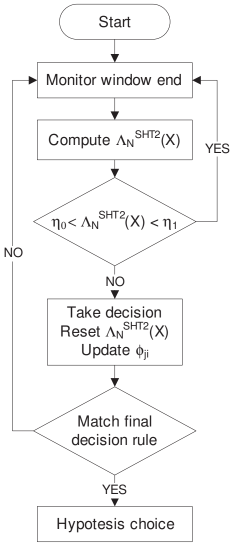
Start
Monitor window end
Compute $\Lambda_N^{SHT2}(X)$
YES
$\eta_0 < \Lambda_N^{SHT2}(X) < \eta_1$
NO
NO
Take decision
Reset $\Lambda_N^{SHT2}(X)$
Update ϕ_{ji}
Match final decision rule
YES
Hypotesis choice

Fig. 3. SHT2 flowchart.

However, although this is a significant information, it has to be evaluated carefully since timeout events might be also due to signaling errors occurred in remote domains [28], [29]. Therefore, a hasty evaluation of this only outcome may lead to false alarms.

Additional information considered for the purpose of attack detection are related to PCReq messages parameters and statistics, namely:

- *Inter-arrival rate of PCReq messages at PCE*: a close sequence of requests generated from a PCE may reveal potential attacks (e.g., under the form of a packet train sequence) to collect a relevant amount of information;
- *Requested LSP bandwidth*: a request for a significant amount of bandwidth should require some careful treatment since it might allow for the discovery of bottlenecks e.g., especially in the case of NO-PATH reply;
- *LSP destination stress*: an excessive amount of requests toward a given target may indicate PCEP anomalous activity (e.g., bottleneck explorations) especially when concentrated on a single node.

III. Sequential Hypothesis Testing: background and problem formulation

In this work an anomaly-based approach based on statistical analysis is used to detect PCE behaviors that fall out of a normal operation. Each time an anomalous behavior occurs an alarm is triggered. Thus, a detection activity of a PCE misbehavior can be shaped as a classification problem faced by leveraging on statistical methods, i.e., as a Sequential Hypothesis Testing (SHT) problem [22].

SHT is a time-continuous statistical procedure that sequentially analyzes a stream of data and stops as soon as a significant result is observed to take a decision [22]. Thus, the decision may be taken in real time without waiting for a complete set of data. Two possible hypothesis are considered: the *null hypothesis* (i.e., non-malicious PCE, H_0), and the *alternative hypothesis* (i.e., malicious PCE, H_1). The hypothesis that best explains the observed data is selected.

Let X a vector of the N observed data received so far, i.e., $\{X^1, X^2, \ldots, X^N\}$, the SHT decision rule can be expressed as follows:

$$\delta(X) = \begin{cases} \text{Choose } H_1 & \text{if } \Lambda_N(X) \geq \eta_1 \\ \text{Need more observations} & \text{if } \eta_0 < \Lambda_N(X) < \eta_1 \\ \text{Choose } H_0 & \text{if } \Lambda_N(X) \leq \eta_0 \end{cases} \quad (1)$$

$\Lambda_N(X)$ is expressed in terms of $Pr[X^k|H_i]$ that is the conditional probability of the observation X^k with respect to the hypothesis H_i:

$$\Lambda_N(X) = \frac{Pr[X|H_1]}{Pr[X|H_0]} = \prod_{k=1}^{N} \frac{Pr[X^k|H_1]}{Pr[X^k|H_0]} = \frac{Pr[X^N|H_1]}{Pr[X^N|H_0]} \Lambda_{N-1}(X) \quad (2)$$

In Eq. (1), η_0 and η_1 are calculated using approximations in [22] starting from the required value of probability of correct H_1 detection (i.e., detection probability, β), and the required value of probability of wrong H_1 detection when H_0 is true, (i.e., false alarm probability, α): $\eta_0 = \frac{(1-\beta)}{(1-\alpha)}$, $\eta_1 = \frac{\beta}{\alpha}$.

A. Multinomial SHT formulation

A multinomial model is formulated to consider the multi-dimensional problem of the malicious PCE detection. The observation X^k is a vector of d values $X^k = \{x_1, x_2, \ldots, x_d\}$. Each value x_j represents a binary *feature* describing a specific aspect of the observation, i.e., the presence or absence of a specific property in the observation X^k.

$$x_j = \begin{cases} 1: & \text{if present} \\ 0: & \text{if absent} \end{cases} \quad (3)$$

Considering H_0 and H_1, the probability of the presence of the property j in the observation when one of the hypothesis is true is expressed by $Pr[x_j|H_i]$. Moreover, any couple of features x_j and x_z belonging to $\{x_1, \ldots, x_d\}$ is assumed to be conditionally independent with respect to H_0 and H_1:

$$Pr[x_j, x_z|H_i] = Pr[x_j|H_i]Pr[x_z|H_i] \quad (4)$$

$Pr[X^k|H_i]$ is then modeled by a multinomial distribution, that, given the above i.i.d. assumption can be written as the product of d binomial distributions $Pr[x_j|H_i]$:

$$Pr[X^k|H_i] = Pr[x_1, \ldots, x_d|H_i] = \prod_{j=1}^{d} Pr[x_j|H_i] \quad (5)$$

Considering N arriving i.i.d. observations characterized by d independent features, the likelihood ratio is expressed as:

$$\Lambda_N(X) = \prod_{k=1}^{N} \frac{Pr[X^k|H_1]}{Pr[X^k|H_0]} = \prod_{k=1}^{N} \frac{\prod_{j=1}^{d} Pr[x_j^k|H_1]}{\prod_{j=1}^{d} Pr[x_j^k|H_0]} = \prod_{j=1}^{d} \frac{\prod_{k=1}^{N} Pr[x_j^k|H_1]}{\prod_{k=1}^{N} Pr[x_j^k|H_0]} \quad (6)$$

By defining the following variables the likelihood ratio $\Lambda_N(X)$ is defined as in Eq. (7):

- ϕ_{j0} the probability of the presence of the feature x_j under the hypothesis H_0, i.e., $Pr[x_j = 1|H_0]$;

- ϕ_{j1} the probability of the presence of the feature x_j under the hypothesis H_1, i.e., $Pr[x_j = 1|H_1]$;
- N_{j0} the number of times the feature x_j is equal to 1 in a sequence of N samples when the hypothesis H_0 is true;
- N_{j1} the number of times the feature x_j is equal to 1 in a sequence of N samples when the hypothesis H_1 is true.

$$\Lambda_N(X) = \prod_{j=1}^{d} \frac{\phi_{j1}^{N_{j1}}(1-\phi_{j1})^{N-N_{j1}}}{\phi_{j0}^{N_{j0}}(1-\phi_{j0})^{N-N_{j0}}} \tag{7}$$

The probabilities ϕ_{ji} would be estimated as relative frequency of x_j in a set of observed data under the hypothesis H_0 and H_1 (e.g., training set). However, in this work ϕ_{ji} are estimated using arriving observations themselves as:

$$\phi_{ji} = Pr[x_j = 1|H_i] = \frac{\nu_{1i}^{j} + 1}{\nu_{1i}^{j} + \nu_{0i}^{j} + 2} \tag{8}$$

where ν_{1i}^{j} is the number of occurrences $x_j = 1$ when H_i is true; ν_{0i}^{j} is the number of occurrences $x_j = 0$ when H_i is true; $\nu_{1i}^{j} + \nu_{0i}^{j}$ is total number of occurrences when H_i is true. A smoothing is applied to each occurrences number (by adding 1 to each value) to avoid null values if a feature does not appear in the considered sequence [22].

IV. PCE Anomaly Detector (PAD)

The proposed PCE Anomaly Detector (PAD) relies on two distinct decision steps. The first step uses a single-feature SHT formulation (i.e., *SHT1*). The decisions taken in this step are assumed as inputs of the second step, which uses a combined multi-feature SHT formulation (i.e., *SHT2*), to take the final decision about the PCE behavior.

The combined use of the two SHT steps improves the detection probability of the overall decision making process by refining the statistical analysis considering additional features. In fact, SHT1 operates on per-request basis considering a single feature derived by incoming PCEP requests. This step is designed to obtain a fast tracking of the PCE behavior and to provide a coarse-grained analysis. SHT2 operates on a number of boolean features considering average values computed within a time-domain window called *Monitoring Window* (MW). SHT2 runs in parallel with SHT1 and aims at performing a more detailed and correlated analysis of the requests set in order to achieve an accurate fine-grained analysis. Moreover, the SHT1 decisions within the same MW are considered a further variable of SHT2 process.

A. SHT1 formulation

The feature considered by the SHT1 step is the RSVP-TE signaling trigger outcome as defined in Sec. II-A. This feature is named x_1^{SHT1} and is computed as:

$$x_1^{SHT1} = \begin{cases} 0 : \text{if the RSVP-TE signaling is triggered} \\ 1 : \text{if the RSVP-TE signaling is not triggered} \end{cases} \tag{9}$$

The flowchart in Fig. 2 describes the SHT1 step. It starts by initializing the values for the likelihood ratio and the probabilities ϕ_{ji}^{SHT1} at $t = 0$. The SHT1 likelihood ratio is expressed as follows:

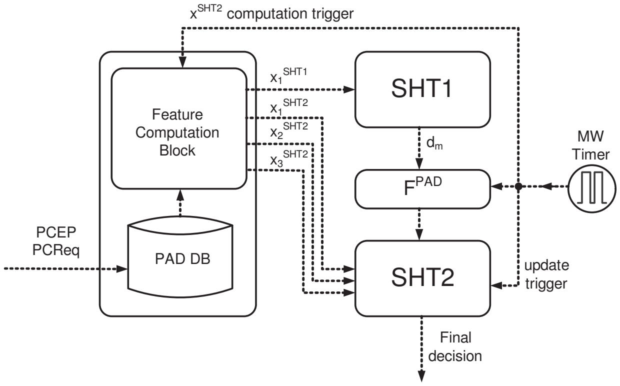

Fig. 4. PAD functional blocks.

$$\Lambda_N^{SHT1}(X) = \frac{(\phi_{11}^{SHT1})^{N_{11}}(1-\phi_{11}^{SHT1})^{N-N_{11}}}{(\phi_{10}^{SHT1})^{N_{10}}(1-\phi_{10}^{SHT1})^{N-N_{10}}} \tag{10}$$

Eq. (10) is computed and updated as soon as a new sample of x_1^{SHT1} is available. If $\Lambda_N^{SHT1}(X)$ crosses one of the two fixed thresholds, an *intermediate decision* d_m is taken by choosing one of the two hypothesis, otherwise the process waits for the next sample. The same process is then repeated to take the decision d_{m+1}, updating the initial parameters ϕ_{1i}^{SHT1}.

In order to obtain a more accurate tracking of the monitored PCE recent behavior, after each intermediate decision, the probabilities ϕ_{1i}^{SHT1} are updated, according to the value of the last obtained value of d_m, see Eq. (8). In particular, upon H_0 (H_1) intermediate decision, only the ϕ_{10}^{SHT1} (ϕ_{11}^{SHT2}) is updated, considering the only occurrences of x_1^{SHT1} according to the decided hypothesis. In general, a variable number I_w of intermediate decisions are taken inside the w-th MW, among which I_w^{H1} decisions related to warning malicious behavior and I_w^{H0} decisions related to normal behavior.

B. SHT2 formulation

The combined multi-feature SHT2 step is applied at the end of each MW. A set of three features is considered, whose values depend on the average of specific parameters collected within MW. The averages are computed resorting to the parameters of requests stored in the PAD database during MW, see Fig. 4. The computed averages are then compared against a fixed threshold to determine the feature value.

The first feature considered by the SHT2 step is based on the first `PCReq` parameter described in Sec. II-A: inter-arrival rate of PCReq messages at PCE, i.e., $\bar{t}$. This feature is named x_1^{SHT2} and is computed as follows, where T is a fixed threshold:

$$x_1^{SHT2} = \begin{cases} 0 : \text{if } \bar{t} > T \\ 1 : \text{if } \bar{t} \leq T \end{cases} \tag{11}$$

The second feature is based on the second `PCReq` parameter described in Sec. II-A: requested LSP bandwidth, i.e., $\bar{b}$. This feature is named x_2^{SHT2} and is computed as follows, where B is a fixed threshold:

$$x_2^{SHT2} = \begin{cases} 0 : \text{if } \bar{b} \leq B \\ 1 : \text{if } \bar{b} > B \end{cases} \tag{12}$$

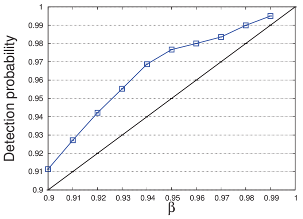

Fig. 5. Detection vs β, $\rho = 1$.

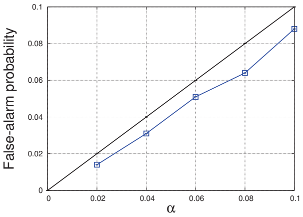

Fig. 6. False alarm vs α, $\rho = 1$.

The third feature is based on the third `PCReq` parameter described in Sec. II-A: LSP destination stress, i.e., $\max_n(\sigma_n)$. This feature is named x_3^{SHT2} and is computed as follows, where S is a fixed threshold:

$$x_3^{SHT2} = \begin{cases} 0 : \text{if } \max_n(\sigma_n) \leq \text{S} \\ 1 : \text{if } \max_n(\sigma_n) > \text{S} \end{cases} \tag{13}$$

where σ_n, referred to node D_n, is defined as the ratio between the number of requests targeting D_n and the total number of requests.

Such features are assumed to be statistically independent. This assumption might be not realistic in case of pure attacks, however, pure attacks would be easily detected by simpler policies or pattern-analysis mechanisms [16]–[19]. The most realistic scenario is a smart attack embedded in the normal set of requests for actual LSPs setup. In this scenario the independence assumption could be acceptable.

The flowchart of Fig. 3 describes the SHT2 process performed at the end of each MW. The process computes the average values considered by the three features and updates the likelihood ratio as follows:

$$\begin{aligned} \Lambda_N^{SHT2}(X) &= (u(I_w^{H1}/I_w) + u(I_w^{H1}/I_w - 0.5)) \\ &\cdot \prod_{j=1}^{3} \frac{(\phi_{j1}^{SHT2})^{N_{j1}}(1-\phi_{j1}^{SHT2})^{N-N_{j1}}}{(\phi_{j0}^{SHT2})^{N_{j0}}(1-\phi_{j0}^{SHT2})^{N-N_{j0}}} \end{aligned} \tag{14}$$

where the term $u(I_w^{H1}/I_w)+u(I_w^{H1}/I_w-0.5)$ connects SHT1 and SHT2 decision making processes. In particular, it depends on the total number I_w of SHT1 intermediate decisions and on the number I_w^{H1} of malicious intermediate decisions, both taken within MW. Thus, SHT2 is tuned according to the SHT1 outcome, e.g., if H_1 decisions are dominant, the likelihood ratio $\Lambda_N^{SHT2}(X)$ is doubled.

The SHT2 decision will be taken after a number of consecutive MWs, as soon as the $\Lambda_N^{SHT2}(X)$ crosses η_0 or η_1. Features probabilities are updated as described for SHT1. Final PAD decision may be taken by considering a fixed number of SHT2 decisions or, alternatively, by considering specific policies based on target parameters [25].

C. PAD functional blocks

Fig. 4 depicts the PAD functional blocks which are assumed to be collocated within the monitoring PCE. The `PCReq` messages received by the monitored PCE are stored with all the relevant parameters (e.g., timestamps and computation outcomes) in the PAD database. The feature computation block uses the database to compute the value of the features and generate the related samples.

TABLE I. PAD SIMULATOR: FEATURES THRESHOLDS AND PROBABILITIES, $t = 0$.

Feature	$Pr[x_j = 1\|H_i]$ H_0	 H_1	Feature threshold
x_1^{SHT1}	0.374	0.05	-
x_1^{SHT2}	0.1	0.7	T = 1 s
x_2^{SHT2}	0.5	0.8	B = 800 Mb/s
x_3^{SHT2}	$1/N_d$	0.99	S = 0.5

x_1^{SHT1} samples are computed by matching the stored path-keys and the path-keys received for decryption, upon incoming RSVP-TE signaling [14]. As defined in Eq. (9) if a stored path-key is not matched by any received path-key within the RSVP-TE timeout, i.e., $x_1^{SHT1} = 1$; otherwise, upon the reception of the matching path-key, $x_1^{SHT1} = 0$.

The three x^{SHT2} samples are contemporarily computed when the MW timer expires. In particular, all the stored `PCReq` messages generated by the monitored PCE and received in the last MW are considered. The same MW timer triggers the SHT2 likelihood ratio update.

V. PERFORMANCE EVALUATION

This section describes the simulations performed for evaluating the PAD. A custom-built event-driven Java simulator is used. The simulator comprises two inter-dependant components: the first component establishes PCEP sessions between PCEs and generates the path-computation requests. The second component runs PAD to evaluate the behavior of the monitored PCE. It takes as input the requests generated by the first component and gives as output the final decision.

Tab. I reports the probabilities $\phi_{ji} = Pr[x_j = 1|H_i]$ at $t = 0$ considered for each feature in the simulations. Such values are obtained for the H_0 hypothesis (i.e., non-malicious PCE) by simulating a standard inter-PCE communication scenario between two IP/MPLS domains. The network topology considered for simulations is illustrated in [21]. It is composed of $D = 2$ domains, $N = 28$ nodes, and $L = 55$ bidirectional links; each link provides a bandwidth of 10 Gb/s per direction. In particular, PAD is evaluated on a PCE controlling one of the two domains composed of $N_d = 14$ nodes. The probability $P[x_1^{SHT1} = 1|H_0]$ in Tab. I is derived from simulations by computing the ratio between the number of signaled inter-domain LSPs and the number of positive inter-domain `PCReq` messages, evaluated at 1600 Erl of load. The probabilities for the H_1 hypothesis and the thresholds are derived from the bandwidth bottleneck attack procedure described in Sec. II-1.

The set of requests submitted to PAD are composed by merging two distinct request sequences: the benign and the malicious sequences. The benign sequence is uniformly distributed among all the N destination nodes, with exponential inter-arrival times (average $1/\lambda = 0.125$ s) and exponential holding time (average $1/\mu = 200$ s), and uniformly distributed bandwidth values in the range $[0, 1]$ Gb/s. For these requests the standard signaling outcome rate is used (Tab. I under H_0 hypothesis). The malicious sequence is modeled by resorting to the path bottleneck exploration procedure described in Sec. II-1: it is a burst of a variable number of requests, with inter-arrival time fixed to 10^{-3} s, targeting only one destination, with bandwidth values in the range $[0.8, 10]$ Gb/s,

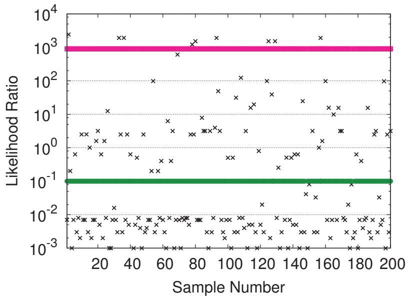

Fig. 7. SHT1 decisions, $\rho = 0.7$.

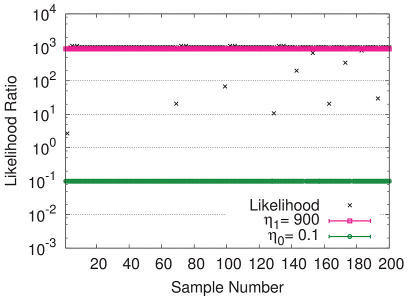

Fig. 8. PAD decisions, $\rho = 0.7$.

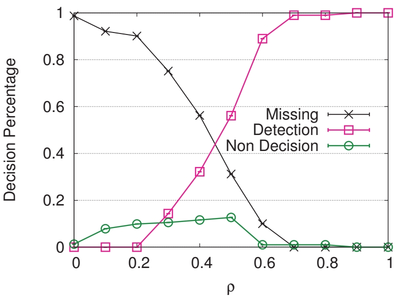

Fig. 9. Smart attack detection vs ρ.

not triggering RSVP-TE signaling. The two sets of requests are properly combined by tuning the *malice percentage* ρ, defined as the ratio between the number of malicious requests and the total number of requests in a single MW.

The maximum number of 20 requests in SHT1 and 10 MWs in SHT2 are considered to take the decision. The first SHT2 decision defines also the final decision rule. The MW duration is set to 10 s. Design constraints $\alpha = 10^{-3}$ and $\beta = 0.9$ are assumed, resulting in the decision thresholds: $\eta_0 = 0.1$, $\eta_1 = 900$. All results are reported with the confidence interval at the 95% confidence level.

A. PAD performance under massive attacks

Massive attacks are defined as attacks in which most of the requests are malicious, i.e., $0.7 \leq \rho \leq 1$.

Fig. 5 and Fig. 6 respectively plot the detection probability and the false alarm probability obtained with $\rho = 1$ (pure attack) as a function of the target performance β and α (see Sec. III). The obtained results always overcome the target performance, therefore PAD effectively detects attacks and avoids false alarms over the required constraints.

To better evaluate the PAD behavior against massive attacks, separate performance of the two steps are evaluated by analyzing the related likelihood ratios trend as a function of time. Fig. 7 plots the likelihood ratio values obtained after a decision related to the only SHT1 process, at $\rho = 0.7$. The plot shows that, although the PCE under evaluation is malicious, the dominant number of decisions fall under η_0 (i.e., not malicious), so that missing probability is high. Moreover, a significant number of samples falls within the non-decision area [η_0,η_1]. This also means that 20 requests are not sufficient to take an effective decision.

Fig. 8 plots the same likelihood ratio values related to PAD (i.e., SHT1+SHT2). The figure shows that PAD practically eliminates missing cases. However, a very limited number of non decision cases is still present. These cases are due to the presence of benign requests ($0.7 < \rho < 1$) that might jeopardize the final decision. Such results highlight the effectiveness of the combined use of two steps with respect to single-feature SHT, even under attack conditions.

B. PAD robustness to smart attacks

A number of simulations have been run focusing on the capability to detect smart attacks (i.e., $\rho < 0.5$). This kind of attacks may affect the likelihood ratio value, that instead of crossing η_1, starts to oscillate between the two thresholds, requiring more time to definitively take a decision and allowing the attacker to gather more confidential information. In Fig. 9, the three probability components (i.e., detection, missing and non-decision) are plotted as a function of ρ. PAD starts to detect a malicious behavior at $\rho \geq 0.2$. Then, the more malicious requests are inserted the more accurate becomes the mechanism. Regarding the non decision probability, it increases for $\rho \leq 0.5$, when the sequence is quite balanced, then drastically decreases. It is kept in any case under 20%.

VI. Conclusion

This paper discussed confidentiality issues in PCE-based multi-domain multi-provider IP/MPLS networks. A novel anomaly-based detection mechanism named PCE Anomaly Detector (PAD) is proposed using the statistical anomaly-based approach based on the Sequential Hypothesis Testing (SHT) procedure. PAD enables the profiling of PCE behaviors through the joint analysis of a number of selected features of the inter-domain path computation requests. PCE behaviors that deviate from normal operations are detected indicating a potential misuse of PCE services.

PAD performance has been evaluated by means of extensive simulations. Results have shown the effectiveness of such approach in terms of detection and responsiveness under several attack scenarios. The double-step multi-feature SHT formulation assures a noticeable trade-off between accuracy and promptness of the detection.

VII. Acknowledgment

This work has been partially supported by the project EMOTICON approved within the 2nd Call for additional beneficiaries of the OFELIA project.

References

[1] F. Paolucci, A. Giorgetti, N. Sambo, L. Valcarenghi, M. Maier, and P. Castoldi, "Enabling transparent lambda services between metro and core networks," *Photonic Netw. Commun.*, vol. 23, no. 2, pp. 137–147, Apr. 2012.

[2] S. Secci, J.-L. Rougier, and A. Pattavina, "On the selection of optimal diverse as-paths for inter-domain ip/(g)mpls tunnel provisioning," in *Telecommunication Networking Workshop on QoS in Multiservice IP Networks, 2008. IT-NEWS 2008. 4th International*, Feb. 2008, pp. 235 –241.

[3] F. Cugini, F. Paolucci, L. Valcarenghi, P. Castoldi, and A. Welin, "PCE communication protocol for resource advertisement in multi-domain BGP-based networks," in *Tech. Dig. OFC 2009*, Mar. 2009.

[4] F. Paolucci, F. Cugini, P. Iovanna, G. Bottari, L. Valcarenghi, and P. Castoldi, "Delay-bandwidth-aware metric abstraction schemes for OIF E-NNI multidomain traffic engineering," *Optical Communications and Networking, IEEE/OSA Journal of*, vol. 2, no. 10, pp. 782 –792, Oct. 2010.

[5] A. Farrel, J. P. Vasseur, and J. Ash, "A Path Computation Element (PCE)-based architecture," *IETF, RFC 4655*, Aug 2006.

[6] J. Vasseur and J. Le Roux, "Path Computation Element (PCE) Communication Protocol (PCEP)," *IETF, RFC 5440*, Mar 2009.

[7] A. Giorgetti, F. Cugini, N. Sambo, F. Paolucci, N. Andriolli, and P. Castoldi, "Path state-based update of PCE traffic engineering database in wavelength switched optical networks," *Communications Letters, IEEE*, vol. 14, no. 6, pp. 575 –577, Jun. 2010.

[8] D. King and A. Farrel, "draft-king-pce-hierarchy-fwk-03.txt," *IETF, PCE WG*, Dec. 2009.

[9] A. Giorgetti, F. Paolucci, F. Cugini, and P. Castoldi, "Impact of intra-domain information in GMPLS-based WSONs with hierarchical PCE," in *Tech. Dig. OFC 2012*, Mar. 2012.

[10] "Security mechanisms and procedures for NGN," Jan. 2010.

[11] S. Polito, M. Chamania, and A. Jukan, "Extending the inter-domain PCE framework for authentication and authorization in GMPLS networks," in *Communications, 2009. ICC '09. IEEE International Conference on*, Jun. 2009.

[12] D. G. Lee, G. W. Kim, J. W. Han, Y.-S. Jeong, and D.-S. Park, "Smart environment authentication: Multi-domain authentication, authorization, security policy for pervasive network," in *Proc. UMC 2008*, Oct. 2008.

[13] S. Polito and H. Schulzrinne, "Authentication and authorization method in multi-domain, multi-provider networks," in *Proc. EuroNGI 2007*, May 2007.

[14] R. Bradford, J.-P. Vasseur, and A. Farrel, "Preserving Topology Confidentiality in Inter-Domain Path Computation Using a Key-Based Mechanism," April 2009.

[15] L. Fang, "Security framework for MPLS and GMPLS networks," *IETF, RFC 5920*, Jul. 2010.

[16] Y. Demchenko, M. Cristea, and C. de Laat, "XACML policy profile for multidomain network resource provisioning and supporting authorisation infrastructure," in *Proc. IEEE POLICY 2009*, Jul. 2009.

[17] S. Polito, S. Zaghloul, M. Chamania, and A. Jukan, "Inter-domain path provisioning with security features: Architecture and signaling performance," *IEEE Trans. Netw. Service Manag.*, vol. 8, no. 3, pp. 219 –233, Sept. 2011.

[18] R. Casellas, R. Martinez, R. Munoz, T. Tsuritani, L. Liu, and M. Tsurusawa, "Lab-trial of multi-domain lightpath provisioning with PCE path computation combining BRPC and path-key topology confidentiality in GMPLS translucent WSON networks," in *Proc. ECOC 2010*, Sept. 2010.

[19] M. Colombo, F. Martinelli, P. Mori, B. Martini, M. Gharbaoui, and P. Castoldi, "Extending resource access in multi-provider networks using trust management," *Int. J. Comp. Netw. and Commun.*, vol. 3, no. 3, pp. 133–147, May 2011.

[20] S. Spadaro, J. Perello and, G. Hernandez-Sola, A. Moreno, F. Agraz, J. Comellas, and G. Junyent, "Analysis of traffic engineering information dissemination strategies in PCE-based multi-domain optical networks," in *Proc. ICTON 2010*, Jun. 2010.

[21] F. Paolucci, M. Gharbaoui, A. Giorgetti, F. Cugini, B. Martini, L. Valcarenghi, and P. Castoldi, "Preserving confidentiality in PCE-based multi-domain networks," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 3, no. 5, pp. 465 –474, may 2011.

[22] A. Wald, "Sequential tests of statistical hypotheses," *The Annals of Mathematical Statistics*, vol. 16, no. 2, pp. 117 –186, Jun. 1945.

[23] C. Fung, J. Zhang, I. Aib, and R. Boutaba, "Dirichlet-based trust management for effective collaborative intrusion detection networks," *IEEE Trans. Netw. Service Manag.*, vol. 8, no. 2, pp. 79 –91, Jun. 2011.

[24] G. Thatte, U. Mitra, and J. Heidemann, "Parametric methods for anomaly detection in aggregate traffic," *IEEE/ACM Trans. Netw.*, vol. 19, no. 2, pp. 512 –525, 2011.

[25] M. Gharbaoui, F. Paolucci, A. Giorgetti, B. Martini, and P. Castoldi, "Statistical approach for detecting malicious PCE activity in multi-domain networks," in *Proc. HPSR 2012*, Jun. 2012.

[26] D. Awduche, L. Berger, D. Gan, T. Li, and V. a. S. G. Srinivasan, "RSVP-TE: extensions to RSVP for LSP tunnels," dec 2001.

[27] L. Valcarenghi, F. Paolucci, F. Cugini, and P. Castoldi, "A recursive distributed topology discovery service for grid clients," *IEEE Commun. Lett.*, vol. 13, no. 7, pp. 549 –551, Jul. 2009.

[28] D. Siracusa, S. Grita, G. Maier, A. Pattavina, F. Paolucci, F. Cugini, and P. Castoldi, "Domain sequence protocol (DSP) for PCE-based multi-domain traffic engineering," *Optical Communications and Networking, IEEE/OSA Journal of*, vol. 4, no. 11, pp. 876 –884, Nov. 2012.

[29] A. Giorgetti, F. Paolucci, F. Cugini, and P. Castoldi, "Hierarchical PCE in GMPLS-based multi-domain wavelength switched optical networks," in *Tech. Dig. OFC 2011*, Mar. 2011.