A passive network monitoring service for PlanetLab Europe

Luca Niccolini [†‡], Giuseppe Iannaccone [†‡], Angelica Lo Duca [†‡]
[†] *University of Pisa,* [‡] *Quantavis s.r.l.*

Introduction

Live information on network behavior plays a fundamental role in network testbeds both for management purposes and for distributed applications debugging. During the demonstration we introduce the new PlanetLab Europe (PLE) packet-tracking infrastructure [1] and show how users can easily and safely inspect their network experiments using a simple web interface. PlanetLab Europe sites can be augmented with network monitoring hardware used both for passive and active monitoring. Here we focus on passive monitoring by means of the CoMo [2] opensource platform provided by Intel research.

The monitoring service is available to all PLE users and the number of monitored sites is growing. The only requirements for CoMo monitoring are a standard Linux machine with at least two NICs and a network switch that supports port mirroring. A proxy component has been developed that coordinates access to network resources and measurement boxes acting as a single secure access point to the monitoring service. The proxy offers both a command-line and a web-based secure interface. Figure 1 illustrates the packet-tracking service architecture.

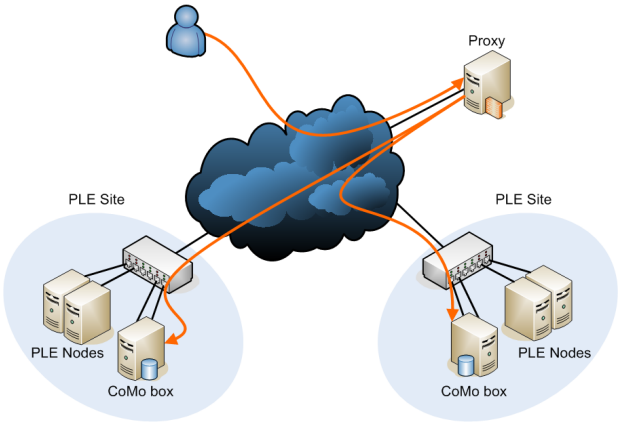

Figure 1: PLE Packet-tracking architecture

Demo description

For the purpose of this demonstration we show only the web interface and its main functionalities. When the user logs into the proxy, using its PLE credentials, the measurement boxes are shown over a world map (see Figure 2). Researchers that are only interested in aggregate information can immediately gather results using CoMo predefined modules. These modules collect metrics such as the number of active flows, the most used port numbers, addresses and protocols by inspecting only packet headers, thus no user sensitive data are shown. The user clicks on the measurement box marker over the map and selects the module to query and the time interval from a pop-up balloon.

CoMo stores all the measurement data in persistent memory thus it is possible to search and visualize past traffic. Results can be presented both in textual or graphical formats. Textual format is better suited for post processing with user-defined scripts. Graphical visualization allows researchers to immediately preview network behavior before deeply inspecting it.

Researchers that want to analyze the packet flow generated by their experiments need to develop their own ad-hoc monitoring application. We show how a simple CoMo module is imple-

Figure 2: CoMo boxes world map

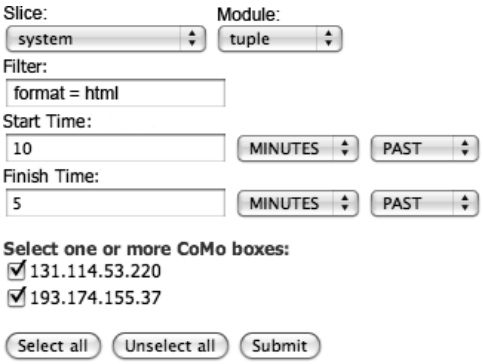

Figure 3: CoMo boxes query form

mented through specific APIs and how it can be pushed to all the monitoring points in the network using the proxy web interface. Our proxy also exposes functionalities for reservation and release of network resources on PLE nodes.

Through a web form the user specifies each PLE node, the slice on which the experiment will run and the port number used by the application. In this way CoMo is automatically configured to restrict the visibility of the user module only to a specific network flow. This allows the system to distinguish between traffic generated from different users and to ensure privacy.

It is now possible for the user to deploy its application onto PLE nodes and to start it. This process can be performed using standard PlanetLab tools like *CoDeploy* [3] or *pssh* [4]. A full demonstration of this procedure is beyond the scope of this demo. CoMo will capture and keep track of every network packet generated by the application at any node. The user can query all the interested nodes together through the *query* page of the proxy web interface in which the form depicted in Figure 3 is displayed.

After the form is submitted, results are shown in the desired output format and can be downloaded for further offline processing.

In this demonstration we show how MSNP [5], an instant messaging protocol, can be inspected in depth using a simple custom module. If a user name is known then we can find user's location in the network as well as the destination of her messages.

Conclusion

The packet-tracking service allows the secure extraction of relevant information about network behavior from PLE nodes. CoMo allows network traffic inspection with packet resolution while our proxy provides a single secure access point for the service and integration of the monitoring architecture within the PlanetLab Europe Internet testbed.

References

[1] G. Iannaccone, L. Niccolini, A. L. Duca, R. Canonico, T. Zseby, D. Witaszek, J. Kaeber, R. Bifulco, and P. D. Gennaro, "Packet tracking architecture." Onelab2 Deliverable 5.1.

[2] "The CoMo Project." `http://como.sourceforge.net`.

[3] "CoDeploy." `http://codeen.cs.princeton.edu/codeploy`.

[4] "Parallel ssh." `http://www.theether.org/pssh/`.

[5] "Unofficial guide to the MSN Messenger protocol." `http://www.hypothetic.org/docs/msn/`.