Simulation and Evaluation of Network Resilience with PReSET

Alberto Schaeffer-Filho*, Andreas Mauthe†, David Hutchison†, Paul Smith‡, Yue Yu§ and Michael Fry§
*Institute of Informatics, Federal University of Rio Grande do Sul, Brazil
Email: alberto@inf.ufrgs.br
†School of Computing and Communications, Lancaster University, United Kingdom
Email: {andreas, dh}@comp.lancs.ac.uk
‡Safety and Security Department, AIT Austrian Institute of Technology, Austria
Email: paul.smith@ait.ac.at
§School of Information Technologies, University of Sydney, Australia
Email: {tinayu, mike}@it.usyd.edu.au

***Abstract*—This technical demonstration presents PReSET, a toolset for the simulation and evaluation of network resilience strategies. The toolset is based on an integration between the Ponder2 policy framework and the OMNeT++ simulator. It permits the offline evaluation of policy-based strategies that perform dynamic reconfiguration of resilience mechanisms to contain malicious attacks and other challenges to a network.**

I. Introduction

Resilience is a key property for the management and protection of network infrastructures but the evaluation of resilience strategies is not straightforward. It requires the on-demand adaptation of network configurations, including specialised resilience functionality, in response to performance degradation, component faults or security threats. This technical demonstration presents PReSET, a toolset for the evaluation of network resilience strategies. PReSET (**P**olicy-driven **Re**silience **S**trategy **E**valuation **T**oolset) allows the modelling of resilience strategies, the offline analysis of a range of attack behaviours, such as Distributed Denial of Service (DDoS) attacks and worm propagation, and permits the evaluation of resilience strategies to detect and mitigate these threats.

PReSET is publicly available for download[1]. It is based on an integration between the Ponder2 policy framework [1] and the OMNeT++ simulator [2]. All tools and packages used in the integration are open source. PReSET has been extensively used at Lancaster University as the main platform for the evaluation of resilience strategies. We particularly expect that the toolset can also assist network operators and security professionals in the offline analysis of network attacks and challenges, where optimal policies may be established. The toolset supports not only the simulation of attack behaviours and algorithms for their detection, but also the corresponding activation of mechanisms that will attempt the remediation of an attack, based on conditions observed during run-time in the simulation. Therefore, instead of evaluating hard-coded protocols only, we are able to evaluate the trade-offs and the interactions between different management policies. Furthermore, policies and resilience configurations that perform well in the simulation environment may be readily deployed in a live network. This work is a companion to our IFIP/IEEE IM 2013 paper [3], where the toolset is presented in more detail.

This work has been done while Alberto Schaeffer-Filho was at the School of Computing and Communications, Lancaster University.

[1]http://www.scc.lancs.ac.uk/PReSET

II. Policy-driven Resilience Simulator

PReSET's integration with a policy framework permits the use of actual policies to reconfigure resilience strategies consisting of instrumented mechanisms running within the simulation, and whose behaviour can be adapted during run-time – e.g., setting flags, dropping connections, adjusting thresholds, triggering or stopping monitoring sessions, etc.

This demonstration will illustrate the overall design of the toolset and the set of policies and resilience mechanisms implemented for a particular set of malicious attacks (we have developed resilience strategies to contain DDoS and worm attacks). More importantly, it will show how changes to existing policies may impact on the operation of the mechanisms running within the simulation, thereby assisting the modelling and analysis of resilience configurations.

A. Architectural Components

Fig. 1 illustrates the architecture of the policy-driven resilience simulator implementation. Instrumented mechanisms in the simulation environment implement an XMLRPC server through the ***MechanismExporter*** component. This component is used to register and export the management interfaces for the resilience mechanisms available in the simulation. These interfaces provide callback functions to management operations that can be used to reconfigure a resilience mechanism, for example, to adjust the throttling rate of a rate limiter. For each type of mechanism, a ***ControlObject*** defines the management functionality to be exported via its management interface, and maps invocations to their respective method implementations on an ***InstrumentedComponent***. This mapping relies on a table $\langle name, pointer \rangle$ that matches different invocations to the correct instance of a specific mechanism.

Events are used to indicate conditions observed in the simulated network. The ***EventPublisher*** component is responsible for establishing a socket connection with a Ponder2 instance, where events from OMNeT++ will be parsed and mapped to

978-3-901882-50-0

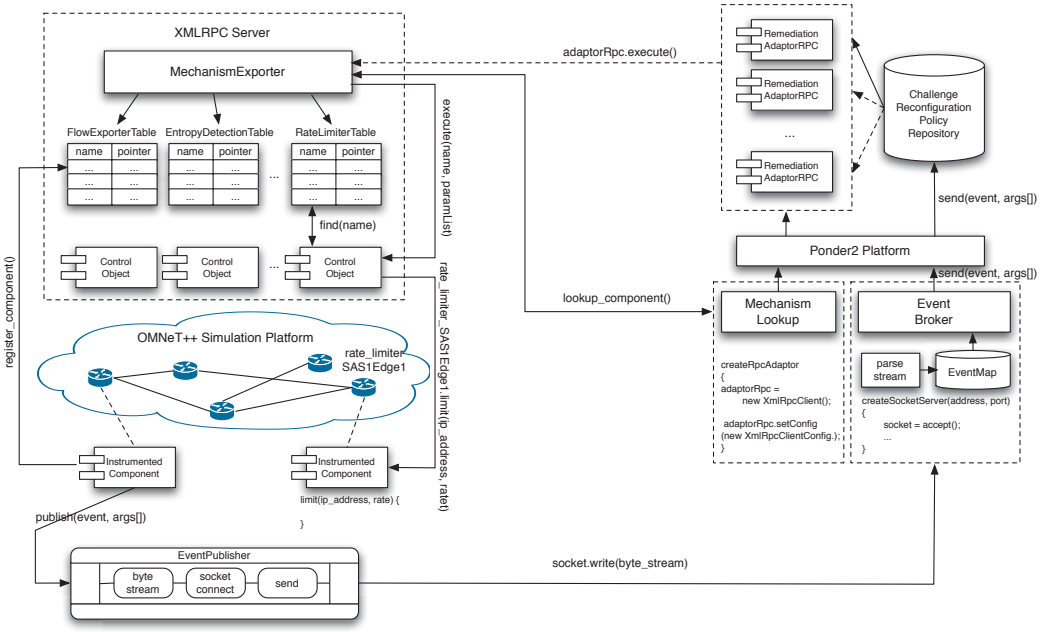

Fig. 1. Policy-driven resilience simulator architecture and main components [3]

Ponder2 events. A Ponder2 event may trigger one or more *event-condition-action* (ECA) policies, which will define what resilience mechanisms should be reconfigured and how.

B. Demonstration: DDoS Attack Detection and Remediation

We have developed experiments for the offline analysis of a range of attack behaviours, including DDoS attacks and worm propagation. We can easily simulate large-scale networks, for example, typically consisting of 20 or 30 autonomous systems, and thousands of hosts, including web and mail servers, to generate background traffic. In our DDoS experiment, a web server in one particular stub autonomous system is configured as the victim to be attacked by *DDoSZombie* hosts across the network.

We implemented various policy-controlled resilience mechanisms that can be activated and reconfigured on demand. These mechanisms include a *Link Monitor* module, which is invoked to monitor link utilisation; an *Entropy Detection* module, which is invoked and configured to monitor traffic features' distributions using Shannon's entropy algorithm; an *Intrusion Detection* module, which uses a threshold-based algorithm to count incoming packets on a particular link; and a *Rate Limiter* module, which can shape network traffic by probabilistically dropping packets from a specified link, IP destination address, or (source, destination) IP address and port number tuple. Other modules, implementing additional resilience functions, are currently being developed.

The toolset allows events generated by components running within the simulation, e.g., indicating that link utilisation has risen above a certain threshold, to be sent to the policy framework. Policies are used to reconfigure the resilience strategy (Fig. 2), e.g., adjusting thresholds or sampling rates. An additional policy can be used to reconfigure a *Rate Limiter* to block all flooding packets, for example, identified through a specific classification algorithm also running in the simulation.

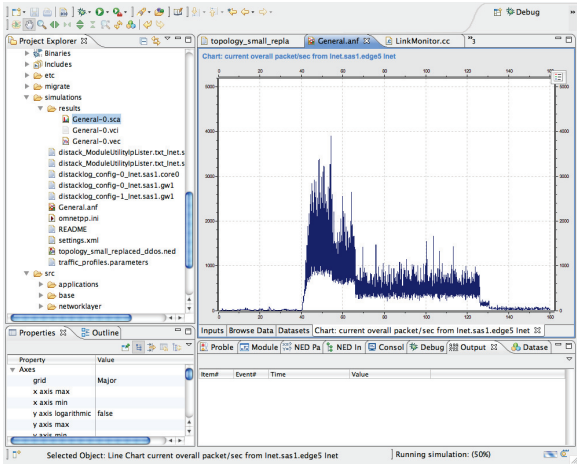

Fig. 2. Screenshot of OMNeT++ showing the onset of a DDoS attack, evidenced by a sudden increase in the number of packets/second, and the effect of policies used to contain this attack

ACKNOWLEDGMENT

This research is supported by the EPSRC funded India-UK Advanced Technology Centre in Next Generation Networking, by the European Union Research Framework Programme 7 via the PRECYSE project with contract number FP7-SEC-2012-1-285181, and by NICTA (National ICT Australia).

REFERENCES

[1] K. Twidle, E. Lupu, N. Dulay, and M. Sloman, "Ponder2 - a policy environment for autonomous pervasive systems," in *POLICY '08: IEEE Workshop on Policies for Distributed Systems and Networks*. Palisades, NY, USA: IEEE Computer Society, 2008, pp. 245–246.

[2] A. Varga and R. Hornig, "An overview of the OMNeT++ simulation environment," in *SIMUTools '08: 1st International Conference on Simulation Tools and Techniques*. Marseille, France: ICST, 2008, pp. 1–10.

[3] A. Schaeffer-Filho, A. Mauthe, D. Hutchison, P. Smith, Y. Yu, and M. Fry, "PReSET: A toolset for the evaluation of network resilience strategies," in *IM'13: IFIP/IEEE International Symposium on Integrated Network Management*, Ghent, Belgium, May 2013.