Detection and Mitigation of Abnormal Traffic Behaviour in Autonomic Networked Environments

[Extended Abstract]

Angelos Marnerides	Dimitrios P. Pezaros	David Hutchison
Computing Department	Computing Department	Computing Department
Infolab21, South Drive	Infolab21, South Drive	Infolab21, South Drive
Lancaster University	Lancaster University	Lancaster University
LA1 4WA, U.K	LA1 4WA, U.K	LA1 4WA, U.K
a.marnerides@comp.lancs.ac.uk	dp@comp.lancs.ac.uk	dh@comp.lancs.ac.uk

ABSTRACT

Autonomic network environments are required to be resilient. Resilience is defined as the ability for a network to provide and maintain an acceptable level of service in the face of various challenges to normal operation [1]. Traffic abnormalities are a great challenge and it is vital for any network to be supported by resilient mechanisms in order to detect and mitigate such events. In this document we present our measurement-based resilience architecture and we argue that the correct combination of already proposed theoretical methodologies and mechanisms present in our architecture compose a powerful defence mechanism that satisfies autonomic properties such as self-protection and self-optimization. In addition we refer to our intentions of testing our proposed architecture within the ANA project [2] in order to justify our hypothesis.

Categories and Subject Descriptors

C.3.2 [**Computer-Communication Networks**]: *Security and protection*

General Terms

Security, Performance

Keywords

Resilience, anomaly detection, anomaly classification, autonomic networks

1.INTRODUCTION

Future networks will be required to autonomously configure, organise and adapt their operation at the onset of

challenges in their environment, and consequently to confront explicit threats coming from external stimuli. These and several other self-* capabilities are in the list of the main objectives within the EU Autonomic Network Architecture (ANA) project that intends to build a novel architecture demonstrating the principles of autonomic networking. The primary aim within ANA is to enable the use of networks beyond the Internet legacy, and to facilitate a dynamic and transparent interaction among the wide range heterogeneous networks and platforms.

Our resilience architecture considers the properties of self-protection and self-optimization and achieves their applicability with the usage of combined mechanisms that are already present in past literature. In parallel our "pluggable" design enables modular decomposition and distributed dynamic binding no matter the physical location of our components. This capability allows detection and mitigation of an anomaly not only on a local but as well on a compartment-wide scenario. Within ANA a compartment refers to the most absolute network entity, which is autonomous and implements all the operational and administrative rules for a given communication context.

2.RESILIENCE ARCHITECTURE

The resilience architecture adopts a componentised design that requires information from a monitoring facility. As showed in Figure 1, a monitoring entity sends information of monitored packets to the Detection Engine (DE) of the system where those are received on the designated interface that we refer to as the Information Dispatch Point (IDP). After processing packet data and grouping flows at a desired level of granularity, the DE internally performs entropy estimation on selected packet features in order to detect an anomaly and applies runtime classification via a supervised Naive Bayes estimator. By these actions the DE is eligible to decide whether the observed flows are the

result of a local or compartment-wide anomaly. As soon as a concrete decision regarding the precise nature of the anomaly is denoted the DE composes a summary specification message that sends to its closest Remediation Engine (RE). In the case of a compartment-wide threat the RE distributes the threat information to regionally close REs. These subsequently decide at which compartment region they should take action for facing the event (e.g perform load balancing on a congested area with multiple links).
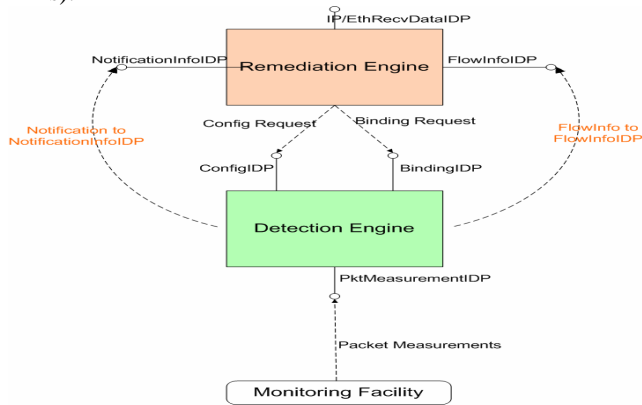

Figure 1: The overall resilient architecture

2.1 The Detection Engine

The DE as shown in Figure 2 is composed by the Logic Brick, the Classifier, the Notifier brick and a configuration manager.
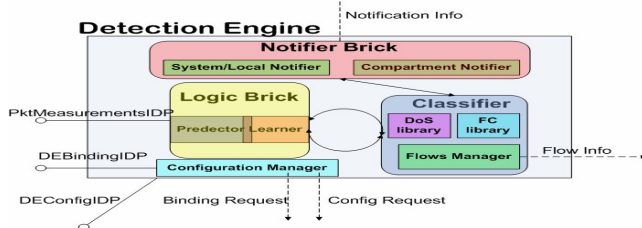

Figure 2: The DE internal architecture

The Predictor unit in the Logic Brick acts according to the estimates given by the distribution of selected packet features (e.g. checksum field) and applies entropy estimation in order to get an understanding for the evolution of the selected fields in each received flow. Entropy estimation provides a detailed and more accurate identification of events that may not be extracted in large traffic volumes [3]. In parallel with the operations made in the Predictor, the Learner unit performs run-time traffic classification, based on the sample entropy results given by the Predictor and the already categorized past events stored in the Classifier. The Learner unit uses a supervised naive Bayes estimator where as a probabilistic classifier accepts a range of training data and classify certain events while on runtime. We have selected this classification method because it has been observed by [4] that such a method has low processing cost and high accuracy percentage. Finally the internal architecture also has a Notifier unit which is in

charge of updating the REs in case of a local or compartment-wide attack diagnosis.

2.2 The Remediation Engine

Figure 3 shows the RE which is the component in charge of mitigating the effects of an anomaly (e.g. high system load, increased bandwidth consumption, congestion, etc.) Remediation algorithms that we consider are region-aware clustering algorithms for facing a local or compartment-wide event (e.g. a Flash Crowd or DDoS) by performing load balancing techniques on the desired regions. The actions performed by region-aware algorithms empower the property of self-optimization. In parallel due to the cluster and location awareness that an RE performs it also possesses the capability of dynamically binding to its intra-compartment closest DE (no matter its actual physical location) where that provides a flexible and autonomic character to the architecture in general. The RE is composed by two main functional modules; the Defender and the Messenger. The Defender executes the remediation algorithms whereas the Messenger distributes the instance of an event to remote REs within the compartment which are also affected by the threat.
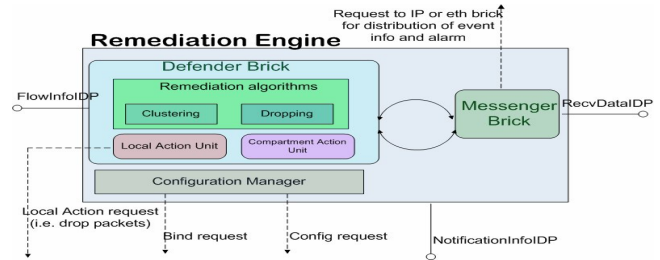

Figure 3: The RE internal architecture

3. CONCLUSIONS & FUTURE WORK

The proposed design of the resilience architecture satisfies core autonomic properties such as self-protection and self-optimization. Using a combination of detection and classification algorithms for abnormal network behaviour, we will demonstrate the applicability and efficiency of a run-time network resilience system. Our main objective is to integrate the resilience architecture with the rest of the ANA software in order to perform experimentation on both intra and inter-compartment scenarios.

4. REFERENCES

[1] Hutchison, D., Sterbenz, J. P.G, Jabbar, A. Sholler, M., 2006 D3.2: Resilience/Security Framework, Deliverable D3.2 ANA December 2006
[2] ANA project: http://www.ana-project.org
[3] Lahkina, A., Crovella, M., Diot, C., 2005, Mining Anomalies Using Traffic Feature Distributions, ACM SIGCOMM 2005, Philadelphia, Pensylvania, USA.
[4] Zuev, D., Moore, W., A., 2005 Traffic Classification using a Statistical Approach, Intel Research Paper, 2005