Research Proposal

Andres Chaves (706801)
Melbourne School of Information
The University of Melbourne

November 22, 2014

Abstract

The purpose of this documents will be to stablish the context and bases of the research proposal which applies concepts of Machine Learning into Network Management Systems.

Throughout this document one will read the relevance of the research, how will the concepts of Machine Learning will be applied to Event-processing Network Management Systems and finally what are the expected results.

Contents

1 Introduction

There is no doubt of the strong development and evolution of Information Technologies in modern world. Nowdays we have access to computing devices in whatever form (Supercomputer, Laptops, Tablets, Mobile, etc.) in conjunction with advanced distributed information systems.

But all this evolution could not be accomplished without a key component: Computer Networks. Networks make possible for data exchange and service consumption and side by side with Information Technology, networking evolved from simple small low bandwidth networks, to high speed wired and wireless ones connecting all the world.

These huge networks require a set of practices, tools and knowledge in order to garantee the availability and speed required by the clients. A discipline called Network Management arised to address all these concerns and nowdays network management comprises all the practices and activities that a carrier must perform in order to fulfill its Service Level Agreements (SLAs) with its clients.

From the information systems perspective, Network Management requires a set of systems called Network Management Systems (NMS) designed to administer either all or a part of the network. These administration comprises a set of functions: Fault Management, Performance Management, Configuration Management and Security Management among others.

Fault Management involves how to detect, classify and inform the Network Operator about conditions that affect or may affect the network services, both from availability and performance perspective.

One of the recent challenges in Network Management is how to monitor ever bigger networks, currently the network devices that a carrier must administer is measured in the range of thousands to millons. With this size a key desired function is only show the relevant alarms that matter to the network operators.

One possible approach to analyse, classify and display only the relevant events to the operator is by the use of a machine learning system that can help the network operator in the processing of events and thus augmenting the network management capacity with the same engineering team.

This project intends to advance in this approach and measure the benefits of the use of a machine learning system to fault management.

2 Objective

The objective of this project is to analyse how machine learning technologies can be applied to Network Management Systems, specifically event/fault management systems in order to provide more quality and key events to the network operator and thus increase the network management capacity of a Network Operation Center.

The Machine Learning technique will be used for correlation rules generation as an id to the human expert. The objective is not to replace the judge and knowledge of the engineer but quickly help him in discovering what correlation rules may be applied to reduce the ratio alarm to operator.

3 Technical Approach

A generic SNMP Network Management System is a stream based system that conceptually can be divided in several stages: Alarm reception, alarm translation and enrichment, event correlation and event presentation. A conceptual schema can be seen on Figure 1

For our testing environment we are going to use several open source components to simulate a Management System. These are:

- Net-SNMP: Net-SNMP is an open source Linux and Unix package that implements the SNMP protocol.[1]
- SNMPTT: SNMPTT or SNMP-Trap Translator is an open source component that takes the SNMP trap (alarm) received by Net-SNMP and by using an alarm dictionary translate it into a more useful string. SNMPTT can also enrich the alarm from a database by executing a shell script.[2]
- SEC: SEC or Simple Event Correlator is an open source component that allows correlation of events streaming to the system.[3]
- MYSQL: MySQL is an open source relational database. For the purposes of this proposal, it will be used as storage for the Configuration Management Database.

The key work will be to apply Machine Learning techniques to the input stream arriving to SEC in order to infer what will be the proper rules to configure this correlation.

There will be also a recording of live networking event data to be used as a sample. For the purposes of the research the recording will be only for alarms of Layer 3 Routing Devices, but the concepts applied must apply to any kind of device/network.

The recording will have a flag to indicate whether the operator consider the alarm is important or not. This field along with the context of the alarm (device, port, location, label) will be the input to the different machine learning algorithms. The output of the algorithms will be a set of infered rules, that will be again evaluated and tested.

The proposed components can be seen on figure 2

4 Time Table and Deliverables

The research project is decomposed by the following tasks and deliverables:

Task	Date	Deliverable
First version of Research Proposal	2014/11/24	Yes
Initial Data Set Acquisition (without Classification)	2014/12/05	No
Establishing ML Techniques to be used	2014/12/16	No
Development of a quick prototype to classify alarms	2014/12/26	No
Data Set Acquisition (with Classification)	2015/01/09	No
Final version of Research Proposal	2015/02/24	Yes
Application of ML Techniques to the dataset	2014/03/24	No
Analysis of each ML technique	2014/04/16	No
First version of the final report (Thesis)	2014/05/11	Yes
Final version of the final report (Thesis)	2014/05/29	Yes

5 Literature Review

As Network Management involves processing and analysis of large datasets there has been several attempts to use Machine Learning techniques to aid or improve this large analysis.

The majority if the reviewed literature attemps to use Machine Learning into traffic flow analysis and Security. Traffic Analysis is one of the key parts in Network Management because it allows to determine patterns and behaviour segmented by type of traffic (HTTP, FTP, P2P, etc). For the security part the intention is to use Machine Learning to aid in the analysis of security logs to detect intrusion or attacks. While these topics are also part of Network Management the objectives and results differ with the purpose of this research.

There are a couple of papers that have explored how to apply Machine Learning to alarm handling, The first one titled "Algorithm of Mining Fuzzy Association Rules in Network Management" attempts to reduce the volume of alarms in a event database by applying the theory of Fuzzy Sets to find the frequent sets and association rules between them.[4].

The second one, named "An Artificial Intelligence Approach to Network Fault Management" discuss what Artificial Intelligence methods can be applied to fault management and suggest the use of either Neural Networks or Bayesian Belief Networks to the problem [5].

References

[1] Net-SNMP website, `http://www.net-snmp.org/`.

[2] SNMPTT website, `http://snmptt.sourceforge.net/docs/snmptt.shtml`.

[3] SEC website, `http://simple-evcorr.sourceforge.net`.

[4] Pei-Qi Liu, Zeng-Zhi Li, Yim-Liang Zhao, *Algorithm of Mining Fuzzy Association Rules in Network Management*. Proceedings of the Second International Conference on Machine Learning and Cybernetics, Xi'an, 2003.

[5] Denise W. Gürer, Irfan Khan, Richard Ogier, Renee Keffer, *An Artificial Intelligence Approach to Network Fault Management*.

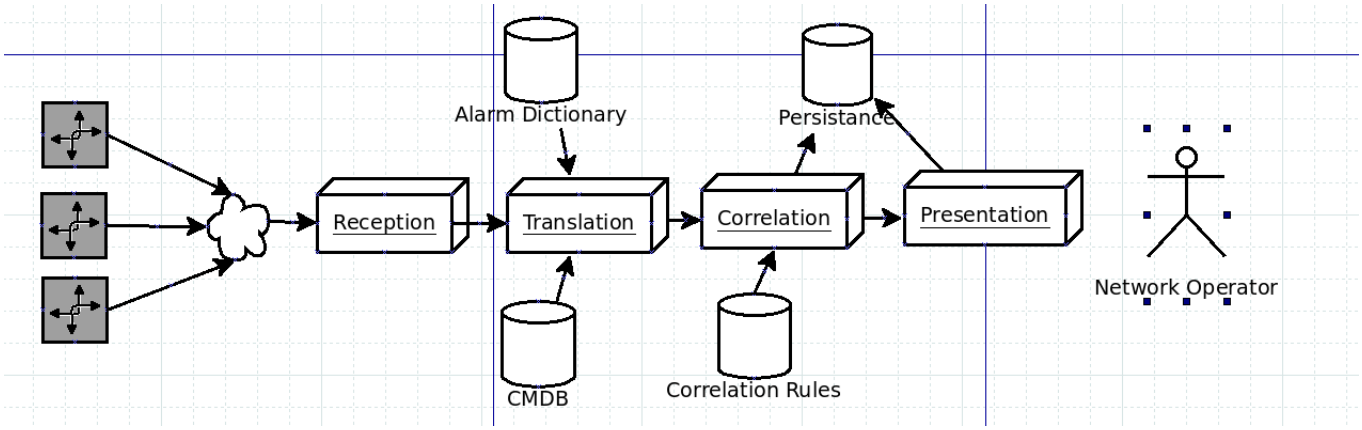

Figure 1: *A schematic of a generic Network Management System*

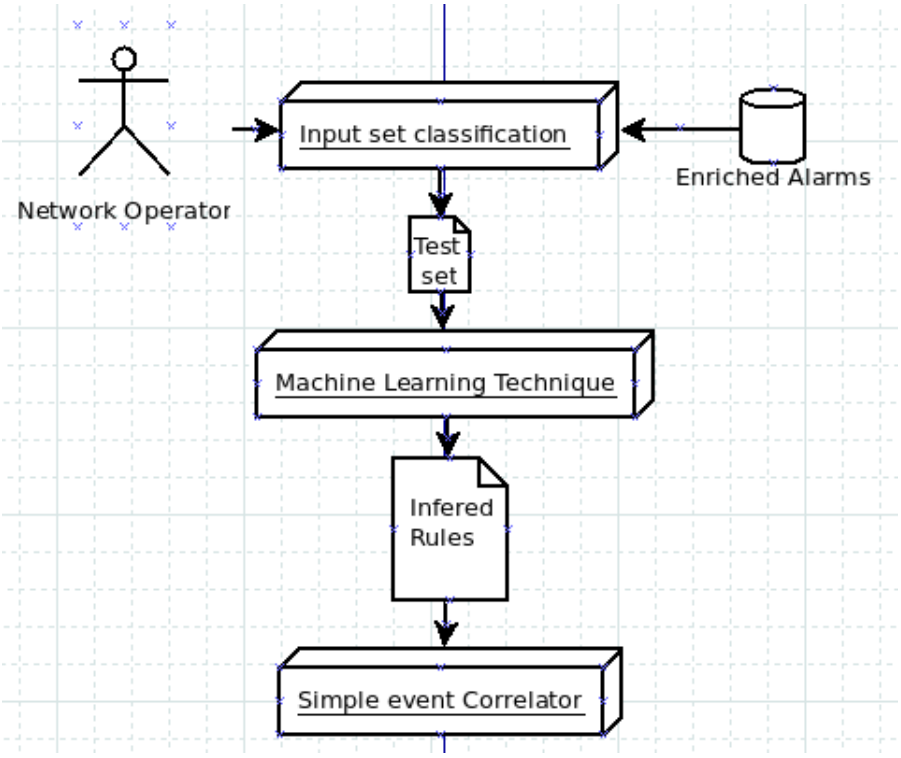

Figure 2: *Proposed Machine Learning Application*