Statistical Approaches for Network Anomaly Detection (4 hours tutorial)

Dr. Christian Callegari
http://wwwtlc.iet.unipi.it/people/ccallegari.shtml
christian.callegari@iet.unipi.it
University of Pisa, Pisa, Italy

Abstract

This tutorial provides an overview of the most relevant statistical approaches for network anomaly detection.
In the first part of the tutorial, starting from the seminal work by Denning, the basic concepts about anomaly detection will be introduced and the classical statistical methods for detecting anomalies in network traffic will be discussed.
In the second part of the tutorial, some of the most recent and relevant works about statistical approaches for anomaly detection will be discussed. Among the others, the tutorial will present algorithms based on: Markovian models, sketch, PCA, clustering, wavelet analysis, and entropy analysis. For each of the presented methods the description of the theoretical background, focusing on the reason why the method should be effective in detecting network anomalies, will be accompanied by a discussion on the type of anomalies that can be detected and on the achievable results.

Outline of the presentation

I. Motivation (10 min)

II. Basics of Statistical Intrusion Detection Systems (30 min)
- General Concepts about Anomaly Detection (10 min)
- IDES - Intrusion Detection Expert System (20 min): the use of a statistical approach to detect anomalies in the network traffic was first introduced by Denning. The author proposed an early, abstract model of an Intrusion Detection Expert System (IDES), based on the statistical characterization of the behavior of a subject with respect to a given object. The basic idea was to realize a profile of the normal behavior of the system.

III. Statistical approaches for anomaly detection (180 min)
- Markovian models (30 min): a Markov Process Model can be used to describe the transition probabilities for a given metric. This kind of approach has been taken into account in relevant papers to detect several kinds of anomalies
- Sketch (30 min): sketches represent an efficient way to randomly aggregate IP flows, thus they can be used to enable a precise identification of the underlying causes of anomalies.
- PCA (30 min): principal component analysis is effectively used to tackle the problem of high dimensional datasets, which usually affects network monitoring systems. In this field, PCA is often used as a detection scheme, applied to reduce the dimensionality of the audit data and to detect anomalies, by means of a classifier that is a function of the principal components.
- Clustering (30 min): clustering is a well-known technique, usually applied to classification problems. In the context of anomaly detection, two distinct approaches have been developed, which will be both discussed: in the first approach, the anomaly detection model is trained using unlabeled data that

consist of both normal as well as attack traffic, while in the second approach, the model is trained using normal data only.
- Wavelet analysis (30 min): due to its properties, the Wavelet transform is quite a "classical" approach to detect irregular patterns in time series. Indeed it can be used to detect the changes caused by flashcrowds, outages, and attacks.
- Entropy analysis (30 min): entropy-based approaches, which determine and report entropy contents of several traffic parameters (e.g. IP addresses), can be used to detect anomalies in the network traffic. Indeed changes in the entropy content can indicate an anomalous network event.

IV. Discussion and perspectives (20 min)

Scope

Due to the wide literature available on the topic, it is impossible to give an in-depth course on network anomaly detection in a three-hour tutorial. Hence, we do not intend to provide an extensive review of all ongoing approaches, but rather to focus on some of the most promising examples, with some references to the speaker experience in the field.

Intended Audience

This tutorial is addressed to all researchers and practitioners working in the field of networking, who can be interested in detecting an anomalous behavior in the network, and in particular to those dealing with intrusion detection systems, anomaly detection, DoS/DDoS attack detection. In addition to this, the tutorial may be of interest to all those people also dealing with statistical approaches for traffic classification.
Since all the theoretical notions necessary to understand the covered topics will be provided in the tutorial, no particular knowledge is required for attendees, except for some basics of networking (IP/ TCP architecture).

Description of the material

The tutorial will be given through standard PDF slides. A .pdf file containing the slides (along with a list of references) will be provided in due advance to facilitate the Organizing Committee to prepare the paper handouts.

Biography of Presenter

Christian CALLEGARI was born in La Spezia, Italy, in 1980. He received the B.E. and the M.E. degrees in telecommunications engineering and the PhD degree in information engineering from the University of Pisa, Pisa, Italy, in 2002, 2004, and 2008, respectively. He was recipient of a scholarship issued by the Italian Ministry of Education for his PhD program.
Since 2005, he has been with the Department of Information Engineering at the University of Pisa. In 2006/07, he was a visiting student research collaborator at the Department of Computer Science at ENST Bretagne, France.
Dr. Callegari is currently a post-doc research fellow and a teaching assistant at the University of Pisa for the Network Security course of the M.E. degree in telecommunications engineering and has given lectures about Anomaly Detection and statistical traffic classification in the framework of a PhD course organized twice by the Euro-NGI Network of Excellence funded by the European Community.

His research interests are in the area of network security, statistical traffic classification, and network simulation.
Moreover, he has co-authored more than 30 papers presented in leading international journals and conferences (http://netgroup.iet.unipi.it/people/ccallegari.shtml), and he serves as a TPC member for several international conferences (e.g. IEEE Globecom and IEEE ICC) and as a reviewer for several international journals (e.g. International Journal of Communication System, Computer Networks Journal) and conferences.

Selected Publications:

- Christian Callegari, Stefano Giordano, Michele Pagano **"New Statistical Approaches for Anomaly Detection"** Accepted in Security and Communication Networks
- Christian Callegari, Rosario G. Garroppo, Stefano Giordano, and Michele Pagano **"Security and Delay issues in SIP Systems"** Accepted in International Journal of Communication Systems
- Christian Callegari, Rosario G. Garroppo, Stefano Giordano, Michele Pagano, and Franco Russo **"A Novel Method for Detecting Attacks towards the SIP protocol"** International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS 2009), Jul 13-16, Istanbul, Turkey
- Christian Callegari, Stefano Giordano, Michele Pagano **"On the Use of Co-Occurrence Matrices for Network Anomaly Detection"** International Wireless Communications and Mobile Computing Conference (IWCMC 2009), June 21-24, Leipzig, Germany
- Christian Callegari, Stefano Giordano, Michele Pagano **"On the Use of Compression Algorithms for Network Anomaly Detection"** IEEE International Conference on Communications (ICC 2009), June 14-18, Dresden, Germany
- Christian Callegari, Stefano Giordano, and Michele Pagano **"An anomaly detector based on Wavelet Packet Transform"** The 3rd Italian Workshop on PRIvacy and SEcurity (PRISE 2008), Oct 20, Rome, Italy
- Christian Callegari, Stefano Giordano, and Michele Pagano **"Application of Wavelet Packet Transform to Network Anomaly Detection"** The 8th International Conference on Next Generation Teletraffic and Wired/Wireless Advanced Networking (NEW2AN 2008), Sep 3-5, St.Petersburg, Russia
- Christian Callegari, Sandrine Vaton, Michele Pagano **"A New Statistical Approach to Network Anomaly Detection"** International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS 2008), Jun 16-18, Edinburgh, UK
- Davide Adami, Christian Callegari, Stefano Giordano, Michele Pagano **"A Statistical Network Intrusion Detection System"** Second Italian Workshop on PRIvacy and SEcurity (PRISE 2007), Jun 6, Rome, Italy
- Christian Callegari **"Self-Learning Intrusion Detection Systems"** DIWALL - Séminaire sur la sécurité des systèm d'information, Feb 7, Brest, France
- Davide Adami, Christian Callegari, Stefano Giordano, Giada Landi, Michele Pagano **"Design, Implementation, and Validation of a Self-Learning Intrusion Detection System"** IEEE/IST Workshop on "Monitoring, Attack Detection and Mitigation (MonAM 2006), Sept. 27-28, Tubingen,Germany