Wavelets and Network Anomaly Detection (3 hours tutorial)

Michele Pagano[♮]

e.mail: {m.pagano }@iet.unipi.it
Dept. of Information Engineering
University of Pisa, Pisa, Italy

[♮]Joint work with Dr. Christian Callegari

Abstract

This tutorial provides a survey on the use of wavelet analysis in the framework of network anomaly detection. After a short overview of the basic concepts about anomaly detection, the first part of the tutorial will introduce the wavelet transforms (continuous, discrete and wavelet packets), focusing on the main features (phase-space localization, multiresolution analysis and edge detection), widely used in signal processing and recently applied to anomaly detection.

The second part of the tutorial will highlight how wavelets can be applied to network data in order to identify the presence of several kinds of anomalies (such as flash crowd, synthetically generated anomalies, DoS and DDoS attacks) at various locations in the network (the distance between the measurement point and the point of anomaly is a key performance factor). Different features of the traffic flows (traffic volumes at different aggregation and resolution levels, correlations among IP header fields) will be analysed, presenting results from synthetic as well as real traces.

Finally, an open discussion on the perspectives of wavelet approaches to anomaly detection will end the tutorial.

Outline of the Presentation

1. Basics of Statistical Intrusion Detection Systems (20 min)
   (a) Motivations and general concepts about Anomaly Detection
   (b) Overview of the main statistical approaches for Anomaly Detection
2. Wavelet Transforms (40 min)
   (a) Time-Frequency analysis of signals: Wavelets vs. Fourier
   (b) Continuous Wavelet Transform
   (c) Discrete Wavelet Transform
   (d) Wavelet Packets and best basis selection
3. Applications of Wavelets to Anomaly Detection (110 min)
   (a) Wavelets and Lipschitz regularity
   (b) Local extrema of CWT as indication of sharp variations
   (c) Wavelet-based analysis of the energy distributions
   (d) Wavelet analysis of the correlations in packets header
   (e) Detection of both short and long-lived anomalies
   (f) Anomalies as deviations from the "self-similar" nature of traffic
   (g) Wavelet packets as a more flexible multiresolution analysis tool
4. Discussion and perspectives (10 min)

Scope

Although wavelets have been used in many different fields (such as image processing and compression, statistical data analysis and compression, pattern recognition, to cite just a few), their use in the framework of statistical intrusion detection is still relatively unexplored.
This tutorial aims at introducing the key features of Wavelet Transforms, skipping most of the mathematical details and focusing on the applicability to anomaly detections, with some references to the speaker experience in the field.

Intended Audience

This tutorial is mainly addressed to all researchers and practitioners working in the field of anomaly detection and statistical traffic classification. In addition to this, the tutorial may be of interest to all those people familiar with wavelets and looking for novel applications of this general and powerful theory.

Since all the theoretical notions necessary to understand the covered topics will be provided in the tutorial (this explains the length of the introductory

sections), no particular knowledge is required for attendees, except for some basics of networking (IP/TCP architecture) and digital signal processing (digital filters and Fourier Transform).

Biography of Presenter

Michele Pagano was born in Lerici (Italy) in 1968. He received laurea (cum laude) in Electronics Engineering in 1994 and a Ph.D. in Electronics Engineering in 1998, both from the University of Pisa.

From 1997 to 2007 he has been *researcher* at the Dipartimento di Ingegneria dell'Informazione of the University of Pisa, and since 2007 he is associate professor at the same Department.

Currently he is the official instructor of the courses of "Telematics", "Performance of Multimedia Networks" and "Network Security" in the laurea course in Telecommunication Engineering at the University of Pisa.
Moreover, in the framework of the Network of Excellence Euro-NGI (Design and dimensioning of the Next Generation Internet), in collaboration with Prof. Sandrine Vaton (ENST Bretagne), in June 2006 and in October 2006 he gave a Joint PhD Courses on "IP traffic characterization, data analysis and statistical methods: Bayesian Methods in Teletraffic Theory".
Furthermore, in the framework of the international inter-university co-operation convention between the University of Pisa and the State University of Petrozavodsk (PSU, in Russia), he gave a short course on "Large Deviation Theory and Rare Event Simulation" (September 2003) and a master course on "Advances in Network Performance Analysis" (November 2008 and February 2010), both at the Mathematical Faculty of PSU.

His research interests are related to statistical characterization of traffic flows and to network performance analysis, mainly in the framework of architectures able to support Quality of Service. In this scenario the research activity deals with analytical approaches for performance evaluation as well as the use of discrete event simulation to better characterize network behaviour and protocols (mainly using NS-2). In particular, in the specific framework of Rare Event Simulation, Importance Sampling techniques and applications of Large Deviation Theory have been investigated.
Finally, a new research field is represented by network security issues, mainly in the frameworks of statistical techniques for intrusion detection and traffic classification.

He has co-authored around 100 papers published in international journals and presented in leading international conferences. Moreover, he serves as a TPC member for several international conferences and as a reviewer for several international journals (e.g., ACM TOMACS, IEEE TOC, EJOR, ETT, Computer Networks and Computer Communications) and conferences.
He has been the local coordinator for the 2006 PRIN (Research projects of national interest) RECIPE (Robust and Efficient traffic Classification in IP nEtworks) and for 2008 PRIN EFFICIENT (Energy eFFIcient teChnologIEs for

the Networks of Tomorrow).

Moreover he participated to international cooperation projects funded by the EC (as INTAS supervisor of Dr. Mikhail Alexander Marchenko) and by the University of Pisa (main investigator of a cooperation project with Peoples' Friendship University of Moscow, Petrozavodsk State University and Siberian Department of the Russian Academy of Science in Novosibirsk).

Tutorial Experience

Michele Pagano gave tutorials on TCP models (2004) Importance Sampling (2005) and Large Deviation Theory (2007) at Het-Nets conference. Moreover, he has a long teaching experience, including tutorials for PhD students in the framework of EuroNGI and cooperation projects with PSU.

Selected Publications (related to statistical anomaly detection)

- Christian Callegari, Sandrine Vaton, Michele Pagano *"A New Statistical Method for Detecting Network Anomalies in TCP Traffic"*, accepted in European Transactions on Telecommunications
- Christian Callegari, Stefano Giordano, Michele Pagano *"New Statistical Approaches for Anomaly Detection"*, Security and Communication Networks, Vol. 2 Issue 6, Pages 611-634 (Nov-Dec 2009)
- Christian Callegari, Rosario G. Garroppo, Stefano Giordano, Michele Pagano *"Security and Delay issues in SIP Systems"*, International Journal of Communication Systems, Vol. 22 Issue 8 (August 2009)
- Christian Callegari, Stefano Giordano, Michele Pagano, Teresa Pepe *"On the Use of Sketches and Wavelet Analysis for Network Anomaly Detection"*, First International Workshop on TRaffic Analysis and Classification (TRAC) 2010 - co-located with IWCMC, Jun 28 - Jul 2, Caen, France
- Christian Callegari, Stefano Giordano, Michele Pagano, Teresa Pepe *"On the Use of bzip2 for Network Anomaly Detection"*, Sixth International Working Conference on Performance Modeling and Evaluation of Heterogeneous Networks (HET-NETs) 2010, Jan 14-16, Zakopane, Poland
- Christian Callegari, Rosario G. Garroppo, Stefano Giordano, Michele Pagano, 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, Michele Pagano *"An anomaly detector based on Wavelet Packet Transform*, 3rd Italian Workshop on PRIvacy and SEcurity (PRISE 2008), Oct 20, Rome, Italy

- Christian Callegari, Stefano Giordano, Michele Pagano *"Application of Wavelet Packet Transform to Network Anomaly Detection"*, 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

- 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