Anomaly Detection of Network Traffic
Based on
Analytical Discrete Wavelet Transform

Author : Marius SALAGEAN, Ioana FIROIU

10 JUNE 2010

Introduction

MAIN OBJECTIVES :

-a new detection mechanism of network traffic anomaly based on Analytical Discrete Wavelet Transform (ADWT) and high-order statistical analysis;

-evaluate our technique with the 1999 DARPA/MIT Lincoln Intrusion Detection Dataset .

> Anomaly Detection of Network Traffic Based on Analytical Discrete Wavelet Transform

Motivation (1)

- the expansion of the Internet and the great number of available services;
- the emergence of a variety of wireless networks;
- the mobility of network hosts;
- the vulnerability of present-day software and protocols;
- companies have increasingly put critical resources online.

Attacks/intrusions :

- virus, spamming, worms, malware, privilege escalation, unauthorized logins, access to sensitive information, attacks against vulnerable services, injection of unwanted packets into the target networks.

The classical solutions to reduce the risks of security problems → **Firewalls**

Cryptographic techniques

INTRUSION DETECTION SYSTEMS (IDS) ← **+**

> Anomaly Detection of Network Traffic Based on Analytical Discrete Wavelet Transform

Intrusion Detection Systems

Detection method :
- Misuse/Signature-based Systems
- Anomaly-based Systems

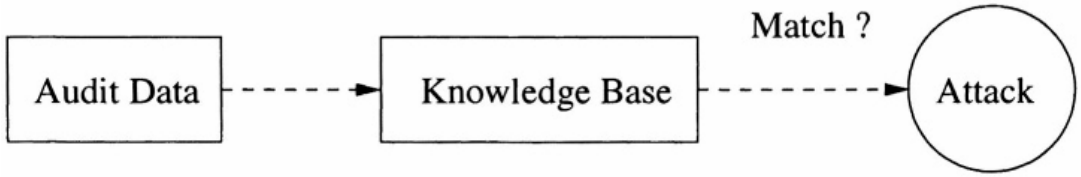


Figure 1. Block Diagram of a Typical Knowledge-Based IDS

Advantage:
- Very accurate in detecting known attack

Disadvantage:
- cannot detect previously unknown attacks

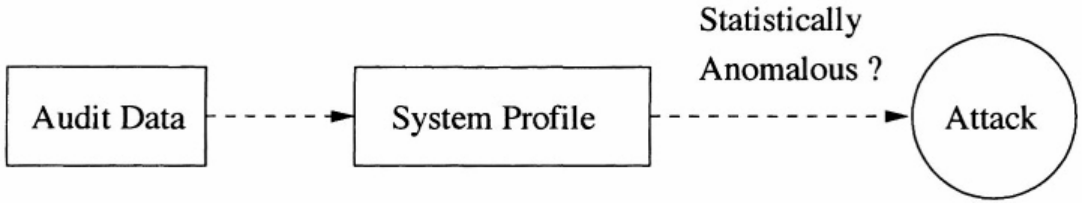


Figure 2. Block Diagram of a Typical Behavior-Based IDS

Benefit:
- Can detect previously unknown attacks

Drawback:
- generation of many false alarms

Anomaly Detection of Network Traffic Based on Analytical Discrete Wavelet Transform

Anomaly based detection IDS based on ADWT (1)

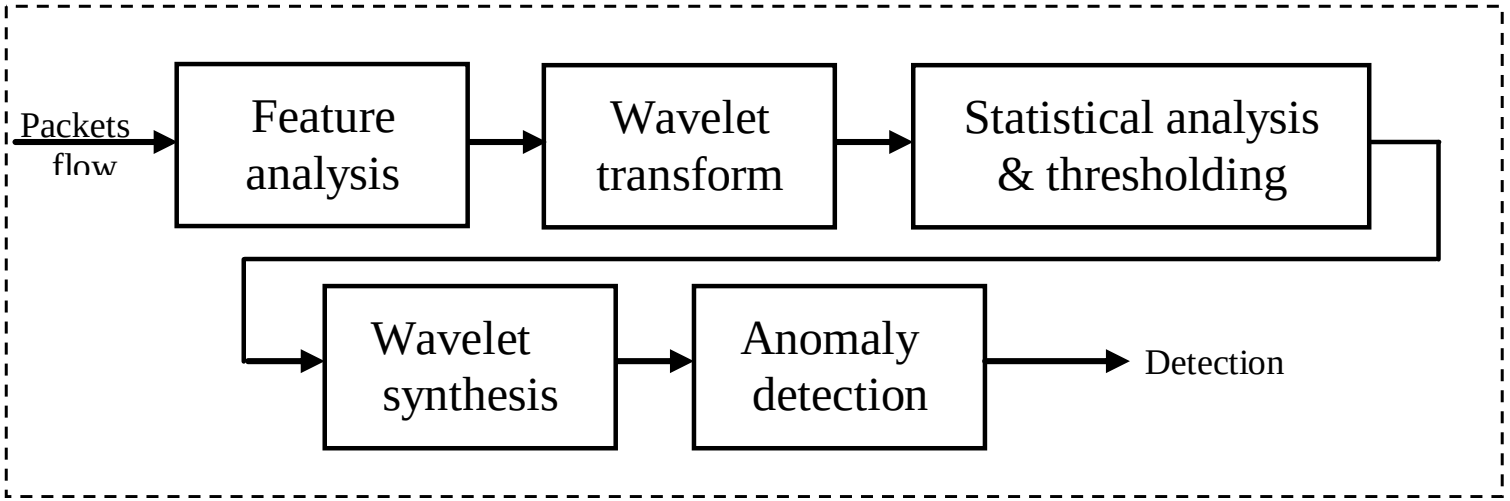
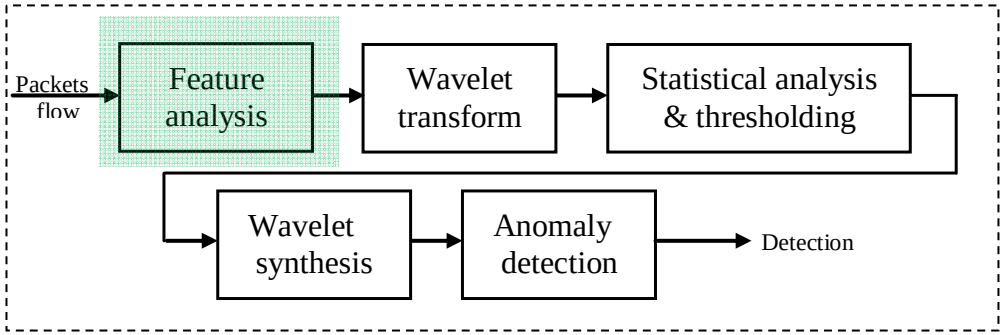


Figure. 3. The model of network traffic anomaly detection

Anomaly Detection of Network Traffic Based on Analytical Discrete Wavelet Transform

Anomaly based detection IDS based on ADWT (2)



Feature Analysis

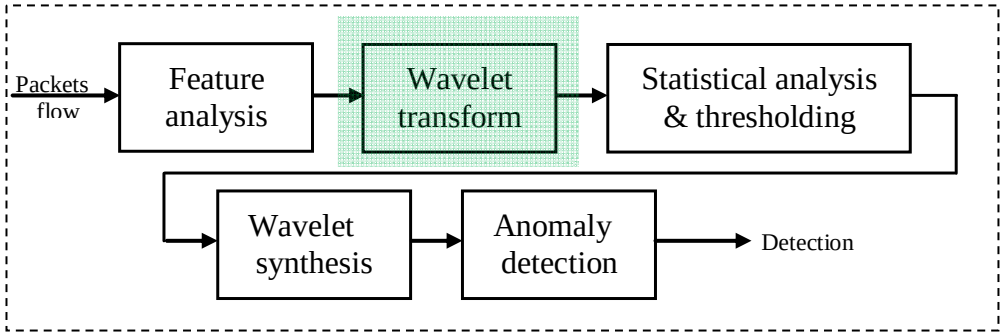
Network flows – TCP, UDP and ICMP

Packets flow (Tcpdump) → **Editcap** → **Tshark** →

flow count over a time period
average number of packets in a flow over a time period
average number of bytes in a flow over a time period
average packet size in a flow over a time period
and ratio of flow count to average packet size

Anomaly Detection of Network Traffic Based on Analytical Discrete Wavelet Transform

Anomaly based detection IDS based on ADWT (3)



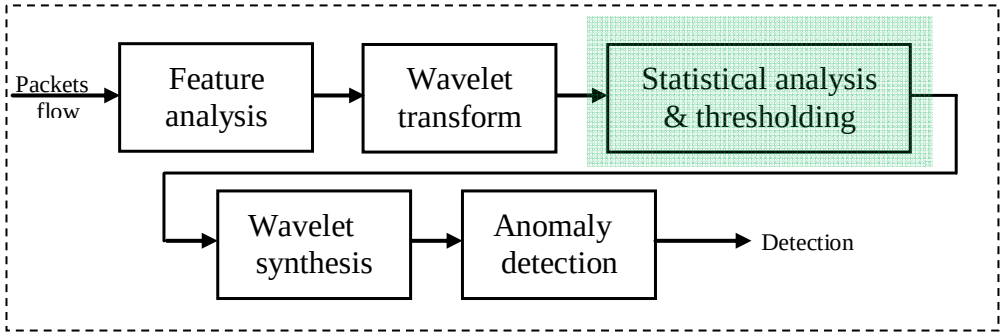
Wavelet transform

Network flows → **ADWT** → **[cA4, cD4, cD3, cD2, cD1]**

- 4 level of decomposition
- Daubechies(db6)
  - localization
  - vanishing moments
  - linearity
  - symmetry

Anomaly Detection of Network Traffic Based on Analytical Discrete Wavelet Transform

Anomaly based detection IDS based on ADWT (4)



Statistical analysis & thresholding

High-order statistics - 4th order cumulant :

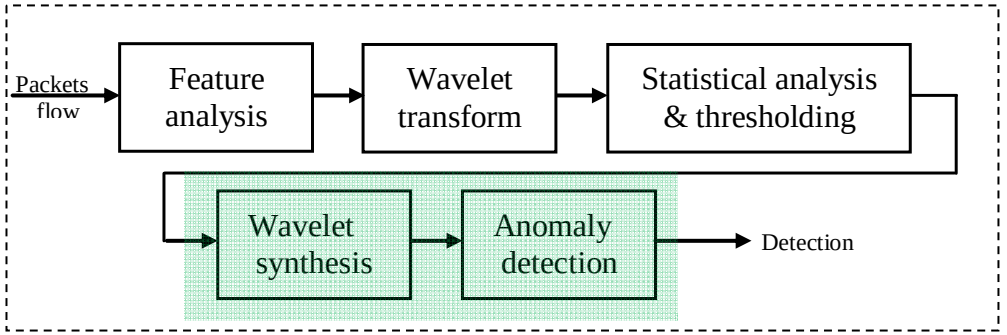
$$\tilde{C}_2^2[s] = \tilde{M}_2^2[s] - 2\left(\tilde{M}_1^1[s]\right)^2 - \tilde{M}_2[s]\tilde{M}^2[s]$$

where $\tilde{M}_p^q$ ***is the complex moment of the signal s .***

The thresholds are set through the research of historic traffic over several days.

Anomaly Detection of Network Traffic Based on Analytical Discrete Wavelet Transform

Anomaly based detection IDS based on ADWT (5)



Wavelet synthesis & Anomaly detection

Filtered signal → **IADWT** → **Anomaly detection** → **Attack**

- better shift-invariance
- simplicity
- flexible structure
- reduced computational time

Anomaly Detection of Network Traffic Based on Analytical Discrete Wavelet Transform

Results (1)

1999 DARPA/MIT Lincoln Intrusion Detection Dataset

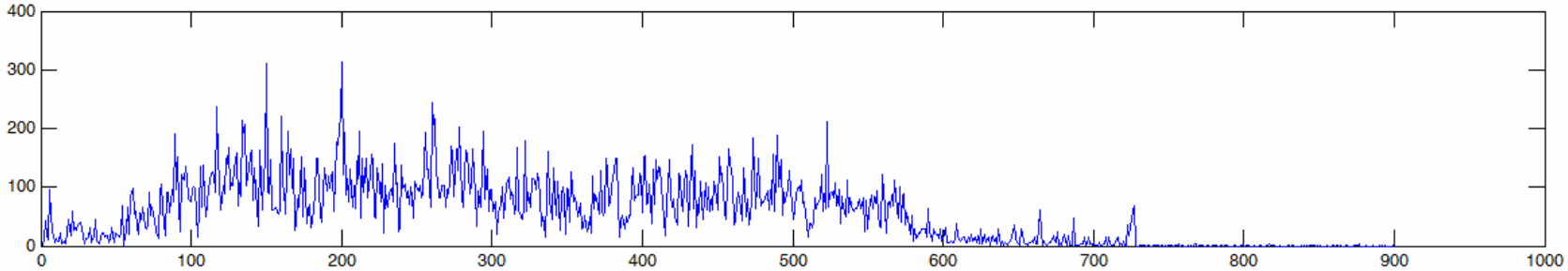
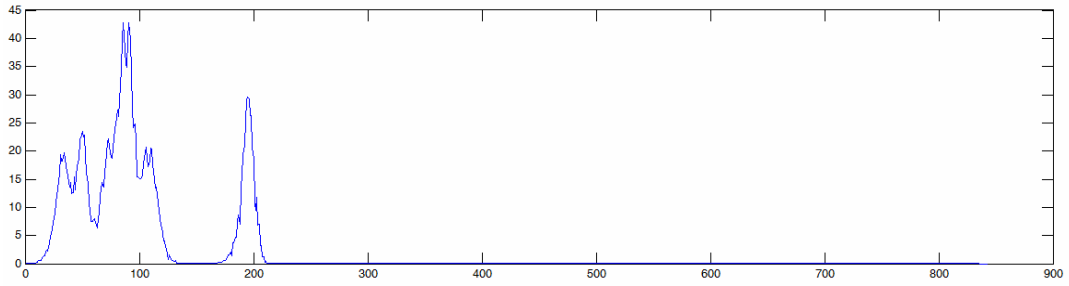


Figure. 4. Number of TCP flows per minute over one day



4 attack detected :

- ***Ntinfoscan***
- ***pod***
- ***back***
- ***httptunnel***

Anomaly Detection of Network Traffic Based on Analytical Discrete Wavelet Transform

Results (2)

1999 DARPA/MIT Lincoln Intrusion Detection Dataset

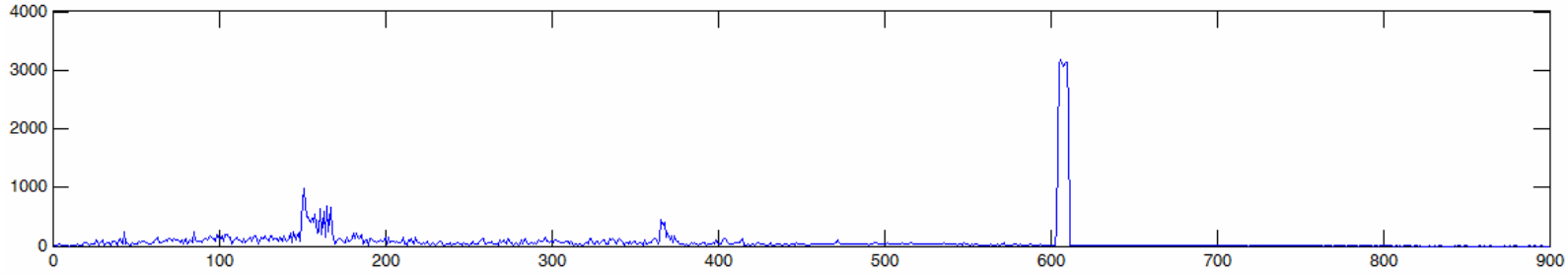
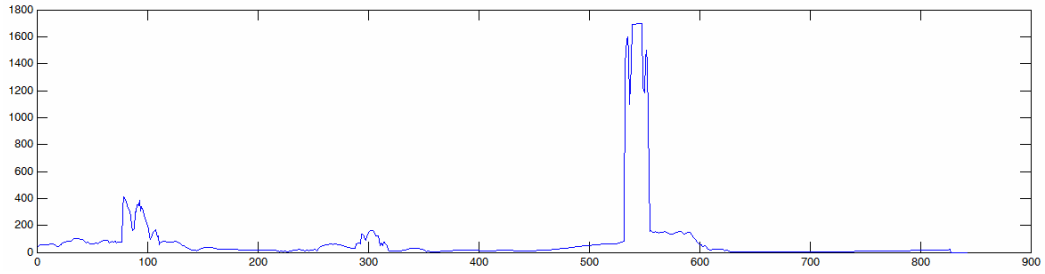


Figure. 5. Number of TCP flows per minute over one day



5 attack detected :

- ***portsweep***
- ***ipsweep***
- ***pod***
- ***apache2***
- ***dict***

Perspectives

PERSPECTIVES :

- Optimal selection of the alert thresholds
- Applying different wavelet basis functions, and study the impact in detecting the attacks
- Implementation of the proposed method in real-time