On Detection and Visualization Techniques for Cyber Security Situation Awareness

Author: Wei Yuy, Sixiao Weiy, Dan Shenz, Misty Blowers,
Erik P. Blasch, Khanh D. Phamq, Genshe Chenz,
Hanlin Zhangy, Chao Luy

Computer and information sciences

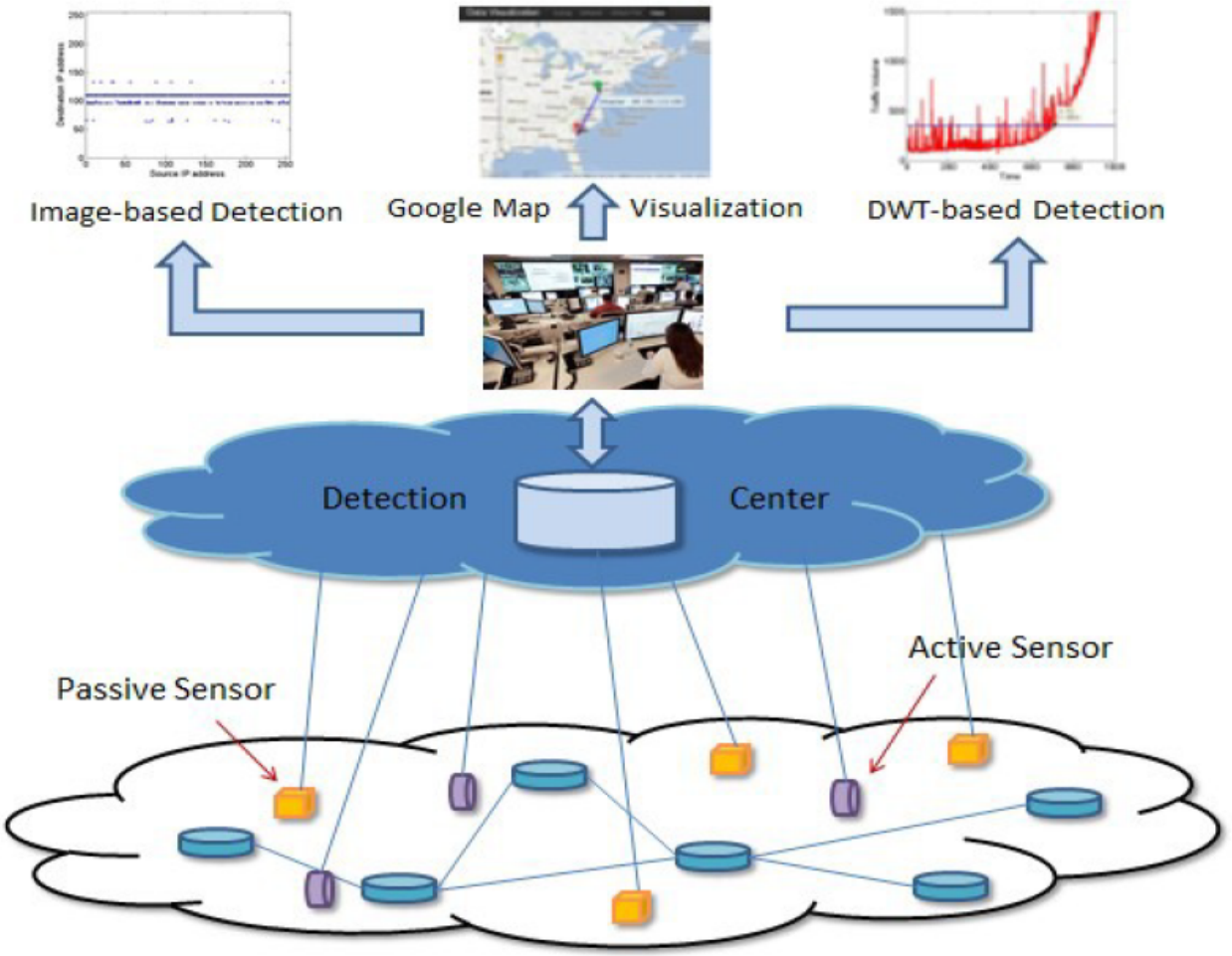
Ruijie Xi

UNIVERSITY OF DELAWARE

1. Introduction

- Prototypical system
- Visualization features
- Image-based track algorithm
- Two detection schemes: Discrete wavelet transform (DWT), traffic volume based approach
- Evaluation

2. System Architecture

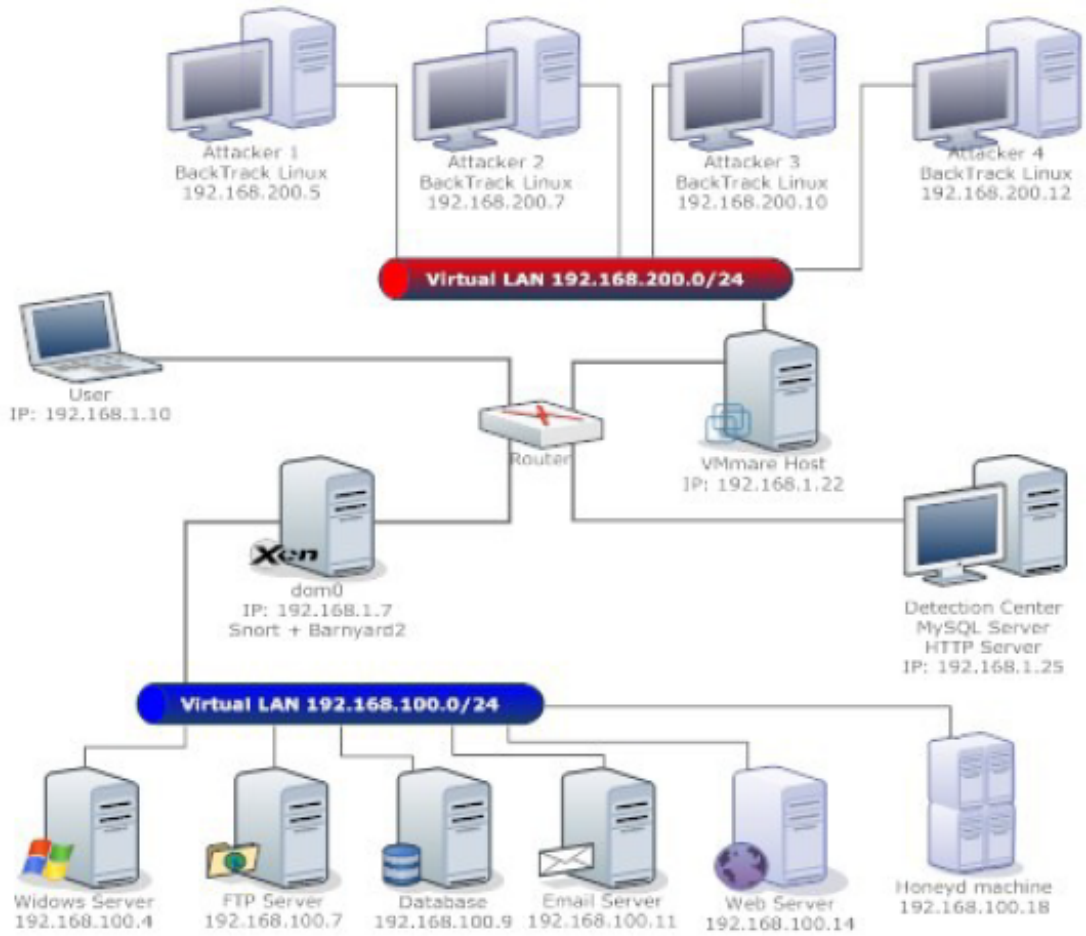


3. Testbed Setup

- Unpatched Windows Server: **vulnerabilities** and **effectiveness**

- BackTraceLinux server: hacking tools

3. Testbed Setup



4. Attack Visualization

- 1D : Network traffic volume.
- 2D : Source IP and destination IP addresses
- 3D : Geological attributes and victims.

5. Attack Detection

- Many to many attacks: worm/malware propagation
- Many-to-one attacks: DDoS
- One-to-many attacks: port-scanning attacks

5. Attack Detection

- **Image based detection scheme(**traffic volume based approach**):**
- 1. Information: packet headers, detection center
- 2. Traffic data: Construct 2D images

5. Attack Detection

- Image-based track algorithm

Algorithm 1: The Image Based Transform Algorithm

Input : Source IP Address $S_{i1}, S_{i2}, S_{i3}, S_{i4}$;
Destination IP Address $D_{i1}, D_{i2}, D_{i3}, D_{i4}$;
Traffic Volume Vector $X = [X_1, X_2, \ldots, X_8]$;
Total Traffic Volume M;

Output : Plot Image Based on Collected Data

Collect Traffic Data:
for $i = 1 : M$ **do**
  for $j = 1 : 4$ **do**
    $X_{ij} = S_{ij}$
    $X_{i(j+4)} = D_{ij}$ % Record Source IP and Destination IP address into Traffic Volume Vector
  end
end
Display Image of Traffic:
Input Traffic Volume Vector: $X = [X_1, X_2, \cdots, X_8]$;
for $i = 1 : M$ **do**
  for $j = 1 : 4$ **do**
    plot($X_{ij}, X_{i(j+4)}$) % Plot Image Based on Collected Data
  end
end
Display 2D Image for Network Traffic

5. Attack Detection

- Image-based track algorithm

Algorithm 2: The Image Based Track Algorithm

Input : Image of Traffic Data;
Traffic Volume Vector: $G = [G_1, G_2, \cdots, G_8]$;
Total Traffic Volume M;
Threshold Parameter: k;

Output : Print Attack IP Addresses

Gray Scale Image Generation:

$I = imread('image.jpg')$; % Read Generated Color Image and save it in an Array

G= rgb2gray(I); % Transform Color Image into Gray Scale Image along with Gray-Level Value

Display Image of Network Traffic:

Input the Array of Gray-Level Value: $G = [G_1, G_2, \cdots, G_N]$;

Define N as the Total Number of Array

$m = mean(G)$

$v = std(G)$ % Calculate Mean Value and Stand Derivation of Data Stored in Array

for $i = 1 : N$ **do**

  if $G_i > m + kv$ **then**

    $j = i$;

  end

end

5. Attack Detection

- Detection schema 1(image based detection):
- Use traffic volume as the detection feature (blue line is the threshold).

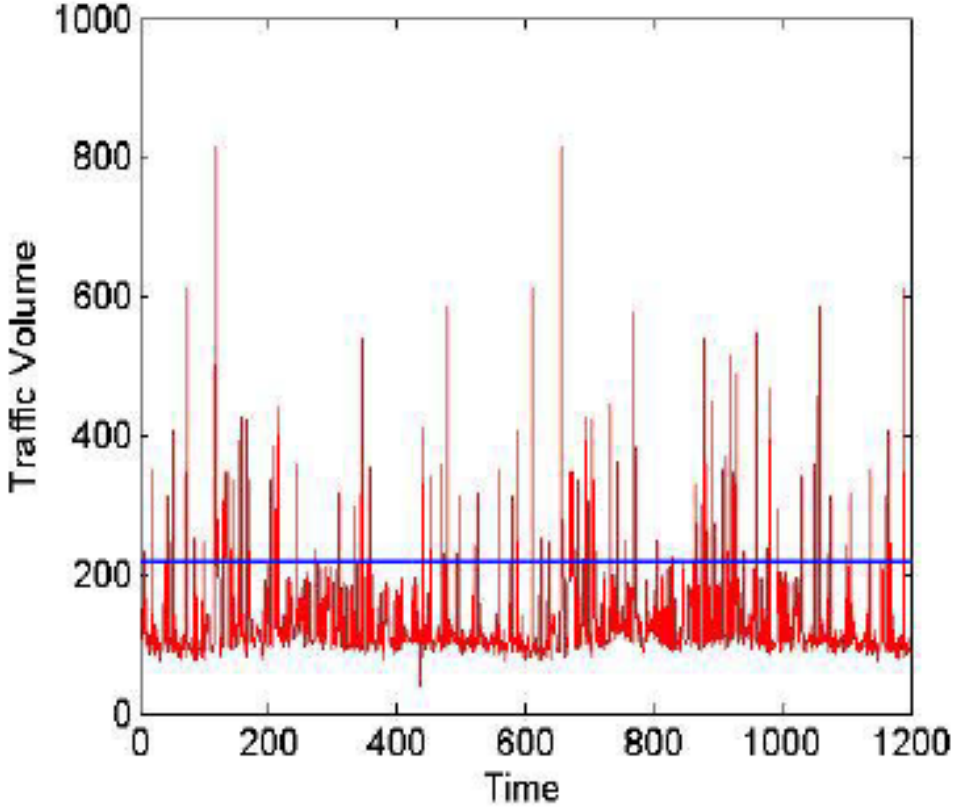


Figure1. random traffic volume

5. Attack Detection

- Detection schema 1(image based detection):
- Use traffic volume as the detection feature (blue line is the threshold).

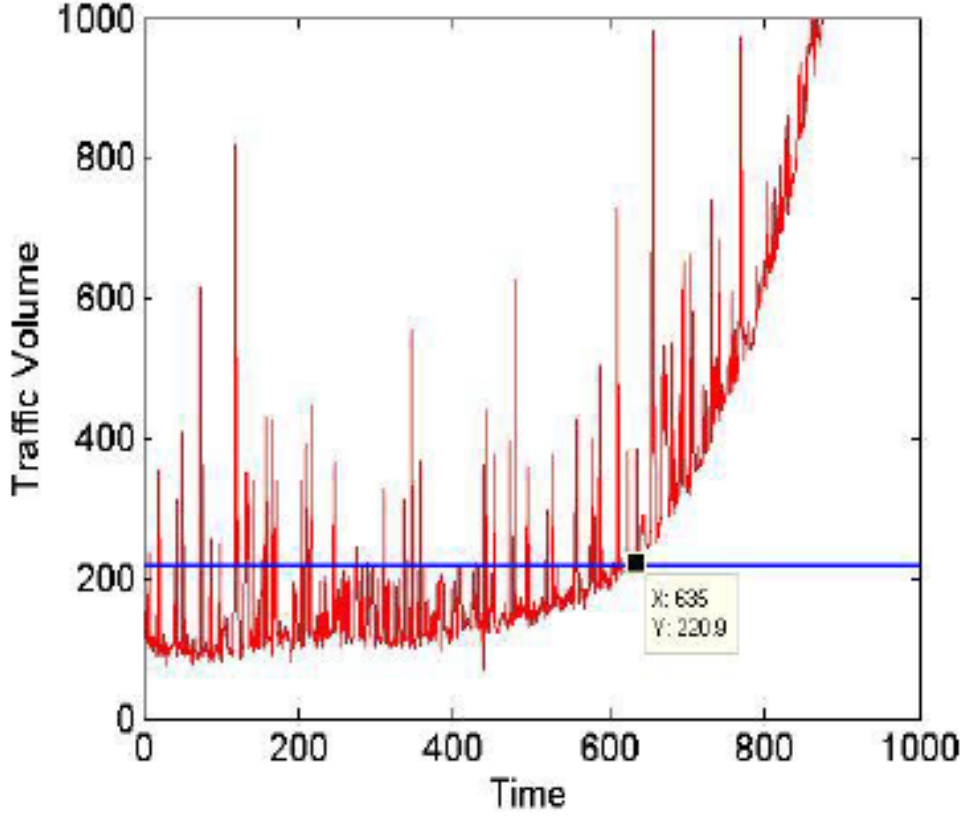


Figure2. mix attack and background traffic

5. Attack Detection

- Detection schema 2(Discrete wavelet transform):

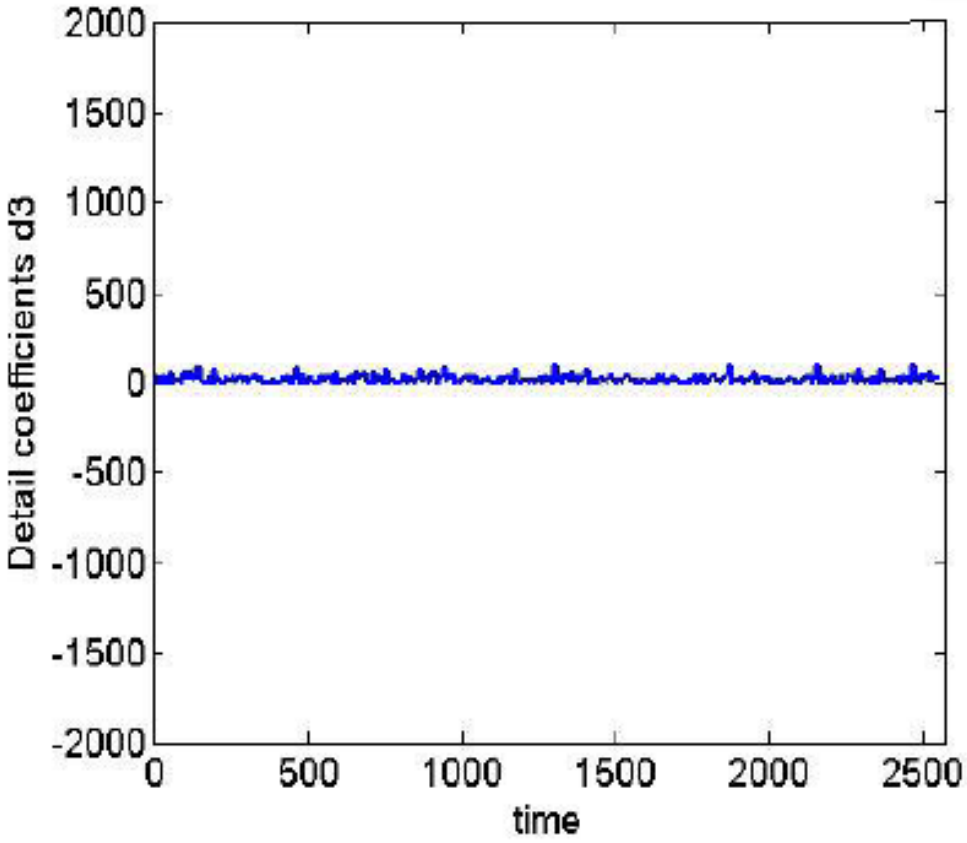


Figure 1:Background traffic

5. Attack Detection

- Detection schema 2(Discrete wavelet transform):

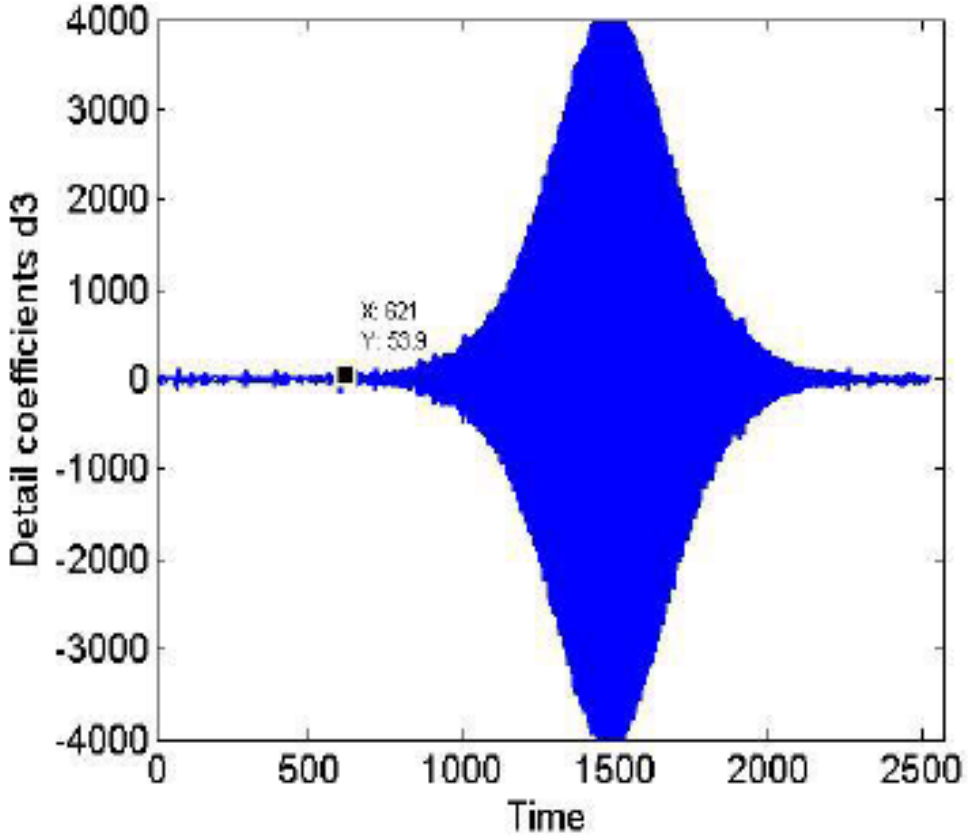


Figure 2: Mixture traffic with attack

6. Evaluation

- 2D visualization:

Figure 1: one-to-one

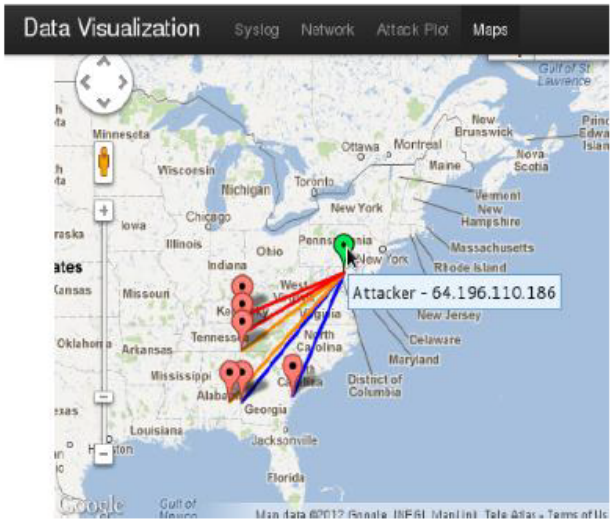


Figure 2: one-to-many

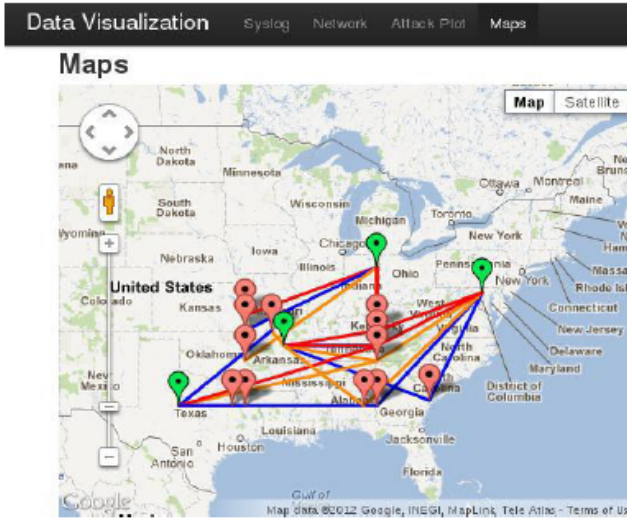


Figure 3: many-to-many

6. Evaluation

- 3D visualization:

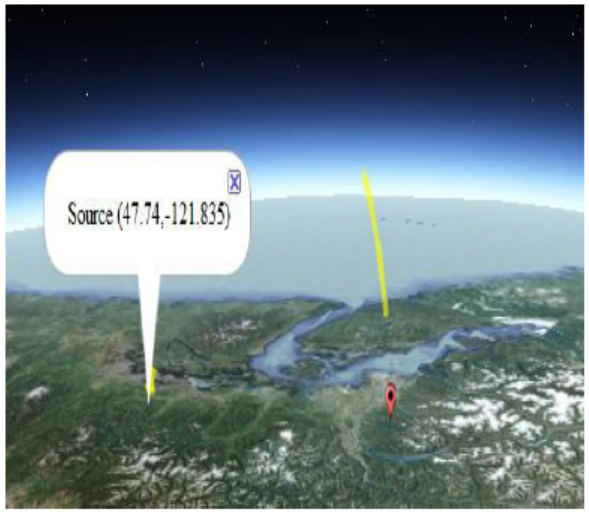


Figure 1: one-to-one

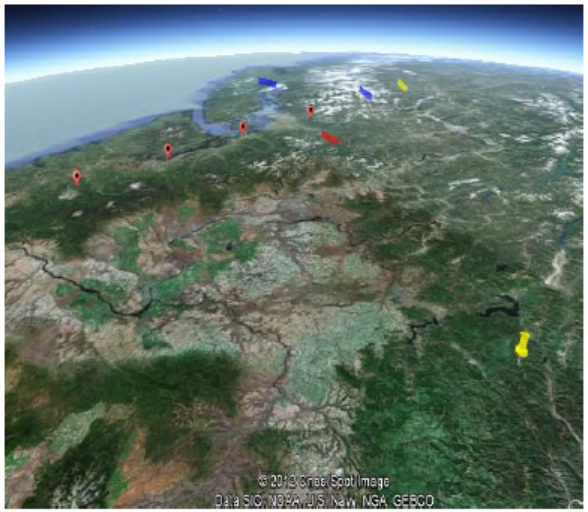


Figure 2: one-to-many

Figure 3: many-to-many

6. Evaluation

- **Detection Rate (Pd):** detection rate
- **False Positive Rate (Pf):** false positive rate
- **Detection Time**

6. Evaluation

- Real-world network traffic
- Propagation attack model
- Calculation

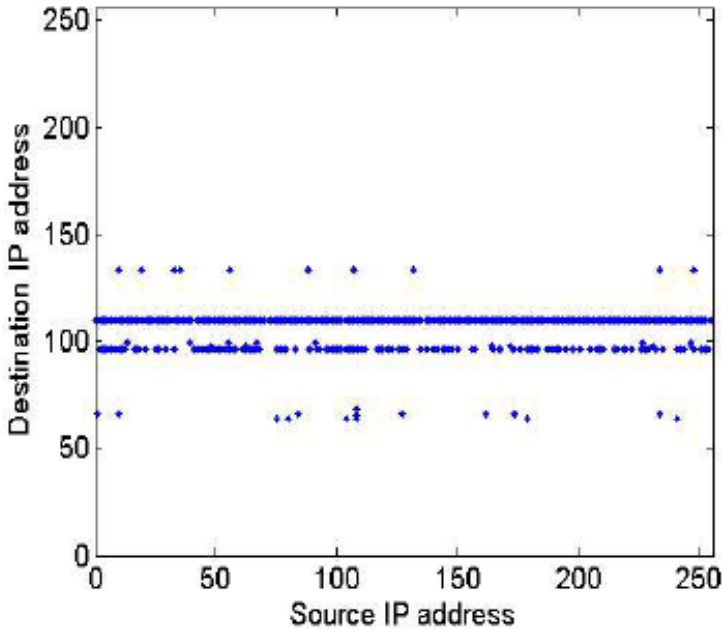


Figure 1: Image generated by related source and destination

6. Evaluation

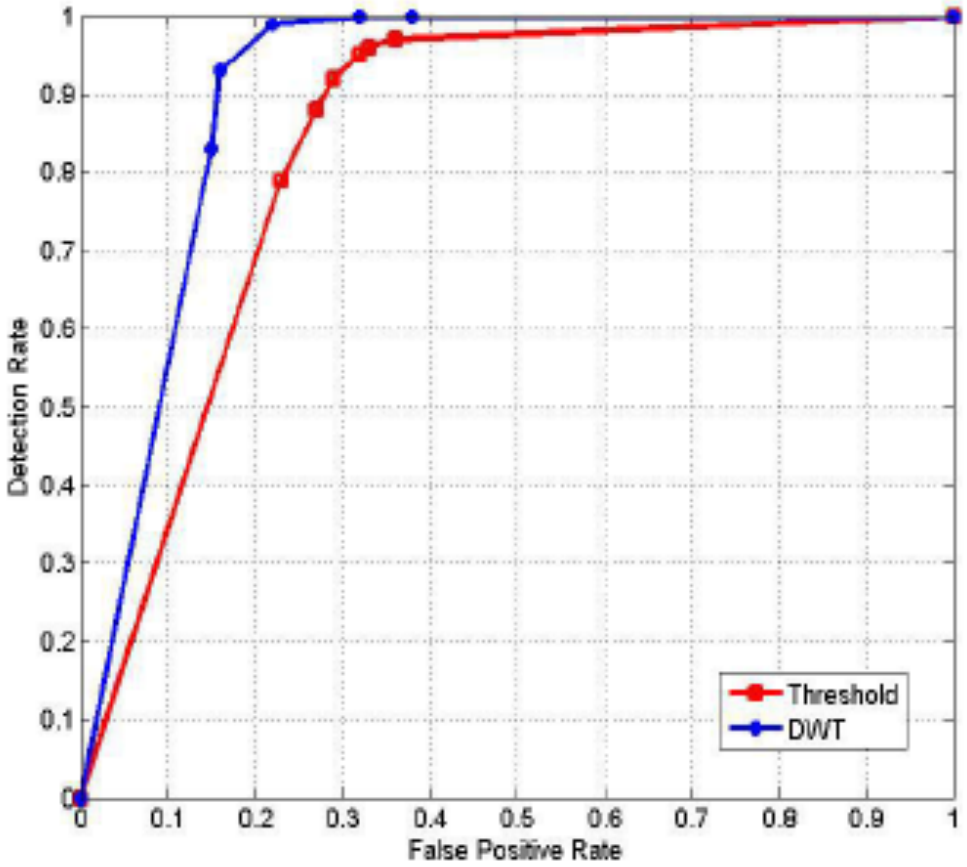


Figure 1: ROC of traffic volume Based and DWT Based detection

6. Evaluation

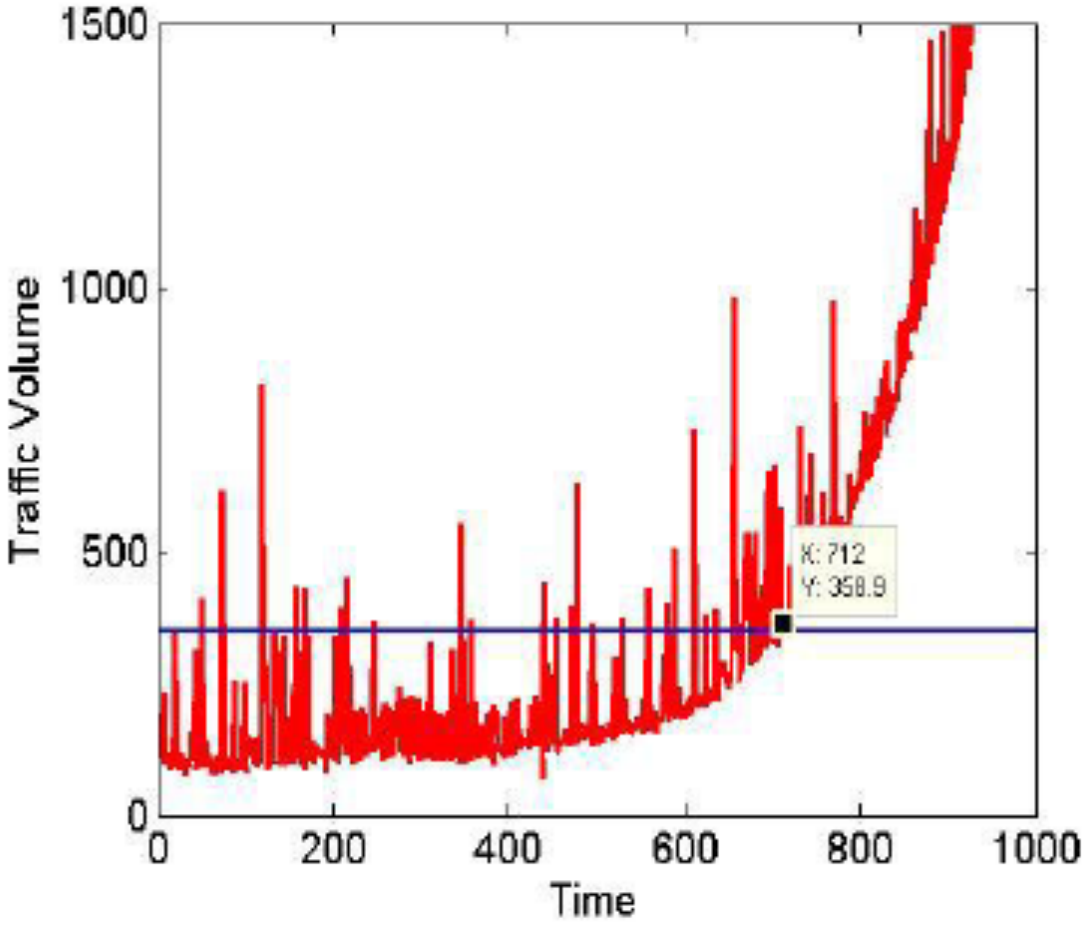


Figure 1: Detection Time of Traffic Volume Based Detection

6. Evaluation

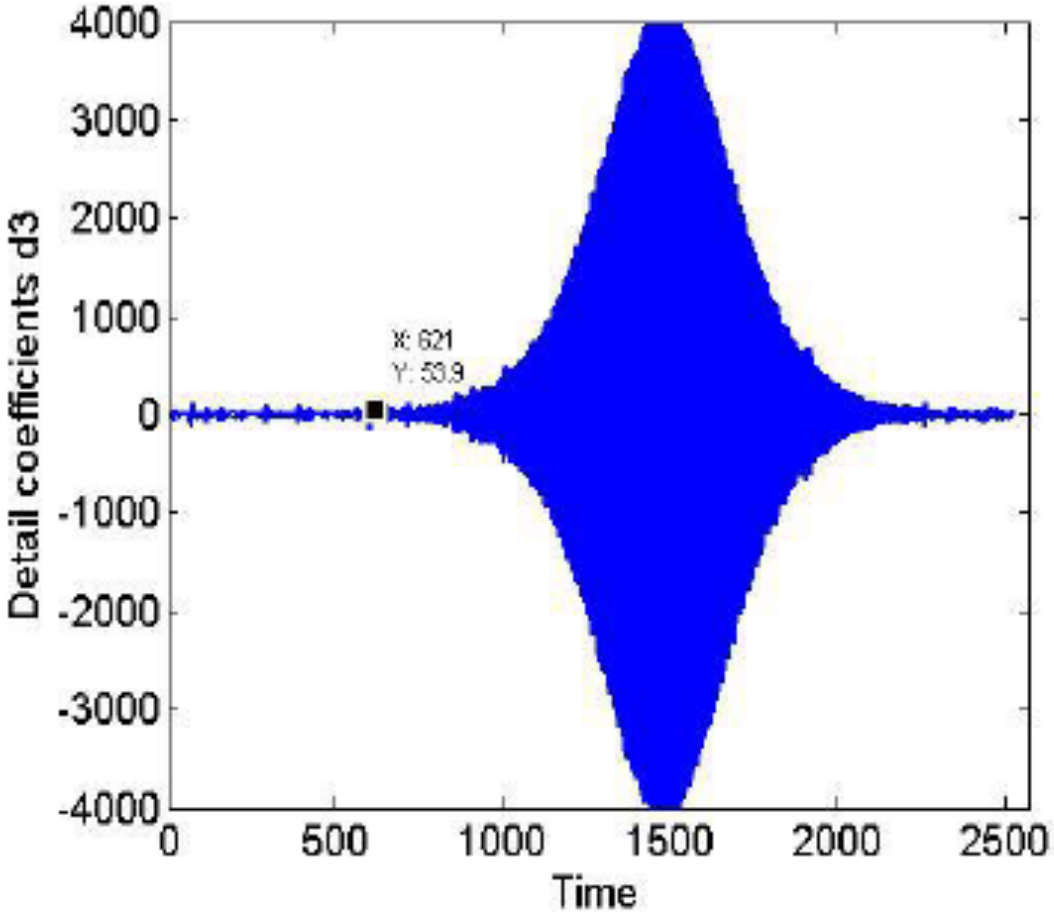


Figure 2: Detection Time of DWT Based Detection

Thank you!