AnNetTe

Analyzing Network Technology

VAST Challenge 2013 Mini-Challenge 3 Award: Outstanding Situation Awareness

Siming Chen[1] Fabian Merkle[3] Hanna Schäfer[3] Hongwei Ai[1] Cong Guo[1] Xiaoru Yuan[1,2] Thomas Ertl[3]

1) Key Laboratory of Machine Perception (Minister of Education), and school of EECS, Peking University, Bejing, China
2) Center for Computational Science and Engineering, Peking University, Beijing, China
3) University of Stuttgart, Stuttgart, Germany

Understand your network

Security Visualization usually shows a large variety of abstract data. AnNetTe makes important features obvious.

Find attacks easily

The clear interaction pipeline creates insight for every user. No large disk space or high performance is required.

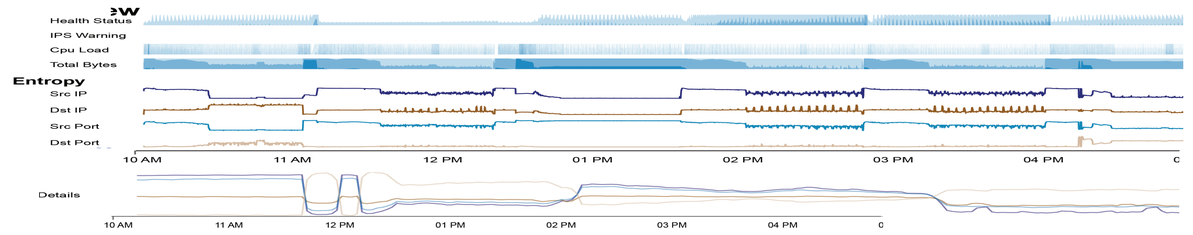
Summarize events

By individualizing the complex information, you can create a clear fingerprint of suspicious network events

Visual Analytics Pipeline

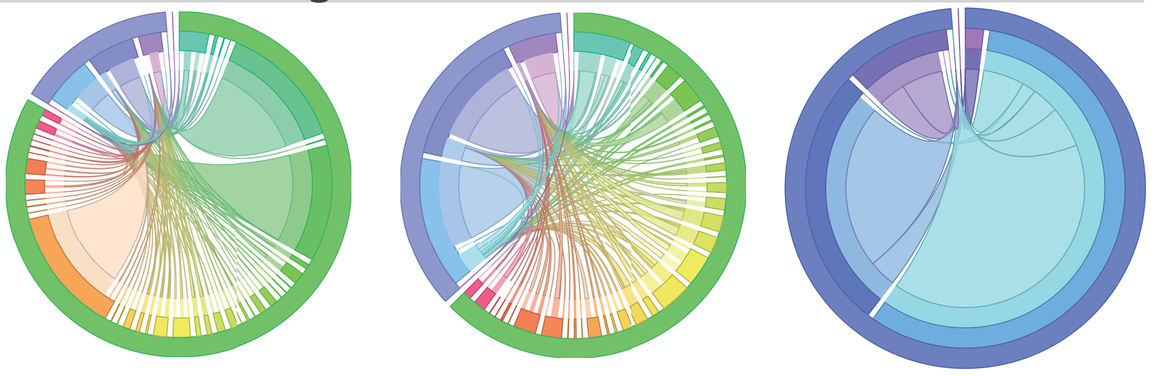
User Interaction: select time → select anomaly

Visualization: Timeline



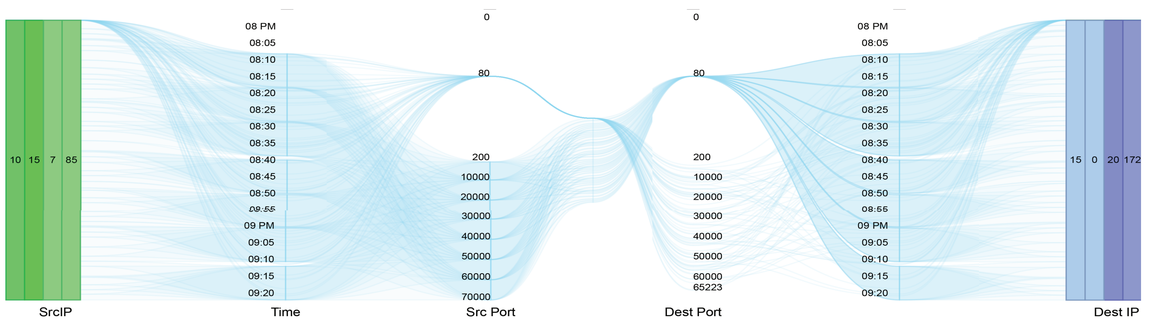
User Interaction: explore → exclude IPs → select IPs

Visualization: IP Ring



User Interaction: explore → exclude connetions → find result

Visualization: Connection River



System Description

Overview

The network status can be viewed for all time and from multiple angles. Entropy lines for IP and port give insight into the connection activity. The entropy shows diversity or disorder over time. After selecting the point of interest, the detail entropy will highlight the next entrance to the connection view.

Middle view

The ring graph shows the connections grouped by subnet. Blue to purple indicates internal IPs while red to green indicates external IPs. Link color is the same as source connection IP. User can watch animation of connection changes along time, reduce information by excluding IPs in any subnet level or select IP group and get all the details in the connection river.

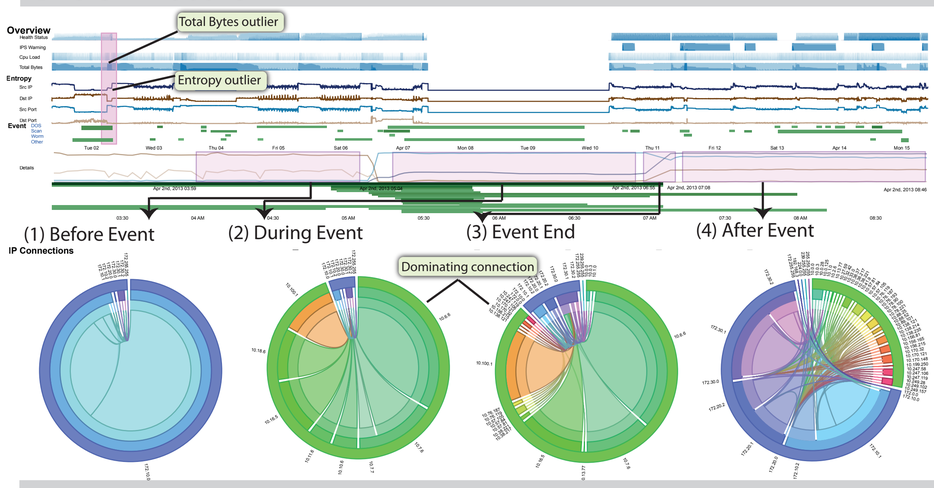
Detail view

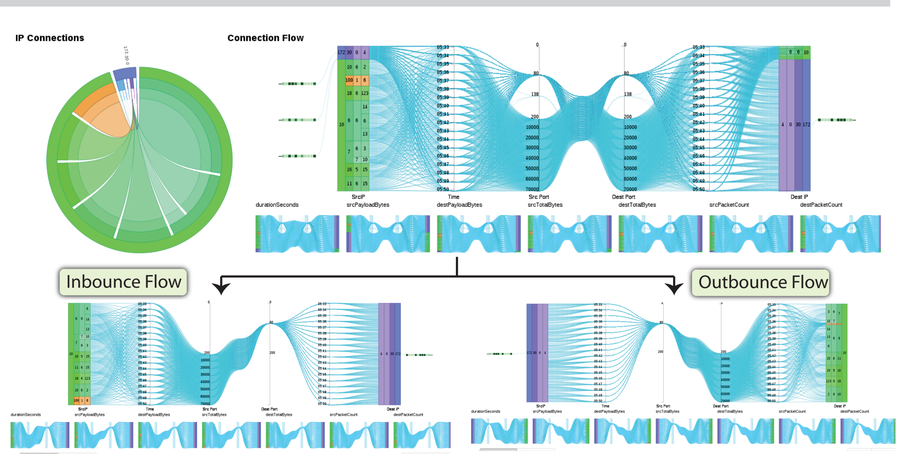
The connection river shows details in an intuitive way. Flowing from source IP to the connection time and then connecting by the ports to a symmetrical destination view, any connection is displayed. User can create a fingerprint by individualizing the setup and choose the most important variable to be displayed as the height variable.

Network Security Event

Case Study

DoS Attack





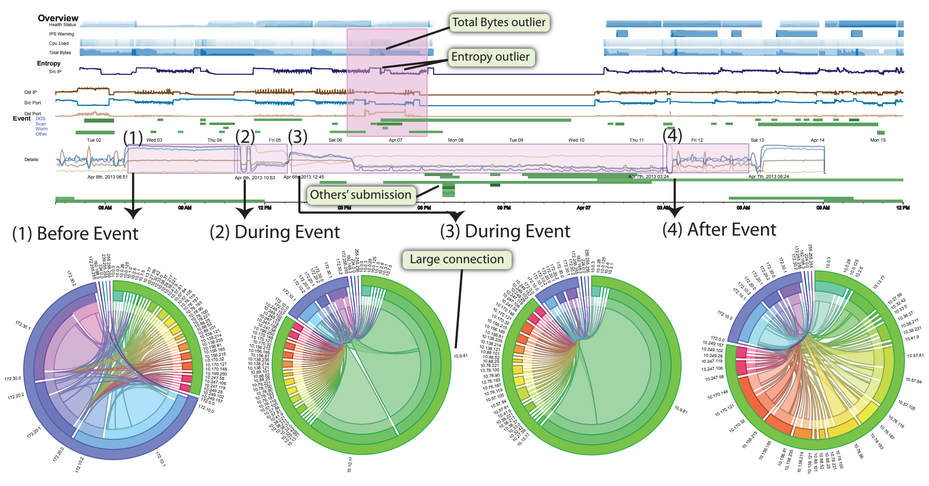
Attack Feature

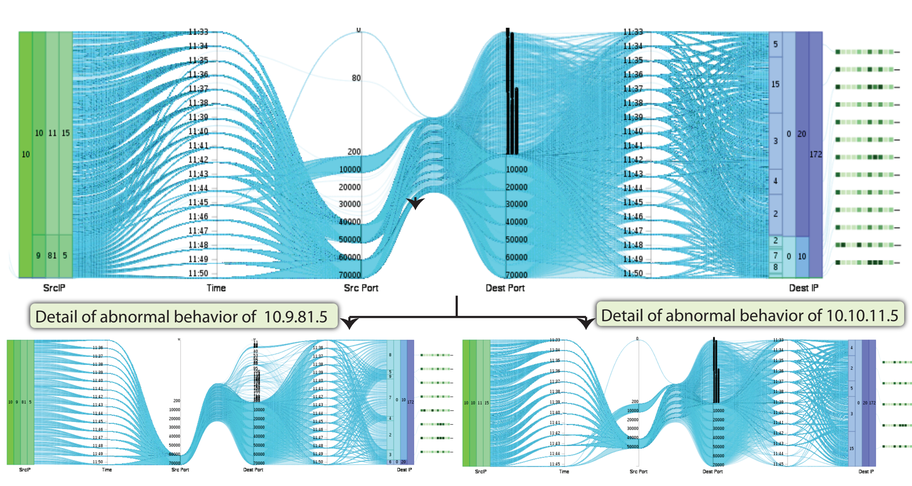
- Low destination IP Entropy
- High source port entropy
- Low destination port entropy
- Dominating suspicious connections
- Large amount of connections

Event Description

IPs 10.6.6.6, 10.6.6.13, 10.6.6.14, 10.7.6.3, 10.7.7.10, 10.11.6.15 and 10.100.1.6 use many ports attacking port 80 of the http server 172.30.0.4.

Network Scan





Attack Feature

- Low destination IP Entropy
- High destination port entropy
- Dominating suspicious connections
- IPS warning of access deny
- Suspicious IP attacks multiple times

Event Description

IPs 10.10.11.15, 10.9.81.5 scan large range of ports of all http servers in the subnet of 172.20.0 and 172.10.0. Health status of servers are not good.

Acknoledgements

This work is supported by National NSFC Project (No. 61170204) and National NSFC Key Project (No. 61232012). We thank domain expert Zhuo Zhang from QIHU Co. for his valuable suggestions and feedback. We thank H. Bosch, S. Koch, R. Krueger and D. Thom for their comments. Hanna is supported by Baden-Wuerttemberg Stiftung for participating in this collaboration.

Contact

xiaoru.yuan@pku.edu.cn http://vis.pku.edu.cn