# HPNAIDM: The High-Performance Network Anomaly/Intrusion Detection and Mitigation System

Yan Chen
Department of Electrical Engineering and Computer Science
Northwestern University
http://list.cs.northwestern.edu/hpnaidm.html

**DOE Collaborators**

- Dr. Wu-chun Feng (Los Alamos National Lab)
- Dr. Don Petravick and Dr. Matt Crawford (Fermi National Lab)
- Dr. Nageswara Rao (Oak Ridge National Lab)

## 1. Brief Abstract

Identifying traffic anomalies and attacks rapidly and accurately is critical for large network operators. With the rapid growth of network bandwidth, such as the next generation DOE UltraScience Network, and fast emergence of new attacks/virus/worms, existing network intrusion detection systems (IDS) are insufficient because they:

- Are mostly host-based and not scalable to high-performance networks;
- Are mostly signature-based and unable to adaptively recognize flow-level unknown attacks;
- Cannot differentiate malicious events from the unintentional anomalies.

To address these challenges, we propose and develop a new paradigm called *high-performance network anomaly/intrustion detection and mitigation* (HPNAIDM) system. The new paradigm is significantly different from existing IDSes with the following features (research thrusts).

- Online traffic recording and analysis on high-speed networks;
- Online adaptive flow-level anomaly/intrusion detection and mitigation;
- Integrated approach for false positive reduction.

## 2. Major Research Activities

Our research activities will focus on the three features as defined above.

1. We propose to leverage the PI's previous work on *k*-ary sketch, an efficient tool for data streaming computation, to record flow-level traffic as the basis for statistical anomaly detection. We will also investigate reversible sketches to infer the characteristics (e.g., source IP) of culprit flows when detected, and then mitigate them.

2. We will design online sketch-based flow-level anomaly/intrusion detection and mitigation for high-speed networks. In addition, we propose multi-dimensional sketches to distinguish multiple types of anomalies for false positive reduction. Furthermore, we will explore the linearity property of sketches to aggregate the data summaries for detecting distributed and insidious attacks.

3. We plan to bridge the traditional gap between the network measurement/trouble shooting research and the intrusion detection research by *integrating the signature-based detection, and network element fault diagnostics* to analyze the traffic anomalies discovered by the statistical methods, and further reduce the false positives. We will develop deterministic network diagnosis techniques to locate the network link congestions/failures. Moreover, effective techniques for detecting multiple polymorphic worms even when mixed with background traffic will be developed.

In addition to publication in strong conferences and journals, we also plan to disseminate our work through timely releases of software, traces, and benchmarks. We have a proven track record of this. We will

prototype and evaluate our system thoroughly, and also plan to test it on site at UltraScience Net testbed, Fermi Lab, and Northwestern University.

## 3. Impact to Specific DOE Science Applications

Many DOE national labs have developed high-performance networks with link rates more than 10Gbps, but these systems are very vulnerable to Internet intrusions. For instance, the current DOE UltraScience Net is only protected by firewall, which is very vulnerable to the new viruses/worms attack. The mobile malcodes can potentially compromise the hosts inside the national labs, and then abuse this ultra high-speed links with denial-of-service attacks, leak out confidential information hidden in the bulk transfer, or simply corrupt the data transmitted over the optical links. The Fermi National Lab only uses primitive and ad hoc scripts to offline analyze the netflow data collected at the routers. This is very inaccurate and cannot provide real-time mitigation. In Fermi Lab, other existing tools like Bro and Snort are used to inspect internal networks with much smaller bit rates. However, as pointed out in this proposal, none of these schemes is scalable to high-speed networks.

The HPNAIDM system can effectively detect and mitigate such intrusions when it happens. Here is a scenario of HPNAIDM system in action. Imagine it is 2010, a for-hire hacker group funded by a neoluddite terrorist organization tries to launch a new type of distributed attack on the UltraScience networks, which use multiple OC-768 (40Gbps) links for Internet access and are monitored by HPNAIDM. Each attack flow has a small rate, is polymorphic and does not match the signatures of any existing attacks. Our HPNAIDM systems online record the traffic with compact sketches, aggregate the traffic over multiple links for detection, and instantly catch the anomaly. The suspect flows are immediately monitored in detail for detection. They do not match any signatures of existing attacks. The overlay network diagnosis does not find any network element fault that will trigger such flows. However, our worm detection systems find these flows are indeed polymorphic worms. Then, alarms are raised and the attacks are filtered.

## 4. Synergy Developed with DOE for Technology Transfer

We will work very closely with our collaborators at DOE National Labs. In addition to some existing collaborations, the PI also proposed some synergy activities as described below.

### 4.1 Collaboration with Fermi and Oak Ridge National Labs

For these two labs, we will mainly focus on using their data traces to evaluate the performance, speed and accuracy of the HPNAIDM system. In particular, we are located in the same area as the Fermi Lab, and we have started collaboration for about a year. The collaboration has led to some joint proposals submitted to other funding agencies like NSF. During the collaboration, we have prototyped a process which routinely collects anonymized netflow records from their edge routers and provide them to our research group. We have given them the anomalies we found, and they are currently investigating the root causes. We plan to meet on a monthly basis to discuss project progress and exchange research ideas.

With Oak Ridge National Lab, we will use their UltraScience Net testbed. In particular, we will explore how to effectively monitor and detect anomaly/intrusions when various types of protocol, middleware and applications that make use of the dedicated channels provisioned by the UltraScience Net. In addition to email exchange, we will have monthly phone meeting. In the summers, we can visit the Lab or invite the collaborators to visit us for more intensive interactions, simulation and experiments.

### 4.2 Collaboration with Los Alamos National Lab

We will focus on integrating the software/hardware component of the HPNAIDM system into the RADIANT project at Los Alamos National Lab. They have developed MAGNET and TICKET projects for host-based measurement and monitoring. We will explore how to integrate the network-based HPNAIDM system with these host-based tools, and investigate their tradeoff and how to complement each other. One possibility is to instrument MAGNET and TICKET to examine the suspicious flows detected by sketch-based detection.