An Internet Routing Forensics Framework for Discovering Rules of Abnormal BGP Events

Shiwoong Kim, Zhen Wu, Vikash Agarwal
Advised by: Professors Jun Li and Dejing Dou
Computer & Information Science Department, University of Oregon, Eugene, OR 97403

UNIVERSITY OF OREGON

1. The Problem

Abnormal BGP events, such as attacks, misconfigurations, electricity failures, or worms, can cause anomalous routing behavior at both the global and network levels.

2. Objective

We aim to develop an Internet Routing Forensics (IRF) framework to systematically process BGP routing data, discover rules of abnormal BGP events, and apply these rules to detect occurrences of these events. IRF must be accurate, fast, and usable, while being able to handle complex BGP data.

3. System Architecture

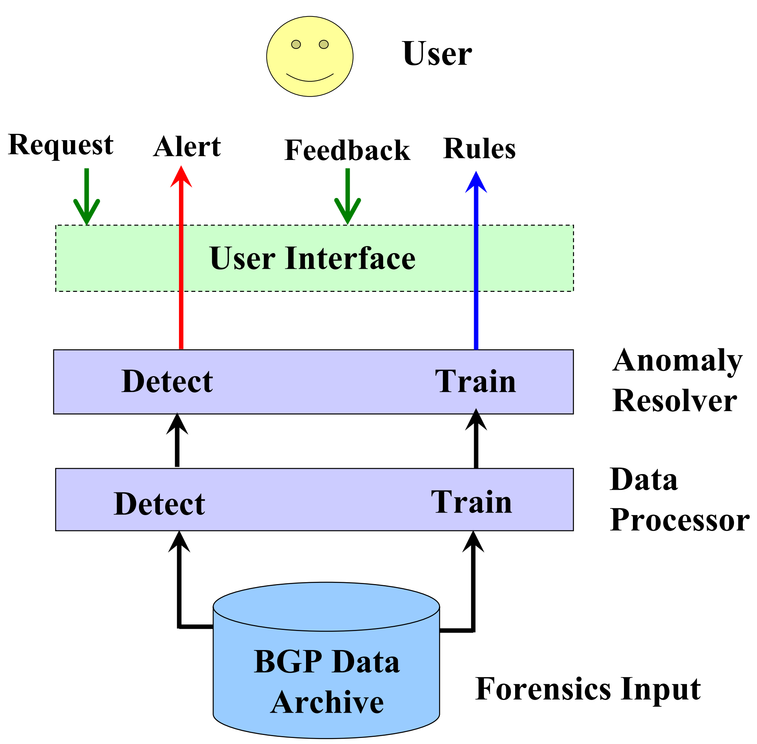


Fig 1. Overall architecture of the IRF framework

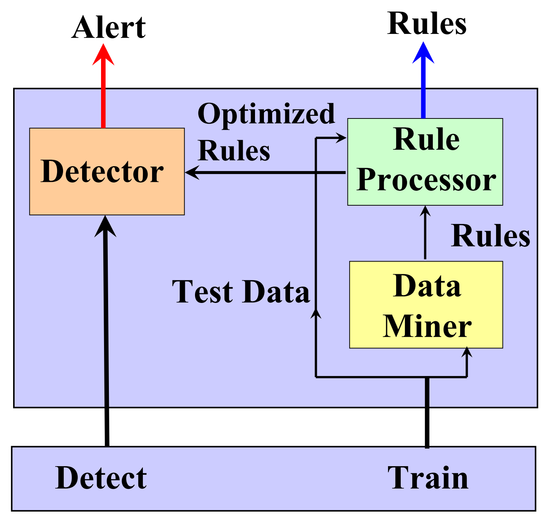


Fig 2. The anomaly resolver

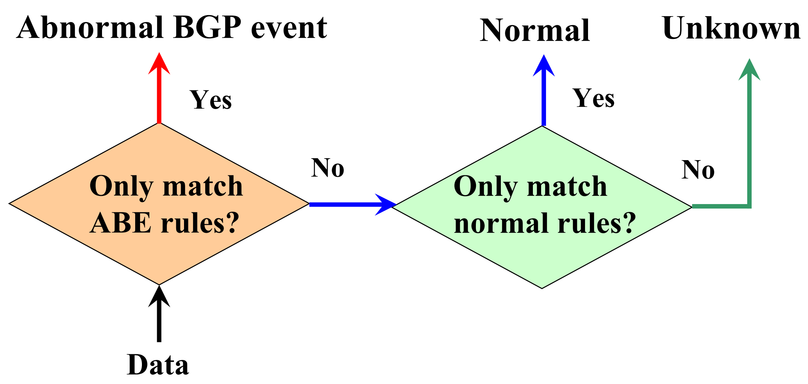
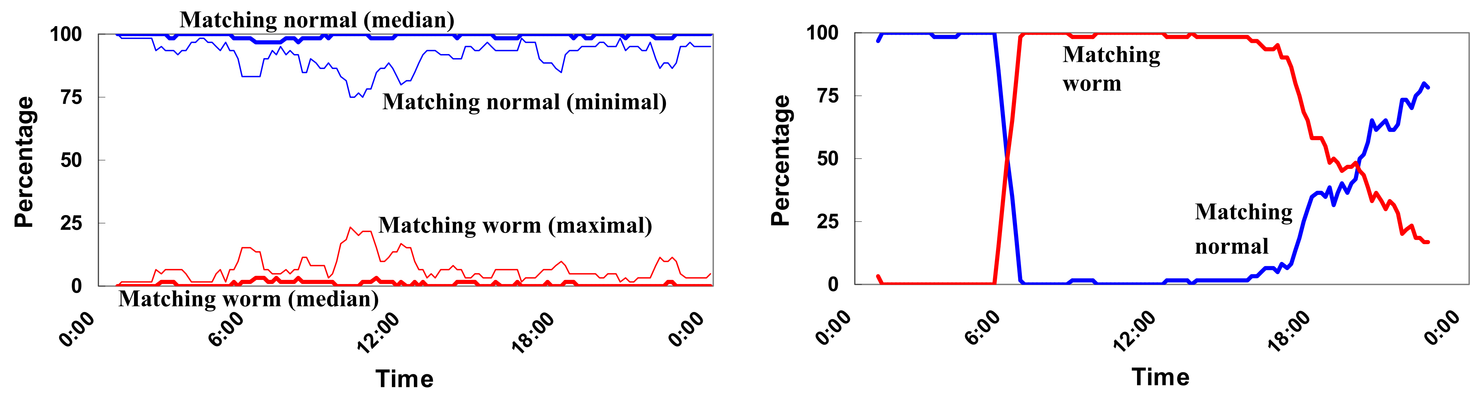


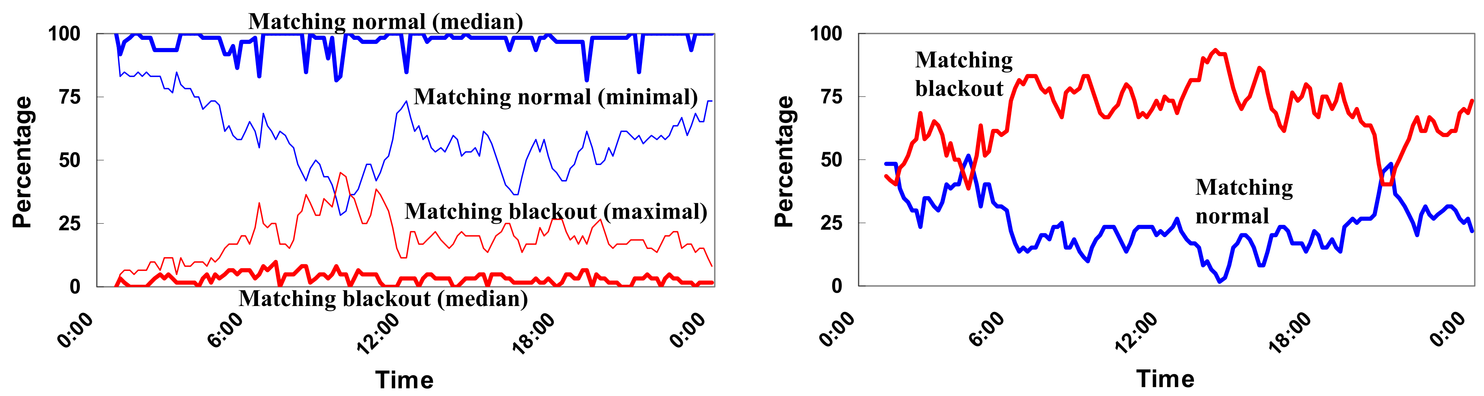
Fig 3. Decision process of the detector

5. Results



Aggregate detection results: Normal test periods — **Detection results: Slammer worm test period**

Fig 4. Case Study I: Percentage of data matching detection rules over normal and Slammer periods



Aggregate detection results: Normal test periods — **Detection results: Hurricane Frances blackout test period**

Fig 5. Case Study II: Percentage of data matching detection rules over normal and Hurricane Frances periods

4. Case Study Methodology

- Select small, optimized set of most distinguishing parameters by calculating information gain.
- Analyze data from abnormal BGP events, such as the CodeRed and Nimda worms or the 2003 East Coast blackout, and contrasting normal periods
- Obtain detection rules from the decision tree algorithm.
- Test rules by feeding rules to the detector. Then, run detector on "unseen" abnormal BGP data, such as the Slammer worm and the Hurricane Frances blackout data.
- Also run detector on normal period data to serve as a baseline for comparison.

6. Conclusions

- The IRF framework provides a new, systematic approach to detecting abnormal BGP events from the control plane.
- Found effective worm-specific classification rules from our first case study, using CodeRed and Nimda periods to train the system, which were able to distinguish unseen Slammer worm data from normal data.
- Similar results were obtained from the blackout study.

7. Future Work

- Get a deeper understanding of the implications of the detection rules discovered during the studies.
- Multi-label classification to distinguish different types of abnormal BGP events (such as different types of worms).
- Studying prefix-level abnormal BGP events that may be more abundant but smaller in scale than those from our case studies.
- More accurate and efficient training and detection mechanisms.

Reference

J. Li, D. Dou, Z. Wu, S. Kim, V. Agarwal. An Internet Routing Forensics Framework for Discovering Rules of Abnormal BGP Events. To appear in the October 2005 issue of the ACM Computer Communication Review.