BGP Anomaly Detection using Wavelet Analysis

Lihua Yuan Jianning Mai

I. Motivation and Objective

Border Gateway Protocol (BGP) is the current de facto standard inter-domain routing protocol in the Internet. Meanwhile, BGP is vulnerable to unintentional faults and intentional intrusions. Abnormal BGP behavior could have a widespread, possibly global impact, and there are known major Internet meltdown related to BGP. Yet the Internet community is striving to understand BGP's anomalies and their root causes, characteristic behavior and consequences.

Given the humongous volume of BGP data, it is impractical for network administrators to manually pinpoint all BGP anomalies and trace their root causes. Therefore, as a very first step in studying BGP anomaly, we need to search for efficient approaches to identify the BGP anomaly, before we can answer why it happened. Teoh *et. al* [1] proposed a visual-based anomaly detection tool for BGP Origin AS Change (OASC) Events. Current research has seen applying signal processing techniques to network anomaly analysis [2].

II. Plan and Approach

The BGP data archives can provide us with a series of BGP events in time domain. Routeviews [3] and RIPE [4] are such two well-known websites for stored BGP data. We plan to begin our analysis with these BGP data.

Next, we have to get familiar with known BGP failures and attacks that other researchers have studied. For instance, the Code Red/Nimda attack has been examined in [5]. In [6] the BGP Origin AS Change (OASC) problem was analysed. And slow convergence and route oscillation were presented by K. Zhang [7].

We also need to investigate into a few BGP data analysis approaches. [8] discussed statistical anomaly detection for the OSPF protocol. The method might apply to the BGP as well. Wavelet analysis method has been utilized to analysis IP and TCP flow scaling behavior in [9], [10], [11]. Barford *et. al* [12] identified anomalies in SNMP data using the same scheme.

We are very interested in applying wavelet analysis technique to our project. Wavelet analysis can reveal the time-frequency behavior of the BGP routing data. By matching the time-frequency behavior with possible patterns, i.e. the signatures, of BGP anomalies, we may devise a program to detect BGP anomalies automatically. Another possible approach is to collect a set of "normal" BGP patterns and use that to identify "abnormal" patterns. The later approach has the potential to identify unknown anomalies. We expect such a tool to be very useful for further study on BGP's behavior.

REFERENCES

[1] S. Teoh, K. Ma, S. Wu, and X. Zhao, "Information Visualization for Anomaly Detection," in *Proceedings of 5th IASTED International Conference in Computer Graphics and Imaging (CGIM)*, Hawaii, 2002.

[2] M. Thottan and C. Ji, "Anomaly Detection in IP Networks," in *IEEE Transaction on Signal Processing, Special Issue of Signal Processing in Networking*, August 2003, pp. 2191–2204.

[3] D. Meyer, "University of Oregon Route Views Project," http://www.routeviews.org/.

[4] "RIPE (Reeaux IP Europeens)," http://www.ripe.net/.

[5] L. Wang, X. Zhao, D. Pei, R. Bush, D. Massey, A. Mankin, S. F. Wu, and L. Zhang, "Observation and Analysis of BGP Behavior under Stress," in *Proceedings of ACM/SIGCOMM Internet Measurement Workshop*, Marseille, France, Nov 2002.

[6] S. Teoh, K. Ma, S. Wu, D. Pei, L. Wang, L. Zhang, D. Massey, and R. Bush, "Visual-Based Anomaly Detection for BGP Origin AS Change (OASC) Events," in *Proceedings of 14th IEEE/IFIP Workshop on Distributed Systems: Operations and Management (DSOM)*, vol. 2867, Heidelberg, Germany, Oct 2003.

[7] K. Zhang, "On Detection of Anomalous Routing Dynamics in BGP," http://seclab.cs.ucdavis.edu/secsem2/Zhang.ppt.

[8] D. Qu, B. M. Vetter, F. Wang, R. Narayan, S. F. Wu, Y. F. Jou, F. Gong, and C. Sargor, "Statistical Anomaly Detection for Link-State Routing Protocols," in *Proceedings of the 1998 International Conference on Network Protocols (ICNP)*, October 1998, pp. 62–70.

[9] N. Hohn, D. Veitch, and P. Abry, "Does Fractal Scaling at the IP Level Depend on TCP Flow Arrival Process ?" in *Proceedings of ACM/SIGCOMM Internet Measurement Workshop*, Marseille, France, Nov 2002, pp. 63–68.

[10] ——, "Investigating the scaling behavior of arrival times of Internet flows," in *International Symposium on Self Similarity and its Applications*, Clermont-Ferrand, France, 2002.

[11] D. Veitch, "Parameter Estimation Issues for Scaling (fractal) Processes," http://www.emulab.ee.mu.oz.au/ darryl/.

[12] P. Barford, J. Kline, D. Plonka, and A. Ron, "A Signal Analysis of Network Traffic Anomalies," in *Proceedings of ACM/SIGCOMM Internet Measurement Workshop*, Marseille, France, Nov 2002.