2019-12

Cyber System Assurance through Improved Network Anomaly Modeling and Detection

Bollmann, Chad A.

Monterey, California: Naval Postgraduate School

NPS NRP Final Report
Title: Cyber Assurance through Improved Network Anomaly Modeling and Detection
Report Date: [10/15/19] Project Number (IREF ID): [NPS-19-N039-A]
Naval Postgraduate School

MONTEREY, CALIFORNIA

CYBER ASSURANCE THROUGH IMPROVED NETWORK ANOMALY MODELING AND DETECTION

Executive Summary Type: Final Report
Period of Performance: [10/01/2018–10/1/2019]

Researchers:
Principal Investigator (PI): CDR Chad Bollmann, Ph.D., GSEAS, Electrical & Computer Engineering (ECE)
Additional Researcher(s):
Mr. Jorge Gonzalez, Ph.D. candidate, Florida Atlantic University, Mathematics
Mr. Joshua Clymer, Naval Research Engineering Internship Program

Prepared for:
Topic Sponsor Lead Organization: N8
Topic Sponsor Name: N81IO Information Warfare Branch, LCDR Khoa Nguyen, USN
Topic Sponsor Contact Information: khoa.h.nguyen@navy.mil

NPS NRP Final Report

Title: Cyber Assurance through Improved Network Anomaly Modeling and Detection
Report Date: [10/15/19] Project Number (IREF ID): [NPS-19-N039-A]
Naval Postgraduate School

Project Summary

Recent studies have shown that aggregated network traffic can possess non-Gaussian, alpha-stable distributions of certain traffic features such as packet volume, but little is known regarding the origin of these non-Gaussian characteristics. Approaching network traffic as the aggregation of individual device traffic impulses permits examining the influence of traffic inputs and measurement methods. Renewal theory can be used to predict the characteristics of aggregated network traffic and generate realistic traffic models. Finally, anomaly detectors based on parametric and non-parametric alpha-stable-derived tests can then improve detection system accuracy when traffic is predicted to be non-Gaussian.

This study used two alpha-stable traffic aggregation theories to show that aggregated network traffic can take either Gaussian or alpha-stable forms, as predicted by the Generalized Central Limit Theorem. Applying volumetric test statistics based on alpha-stable parameters was shown to significantly improve anomaly detection system performance under non-Gaussian conditions and suffer no degradation under Gaussian conditions, improving real-time system performance by more than ten percent at low false-alarm rates. These results suggest that alpha-stable-based models can be developed to more accurately predict traffic patterns, and alpha-stable tests can be used to improve the accuracy and responsiveness of current anomaly detection methods.

Keywords: *alpha-stable, network anomaly detection, renewal theory, generalized central limit theorem*

Background

It has become an accepted fact that some aspects of aggregated network traffic (e.g., inter-arrival times, packet and byte volumes per unit time) can be more accurately characterized using heavy-tailed models (Bollmann, C., Tummala, M., McEachen, J., Scrofani, J., & Kragh, M., 2018, p. 5524; Paxson, V., & Floyd, S., 1995, p. 226; Simmross-Wattenberg, F., Asensio-Perez, J. I., Casaseca-de-la-Higuera, P., Martin-Fernandez, M., Dimitriadis, I. A., & Alberola-Lopez, C., 2011, p. 494). This acceptance is complicated by observations that in smaller networks or under certain traffic conditions, the same features are near- (i.e., effectively) exponential-tailed or Gaussian. Little theoretical explanation exists for the co-existence of both heavy (i.e., alpha-stable) and exponential (i.e., Gaussian) traffic distributions.

If aspects of network traffic are heavy-tailed, non-parametric (i.e., distribution-agnostic) test statistics developed for heavy-tailed inputs should theoretically outperform Gaussian tests such as mean and variance. If network traffic can be shown to be alpha-stable, then parametric test statistics (which require the presumption of a specific distribution) based on alpha-stable distributions should also demonstrate superior performance. The principle investigator (PI) has previously shown that non-parametric, alpha-stable test statistics outperform Gaussian tests (Bollmann, C., 2018), but combinations of parametric test statistics have not been evaluated.

NPS NRP Final Report

Title: Cyber Assurance through Improved Network Anomaly Modeling and Detection
Report Date: [10/15/19] Project Number (IREF ID): [NPS-19-N039-A]
Naval Postgraduate School

Findings and Conclusions

The motivations for this line of research are grounded in the hypotheses that alpha-stable models more accurately describe network traffic than Gaussian models, thus alpha-stable detection methods should provide superior accuracy over Gaussian approaches. The increased accuracy of alpha-stable test statistics may also be able to differentiate between (i.e., classify) different types of anomalies and cyber attacks. The increased precision of the studied traffic models and detectors should also permit more rapid detection of anomalies, enabling faster network defender response to adversary action. The ultimate intention of the PI is to use the findings of this work to refine the developed tools and test them on Department of Defense networks, and enter into cooperative research and development agreements with cyber-security firms that defend DoD networks.

The ultimate intention of this work is to refine the developed tools and test them on Department of Defense (DoD) networks, and enter into cooperative research and development agreements with cyber-security firms that defend DoD networks. This research makes progress towards addressing current network defense gaps identified by the research sponsor, particularly in the process step of Detect (part of the cyber response framework of Identify, Detect, Protect, React, and Restore).

For the work described in this paper, our objectives were to investigate the source of the dual natures of network traffic (i.e., Gaussian and alpha-stable) in order prove the merit of further development, improvement, and application of non-parametric and parametric, alpha-stable network anomaly detectors. This results of this portion of the study have been accepted for publication (Gonzalez, J., Clymer, J., & Bollmann, C., 2019).

In parallel to justifying the application of alpha-stable methods, parametric alpha-stable detection techniques were examined using four different, publicly-available network traffic captures (i.e., traces) containing real background network traffic and attacks with clear benign and attack periods.

This study began with a literature review of network anomaly detection work grounded in heavy-tailed processes; it was found that no significant additional works that would inform this study had been published since the PI's dissertation literature review.

An additional literature review into the history of alpha-stable network traffic theory was completed; a series of works linking self-similarity, long-range dependence, heavy-tailed traffic characteristics, and alpha-stable distribution theory were identified. Most of these works were written by the same core group of authors led by Taqqu and Willinger and are cited in (Willinger, W., Paxson, V., & Taqqu, M. S., 1998, p. 27). This association of alpha-stable and self-similar process (Willinger et al., 1998, p. 27) provides strong support for the argument that traffic is alpha-stable, as self-similarity has long been accepted as a characteristic of network traffic.

From the assumption that network communications from an individual device can be treated as independent, identically-distributed (IID) random processes, two proven literature models support the

aggregation of these IID processes to an alpha-stable result. The first, impulsive-based model, via the Generalized Central Limit Theorem, demonstrates that IID processes of infinite variance will produce an alpha-stable result. When the individual IID processes exhibit finite variance, which can occur when devices and processes are relatively similar, a Gaussian aggregation results.

The second aggregation model, based on renewal theory (Taqqu, M. & Levy, J., 1986, p.73) that individual traffic impulses possessing varying "on" and "off" times can similarly aggregate to alpha-stable or Gaussian processes. For the renewal case, the resulting distribution depends on the variation of the input processes, characterized in this case as number of devices M and number of processes on each device T. For cases where $T >> M$, as would be expected in larger commercial networks comprised of a diverse device population, the limiting distribution will be alpha-stable. When $T << M$, such as smaller networks where the population of devices and processes are similar, renewal theory predicts a fractional Brownian motion (i.e., Gaussian) result (Taqqu & Levy, 1986, p. 73).

The modeling portion of this work concluded after developing two primitive modeling algorithms to validate the aggregation theories. Individual device impulses (i.e., inputs) were obtained from five seconds of four different network traffic traces based on source and destination internet protocol addresses and port numbers. After assessing the IID and ergodicity assumptions required to apply the aggregation theories, the individual inputs were re-aggregated using random sampling. The aggregated distributions were then compared to the original traffic distributions using cumulative distribution function (CDF) plots and Kolmogorov-Smirnov (KS) test value as a similarity measure, as shown in Figure 1. The values of the KS test indicate that the renewal model generates more accurate results than the impulse model, but both models predict the original distribution with satisfactory accuracy, given that time constraints prevented any significant refinement of the models.

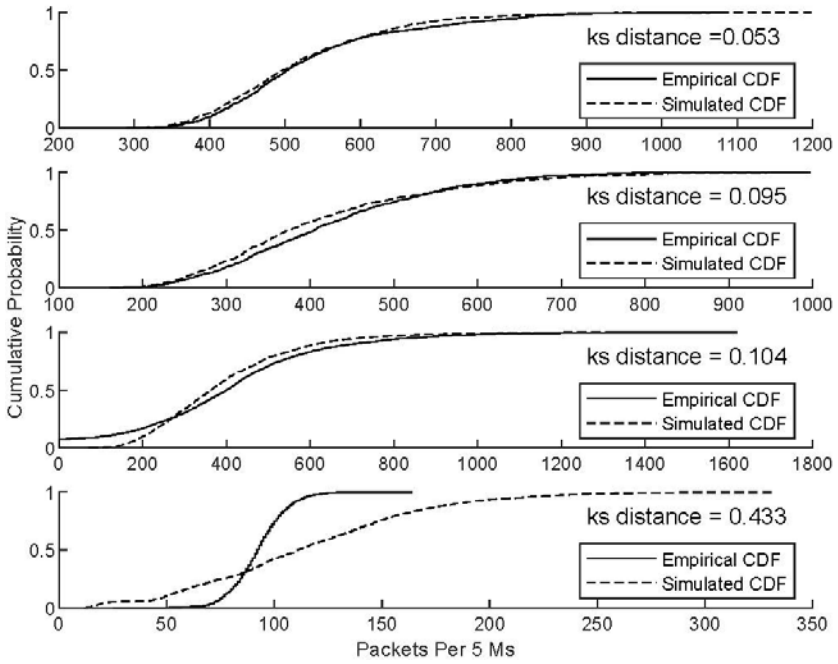

Figure 1. CDF plots of packet volume per subwindow for four different measured and modeled datasets: MAWI April, MAWI Nov, NPS, and residential ISP, from top to bottom. Solid lines indicated measured values while dashed lines indicate simulated distributions generated using the renewal model. KS distance is given for each trace. Source: Gonzalez et al., 2019.

Note that neither model accurately recreated the lowest-volume, residential internet service provider (ISP) trace, shown at the bottom of Figure 1. This is because the low-volume ISP trace has relatively low device and process diversity leading to Gaussian distributions per renewal theory. The Gaussian distribution of this ISP traffic was validated through MATLAB analysis of the trace packet rate.

The ability of the impulse and renewal models to support either Gaussian or alpha-stable distributions validates our hypothesis that alpha-stable models more accurately describe network traffic. Because the Gaussian is a special case of the alpha-stable distribution (where the tail parameter $\alpha = 2$), the alpha-stable distribution becomes the only logical choice for network traffic models and, by implication, anomaly detection test statistics.

After theoretically supporting the alpha-stable distribution of traffic, the study's work shifted developing and assessing alpha-stable parametric tests for varying amplitudes of volumetric denial-of-service attacks. First, the Measurement and Analysis of the Wide Internet (MAWI) archive was examined for suitable traces using characteristics such as normal and abnormal traffic periods of sufficient length and presence of a volumetric denial-of-service attack. Ultimately, four different candidate datasets were identified, though the length of this study only permitted focusing on a low-volume and high-volume case.

These cases were then separated and labeled as benign, or normal, and attack traffic. Custom algorithms

were developed and applied to these traces, separating them into varying data windows on the order of 1 – 6 seconds and subwindows (i.e., counting periods) on the order of 1 – 10 milliseconds. Finally, the packet counts per sub-window were determined for each case.

The first analysis efforts examined the impact of varying window and subwindow size on the distribution of packet counts per subwindow, with the intention of identifying window and subwindow limits that would result in sample distributions inconsistent with the original trace. Qualitatively, for trace volumes on the order of one gigabit per second, we found that modeling accuracy was relatively invariant to subwindow sizes greater than 2 – 3 ms and larger sub-window sizes did not lead to more Gaussian packet rate distributions. Similarly, window sizes greater than 2 – 3 seconds provided good accuracy, though packet rate distributions tended to become more Gaussian (and less alpha-stable) as window sizes grew significantly greater than ten seconds.

After identifying optimal window sizes and bounds for parametric alpha-stable fit accuracy, a variety of non-parametric and parametric alpha-stable test statistics were applied to low- and high-attack volume MAWI traces. The non-parametric tests were developed in the PI's dissertation research and are described in (Bollmann, 2018). The results of one such evaluation trial are shown in Figure 2.

Figure 2 validates our hypothesis that alpha-stable test statistics outperform Gaussian tests, and that parametric tests slightly outperform non-parametric tests. One important result is that the alpha-stable accuracy improvement margin is greater at lower false alarm rates; for any statistical implementation to be commercially viable, detection thresholds must be set such that false alarm rates less than one percent.

The period of performance for this project concluded before additional MAWI traces could be evaluated and all intended detector implementations could be evaluated. An eventual goal of this work is to use the labeled data and alpha-stable fits as input to a machine learning detection approach; preliminary qualitative evaluation has shown that the results would be well-suited to a clustering approach due to easily-identifiable separation boundaries between benign and attack traffic cases.

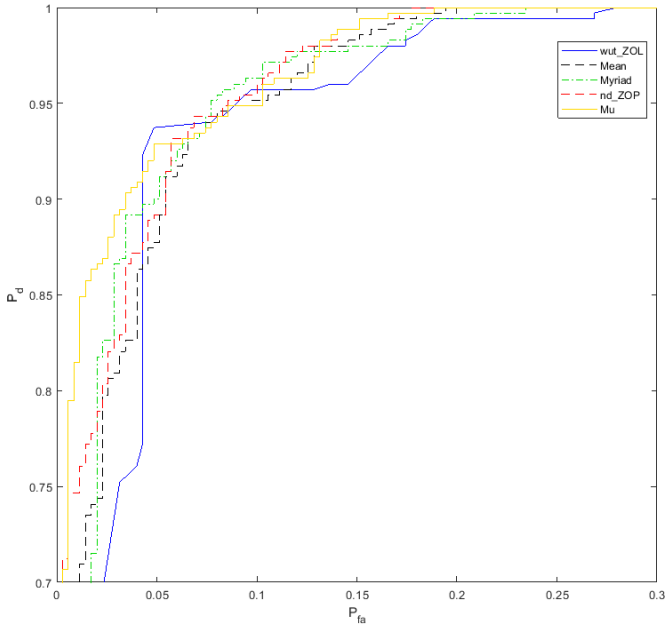

Figure 2. Receiver operating characteristic plot comparing the performance of alpha-stable test statistics to the Guassian-based mean when detecting a denial-of-service attack contained in the January 28, 2018 MAWI dataset. Mu is a parametric alpha-stable statistic evaluated in this study, while myriad, ZOL, and ZOP are non-parametric alpha-stable statistics described in (Bollmann, 2018). Note that Mu offers approximately a 10% detection improvement over mean at the lowest false alarm rates.

As previously discussed, the overall results from this study integrate nicely with the existing body of work describing Internet traffic as self-similar and long-range dependent with scaling properties; these characteristics all relate to or result from alpha-stable network traffic. The characterization of traffic inputs as impulsive provides an intuitive method of using established renewal theory to show that aggregated traffic should approach Gaussian or alpha-stable limits. Additionally, this study is the first to propose an explanatory method of predicting aggregated traffic distributions and characteristics that have long been determined only empirically. The long-term implications of this study are that the accuracy of network traffic measurement and analysis may be significantly improved through utilization of existing alpha-stable-based approaches as well as development and application of novel alpha-stable methods, particularly with respect to machine learning.

Note that the data used in this work is evaluated as highly reliable and reflective of real-world network traffic. The traffic traces used to develop and evaluate the impulse and renewal traffic models originated from the PI's own devices. Four publicly-available traces from the MAWI archive were used to evaluate the parametric alpha-stable anomaly detectors; two MAWI traces, one trace collected by staff at NPS, and one publicly-available trace from a residential internet service provider were used to evaluate the traffic modeling work. No NPS master's students were involved in this study, though two interns made significant contributions to the theoretical traffic model development portion of this work.

NPS NRP Final Report

Title: Cyber Assurance through Improved Network Anomaly Modeling and Detection
Report Date: [10/15/19] Project Number (IREF ID): [NPS-19-N039-A]
Naval Postgraduate School

Recommendations for Further Research

Several areas of this research topic warrant additional exploration. First, both the impulse and renewal process models must be evaluated more rigorously. The model accuracies should be assessed both qualitatively and quantitatively against network traffic traces consisting of different numbers and types of devices. The extensibility of this model to wireless network traffic also bears investigation, as different protocols facilitating the multiple access environment will alter the ON-OFF times of device transmissions. Examination of the quantitative results would permit selecting either the impulse or renewal model as the frequently "best" alternative for future research and development.

Once validated, fingerprinting methods should be evaluated for the renewal process model with a goal of identifying optimum quantities of stored network trace data. Development of a fingerprinting method could permit saving high-quality, reduced-volume samples (i.e., snapshots) of network traffic sources and aggregated traffic that could serve to inform long-term models and anomaly detection systems.

Third, the network anomaly detection work should be extended in multiple ways. Ensemble anomaly detection systems consisting of combinations of both parametric and non-parametric alpha-stable test statistics can be developed, evaluated, and optimized. These systems could integrate Gaussian test statistics in order to reduce computational overhead and detection delays when the traffic modeling and evaluation system senses Gaussian traffic characteristics. Finally, the ability of the detection system to rapidly detect anomalies should be rigorously examined; the resistance of the alpha-stable methodology to outlier skew implies that anomalies could be reliably identified using a minimum of subsequent samples. These minimum-repeatability tests would significantly improve overall detection system performance and system response times to denial-of-service attacks, improving network resiliency.

References

Bollmann, C. (2018). *Network Anomaly Detection with Stable Distributions*. Ph.D. dissertation submitted for publication.

Bollmann, C., Tummala, M., McEachen, J., Scrofani, J., & Kragh, M. (2018). Techniques to improve stable distribution modeling of network traffic. *Proceedings of the 51st Hawaii International Conference on System Sciences*, 5524–5531. http://hdl.handle.net/10125/50578

Gonzalez, J., Clymer, J., & Bollmann, C. (2019). Aggregated Impulses: Towards explanatory models for self-similar alpha stable network traffic. Paper presented at the 13th International Conference on Signal Processing and Communication Systems, Surfer's Paradise, Queensland, Australia.

Paxson, V., & Floyd, S. (1995). Wide area traffic: the failure of Poisson modeling. *IEEE/ACM Transactions on networking*, *3*(3), 226-244.

(Paxson & Floyd, 1995, p. 226)

Simmross-Wattenberg, F., Asensio-Perez, J. I., Casaseca-de-la-Higuera, P., Martin-Fernandez, M., Dimitriadis, I. A., & Alberola-Lopez, C. (2011). Anomaly Detection in Network Traffic Based on Statistical Inference and α-Stable Modeling. *IEEE Transactions on Dependable and Secure Computing*, *8*(4), 494-509.

Taqqu, M. S., & Levy, J. B. (1986). Using renewal processes to generate long-range dependence and high variability. In *Dependence in probability and statistics* (pp. 73-89). Birkhäuser, Boston, MA.
Willinger, W., Paxson, V., & Taqqu, M. S. (1998). Self-similarity and heavy tails: Structural modeling of network traffic. *A practical guide to heavy tails: statistical techniques and applications*, *23*, 27-53.

Acronyms

cumulative distribution function	CDF
Generalized Central Limit Theorem	GCLT
independent, identically-distributed	IID
internet service provider	ISP
Kolmogorov-Smirnov	KS
principle investigator	PI
Measurement and Analysis of the WIDE Internet	MAWI
Naval Postgraduate School	NPS