2013 IEEE 12th International Symposium on Network Computing and Applications

Towards a Forecasting Model for Distributed Denial of Service Activities

Claude Fachkha, Elias Bou-Harb, Mourad Debbabi
Computer Security Laboratory, CIISE, Concordia University & NCFTA Canada
Montreal, QC, Canada
{c_fachkh, e_bouh, debbabi}@encs.concordia.ca

***Abstract*—Distributed Denial of Service (DDoS) activities continue to dominate today's attack landscape. This work proposes a DDoS forecasting model to provide significant insights to organizations, security operators and emergency response teams during and after a targeted DDoS attack. Specifically, the work strives to predict, within minutes, the attacks' impact features, namely, intensity/rate (packets/sec) and size (estimated number of used compromised machines/bots). The goal is to understand the future short term trend of the ongoing DDoS attack in terms of those features and thus provide the capability to recognize the current as well as future similar situations and hence appropriately respond to the threat. Our analysis employs real darknet data to explore the feasibility of applying the forecasting model on targeted DDoS attacks and subsequently evaluate the accuracy of the predictions. To achieve its tasks, our proposed approach leverages a number of time series fluctuation analysis and forecasting methods. The extracted inferences from various DDoS case studies exhibit promising accuracy reaching at some points less than 1% error rate. Further, our model could lead to better understanding of the scale and speed of DDoS attacks and should generate inferences that could be adopted for immediate response and hence mitigation as well as accumulated for the purpose of long term large-scale DDoS analysis.**

I. Introduction

Denial of Service (DoS) attacks are characterized by an explicit attempt to prevent the legitimate use of a service. DDoS attacks employ multiple attacking entities (i.e., compromised machines/bots) to achieve their intended aim. Indeed, DDoS activities continue to dominate today's attack landscape. In a recent report by Arbor Networks [1], it was concluded that 48% of all cyber threats are DDoS. Further, it was stated that the top 4 perceived threats for the next 12 months will be DDoS related, targeting customers, network and service infrastructure. Governmental organizations, corporations as well as critical infrastructure were also recently deemed as DDoS victims [2, 3, 4]. Moreover, a recent event demonstrated that even a cyber security organization, namely Spamhaus, became a victim of a large (i.e., 300 Gbps) DoS attack [5]. Thus, DDoS attacks are and will continue to be a significant cyber security problem, causing momentous damage to a targeted victim as well as negatively affecting, by means of collateral damage, the network infrastructure (i.e., routers, links, etc.), the finance, the trust in, and the reputation of the organization under attack. When an organization is subject to a DDoS, it becomes essential for its IT security staff to answer the following questions:

- During a DDoS attack, what is the future short term trend (i.e., within minutes) of the attack in terms of intensity/rate and size?
- After a DDoS attack, in terms of those impact features, what was the impact of the attack and what are the lessons learned?

The answers to these questions greatly influence the actions and the resources that the organization will choose to employ in responding to such malicious activity for the current incident as well as for future occurrences. For instance, the organization would often care more about high impact DDoS attacks, those that can cause serious disruption of a service in a relatively timely manner. If the latter is observed, the organization can immediately respond and tweak its mitigation methods to gauge the threat (i.e., forward the attack flow to a specific number of servers and/or dynamically assign specific firewall rules to handle the flood). This can reduce the response time and cost for an organization. Note that, low-rate DDoS attacks could be as worrisome as high impact ones, which might indicate that the DDoS attack is attempting to evade detection and at the same time exhaust the victim with long-lived flows [6]. Moreover, having knowledge about the short term (i.e., in terms of minutes) predicted impact features of the ongoing DDoS would provide various inferences to the organization and aid in answering the following questions; will the DDoS increase or decrease in its intensity? will the attack rate fluctuates? will the botnet targeting that specific organization increase? will the DDoS cease after few minutes or will it persist for a longer period of time? Further, the insights extracted from such an analysis on numerous DDoS occurrences targeting that organization could generate attack patterns that could be useful for future mitigation. For example, if the organization observes 5 distinct DDoS attacks in different time periods where they all possess similar rates, size and prediction parameters, then it can be inferred that the attacks originate from a single (or at least similar) botnet and hence point to a suspicious DDoS campaign. At a larger scale, such analysis aims at providing computer emergency response teams and observers of cyber events with DDoS trends, taking into consideration the botnet size and the bots geo-distribution, the victims geolocation, types of DDoS and bots that could be inferred from rate and intensity distributions, as well as future short term DDoS trends targeting various global-scale organizational sites. The latter outcome could be used for immediate response and alerting for mitigation purposes as well as for long term large-scale DDoS analysis.

978-0-7695-5043-5/13 $26.00 © 2013 IEEE
DOI 10.1109/NCA.2013.13

In this context, the paper's contributions are as follows:

- Proposing and adopting a systematic approach for inferring DDoS activities, testing for predictability of DDoS traffic and applying prediction models.
- Leveraging various time series analysis and forecasting methods, including, detrended fluctuation analysis, moving average, weighted moving average, exponential smoothing and linear regression.
- Characterizing and predicting DDoS attacks' impact features, namely, intensity/rate and size.
- Evaluating the proposed approach using real DDoS traffic.

The remainder of this paper is organized as follows: In Section II, we survey the related work. In Section III, we present our proposed approach and discuss various aspects of its components. In Section IV, we empirically evaluate the approach and present several DDoS case studies. Finally, Section V summarizes the paper and discusses the future work.

II. Related Work

In this section, we provide a review of some relevant literature work in the area of threat prediction. In [7], the authors propose a method for threat prediction based on security events using a security monitoring system. Their approach consists of methods to collect and pre-treat security monitoring events, extract threads and sessions, create attack scenarios through correlation analysis, predict intrusions and express the analytical results. The authors evaluate the effectiveness of their prediction model by leveraging real security monitoring events. Dagon et al. [8] adopt a model to accurately predict botnet population growth. The authors use diurnal shaping functions to capture regional variations in online vulnerable populations. They state that since response times for malware outbreaks is measured in hours, the ability to predict short-term propagation dynamics permit resource allocation in a more effective and a suitable manner. The authors use empirical data from botnets collected at a sinkhole to evaluate their analytical model. Moreover, Fachkha et al. [9] present and discuss various darknet-triggered threats and their corresponding severity level. Furthermore, they explore the inter-correlation of such threats, by applying association rule mining techniques, to build threat association rules. Their work demonstrate that in fact certain darknet threats are correlated when targeting specific network destinations. Moreover, it provides insights about threat patterns and allows the building of a classification model for prediction purposes. In another work, Qibo et al. [10] propose an approach to detect and predict DoS SYN flooding attacks using non-parametric cumulative sum algorithm along with an ARIMA model. Instead of managing all real-time ongoing traffic on the network, the approach only monitors SYN packets to predict the attack in the near future. To perform the prediction, the authors propose the auto-regressive integrated moving average model. The authors also run some simulations to validate the effectiveness of the approach. In [11], the authors propose a forecasting mechanism called FORE (FOrecasting using REgression analysis) through a real-time analysis of randomness in network traffic. According to the authors, FORE can respond against unknown worms 1.8 times faster than other detection mechanisms. Evaluation results using real malware traffic demonstrate the efficiency of the proposed mechanism, including its ability to predict worm behaviors starting from 0.03% infection rate.

Most of the above discussed related work assumes that the threat traffic that needs to be predicted is in fact predictable. We argue that such assumption, without essential validation, might result in erroneous forecasting results, regardless of which forecasting approach has been employed. In contrary, in our work, we first statistically test for predictability before attempting to forecast. Additionally, we state that our work in terms of DDoS impact features characterization and prediction is distinctive since the leveraged DDoS inference algorithm is highly accurate and established [12] and does not depend solely on SYN packets. Moreover, our work has wide-scope benefits for security operators, security response teams as well as specific organizations for the short term as well as for the long term large-scale DDoS analysis. Moreover, our proposed approach is designed to effectively work on near real time data. Last but not least, for empirical evaluation purposes, we utilize a significant amount of real network traffic.

III. Proposed Approach

This section presents and discusses various aspects of our forecasting model.

Our dataset is based on real darknet data that we possess. Darknet analysis has been proven to be an effective approach for inferring DDoS activities [12]. In a nutshell, darknet traffic is Internet traffic destined to routable but unused Internet addresses (i.e., dark sensors). Since these addresses are unallocated, any traffic targeting to them may be suspicious and hence need to be investigated. Darknet analysis has shown to be an effective method to generate cyber threat intelligence [13, 14, 15]. Darknet traffic is typically composed of three types of traffic, namely, scanning, misconfiguration and backscattered traffic [16]. Scanning arises from bots and worms while misconfiguration traffic is due to network/routing or hardware/software faults causing such traffic to be sent to the darknet sensors. On the other hand, backscattered traffic commonly refers to unsolicited traffic that results from responses to DoS attacks with spoofed source IP addresses.

The main components of our proposed approach is depicted in Figure 1. In short, the approach is rendered by extracting backscattered data and session flows from darknet traffic. Subsequently, DDoS activities are inferred and consequently tested for predictability. Finally, prediction techniques are applied on DDoS traffic, when applicable. The proposed approach is detailed next.

A. Extracting Backscattered Packets

In order to extract backscattered packets, we adopt the technique from [16] that relies on flags in packet headers, such as TCP SYN+ACK, RST, RST+ACK, and ACK. However, this technique might cause misconfiguration as well as scanning probes (i.e., SYN/ACK Scan) to co-occur within the backscattered packets. In order to filter out the misconfiguration, we use a simple metric that records the average number of sources per destination darknet address. This metric should be significantly larger for misconfiguration than scanning traffic [17]. The scanning packets are filtered out in the next step.

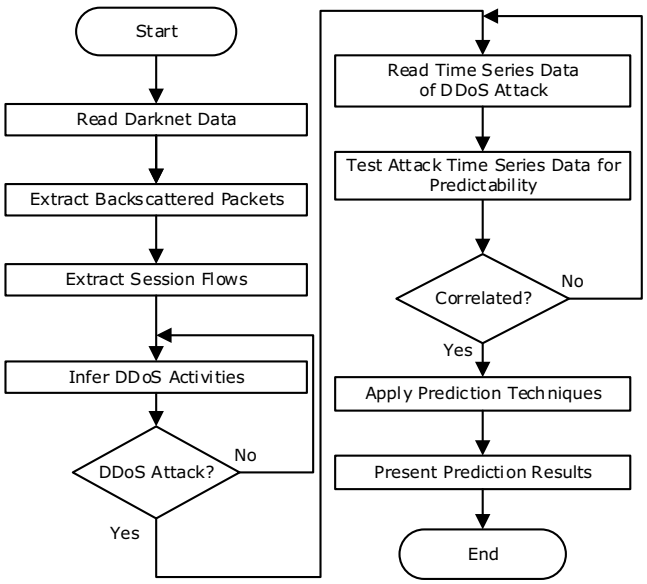

Fig. 1: Flow Chart of the Proposed Approach

B. Extracting Session Flows

In order to filter out the scanning activities, we split the connections into separate session flows, where each session consists of a unique source and destination IP/port pair. The rationale for this is that DDoS attempts possess a much greater number of packets sent to one destination (i.e., flood) whereas portsweeps scanners have one or few attempts towards one destination (i.e., probe).

C. Inferring DDoS Activities

We next aim to confirm that all the extracted sessions in fact reflect real DDoS attempts. To accomplish this, we employ the DDoS detection parameters from [12] to label a session as a single DoS attack. We decided to leverage the latter work since it is directly applicable to our work, which is based on a flow-based approach and leverages backscattered traffic to infer DoS attacks from darknet traffic. We proceed by merging all the previously extracted sessions that have the same source IP (i.e., victim) to extract the DDoS attack.

D. Testing for Predictability

A time series is a sequence of data values that is measured at successive points in time and spaced at uniform time intervals [18]. In order to predict DoS features, we aim to test if the time series of DDoS flows are first correlated. Otherwise, our prediction model would be irrelevant. In order to accomplish this, we statistically test for predictability in such time series using the Detrended Fluctuiona Anlaysis (DFA) technique. DFA was first proposed in [19] and has since been used in many research areas to study signals correlation. The DFA technique is summarized next.

The DFA method of characterizing a non-stationary time series is based on the root mean square analysis of a random walk. DFA is advantageous in comparison with other methods such as spectral analysis [20] and Hurst analysis [21] since it permits the detection of long range correlations embedded in a seemingly non-stationary time series. It avoids as well the spurious detection of apparent long-range correlations that are an artifact of non-stationarity. Another advantage of DFA is that it produces results that are independent of the effect of the trend [22]. Last but not least, this technique is applicable to darknet traffic [23].

Given a traffic time series, the following steps need to be applied to implement DFA:

- Integrate the time series; The time series of length N is integrated by applying

$$y(k) = \sum_{i=1}^{k} (B(i) - B_{ave})$$

  where $B(i)$ is the i^{th} interval and B_{ave} is the average interval.

- Divide the time series into "boxes" (i.e., bin size) of length n.
- In each box, perform a least-squares polynomial fit of order p. The y coordinate of the straight line segments is denoted by $y_n(k)$.
- In each box, detrend the integrated time series, $y(k)$, by subtracting the local trend, $y_n(k)$. The root-mean-square fluctuation of this integrated and detrended time series is calculated by

$$F(n) = \sqrt{\frac{1}{N} \sum_{k=1}^{N} (y(k) - y_n(k))^2}$$

- Repeat this procedure for different box sizes (i.e., time scales) n

The output of the DFA procedure is a relationship $F(n)$, the average fluctuation as a function of box size, and the box size n. Typically, $F(n)$ will increase with box size n. A linear relationship on a log-log graph indicates the presence of scaling; statistical self-affinity expressed as $F(n) \sim n^{\alpha}$. Under such conditions, the fluctuations can be characterized by a scaling exponent α, which is the slope of the line relating $logF(n)$ to $log(n)$. The scaling exponent α can take the following values, disclosing the "correlation status" of the traffic time series:

- $\alpha < 0.5$: anti-correlated
- $\alpha \approx 0.5$: uncorrelated or white noise
- $\alpha > 0.5$: correlated
- $\alpha \approx 1$: $1/f$-noise or pink noise
- $\alpha > 1$: non-stationary, random walk like, unbounded
- $\alpha \approx 1.5$: Brownian noise

In our work, if the application of DFA on the DDoS traffic time series outputs a "correlated" status, then we assert that it is predictable; else, we extract another DDoS flow and re-test it for predictability.

E. Forecasting DDoS

Finally, to perform the predictions, we apply different types of forecasting techniques, namely, moving average, weighted moving average, exponential smoothing and linear regression. We have selected to leverage these techniques instead of other complex well-known models such as ARIMA and GARCH [24] since the latter require long-term (weekly, monthly, yearly, etc.) seasonal time series data, which is not true in our case that deals with short-term DDoS traffic. The selected methods are briefed next.

Moving Average (MA): The single parameter of the model is estimated as the average of the previous x data points at time t in the time series. The MA is given by:

$$\widehat{x}_{t+1} = \frac{1}{k} * (x_t + x_{t-1} + ... + x_{t-k-1}),$$

where k is the smoothing window or period. Note that, the forecast in this technique should not begin until the specified previous data are available.

Weighted Moving Average (WMA): This technique is based on a numeric value known as the weight. In general, a WMA is more responsive to change in the time series data than a simple MA. The computation of the WMA estimated temporal average is given by [25]:

$$\widehat{x}_{t+1} = \frac{w_{t-k}x_{t-k} + ... + w_t x_t}{h},$$

where k is the chosen window size and h is the sum of the temporal weight, $h = w_{t-k} + ... + w_t$. In general, to obtain better results, highest weight is given to the most recent periods. In our work, we run a solver [26] to automatically obtain the weight values that produces a relatively better prediction results.

Note that in our work, for the above two techniques, namely, the MA and the WMA, we adopt a time window that is equivalent to three data points in the time series. We believe this provides a good estimate for such models as also demonstrated in [27]. Future work would extend such analysis by experimenting with different time window sizes.

Exponential Smoothing (ES): This technique calculates the parameter of the estimated prediction value b as the weighted average of the last observation and the last estimate. The estimated value is given by:

$$\widehat{x}_{t+1} = \alpha x_t + (1 - \alpha)\widehat{x}_t,$$

where α is the smoothing factor and has a value between [0,1]. In our analysis, we again run a solver [26] to automatically choose the best value of α that optimizes the prediction error rate.

Linear Regression (LR): This technique performs statistical analysis that assesses the association between two variables. This method is used to pinpoint the relationship among these variables. A simple LR is given by:

$$LR(y) = a + bx,$$

where x and y are the variables, b is the slope of the regression line, a is the intercept point of the regression line and the y-axis.

Two main elements characterize this model, namely, the slope and the intercept, given by:

$$Slope(b) = \frac{N\sum XY - \sum X \sum Y}{N\sum X^2 - (\sum X)^2},$$

$$Intercept(a) = \frac{\sum Y - b\sum X}{N},$$

where N is the number of values or elements, X is the first score and Y is the second score. The slope describes the incline or grade of the line whereas the intercept is the point where the graph of a function intersects with the y-axis of the coordinate scheme.

We refer interested readers to [28, 29] for more details on the above mentioned prediction techniques.

To evaluate the performance of the prediction methods, we compute the absolute prediction error. The equation of the absolute prediction error is given by:

$$r(t) = \frac{|\widehat{X}_i(t) - X_i(t)|}{X_i(t)}$$

This error metric is defined as the absolute difference of the predicted value from the actual value divided by the actual value. The latter is a de-facto metric when computing the performance of a prediction model [29, 30].

IV. Empirical Evaluation

In this section, we present the empirical evaluation results. We abide and closely follow the steps of our proposed approach that were discussed in Section III to present three real (D)DoS case studies targeting three different servers. The case studies respectively consist of TCP SYN flooding targeting an HTTP (web) server, TCP SYN flooding targeting a Domain Name System (DNS) and an ICMP (ping) flooding. The three case studies are summarized in Table I.

Case Study	Analyzed Attack Duration (second)	Intensity (packet)	Rate (pps)	DFA Value	Size of Spoofed IPs
TCP SYN Flooding (HTTP)	3194	1799228	563.31	0.91	24
TCP SYN Flooding (DNS)	3550	29016	8.17	0.93	206
ICMP Flooding	3599	3577	1.00	0.67	1

TABLE I: Summary of the Analyzed (D)DoS Case Studies

The table shows the analyzed duration of the attack (in seconds), the attack's intensity in terms of number of generated packets, its average rate (packets/sec), its DFA value and its size in terms of number of used compromised machines/bots. In regards to our dataset, the possessed darknet data is being received on a daily basis from a trusted third party. The darknet sensors are distributed in many countries and monitor /13

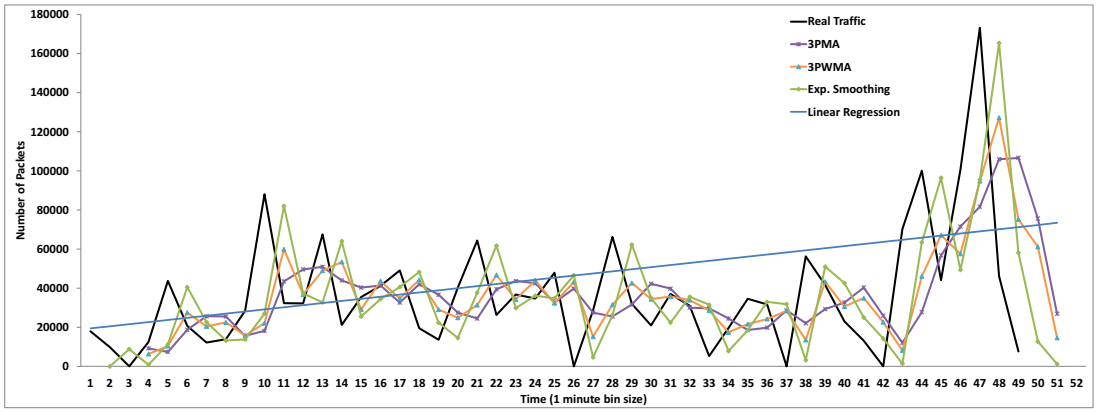

Fig. 2: TCP SYN Flooding on an HTTP Server - Intensity Distribution & Prediction

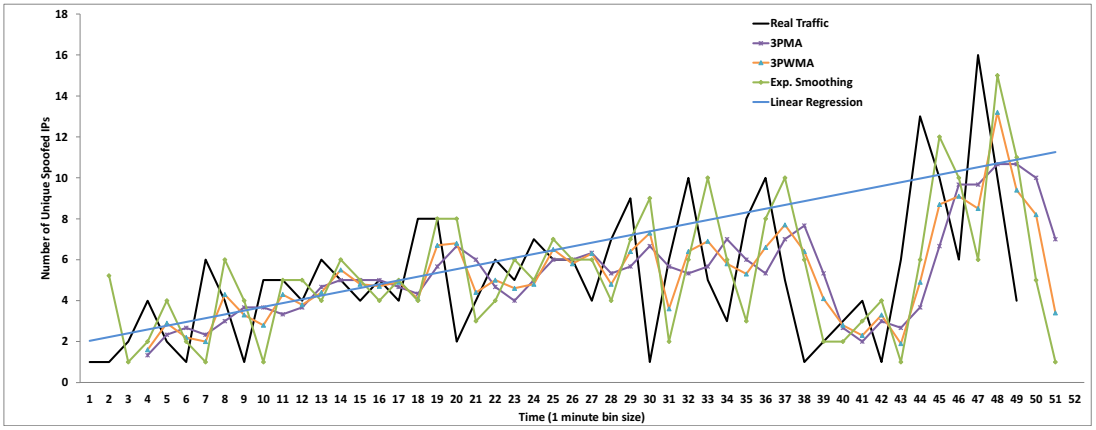

Fig. 3: TCP SYN Flooding on an HTTP Server - Size Distribution & Prediction

address blocks. In terms of DFA computation, we utilize the DFA MATLAB code found in [31] and used 1ms as the bin size. Further, when applying the forecasting techniques, for the purpose of error calculation, we use two thirds (66.66%) of the DDoS traffic time series for training and one third (33.33%) for testing. It is also noteworthy to mention that when performing the prediction analysis, depicted in Figures 2 to 6, we chose a time series with bin size equals to one minute. We argue that such a choice is rational and should provide enough resources (i.e., time) to the organization under attack to act upon the observed values. The case studies are elaborated next.

TCP SYN Flooding on an HTTP Server: This case study refers to a DDoS TCP SYN flooding targeting an HTTP web server. From Table I, we notice that this attack lasted 53 minutes, generated around 1.8 million TCP SYN packets, with an average of 560 packets per second from 24 unique spoofed IPs (i.e., bots). The value of the rate of the attack demonstrates the severity of this DDoS attack.

Moreover, Figures 2 and 3 demonstrates the application of the forecasting techniques. Note that, we attempt to predict this DDoS since its corresponding DFA result was shown to be "correlated" with value $= 0.91$ as stated in Section III-D). Figure 2 illustrates the attack's intensity distribution with its corresponding forecasting techniques. It is shown that the attack peaks with around 175 thousand packets at the 46^{th} minute. The predicted values (within the future 3 minutes) of such distribution reveal that the attack will decrease in intensity and fluctuates between 9000 and 3500 packets. On the other hand, Figure 3 illustrates the attack's size in terms of number of used spoofed IPs. It is shown that the number of spoofed IPs peak to 16 in the 48^{th} minute. Similar to the intensity, it is shown from the prediction techniques that the size will as well decrease, hinting that the DDoS might soon diminish in size. The absolute prediction error of the forecasting techniques for this DDoS case study is summarized in Table II.

	Prediction Techniques			
	MA	WMA	ES	LR
Intensity	0.57	0.39	0.19	0.86
Size	0.70	0.53	1.34	0.22

TABLE II: TCP SYN Flooding on an HTTP Server - Absolute Prediction Error (%)

We can notice that all the techniques for both impact features recorded an error less than 1%. Further, the exponential smoothing algorithm was best in predicting the intensity while the linear regression was best in predicting the size of the

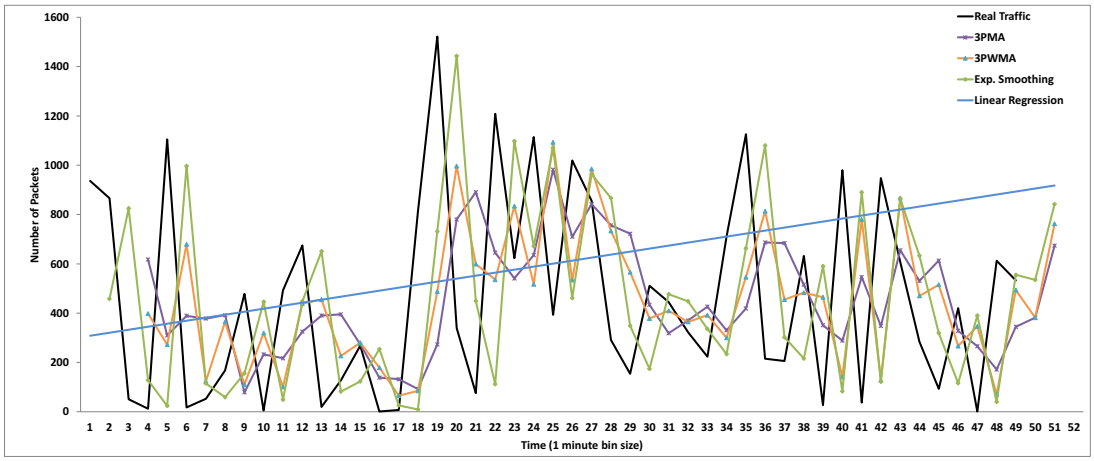

Fig. 4: TCP SYN Flooding on a DNS Server- Intensity Distribution & Prediction

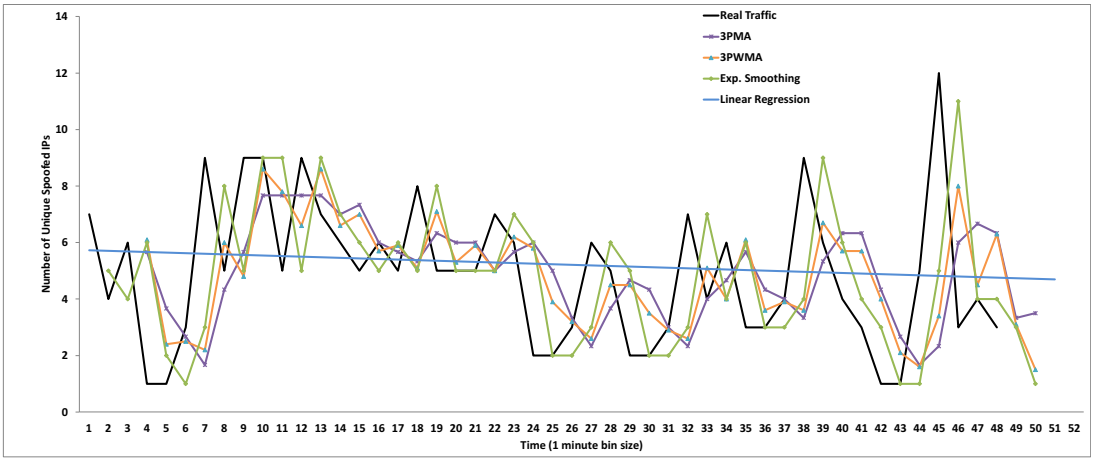

Fig. 5: TCP SYN Flooding on a DNS Server- Size Distribution & Prediction

attack. This case study allows the organization whose web server is under a targeted DDoS to gain insight in terms of the current and future short term trend of the ongoing attack in terms of the defined attack impact features. Moreover, assuming that the organization modified its mitigation methods before predicting the future impact distributions, reveal that such modifications are effective.

TCP SYN Flooding on a DNS Server: This case study refers to a DDoS TCP SYN flooding targeting a DNS server. From Table I, we notice that this attack lasted 59 minutes, generated around 29 thousand TCP SYN packets, with an average of 8 packets per second from 206 unique spoofed IPs (i.e., bots). Although the size of this DDoS attack is larger than the first case study, however, its intensity in terms of the generated packets and hence rate is significantly lower.

Figures 4 and 5 depict the characterization in addition to demonstrating the application of the forecasting techniques. We also predicted this DDoS attack since its corresponding DFA result was shown to be "correlated" with value = 0.93. Figure 4 illustrates the attack's intensity and prediction distributions. It is shown that the attack peaks around 1600 packets at the 19^{th} minute. The predicted values of such distribution shows insights of increase in the attacks intensity. On the other hand, Figure 5 reveals the attack's size in terms of number of used compromised machines/bots. It is shown that the number of spoofed IPs peaks to 12 in the 45^{th} minute. Furthermore, it is shown from the prediction models that the attack size will either stay constant or slightly decrease. The absolute prediction error of the forecasting techniques for this DDoS case study is summarized in Table III. We notice that the linear regression poorly performs with regards to this case study. Moreover, the exponential smoothing algorithm was best in predicting both the intensity and the size. This case study allows the organization whose DNS server is under a DDoS

	Prediction Techniques			
	MA	WMA	ES	LR
Intensity	12.46	5.24	2.75	35.71
Size	0.51	0.37	0.16	0.72

TABLE III: TCP SYN Flooding on a DNS Server - Absolute Prediction Error (%)

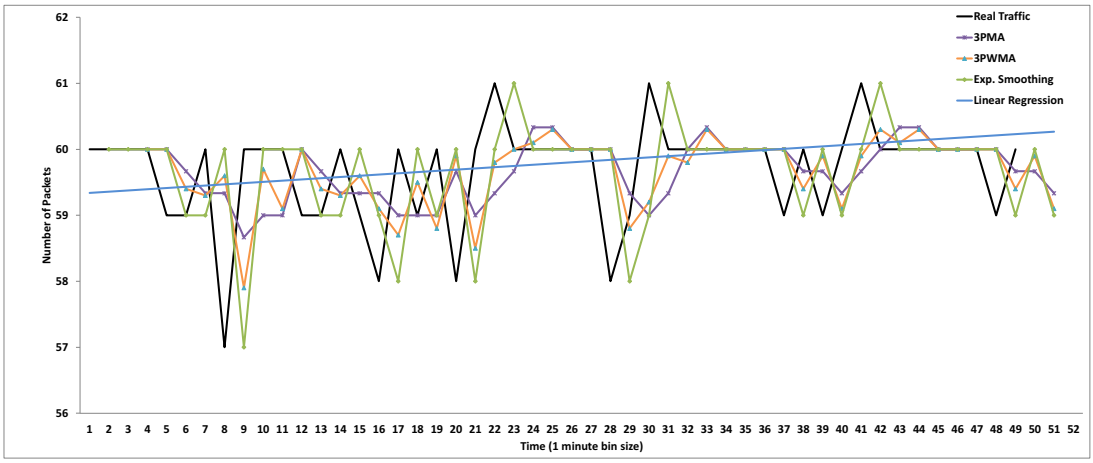

Fig. 6: ICMP (ping) Flooding - Intensity Distribution & Prediction

attack to be alerted that the attack's intensity might increase. This provides the organization the capability to comprehend the situation and hence adaptively respond to the threat.

ICMP (ping) Flooding: This case study refers to a DoS ICMP (ping) flooding targeting a server. The major difference between this attack and the former case studies is that this attack is generated from only one machine (i.e., not distributed) and it could be attempting to evade detection by using a relatively low attack rate (1 packet/second). Further, its DFA result shows signs of strong correlation (the DFA scaling exponent α = 0.67) in its attack signal. This is confirmed in Figure 6 where the intensity distribution fluctuates around 60 packets. From the prediction techniques, we can observe that the attack's intensity will continue to be close to 60 packets or slightly increase. The summary of the result is shown in Table IV. Moreover, the attack's correlation and intensity features allow the organization whose server is under this type of DoS attack to infer that the attack is relatively of low impact and non-distributed and hence current mitigation methods will be sufficient.

	Prediction Techniques			
	MA	WMA	ES	LR
Intensity	0.13	0.13	0.12	0.13

TABLE IV: ICMP (ping) Flooding - Absolute Prediction Error (%)

It should be noted that the generated inferences from the above case studies aim to better understand the scale and rate of DDoS attacks that could be adopted by organizations for immediate response and hence mitigation as well as accumulated by security operators, emergency response teams and observers of large-scale Internet DDoS events for the purpose of long term large-scale DDoS analysis, clustering and correlation.

V. Conclusion

This paper proposed an approach that is rendered by a DDoS forecasting model. The aim is to provide the organization under attack the capability to comprehend the situation and hence adaptively respond to the threat. We characterize and predict, within minutes, the attacks' impact features, namely, intensity/rate (packets/sec), and size (number of used compromised machines/bots). Our proposed approach leverages real darknet data to infer DDoS activities, test for predictability of DDoS traffic and apply prediction techniques, when applicable. Empirical evaluations presented three attack case studies to demonstrate possible extracted insights and inferences. For future work, we intend to experiment with more complex forecasting methods that can operate on probability and long-term bases as well as implementing our proposed approach in a real-time fashion.

References

[1] Arbor Networks, "2012 Infrastructure Security Report," http://tinyurl.com/ag6tht4, last accessed on April 2013.
[2] Forbes, "Testing The Limits, LulzSec Takes Down CIA's Website," http://tinyurl.com/bfhzbta, last accessed on March 2013.
[3] PcWorld, "Hacker Arrested for DDoS Attacks on Amazon.com," http://tinyurl.com/d22myng, last accessed on March 2013.
[4] ITPRO, "InfoSec 2011: Energy firms pummelled by DDoS attacks," http://tinyurl.com/cpqodbx, last accessed on March 2013.
[5] Ars Technica, "When spammers go to war: Behind the Spamhaus DDoS," http://tinyurl.com/d9vkegg, 2013, last accessed on April 2013.
[6] A. Kuzmanovic and E. W. Knightly, "Low-rate tcp-targeted denial of service attacks: the shrew vs. the mice and elephants," in *Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications*. ACM, 2003.
[7] N. Park and W. H. Park, "Cyber threat prediction model

using security monitoring system event," in *IT Convergence and Security 2012*. Springer, 2013.

[8] D. Dagon, C. Zou, and W. Lee, "Modeling botnet propagation using time zones," in *Proceedings of the 13th annual network and distributed system security symposium (NDSS06)*, 2006.

[9] C. Fachkha, E. Bou-Harb, A. Boukhtouta, S. Dinh, F. Iqbal, and M. Debbabi, "Investigating the dark cyberspace: Profiling, threat-based analysis and correlation," in *7th International Conference on Risk and Security of Internet and Systems (CRiSIS)*. IEEE, 2012.

[10] S. Qibo, W. Shangguang, Y. Danfeng, and Y. Fangchun, "Arm-cpd: Detecting syn flooding attack by traffic prediction," in *2nd IEEE International Conference on Broadband Network Multimedia Technology*, 2009.

[11] H. Park, S.-O. D. Jung, H. Lee, and H. P. In, "Cyber weather forecasting: Forecasting unknown internet worms using randomness analysis," in *Information Security and Privacy Research*. Springer, 2012.

[12] D. Moore, C. Shannon, D. J. Brown, G. M. Voelker, and S. Savage, "Inferring internet denial-of-service activity," *ACM Transactions on Computer Systems (TOCS)*, 2006.

[13] M. Bailey, E. Cooke, F. Jahanian, J. Nazario, D. Watson *et al.*, "The internet motion sensor: A distributed blackhole monitoring system," in *Proceedings of the 12th ISOC Symposium on Network and Distributed Systems Security (SNDSS)*, 2005.

[14] V. Yegneswaran, P. Barford, and D. Plonka, "On the design and use of internet sinks for network abuse monitoring," in *Recent Advances in Intrusion Detection*, ser. Lecture Notes in Computer Science, E. Jonsson, A. Valdes, and M. Almgren, Eds. Springer Berlin / Heidelberg, 2004.

[15] Team Cymru - Community Services, "The Darknet Project," http://www.cymru.com/Darknet, last accessed on April 2013.

[16] E. Wustrow, M. Karir, M. Bailey, F. Jahanian, and G. Huston, "Internet background radiation revisited," in *Proceedings of the 10th annual conference on Internet measurement*. ACM, 2010.

[17] Z. Li, A. Goyal, Y. Chen, and V. Paxson, "Towards situational awareness of large-scale botnet probing events," *IEEE Transactions on Information Forensics and Security*, 2011.

[18] J. D. Hamilton, *Time series analysis*. Cambridge Univ Press, 1994.

[19] C.-K. Peng, S. V. Buldyrev, S. Havlin, M. Simons, H. E. Stanley, and A. L. Goldberger, "Mosaic organization of DNA nucleotides," *Phys. Rev. E*, 1994.

[20] M. Priestley, *Spectral analysis and time series*. Academic press, 1981.

[21] J. Matos, S. Gama, H. Ruskin, A. Sharkasi, and M. Crane, "Time and scale hurst exponent analysis for financial markets," *Physica A: Statistical Mechanics and its Applications*, 2008.

[22] K. Hu, P. Ivanov, Z. Chen, P. Carpena, and H. Stanley, "Effect of trends on detrended fluctuation analysis," *Physical Review E*, 2001.

[23] K. Fukuda, T. Hirotsu, O. Akashi, and T. Sugawara, "Correlation among piecewise unwanted traffic time series," in *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE*. IEEE, 2008.

[24] B. Zhou, D. He, Z. Sun, and W. H. Ng, "Network traffic modeling and prediction with arima/garch," in *HET-NETs 06 Conference*. Citeseer, 2005.

[25] Y. Zhuang, L. Chen, X. Wang, and J. Lian, "A weighted moving average-based approach for cleaning sensor data," in *27th International Conference on Distributed Computing Systems ICDCS*, 2007.

[26] D. Fylstra, L. Lasdon, J. Watson, and A. Waren, "Design and use of the microsoft excel solver," *Interfaces*, vol. 28, no. 5, 1998.

[27] W.-K. Wong, M. Manzur, and B.-K. Chew, "How rewarding is technical analysis? evidence from singapore stock market," *Applied Financial Economics*, vol. 13, no. 7, 2003.

[28] The University of Texas at Austin, "Time Series and Forecasting," http://tinyurl.com/bsxscwx, 2002, last accessed on April 2013.

[29] M. Papadopouli, E. Raftopoulos, and H. Shen, "Evaluation of short-term traffic forecasting algorithms in wireless networks," in *2nd Conference onNext Generation Internet Design and Engineering, NGI.* IEEE, 2006.

[30] A. Goia, C. May, and G. Fusai, "Functional clustering and linear regression for peak load forecasting," *International Journal of Forecasting*, vol. 26, no. 4, 2010.

[31] M. Little, P. McSharry, I. Moroz, and S. Roberts, "Nonlinear, biophysically-informed speech pathology detection," in *Acoustics, Speech and Signal Processing. ICASSP Proceedings.*, vol. 2, 2006.