WIRELESS COMMUNICATIONS AND MOBILE COMPUTING
Wirel. Commun. Mob. Comput. 2015; **15**:1066–1078
Published online 6 August 2014 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/wcm.2510

SPECIAL ISSUE PAPER

On the inference and prediction of DDoS campaigns

Claude Fachkha*, Elias Bou-Harb and Mourad Debbabi

Computer Security Laboratory, CIISE, Concordia University and NCFTA Canada, Montreal, QC, Canada

ABSTRACT

This work proposes a distributed denial-of-service (DDoS) inference and forecasting model that aims at providing insights to organizations, security operators, and emergency response teams during and after a DDoS attack. Specifically, our work strives to predict, within minutes, the attacks' features, namely intensity/rate (packets/second) 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. Further, our work aims at investigating DDoS campaigns by proposing a clustering approach to infer various victims targeted by the same campaign and predicting related features. Our analysis employs real darknet data to explore the feasibility of applying the inference and forecasting models on DDoS attacks and evaluate the accuracy of the predictions. To achieve our goal, our proposed approach leverages a number of time series and fluctuation analysis techniques, statistical methods, and forecasting approaches. The extracted inferences from various DDoS case studies exhibit a promising accuracy reaching at some points less than 1% error rate. Further, our approach could lead to a better understanding of the scale, speed, and size of DDoS attacks and generates inferences that could be adopted for immediate response and mitigation. Moreover, the accumulated insights could be used for the purpose of long-term large-scale DDoS analysis.

KEYWORDS
DDoS attacks; campaigns; prediction; forecasting

***Correspondence**
Claude Fachkha, Computer Security Laboratory, CIISE, Concordia University and NCFTA Canada, 1455 De Maisonneuve Blvd, Montreal, QC H3G 1M8, Canada.
E-mail: c_fachkh@encs.concordia.ca

1. INTRODUCTION

Denial-of-service (DoS) attacks are characterized by an explicit attempt to prevent the legitimate use of a service. 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 four perceived threats for the next 12 months will be DDoS related, targeting customers, network, and service infrastructures. Some governmental organizations, corporations, and critical infrastructure were also recently deemed as DDoS victims [2–4]. Moreover, a recent event demonstrated that one of the largest cyber security organizations, namely Spamhaus, became a victim of a 300 Gbps DDoS attack [5]. Thus, DDoS attacks are a significant cyber security problem, causing momentous damage to several victims as well as negatively affecting, by means of collateral damage, the availability of services, business operations, market share, and the trust in, as well as the reputation of the organization under attack. When an organization is subject to a DDoS, it becomes essential for its IT security operators and emergency response teams to answer the following questions:

- What are the characteristics of a DDoS attack?
- What is the future short-term trend of the attack in question?
- Is it an isolated DDoS attempt or a campaign of attacks against multiple victims?

The answers to these questions greatly influence the actions and the resources that organizations and Internet security response teams 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 trigger 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. E-commerce sites, for instance, are very sensitive to DDoS attacks; each 1 min of downtime could cost them more than $30,000 [6]. Note that low-rate DDoS attacks could evade detection and, at the same time, exhaust the victim with long-lived flows [7]. Moreover, having knowledge about the short-term (i.e., in terms of minutes) predicted 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 DDoS cease after few minutes or will it persist for a longer period? 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 distinct DDoS attacks in different 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) 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 campaign size and its corresponding machines geodistribution, the victims geolocation, types of DDoS that could be inferred from rate and intensity distributions, and future short-term DDoS trends targeting various 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.

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

- Proposing and adopting a systematic approach for inferring DDoS activities, characterizing and testing for predictability of DDoS traffic.
- Applying forecasting models on predictable DDoS attacks.
- Proposing a clustering approach to infer similarities among attack traces for DDoS campaign detection.
- Evaluating the proposed approach on real darknet traffic.

The remainder of this paper is organized as follows. In Section 2, we survey the related work. In Section 3, we present our proposed approach and discuss various aspects of its components. In Section 4, we empirically evaluate the approach and present several DDoS case studies. Finally, Section 5 summarizes the paper and discusses the future work.

2. RELATED WORK

In this section, we provide a review of some relevant literature work in the area of threat prediction. In [8], 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 and extract threads and sessions. Moreover, it consists of techniques to 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.* [9] 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 because 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 suitable manner. The authors use empirical data from botnets collected at a sinkhole to evaluate their analytical model. Moreover, Fachkha *et al.* [10] present and discuss various darknet-triggered threats and their corresponding severity level. Furthermore, they explore the intercorrelation of such threats, by applying association rule mining techniques, to build threat association rules. Their work demonstrates 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.* [11] propose an approach to detect and predict DoS SYN flooding attacks using non-parametric cumulative sum algorithm along with an autoregressive integrated moving average (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 ARIMA model. The authors also run some simulations to validate the effectiveness of the approach. In [12], 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 previously 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 is distinctive because the leveraged DDoS inference algorithm is highly accurate and established [13] and does not depend solely on SYN packets. Moreover, our work has wide-scope benefits for security operators, security response teams, and specific organizations for the short-term as well as the long-term large-scale DDoS analysis. Further, our proposed approach is designed to effectively work on near real-time data. Last

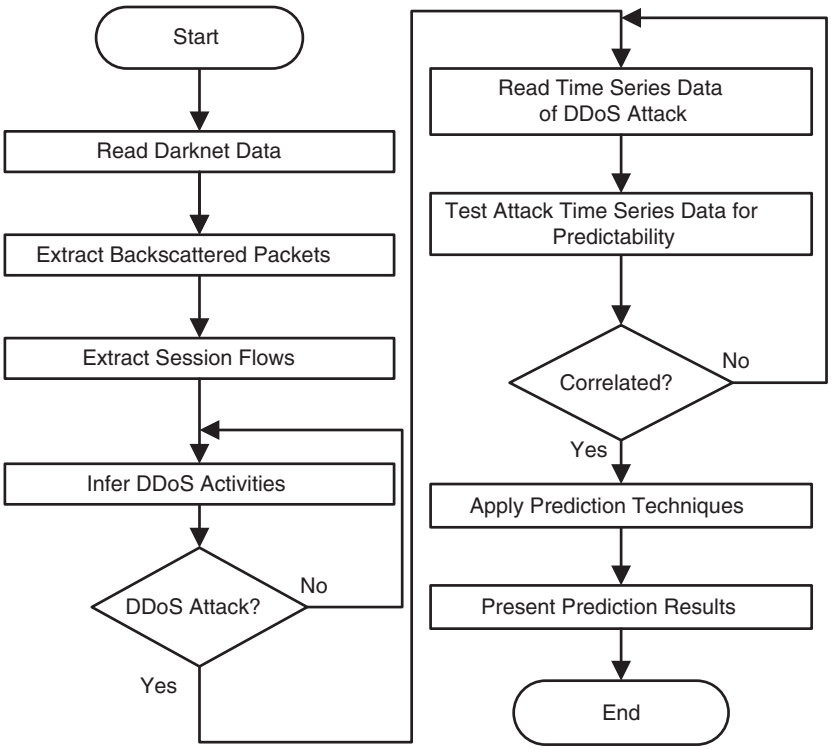

Figure 1. Flowchart of the proposed approach.

but not least, for empirical evaluation purposes, we utilize a significant amount of real network traffic.

3. PROPOSED APPROACH

This section, initially, presents and discusses various aspects of the DDoS inference and forecasting model. Subsequently, the model is extended to enable the capturing and the prediction of DDoS campaigns that target multiple victims.

Our dataset is based on real darknet data that we possess. Darknet analysis has been proven to be an effective approach for inferring IPv4 and IPv6 [14] threats such as DDoS [13], scanning [15], and other large-scale cyber events [16–20]. In a nutshell, darknet traffic is Internet traffic destined to routable but unused Internet addresses (i.e., dark sensors). Because these addresses are unallocated, any destined traffic may be suspicious and hence need to be investigated. Darknet analysis has shown to be an effective method to generate cyber threat intelligence [21–23]. Darknet traffic is typically composed of various types of traffic, namely DDoS [24], scanning [25,26], misconfiguration, and backscattered traffic [27]. Scanning arises from bots and worms, whereas 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 the DDoS inference and forecasting 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.

3.1. Extracting backscattered packets

In order to extract backscattered packets, we adopt the technique from [27] 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 [28]. The scanning packets are filtered out in the next step.

3.2. 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

Table I. DDoS inference parameters.

Parameter	Value
Flow timeout	5 min
Packet threshold	>25 packets
Attack duration	>60 s
Packet rate	>0.5 packets/s

a much greater number of packets sent to one destination (i.e., flood), whereas portsweep scanners have one or few attempts toward one destination (i.e., probe).

3.3. Inferring DDoS activities

Next, we aim to confirm that all the extracted sessions reflect real DDoS attempts. To accomplish this, we employ the DDoS detection parameters of Table I, leveraged from [13]. In the following, we briefly describe the selected parameters.

3.3.1. Flow timeout.

The flow timeout parameter is the maximum time interval between two reply packets from the same source victim. This parameter helps in discarding attacks that do not cause significant harm on the victims.

3.3.2. Packet threshold.

The packet threshold parameter is the minimum number of packets sent by a victim on the darknet sensors. For a given set of flows, higher packet thresholds result in few attacks. The packet threshold is a good indicator of the intensity of the attack.

3.3.3. Attack duration.

The attack duration is the minimum amount of time between the first and last packet of the flow. A larger value generate fewer attacks. The goal of the attack duration is to filter out short attacks, which have negligible affect on a machine.

3.3.4. Packet rate.

The packet rate parameter defines the speed of the attack. This parameter is useful to extract DoS attacks with high impact.

In this work, we leverage the results of Moore *et al.* [13] because it is directly applicable to our work, which is based on a flow-based approach and employs 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.

3.4. Testing for predictability

A time series is a series of data values that is measured at successive points in time and spaced at uniform time intervals [29]. In order to predict DoS features, we aim to test if the time series of DDoS flows are first correlated. Otherwise, our prediction would be irrelevant. In order to accomplish this, we statistically test for predictability in such time series using the detrended fluctuation analysis (DFA) technique. DFA was first proposed in [30] and has since then been used in many research areas to study signals correlation. The DFA technique is summarized next.

The DFA method, which consists of characterizing a non-stationary time series, is based on the square root average study of a random walk. DFA is advantageous in comparison with other methods such as spectral analysis [31] and Hurst analysis [32] because it allows the inference of long-term correlations inside an apparently non-stationary time series. It avoids as well the non-stationary correlations. Another advantage of DFA is that it produces results that are independent of the effect of the trend [33]. Last but not least, this technique is applicable to darknet traffic [34].

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

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

  where $B(i)$ is the ith 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-axis represents the $y_n(k)$.
- In each box, detrend the time series that is integrated, $y(k)$, by taking away the local trend, $y_n(k)$. This integrated and detrended time series has a root-mean-square fluctuation that 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 mean fluctuation as a function of n (box size). Generally, $F(n)$ increases with the box size n. Scaling appears when there is a linear relationship on a log-log graph; statistical self-affinity is expressed as $F(n) \sim n^{\alpha}$. Hence, the fluctuations can be described by a scaling exponent α, which is the slope of the line relating $\log F(n)$ 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
- $\alpha \approx 1.5$: 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.

3.5. Predictability analysis and forecasting

To perform the predictions, we apply different types of forecasting techniques, namely moving average (MA), weighted moving average (WMA), exponential smoothing (ES), and linear regression (LR). We have selected to leverage these techniques instead of other complex well-known models such as ARIMA and generalized autoregressive conditional heteroskedasticity [35] because 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 briefly recalled in what follows.

3.5.1. Moving average.

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 the following:

$$\hat{x}_{t+1} = \frac{1}{k} * (x_t + x_{t-1} + \ldots + x_{t-k-1})$$

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.

3.5.2. Weighted moving average.

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 the following [36]:

$$\hat{x}_{t+1} = \frac{w_{t-k}x_{t-k} + \ldots + w_t x_t}{h}$$

where k is the chosen window size and h is the sum of the temporal weight, $h = w_{t-k} + \ldots + w_t$. In general, to obtain better results, the highest weight is given to the most recent periods. In our work, we run a solver [37] to automatically obtain the weight values that produce a relatively better prediction results.

Furthermore, 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 demonstrated in [38]. Future work would extend such analysis by experimenting with different time window sizes.

3.5.3. Exponential smoothing.

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 the following:

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

where α is the smoothing factor and has a value between [0,1]. In our analysis, we again run a solver [37] to automatically choose the best value of α that optimizes the prediction error rate.

3.5.4. Linear regression.

This technique performs statistical analysis that assesses the association between two variables. A simple LR is given by the following:

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

where x and y are the variables, b is the slope of the regression line, and 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 the following:

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

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

where N is the number of elements, X is the first value, and Y is the second value. 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 the interested reader to [39,40] for more details on the aforementioned 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 the following:

$$r(t) = \frac{\left|\hat{X}_i(t) - X_i(t)\right|}{X_i(t)}$$

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 [39,41].

3.6. Clustering of DDoS campaigns

In the previous sections, we elaborated on the components of the systematic approach for inferring DDoS activities targeting a unique organization, testing for predictability of such DDoS traffic and subsequently applying the prediction methods. In this section, we extend the model by

Table II. Summary of the analyzed DDoS case studies.

Case study	Victim	Analyzed attack duration (seconds)	Intensity (packet)	Average rate (pps)	DFA value	Size of spoofed IPs
TCP SYN flooding (HTTP)	Unique	3194	1799228	563.31	0.91	24
TCP SYN flooding (DNS)	Unique	3550	29016	8.17	0.93	206

proposing a clustering approach to infer DDoS campaigns that target multiple victims. The aim is to predict DDoS campaigns. Moreover, this permits the fingerprinting of the nature of such campaigns. For example, it could be identified that a specific DDoS campaign is specialized in targeting financial institutions while another campaign is focused on targeting various critical infrastructures. Further, such clustering approach allows the elaboration on the actual scope of the DDoS campaign to provide cyber security situational awareness; how large is the campaign and what is its employed rates, when attacking the various victims. Additionally, the proposed approach could be leveraged to predict the campaign's features in terms of rate and number of involved machines. To accomplish these goals, the approach employs the following statistical-based mechanism. First, backscattered sessions are extracted as previously discussed in Sections 3.1 and 3.2. Second, the notion of fuzzy hashing [42] between the different sessions is applied. Fuzzy hashing is advantageous in comparison with typical hashing as it can provide a percentage of similarity between two traffic samples rather than producing a null value if the samples are different. This popular technique is derived from the digital forensics research field and is typically applied on files or images [42,43]. Our approach explores the capabilities of this technique on backscattered DDoS traffic. We select the sessions that demonstrate at least 20% similarity. We concur that this threshold is a reasonable starting point and aids in reducing false negatives. Third, from those sessions, we employ two statistical tests, namely the Euclidean test and the Kolmogorov–Smirnov test [44], to measure the distance between the latter selected sessions. We select those sessions that minimize the statistical distance and overlap after executing both tests. The rationale of the latter approach stems from the need to cluster the sessions belonging to multiple victims that share similar traffic behavior while minimizing the false positives by confirming such similarity using both tests. Note that we hereafter refer to the use of the previous two techniques as the fusion technique. The outcome of the proposed approach is clustered diverse victims that are inferred to be the target of the same DDoS campaign.

4. EMPIRICAL EVALUATION

In this section, we present the empirical evaluation results. First, we follow the steps of the DDoS inference and forecasting approach as discussed in Section 3 to present two real DDoS case studies targeting two different servers. The case studies respectively consist of two TCP SYN flooding attacks targeting an HTTP (Web) server and a domain name system (DNS) service. Second, we employ the DDoS campaign clustering model as discussed in Section 3.6 to demonstrate how multiple victims could be modeled as being the target of the same campaign.

The two case studies generated using the DDoS inference and forecasting model are summarized in Table II. 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/second), its DFA value, and its size in terms of number of used compromised machines/bots. With regard to our dataset, the possessed darknet data are being received on a daily basis from a trusted third party. The darknet sensors are distributed in many countries and monitor /13 address blocks. In terms of DFA computation, we utilize the DFA MATLAB code [45]. Further, when applying the forecasting techniques, for the purpose of error calculation, we use two thirds of the DDoS traffic time series for training and one third for testing. It is also noteworthy to mention that when performing the prediction analysis, we chose a time series with bin size equals to 1 min. 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. Next, we elaborate on the case studies.

4.0.1. TCP SYN flooding on an HTTP server.

This case study refers to a DDoS TCP SYN flooding targeting an HTTP Web server. From Table II, we notice that this attack 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 demonstrate the application of the forecasting techniques. Note that we attempt to predict this DDoS because its corresponding DFA result was shown to be "correlated" with a value of 0.91 as stated in Section 3.4). Figure 2 illustrates the attack's intensity distribution with its corresponding forecasting techniques. It is shown that the attack peaks with around 175 000 packets at the 46th minute. The predicted values (within the future 3 min) of such distribution reveal that the attack will decrease in intensity and will fluctuate 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

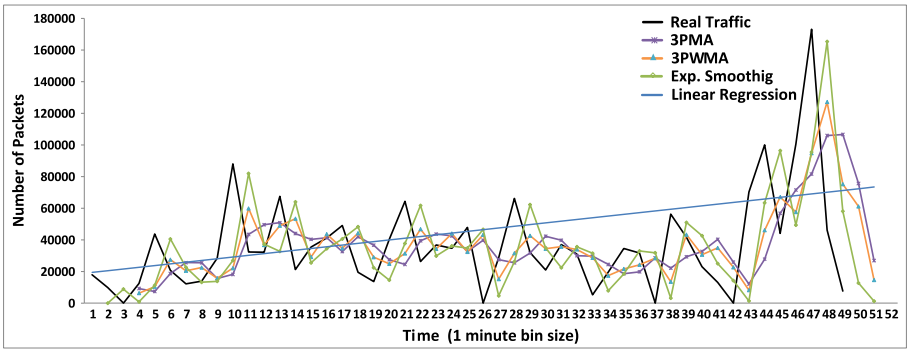

Figure 2. TCP SYN flooding on an HTTP server - intensity distribution and prediction.

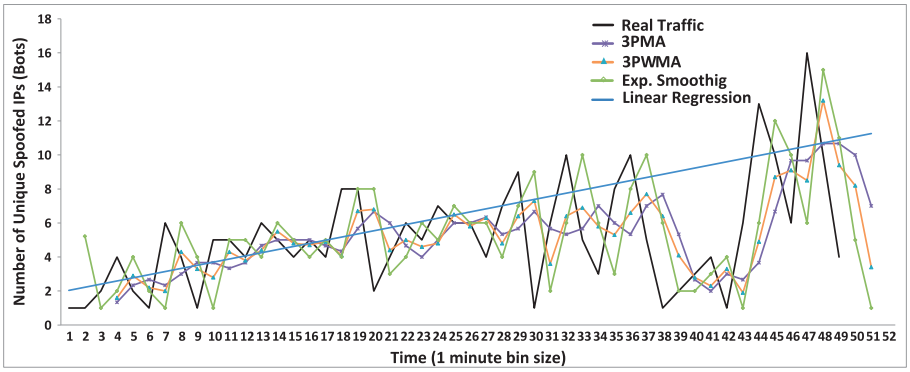

Figure 3. TCP SYN flooding on an HTTP server - size distribution and prediction.

Table III. TCP SYN flooding on an HTTP server - absolute prediction error (%).

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

48th minute. Similar to the intensity, it is shown from the prediction techniques that the size will decrease as well, 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 III.

Notice that all the techniques for both impact features (rate/intensity and number of involved machines) recorded an error less than 1%. Further, the ES algorithm was best in predicting the intensity, whereas the LR was best in predicting the size of the attack. This case study allows the organization whose Web server is under a targeted DDoS to gain insight on 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.

4.0.2. TCP SYN flooding on a DNS server.

This case study refers to a DDoS TCP SYN flooding targeting a DNS server. From Table II, we notice that this attack generated around 29 000 TCP SYN packets, with an average of eight packets per second from 206 unique spoofed IPs (i.e., bots). Although the size of this DDoS attack is larger than the one of the first case study, its intensity in terms of the generated packets and hence rate is significantly lower.

Figures 4 and 5 demonstrate the application of the forecasting techniques on the DNS server. We also predicted this DDoS attack because its corresponding DFA result was shown to be "correlated" with a value of 0.93. Figure 4 illustrates the attack's intensity and prediction distributions. It is shown that the attack peaks around 1600 packets at the 19th minute. The predicted values of such distribution show an 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 45th 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 IV.

Notice that the LR poorly performs with regard to this case study. Moreover, the ES algorithm was best in predicting both the intensity and the size. This case study allows

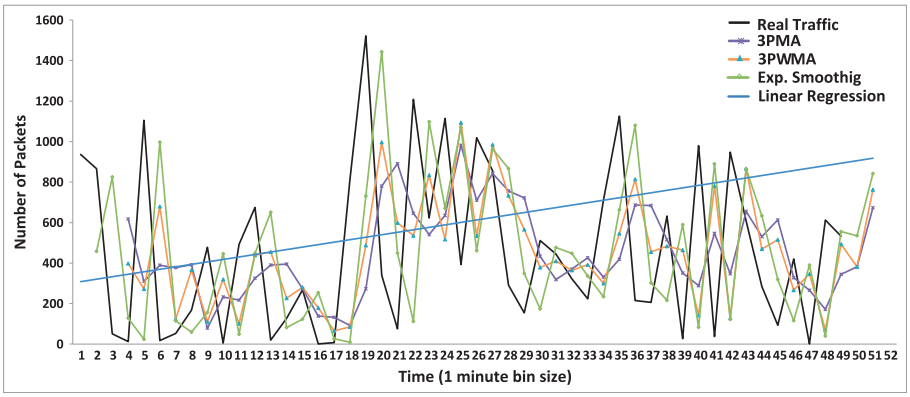

Figure 4. TCP SYN flooding on a DNS server - intensity distribution and prediction.

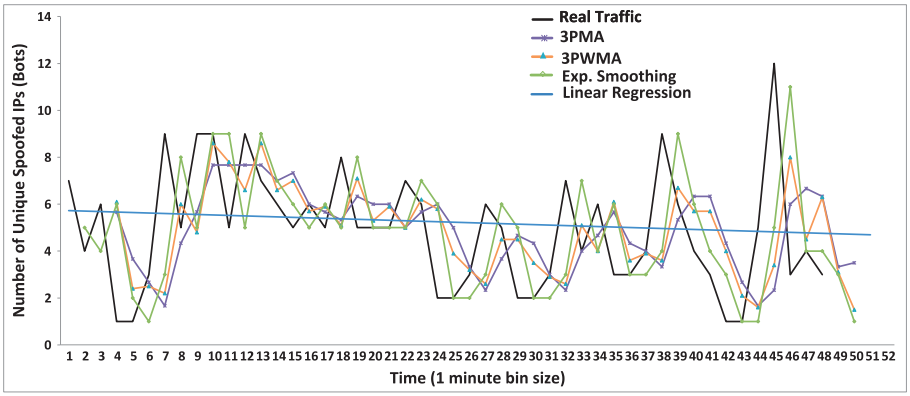

Figure 5. TCP SYN flooding on a DNS server - size distribution and prediction.

Table IV. TCP SYN flooding on a DNS server - absolute prediction error (%).

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

the organization whose DNS server is under a DDoS 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.

4.0.3. TCP SYN flooding on multiple HTTP servers.

We now move our attention to elaborate on the results of the DDoS campaign clustering approach. Recall that the aim is rendered by the capability to infer multiple victims that are being the target of the same campaign. This facilitates the fingerprinting of the type and scope of the DDoS campaign, as previously mentioned in Section 3.6.

To demonstrate the effectiveness of the approach, we experiment with a 1-day sample retrieved from our darknet dataset. In accordance with the approach of Section 3.6, we extract 680 backscattered DDoS sessions and apply fuzzy hashing between the sessions, by leveraging deeptoad,[†] a fuzzy hashing implementation. The outcome of this operation is depicted in Figure 6, where the victims are represented by round circles while directed arrows illustrate how the various victims were shown to be statistically close to other targeted victims. It is important to note that we anonymize the real identity of the victims due to sensitivity and legal reasons. Subsequently, the Euclidean and Kolmogorov–Smirnov tests are executed to exactly pinpoint and cluster the victims that demonstrate significant traffic similarity. Figure 7 shows such result, whereas Table V summarizes the outcome of the proposed DDoS campaign clustering approach. From Figure 7, one can notice the formation of root nodes, advocating that the approach is successful in clustering various victims that are the target of the same DDoS campaign.

In general, the approach yielded, for 1-day dataset, 13 unique campaigns where each campaign clusters a number of victims ranging from 2 to 125 targets. Recall that the fusion technique resembles the execution and overlap of

[†]https://code.google.com/p/deeptoad/

Table V. Summary of the DDoS campaign clustering approach.

Technique	Unique campaign count	Campaign of 2 victim machines	Campaign of 3 victim machines	Campaign of 4 victim machines	Campaign of 5 victim machines	Campaign of 6 victim machines	Campaign of 125 victim machines
Euclidean	16	6	2	3	3	1	1
Kolmogorov–Smirnov	16	6	2	3	2	2	1
Fusion	13	6	1	2	2	1	1

Table VI. Summary of the analyzed DDoS campaign case study.

Case study	Victim	Analyzed attack duration (seconds)	Intensity (packet)	Average rate (pps)	DFA value	Size of spoofed IPs
TCP SYN flooding (HTTP)	125	85322	649299	7.61	0.81	92296

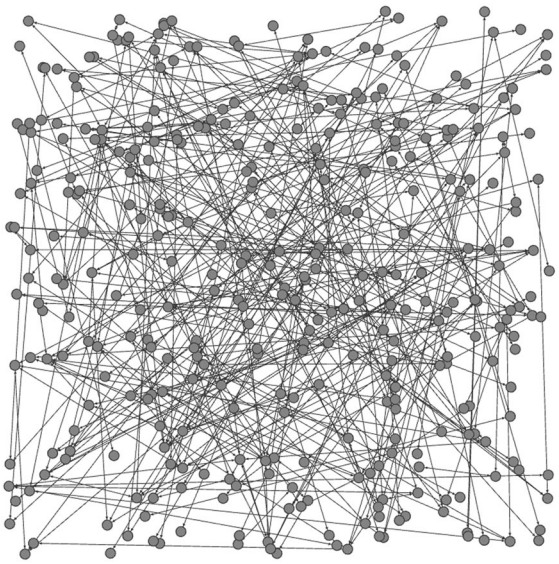

Figure 6. Clustered victims through fuzzy hashing.

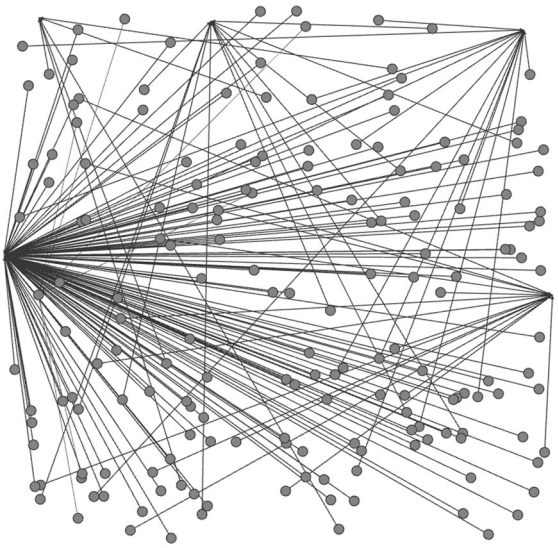

Figure 7. Clustered victims through the fusion technique.

the Euclidean and Kolmogorov–Smirnov statistical tests, as previously discussed in Section 3.6.

We proceed by attempting to predict the impact features, namely intensity and size, of one of the previously inferred DDoS campaigns. We select the last campaign of Table V because it targeted the most victims.

Table VII. TCP SYN DDoS campaign flooding on multiple HTTP servers: absolute prediction error (%).

	Prediction techniques			
	MA	WMA	ES	LR
Intensity	1.27	1.51	0.09	2.16
Size	1.26	1.11	0.09	2.14

This case study refers to a campaign of DDoS TCP SYN flooding targeting various HTTP servers related to 16 victim organizations. From Table VI, we notice that this campaign lasted almost 1 day and generated around 650 000 TCP SYN packets, with an average of seven packets per second from 92 296 unique spoofed IPs (i.e., bots). Further, Figures 8 and 9 depict the characterization and demonstrate the application of the forecasting techniques. We also predicted this DDoS attack because its corresponding DFA result was shown to be "correlated" with a value of 0.81. Figure 8 illustrates the attack's intensity and prediction distributions. It is shown that the attack peaks around 8000 packets at the 47th minute. The predicted values of such distribution shows insights of decrease in the attack's intensity. On the other hand, Figure 9 reveals the attack's size in terms of number of used compromised machines/bots. It is shown that the number of spoofed

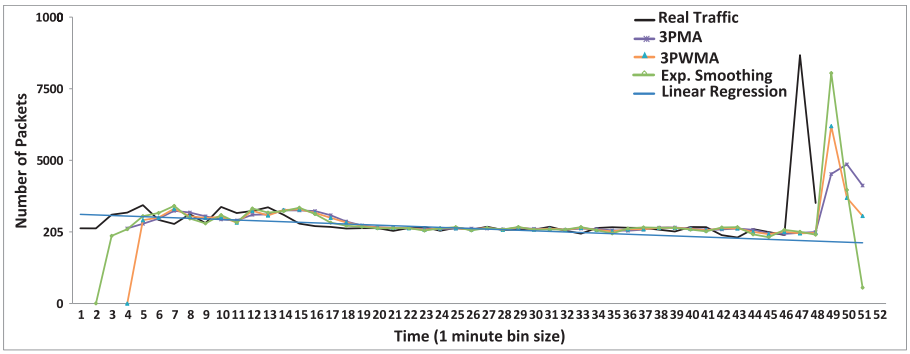

Figure 8. TCP SYN DDoS campaign flooding on multiple HTTP servers - intensity distribution and prediction.

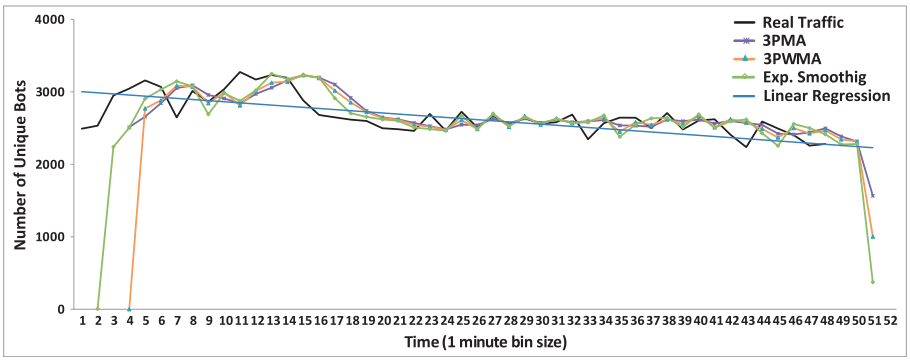

Figure 9. TCP SYN DDoS campaign flooding on multiple HTTP servers - size distribution and prediction.

IPs peaks to 3100 in the 10th minute. Furthermore, it is shown from the prediction models that the attack size will stay constant for some time and then decreases. The absolute prediction error of the forecasting techniques for this DDoS campaign case study is summarized in Table VII. Notice that the LR poorly performs with regard to this case study. Moreover, the ES algorithm was best in predicting both the intensity and the size.

It should be noted that the generated inferences from all the aforementioned case studies aim to better understand the scale, rate, and trend of DDoS attacks. This study 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.

5. CONCLUSION

This paper first proposed an approach that is rendered by a DDoS inference and forecasting model. The aim is to provide the organization under attack the capability to comprehend the situation and hence adaptively respond to the threat. Second, the paper proposed a DDoS campaign clustering approach that captures the similarity between backscattered sessions. The goal is to cluster various victims that are targeted by the same DDoS campaign. We characterized and predicted, within minutes, the attacks' impact features, namely intensity/rate (packets/sec) and size (number of used compromised machines/bots). Our proposed approaches leverage 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 or graph theory and long-term bases as well as implementing our proposed approach in a real-time fashion.

REFERENCES

1. Arbor Networks. Infrastructure Security Report, 2012. http://tinyurl.com/ag6tht4 [accessed on April 2013].
2. Forbes. Testing The Limits, LulzSec Takes Down CIA's Website. http://tinyurl.com/bfhzbta [accessed on July 2014].
3. ITPRO. InfoSec 2011: Energy Firms Pummelled by DDoS Attacks. http://tinyurl.com/cpqodbx [accessed on March 2013].

4. PcWorld. Hacker Arrested for DDoS Attacks on Amazon.com. http://tinyurl.com/d22myng [accessed on July 2014].
5. Ars Technica. When Spammers Go to War: Behind the Spamhaus DDoS, 2013. http://tinyurl.com/d9vkegg [accessed on April 2013].
6. Cnet. Amazon Suffers U.S. Outage on Friday, 2013. http://news.cnet.com/8301-10784_3-9962010-7.html [accessed on October 2013].
7. Kuzmanovic A, Knightly EW. 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, New York, NY, USA, 2003; 75–86.
8. Park N, Park WH. Cyber threat prediction model using security monitoring system event. In *IT Convergence and Security 2012*. Springer, South Korea, 2013; 233–239.
9. Dagon D, Zou CC, Lee W. Modeling botnet propagation using time zones. In *Proceedings of the 13th Network and Distributed System Security Symposium,* NDSS, San Diego, California, USA, 2006; 2–13.
10. Fachkha C, Bou-Harb E, Boukhtouta A, Dinh S, Iqbal F, Debbabi M. 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; 1–8.
11. Qibo S, Shangguang W, Danfeng Y, Fangchun Y. ARM-CPD: detecting SYN flooding attack by traffic prediction. In *2nd IEEE International Conference on Broadband Network & Multimedia Technology (IC-BNMT'09),* IEEE, Beijing, China, 2009; 443–447.
12. Park H, Jung S-OD, Lee H, In HP. Cyber weather forecasting: forecasting unknown internet worms using randomness analysis. In *Information Security and Privacy Research*. Springer, 2012; 376–387.
13. Moore D, Shannon C, Brown DJ, Voelker GM, Savage S. Inferring internet denial-of-service activity. *ACM Transactions on Computer Systems (TOCS)* 2006; **24** (2): 115–139.
14. Czyz J, Lady K, Miller SG, Bailey M, Kallitsis M, Karir M. Understanding IPv6 internet background radiation. In *Proceedings of the 13th ACM SIGCOMM Conference on Internet Measurement (IMC 13)*, Barcelona, Spain, 2013; 105–118.
15. Dainotti A, King A, Claffy KC, Papale F, Pescape A. Analysis of a/0 stealth scan from a botnet. In *Proceedings of the 2012 ACM Conference on Internet Measurement Conference,* ACM, Boston, Massachusetts, USA, 2012; 1–14.
16. Benson K, Dainotti A, Claffy KC, Aben E. Gaining insight into as-level outages through analysis of internet background radiation. In *2013 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS),* IEEE, New York, NY, USA, 2013; 447–452.
17. Dainotti A, Benson K, King A, Claffy KC, Kallitsis M, Glatz E, Dimitropoulos X. Estimating internet address space usage through passive measurements. *SIGCOMM Computer Communication Review* 2013; **44**(1): 42–49.
18. Irwin B. A baseline study of potentially malicious activity across five network telescopes. In *5th International Conference on Cyber Conflict (CyCon)*, Tallinn, Estonia, June 2013; 1–17.
19. King A, Huffaker B, Dainotti A, Claffy KC. A coordinated view of the temporal evolution of large-scale internet events. *Computing* 2014; **96**(1): 53–65.
20. Quan L, Heidemann J, Pradkin Y. Trinocular: understanding internet reliability through adaptive probing. In *Proceedings of the ACM SIGCOMM 2013 Conference on SIGCOMM,* ACM, 2013; 255–266.
21. Bailey M, Cooke E, Jahanian F, Nazario J, Watson D. The internet motion sensor: a distributed blackhole monitoring system. In *Proceedings of the 12th ISOC Symposium on Network and Distributed Systems Security (SNDSS)*, San Diego, California, USA, 2005; 167–179.
22. Team Cymru - Community Services. The Darknet Project. http://www.cymru.com/Darknet [accessed on July 2014].
23. Yegneswaran V, Barford P, Plonka D. On the design and use of internet sinks for network abuse monitoring. In *Recent Advances in Intrusion Detection,* Springer: Sophia Antipolis, France, 2004; 146–165.
24. Fachkha C, Bou-Harb E, Debbabi M. Fingerprinting internet DNS amplification DDoS activities. In *Proceeding of the 6th International Conference on New Technologies, Mobility and Security, NTMS,* IEEE, UAE, Dubai, 2014; 1–5.
25. Bou-Harb E, Debbabi M, Assi C. Cyber scanning: a comprehensive survey. *IEEE Communications Surveys Tutorials* 2013; **PP**(99): 1–24.
26. Bou-Harb E, Debbabi M, Assi C. On fingerprinting probing activities. *Computers & Security* 2014; **43**: 35–48.
27. Wustrow E, Karir M, Bailey M, Jahanian F, Huston G. Internet background radiation revisited. In *Proceedings of the 10th Annual Conference on Internet Measurement,* ACM, New York, NY, USA, 2010; 62–74.
28. Li Z, Goyal A, Chen Y, Paxson V. Towards situational awareness of large-scale botnet probing events. *IEEE*

Transactions on Information Forensics and Security 2011; **6**(1): 175–188.
29. Hamilton JD. *Time Series Analysis*, Vol. 2. Cambridge Univ Press, 1994.
30. Peng C-K, Buldyrev SV, Havlin S, Simons M, Stanley HE, Goldberger AL. Mosaic organization of dna nucleotides. *Physical Review E* 1994; **49**(2): 1685.
31. Priestley MB. *Spectral Analysis and Time Series*. Academic Press, 1981.
32. Matos J, Gama S, Ruskin HJ, Sharkasi AA, Crane M. Time and scale hurst exponent analysis for financial markets. *Physica A: Statistical Mechanics and its Applications* 2008; **387**(15): 3910–3915.
33. Hu K, Ivanov PCh, Chen Z, Carpena P, Stanley HE. Effect of trends on detrended fluctuation analysis. *Physical Review E* 2001; **64**(1): 011114.
34. Fukuda K, Hirotsu T, Akashi O, Sugawara T. Correlation among piecewise unwanted traffic time series. In *Global Telecommunications Conference, IEEE GLOBECOM*, 2008; 1–5.
35. Zhou B, He D, Sun Z, Ng WH. Network traffic modeling and prediction with ARIMA/GARCH. In *Proceedings of HET-NETs Conference*, Citeseer, 2005; 1–10.
36. Zhuang Y, Chen L, Wang XS, Lian J. A weighted moving average-based approach for cleaning sensor data. In *27th International Conference on Distributed Computing Systems ICDCS*, Toronto, Ontario, Canada, 2007; 38–38.
37. Fylstra D, Lasdon L, Watson J, Waren A. Design and use of the microsoft excel solver. *Interfaces* 1998; **28** (5): 29–55.
38. Wong W-K, Manzur M, Chew B-K. How rewarding is technical analysis? Evidence from singapore stock market. *Applied Financial Economics* 2003; **13** (7): 543–551.
39. Papadopouli M, Raftopoulos E, Shen H. Evaluation of short-term traffic forecasting algorithms in wireless networks. In *2nd Conference on Next Generation Internet Design and Engineering, NGI,* IEEE, Valencia, Spain, 2006; 8–pp.
40. The University of Texas at Austin. *Time Series and Forecasting*, 2002. http://tinyurl.com/bsxscwx [accessed on April 2013].
41. Goia A, May C, Fusai G. Functional clustering and linear regression for peak load forecasting. *International Journal of Forecasting* 2010; **26**(4): 700–711.
42. Kornblum J. Identifying almost identical files using context triggered piecewise hashing. *Digital Investigation* 2006; 3: 91–97. The Proceedings of the 6th Annual Digital Forensic Research Workshop (DFRWS '06).
43. Huang Y-P, Chang T-W, Sandnes F-E. An efficient fuzzy hashing model for image retrieval. In *Annual Meeting of the North American Fuzzy information Processing Society (NAFIPS)*, Montreal, Quebec, Canada, 2006; 223–228.
44. Lilliefors HW. On the Kolmogorov-Smirnov test for normality with mean and variance unknown. *Journal of the American Statistical Association* 1967; **62**(318): 399–402.
45. Little M, McSharry P, Moroz I, Roberts S. Nonlinear, biophysically-informed speech pathology detection. In *International Conference on Acoustics, Speech and Signal Processing (ICASSP),* volume 2, IEEE, Toulouse, France, 2006; II–II.

Claude Fachkha earned a Bachelor of Engineering in Computer and Telecommunication from Notre Dame University in 2008, then enrolled at Concordia and completed a Masters of Engineering in Information Systems Security with high distinction 2 years later. After receiving a 4-year scholarship, he is continuing his studies at Concordia as a PhD candidate in Electrical and Computer Engineering. In 2013, Claude has been awarded the prestigious FQRNT award. In addition to his work as a research assistant for various graduate cyber security courses and projects, Claude is the President of the Engineering and Computer Science Alumni Chapter. Further, he served as a Vice President at the Engineering and Computer Science Graduate Association and a councilor at the Graduate Student Associations. Moreover, Claude is affiliated with the National Cyber Forensics and Training Alliance (NCFTA, Canada). His research focuses on analyzing large-scale Internet threats such as Distributed Denial of Service attacks, botnet, malware and scanning activities.

Elias Bou-Harb is a network security researcher pursuing his PhD in Computer Science at Concordia University, Montreal, Canada. Previously, he has completed his MASc degree in Information Systems Security at the Concordia Institute for Information Systems Engineering. He is also a member of the NCFTA, Canada. His research interests focus on the broad area of cyber security, including operational cyber security for critical infrastructure, LTE 4G mobile network security, VoIP attacks and countermeasures and cyber scanning campaigns. He is supported by the prestigious Alexander Graham Bell Canada Graduate Scholarship from the Natural Sciences and Engineering Research Council of Canada.

Dr Mourad Debbabi is a Full Professor at the Concordia Institute for Information Systems Engineering. He holds the Concordia Research Chair Tier I in Information Systems Security. He is also the President of the NCFTA (Canada). He is the founder and one of the leaders of the Computer Security Laboratory at Concordia University. In the past, he was the Specification Lead of four Standard Java Intelligent Networks Java Specification Requests dedicated to the elaboration of standard specifications for presence and instant messaging. Dr Debbabi holds PhD and MSc degrees in computer science from Paris-XI Orsay, University, France. He published two books more than 230 research papers in journals and conferences on computer security, cyber forensics, privacy, cryptographic protocols, threat intelligence generation, malware analysis, reverse engineering, specification and verification of safety-critical systems, formal methods, Java security and acceleration, programming languages and type theory. He supervised to successful completion 20 PhD students and more than 60 Master students. He served as a Senior Scientist at the Panasonic Information and Network Technologies Laboratory, Princeton, New Jersey, USA; Associate Professor at the Computer Science Department of Laval University, Quebec, Canada; Senior Scientist at General Electric Research Center, New York, USA; Research Associate at the Computer Science Department of Stanford University, California, USA; and Permanent Researcher at the Bull Corporate Research Center, Paris, France.

Wirel. Commun. Mob. Comput. 2015; **15**:1066–1078 © 2014 John Wiley & Sons, Ltd.
DOI: 10.1002/wcm