COMPUTERS & SECURITY 82 (2019) 284–295

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Efficient DDoS flood attack detection using dynamic thresholding on flow-based network traffic☆

Jisa David[a,*], *Ciza Thomas*[b]

[a] *Department of Electronics and Communication Engineering, Rajagiri School of Engineering and Technology, Kerala, India*

[b] *Department of Electronics and Communication Engineering, College of Engineering Trivandrum, Kerala India*

ARTICLE INFO

Article history:
Received 7 July 2018
Revised 2 December 2018
Accepted 2 January 2019
Available online 11 January 2019

Keywords:
DDoS attack
Network security
Dynamic threshold
Network traffic
Traffic features

ABSTRACT

Internet applications are used in various sectors as it contributes in enhancing the system usage in many respects. However, the interconnected computer systems and networks are vulnerable to very large number of attacks; Distributed Denial of Service being a major one. This paper analyses the features of network traffic and the existing algorithms to detect Distributed Denial of Service attacks and proposes an efficient statistical approach to detect the attacks based on traffic features and dynamic threshold detection algorithm. Dynamic threshold is made use of since both network activities and user's behaviour could vary over time. The proposed algorithm extract different traffic features, calculate four attributes based on the characteristics of Distributed Denial of Service and the attack gets detected when the calculated attributes within a time interval is greater than the threshold value. MIT Lincoln Laboratory DARPA datasets and dataset developed in an university laboratory are used to validate the algorithm and the model proposed in this paper and also to measure the performance of the proposed approach. Experimental results demonstrate the improved performance of the proposed approach with significantly higher detection rate and accuracy and lesser processing time compared to the existing methods.

1. Introduction

Internet usage through various applications have evolved in modern times in leap and bounds. Along with the exponential increase in the usage of Internet and advances in Internet, the security threats especially Denial of Service (DoS) and Distributed Denial of Service (DDoS) have also increased in an exponential fashion. A typical example is the interruption in Amazon's services for almost two hours on oct 21, 2016 due to DDoS attack. Such interruptions in the services cause huge financial loss, which also exponentially increases with time. The loss was $209 million in the first quarter of 2016 as compared to $24 million for all of 2015 (Gillison, 2016). According to the Worldwide Infrastructure Security Report (Network, 2015), high-rate DDoS attacks (HR-DDoS) are leading nowadays, having traffic volume more than 600 Gbps. It is very difficult to detect such high-rate DDoS attacks in real time in order to ensure the timely delivery of the widely used Internet-based services and applications.

DoS and DDoS have become a major challenge in the networks as it affects the networks in different significant levels.

☆ Fully documented templates are available in the elsarticle package on CTAN since 1880.

* Corresponding author.
E-mail addresses: jisadavid@yahoo.com, jisa_d@rajagiritech.edu.in (J. David).

https://doi.org/10.1016/j.cose.2019.01.002
0167-4048/

As DoS attacks are one-to-one attack, using only one compromised host, it influences only smaller network bandwidth. Also, the severity of the after effects are less comparatively. The DDoS uses multiple compromised hosts or zombies and will flood the system/network with a large traffic that will overwhelm the victim machine or its network. DoS occurs by significantly consuming victim machine's bandwidth or key resources, preventing service provision to legitimate users, resulting in authorized service denial. DDoS usually exploits the immense resource limitations at the victim compared to the Internet. Due to its many-to-one attack dimension, the DDoS are successful in blocking the victim against its defence measures. This leads to traffic overhead and bandwidth wastage. Recently, botnet is used as an attacking platform to form large scale of flooding DDoS attacks, and attack flows become more distributed and even more harmful, making it increasingly hard to detect effectively (Mirkovic and Reiher, 2004).

The threatening fact is that there are so many automated tools available today, which increases the severity of the attacks. These are readily available in the software market at a very low cost, which makes it easily accessible to attackers. Also, these are designed in a very user-friendly manner, and there is no need of much technical knowledge in using these tools. It takes very less time to install the tool and attack the vulnerable machines. Trin00, TFN, Tribe Flood Network 2000 (TFN2K) and Stacheldraht are tools that are being used to launch even stealthier attacks.

In case of Trinoo or Trin00, initially attacker will find out systems which are having some vulnerability in security aspects. Now the attacker will compromise these systems, exploiting the available vulnerabilities. The compromised systems can be considered as a handler or master daemon of the attacker. Using these handlers, the attacker will find out other machines in different networks having security based vulnerabilities and they will run the script to convert them to compromised hosts of the handlers. These are referred as Daemons. Through these Daemons, Trin00 is capable of conducting very powerful attacks that spreads through different networks. It is capable of conducting TCP-SYN flooding, ICMP-flooding, UDP flooding, smurfing etc. Also, it is capable of creating packets with spoofed IPs. TFN, Tribe Flood Network 2000 (TFN2K) and Stacheldraht are enhanced versions of Trin00.

Hussain et al. (2003) proposed an efficient frame work for detecting the Denial of Service attacks using the header details, transient ramp-up behavior and spectral analysis. Even though the header can easily be forged, the detection becomes successful in their work as attack ramp-up and attack spectrum characteristics are extremely difficult to spoof.

Feinstein et al. (2003) in their work suggest that DDoS attacks can be detected by computing the entropy and frequency-sorted distributions of selected packet attributes. This is because DDoS attacks show anomalies in the characteristics of selected packet attributes. The results of their work indicate that these methods can be effective against DDoS attacks and provide recommendations for improving detection of more stealthy attacks. They also describe detection-response prototype and how the detectors can be extended to make effective response decisions.

Braga et al. (2010); Feng et al. (2009); Kim et al. (2004) propose a method for DDoS attack detection based on traffic flow features. The extraction of the information is done with a very low overhead compared to traditional approaches. Entropy based approaches have been proposed in the literature using different variations of entropy and divergence measures. However, Shannon entropy, Renyi entropy, Tsallis entropy Kullback–Leiber distance and generalized information distance are used commonly to detect different types of DDoS attacks (Ma and Chen, 2014; Nychis et al., 2008; Wang et al., 2010; Yu and Zhou, 2008; Zhang et al., 2010).

In DDoS attack detection, different time series models are used for preprocessing network traffic (Cabrera et al., 2001; Chen et al., 2013). However, these approaches takes large computation time for processing. Hence, its very difficult for early detection of DDoS attack.

According to the survey, Gillison (2016) conducted regarding DoS and DDoS it is found to be increasing in an exponential fashion every year. If an organization is not properly protected from these types of attacks, the systems might get infected leading to financial loss and reputational damage for the organization. Hence, for the survival of any organization, it is a vital factor to have proper security measures. This is pointing to the fact that with the presently available measures, there is still room for improvement in detection and counter measure mechanism.

The rest of this paper is organized as follows: Section 2 reviews the related work, Section 3 describes the proposed approach, Section 4 provides details on experimental simulation setup and its validation and Section 5 concludes the paper.

2. Related work

Different DDoS attack detection techniques have been proposed by many researchers. Advancement in technology has brought latest detecting algorithms and metrics.

Nezhad et al. (2016) suggest an ARIMA time series model used to predict the number of packets in every minute. Then, the chaotic behavior of prediction error time series is examined by computing the maximum Lyapunov exponent. This approach is not suitable to detect DDoS attack and introduce many false positives and computation time is more because the method uses time series model. Qin et al. (2015) introduce a novel entropy-based DDoS attack detection method. The entropy vectors of different features are found from the traffic flows and the normal patterns are modeled using clustering algorithm. This approach cannot detect new attacks and its computation time is high.

Bhuyan et al. (2015b) propose the Partial Rank Correlation based Detection (PRCD) scheme to detect both low-rate and high-rate DDoS attacks. This method is based on static threshold so that its detection accuracy is less. Jun et al. (2014) propose a DDoS attack detection system by using packet sampling and flow feature in order to guarantee the transmission of normal traffic and prevent the flood of abnormal traffic. This method is based on fixed threshold and hence its detection accuracy is less.

Dong et al. (2016) suggest effective detection method for DDoS attack and also locate the compromised interfaces the malicious attackers have connected. In this method, flow events associated with an interface are first classified

Table 1 – Summary of related work.

References	Methdology	Performance
Nezhad et al. (2016)	ARIMA time series model is used to predict the number of packets in every minute and is examined by computing the maximum Lyapunov exponent.	Can classify chaotic and non chaotic behaviours. Disadvantages are high false positives and increased computation time as time series model is used.
Qin et al. (2015)	Entropy-based DDoS attack detection - The entropy vectors of different features are found from the traffic flows and the normal patterns are modelled using clustering algorithm.	Can achieve high detection accuracy with larger training dataset size. Disadvantages include increased computational complexity and inability to detect new attacks.
Bhuyan et al. (2015b)	Partial Rank Correlation based Detection (PRCD) scheme to detect DDoS attacks.	Can detect low rate and high rate DDoS attacks. Method is based on static threshold and hence its detection accuracy is less.
Jun et al. (2014)	Packet sampling and flow feature.	Able to control the attacker or zombie hosts once the DDoS attack is detected. Effective in detecting DDoS attack using only a small amount of traffic. Method is based on fixed threshold and hence its detection accuracy is less.
Zhang et al. (2012)	Congestion Participation Rate (CPR) to identify LDDoS flows.	Can effectively detect and filter even LDDoS attacks. Predefined CPR threshold leading to reduced detection accuracy.

and decision is made using Sequential Probability Ratio Test (SPRT), which has bounded false negative and false positive error rates. This approach is also based on static threshold. However network behaviour could change over time and hence detection efficiency reduces.

Chen et al. (2013) suggest a network anomaly detection algorithm (NADA) to detect the attacks on network traffic. In this approach pre-processing is done first on the network traffic by cumulative averaging with a time range followed by the simple linear AR model to generate the prediction of network traffic. The method assumes the prediction error to behave chaotically and hence use chaos theory to analyze it. Subsequently, training is done using a neural network with the attack traffic to detect DDoS attacks. This method has less attack detection rate and the computation time is more.

No and Ra (2009, 2011) suggest that DDoS attack detection using fast entropy approach shows significant reduction of computational time compared to conventional entropy computation while it maintains detection accuracy. However, the computation of entropy is still time consuming.

Wei et al. (2013), propose the Rank Correlation based Detection (RCD) algorithm as an effective method for detecting Distributed Reflection Denial of Service(DRDoS) attack. The idea behind this method is that when an attack is performed with the same attacking pattern, the corresponding flows will have the same characteristics. Once suspicious flows are found, RCD will calculate the rank correlation between flow pairs and give final alert according to preset threshold. The result gives a clear indication of the malicious flows that can be either picked out or discarded. It can differentiate reflection flows from legitimate ones efficiently and effectively. Thus it can be used as a useable indicator for DRDoS. However, they have not experimented against sophisticated scenarios and real DRDoS in the Internet.

A novel metric named Congestion Participation Rate (CPR) is proposed in the work of Zhang et al. (2012) to detect and filter Low-rate Distributed Denial of Service(LDDoS) attacks for causing network congetion. CPR is the ratio of the incoming packets during congestion to the total incoming packets. The major innovation of the CPR-based approach is its ability to identify LDDoS flows. A flow with a CPR higher than a predefined threshold is classified as an LDDoS flow, and consequently all of its packets will be dropped. By analyzing the average CPR of the difference between normal TCP flows and LDDoS flows, we can identify attack flows. Moreover this can also be applied to detect a number of variants of LDDoS attacks, such as LDDoS attacks against application servers and LDDoS attacks against 3G/WiMax wireless networks. However, more experiments and analyses using real datasets are needed to test its effectiveness.

Based on the distribution difference of the packet size, Zhou et al. (2017) propose an approach to distinguish two typical low-rate DDoS attacks, the constant attack and the pulsing attack, from legitimate traffic. An Expectation of Packet Size(EPS) based approach to measure the distribution difference of the packet size. The probability distributions of the packet size of the constant attack and the pulsing attack are quite different compared with that of legitimate traffic. The simulations are done using real datasets to demonstrate that the false-negative rate is small. The method is independent of network topology, arrival patterns, and pulse patterns of attack packets. However, the network delay caused by network congestion is not considered. Related work is summarized in Tables 1 and 2, which highlight the differences of existing approaches in terms of methodology and performance.

Most of the existing research has widely used datasets for the evaluation of the proposed schemes. It includes MIT Lincoln DARPA (DARPA, 2000), CAIDA (Hick et al., 2007), and KDD (Tavallaee et al., 2012) dataset. However, these datasets are out dated dataset in today's world, and no benchmark datasets available for the evaluation of DDoS related research (Mirkovic et al., 2006). So, for the evaluation of DDoS related work many researchers have to synthetically generates real data sets (Behal and Kumar, 2016; Bhatia et al., 2014; Bhuyan et al., 2015a; Calvet et al., 2010; Spognardi et al., 2012).

Table 2 – Summary of related work.

References	Methdology	Performance
Dong et al. (2016)	DDoS attack detection against sdn controllers by vast new low-traffic flows using Sequential Probability Ratio Test (SPRT).	Can detect DDoS attack and further locate the compromised interfaces the malicious attackers have connected. Method is based on static threshold and as the network behaviour varies with time, the detection efficiency is low.
Chen et al. (2013)	Cumulative averaging with a time range followed by the simple linear AR model is used to generate the prediction of network traffic. Subsequently, training is done with the attack traffic using a neural network.	Achieves high detection rate of 93.75%. Detection rate can be further increased with more training samples but at the expense of computation time.
Wei et al. (2013)	Rank Correlation based Detection (RCD).	Detecting DRDoS attack independent of specific protocols. Uses preset threshold and hence low detection efficiency.
No and Ra (2009, 2011)	DDoS attack detection using fast entropy approach.	Computation complexity is less compared to conventional entropy approach.
Zhou et al. (2017)	EPS(Expectation of Packet Size) based approach is used to measure the distribution difference of the packet Size and distinguish two typical low-rate DDoS attacks.	Method is independent of network topology, arrival patterns, and pulse patterns of attack packets. However, they failed to consider the network delay caused by network congestion.

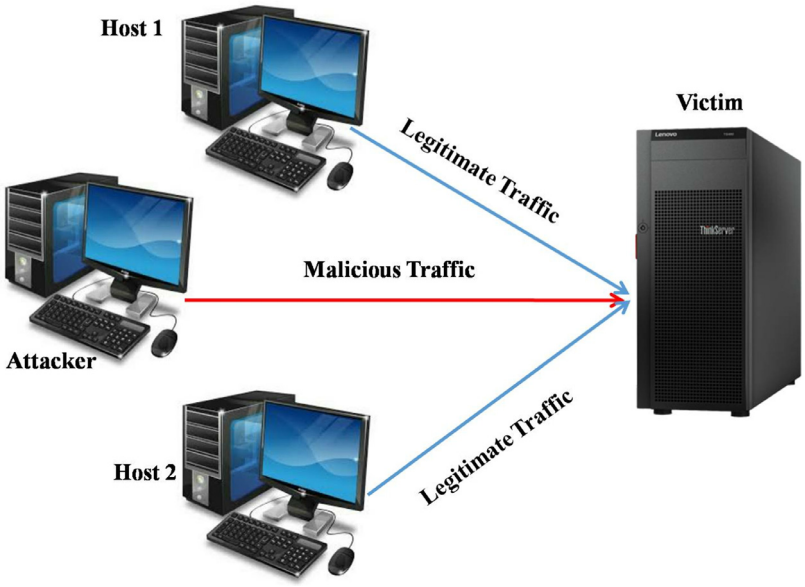

Fig. 1 – System Modelling.

In this paper, the statistic approach has been used to identify DDoS attack. Network traffic features like number of packets, sources IP, destination IP, source protocols are considered. DDoS attack is detected by applying dynamic threshold algorithm on various packet attributes. A dataset developed in the university laboratory and DARPA dataset are used to validate the analytical results.

3. Proposed approach

The proposed DDoS attack detection approach includes:

- Attack Traffic Generation
- Feature Extraction
- Dynamic Threshold Algorithm

3.1. *Attack Traffic Generation-system modeling*

It is very difficult to create a real world scenario of DDoS except through simulation. Omnet, Omnet++, Opnet, NS2, NS3 and Netsim are some of the tools used to create network setup mimicking real world scenario. However, these tools have the disadvantage of setting numerous parameters regarding LAN set up.

In this work a virtual network using Virtualbox tool is set up. Required LAN set up is shown in Fig. 1, with four virtual machines configured using Virtualbox. The legitimate clients

are identified as host1 and host2. Host1 is installed with Windows 8.1 and Host2 is installed with Ubuntu 14.04. Attacker runs Kali OS, which is equipped with several DDoS attacking tools such as Hping3, Hyenae, and Metasploit. Hping3 is normally used by system administrators and ethical hackers basically for pinging or for advanced tasks as it can bypass the firewall filter. It uses TCP, UDP, ICMP and RAW-IP protocols. It also has the traceroute mode and the ability to send files between covered channels. Hyenae is a packet generator tool that is used to create forged packets to dump the server. This tool is platform independent and is used as a network packet producer that can initiate DDoS, DoS and MITM attacks. Metasploit tool can trigger remote attacks by choosing and configuring an exploit code that enters a target system by taking advantage of one of its vulnerabilities. Metasploit runs on Unix and on Windows. This tool can also group zombies and trigger is capable of triggering remote attacks. The victim machine is having Windows12 R2 server OS and is installed with Apache web server.

3.1.1. *Generation of Attack Traffic*

The steps invloved in generation of attack traffic are as follows:

1. Turn on virtual box.
2. Turn on all virual machines(host1, host2, attacker and victim).
3. Run Wireshark on victim machine to capture packets.
4. Attacker uses hping3 or hyenae to launch different types of attacks (syn flood, IP spoof etc.).
5. Host1 and host2 access Apache web server (victim) by typing 192.168.101.28 (web browser of Ubuntu system) or airliss.vnet (web browser of Ubuntu system).
6. Wireshark captures network traffic (Attack and normal Traffic) from victim machine.

Fig. 2 shows packet capture (sample) using wire shark tool. The proposed method is evaluated using this generated attack traffic. For comparison purpose, the evaluation is also carried on DARPA 98 and DARPA 2000(LLDoS1.0)

3.2. *Feature extraction*

The DDoS attacks are identified by using a number of traffic distinguishable features. The number of packets, source IP address, destination IP address, destination port and protocol are extracted using wireshark tool. In DDoS attack situation, attacker normally chooses random source IP addresses for the same destination address (victim). Some types of DDoS attack use random destination port numbers. DDos attack uses specific packet types like ICMP or UDP flood attacks. Finally, the agents generate large volume of network packets directed towards the victim during the attack period and the network gets jammed. The large number of packets is a clear sign of occurrence of the DDoS attack.

Characteristics of traffic during DDoS attack

- Huge number of unique source IP addresses (by using DDoS attack tool).
- Destination IP address will be same. Destination port may be random.
- Huge number of packets.
- Protocol remains the same.
- Packet length will be in the range of 40–60 bytes.

Four attributes are calculated from all extracted traffic features. Each parameter is aggregated every T seconds. Let X_i be the number of packets aggregated in every ith second and considered to be first attribute($A1_i$). Let $USIP_i$ be the number of unique source IP addresses of network nodes aggregated in every ith second and considered to be second attribute($A2_i$). Let $UDIP_i$ be the number of unique destination IP addresses of network nodes in every ith second. Let Pr_i be the number of unique protocol of network nodes in every ith second. To detect DDoS attack (Source IP address is dispersed) we consider third attribute as $A3_i$ being the ratio of number of unique source IP to number of unique destination IP address in every i^{th} second as shown in Eq. (1) and to detect DoS attack (some times Source IP address is concentrated) $A3_i$ is considered to be ratio of number of packets to number of unique Destination IP address in every ith second shown in Eq. (2). Similarily considered the fourth attribute $A4_i$ as the ratio of number of unique source IP to number of unique protocol in every ith second as shown in Eq. (3) to detect DDoS attack and to detect DoS attack we consider Eq. (4). All these attribute values are normalized by dividing each attribute with its maximum value.

$$A3_i = USIP_i/UDIP_i \tag{1}$$

$$A3_i = X_i/UDIP_i \tag{2}$$

$$A4_i = USIP_i/UPR_i \tag{3}$$

$$A4_i = X_i/UPR_i \tag{4}$$

Here $NA1_i$, $NA2_i$, $NA3_i$ and $NA4_i$ are normalised attributes are considered to be 4 features to detect DDoS attack. Where

$$NA1_i = X_i/max(X_i) \tag{5}$$

$$NA2_i = A2_i/max(A2_i) \tag{6}$$

$$NA3_i = A3_i/max(A3_i) \tag{7}$$

If sourceIP addresses are dispersed, Eq. (6) will be considered. If sourceIP addresses are concentrated, then

$$NA2_i = X_i * A2_i/max(X_i * A2_i) \tag{8}$$

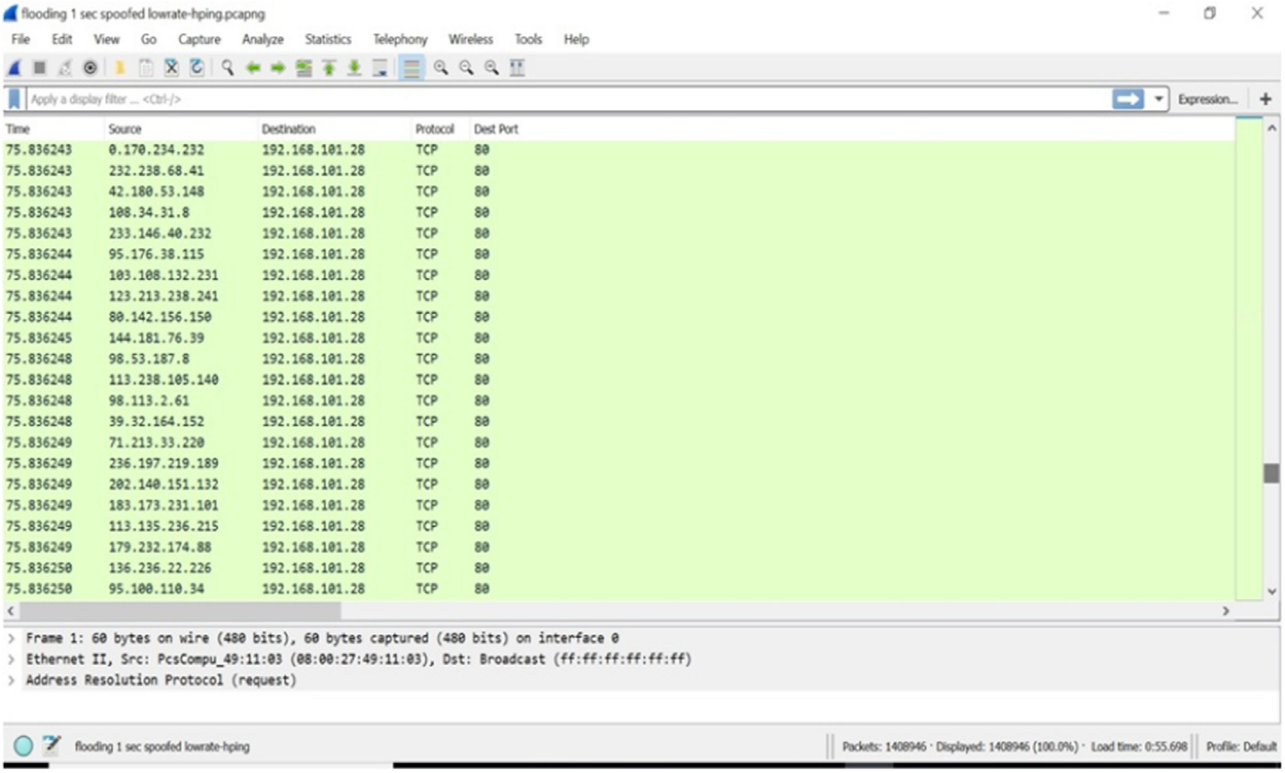

Fig. 2 – Packet capture using wireshark tool.

3.3. *DDoS detection using dynamic thresholding algorithm*

The DDoS attacks are identified using a number of distinguishable traffic features. Packet header features are extracted using wireshark tool. These features are aggregated every T seconds. Four Attributes A1, A2, A3 and A4 are computed using these extracted traffic features. The sliding window concept is used to calculate the mean (μ) and variance (σ) of different attributes. The threshold value is then adaptively changed based on the value of mean and variance of each attribute. If attribute value exceeds the threshold, it gets detected as DDoS attack.

Algorithm 1 explains the steps involved in detection process. It is a dynamic threshold algorithm applied to all the four attributes of the network traffic. Here, the mean and variance of each attribute is computed for window size K and with overlapping interval. The threshold for each attribute is determined by mean, variance and multiplication factor β. The multiplication factor β changes in accordance with the packet condition of the network traffic used in the simulation. The attack detector is unable to detect the attacks with high value of β when the attacker sends malicious traffic with small variation in traffic at the time when the channel is stable. Due to the steady channel condition and stealthy attack pattern, the detection becomes difficult with highly set value of β. On the other hand, with a burst channel and the detector having small β, the detector will be extremely sensitive. This will lead to several false positives, resulting in an inefficient detection. We obtain the trade-off between the detection rate and the false positive rate for the proposed approach through a comprehensive set of experiments. This trade-off provides experimental guidance for choosing β value in practice (David and Thomas, 2015; No and Ra, 2009; 2011). Here β is initialised with 1.5 and threshold $Th = (\mu + \sigma) * \beta$. If the mean value of current interval is twice greater than the previous interval, then β value is increased by 0.5 otherwise it is decreased by 0.5 and threshold is computed as $Th = (\mu + \sigma)/\beta$. This process is continued for all the intervals.

This algorithm is executed for all the attributes. DDoS attack is confirmed if and only if the threshold gets exceeded for all the four attributes. The proposed DDoS attack detection methdology is shown in Fig. 3.

4. Simulation results and performance analysis

The university network data set is used for analysis. MIT Lincoln Laboratory DARPA 98 (Friday of week five is used in standard) and DARPA 2000 (LLDoS1.0) data set is also used for evaluating performance of proposed algorithm (Thomas et al., 2008). In DARPAA 98, attack times are 54 minutes long continuously and in DARPA 2000 (LLDoS1.0) DDoS attack of 5 seconds duration against the victim with IP Number 131.84.1.31.

Attack Data Sets are extracted in Wireshark and the screen shot shown in Fig. 2. Here simulation result is obtained using DARPA 2000 (LLDoS1.0). By analyzing packet features, DDoS attack can be detected. During DDoS attack, packet features like the source IP addresses appear to be dispersed and

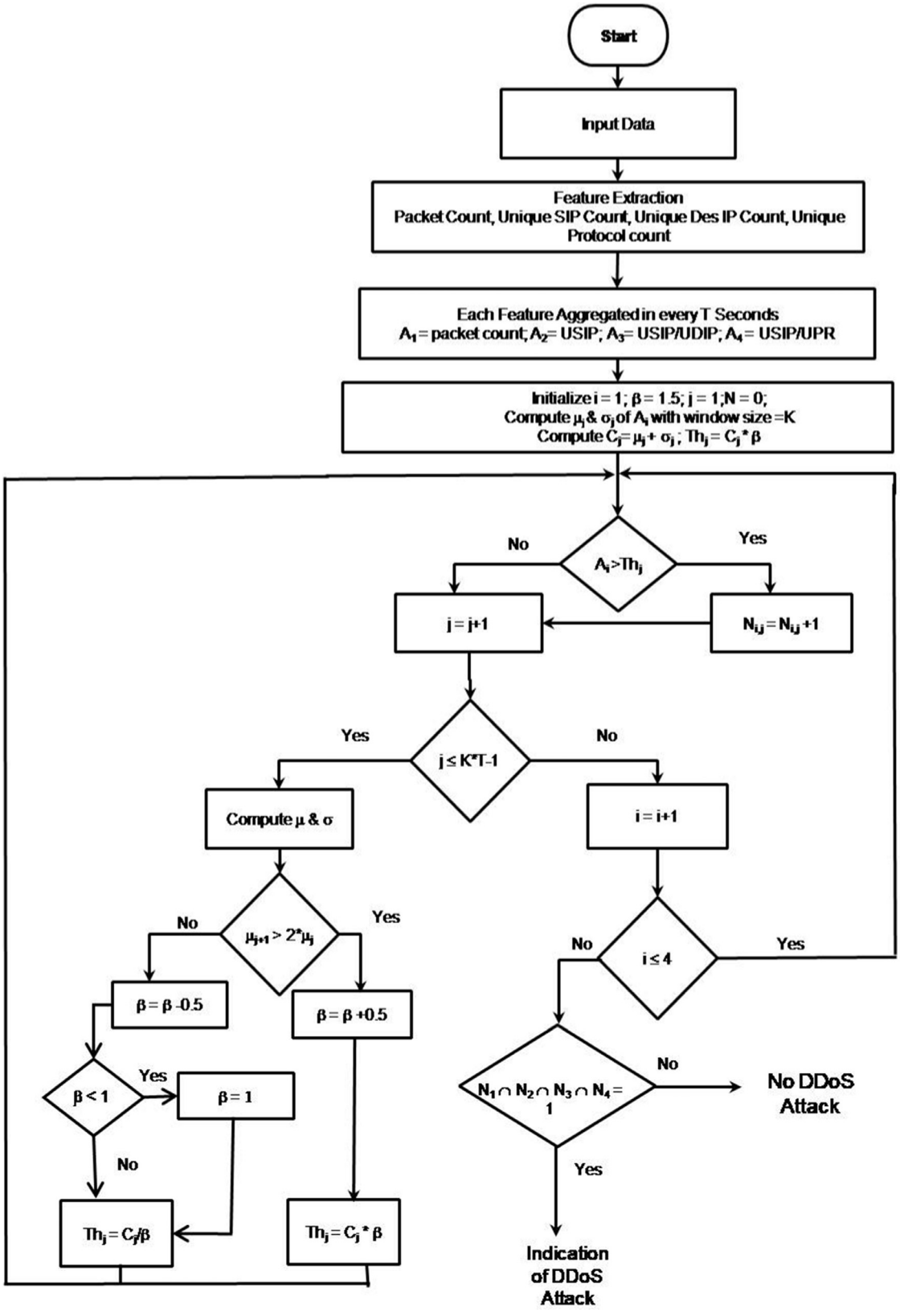

Fig. 3 – Process diagram of the proposed DDoS attack detection system.

Algorithm 1 Proposed detection algorithm.

Set
$P \leftarrow$ Period
$T \leftarrow$ Sampling interval
$K \leftarrow$ Window Size
$Th \leftarrow$ Threshold
$\beta \leftarrow$ Thresholding factor
$\mu \leftarrow$ mean
$\sigma \leftarrow$ Variance
Initialize $\beta = 1.5$
Analyze the Traffic and extract packet header features and aggregate every T seconds
Compute four Attributes A1, A2, A3 and A4
Consider first attribute A1
Compute μ_j and σ_j of A1; $C_j = \mu_j + \sigma_j$ with window size = K
Compute $Th = C_j * \beta$
if $A_1 > Th$ **then**
    indicate chance of DDoS attack ▷ one condition is satisfied
else
    not DDoS attack ▷ confirmed not a DDoS attack
end if
Compute μ_{j+1} and σ_{j+1} of A1; $C_{j+1} = \mu_{j+1} + \sigma_{j+1}$
if $\mu_{(j+1)} > 2 * \mu_j$ **then,**
    $\beta = \beta + 0.5$ (where j+1 is the next overlapping sampling interval)
    $Th = C_j * \beta$
else
    $\beta = \beta - 0.5$
    $Th = C_j/\beta$
    if $\beta < 1$ **then**
        $\beta = 1$
    end if
end if
Repeat steps 8 to 23 for next attribute till all attributes are done.
DDoS attack is confirmed if and only if the algorithm for four attributes exceeds the threshold.
The algorithm detects attack for two attributes and violates for other attribute, then that is not DDoS attack.

destination IP address is concentrated to a single victim. The attacker is seen to scan on different destination ports using the same protocol.

We choose to group the packets in every three seconds (DARA 2000 data set) and in every one minute (DARPA 98 Dataset); its execution is done on MATLAB. In the analysis, we compute unique source IPs, unique destination IPs and unique protocol in every three seconds.

In Figs. 4–7 the number of packets, unique source IPs, unique destination IPs and unique protocols is plotted respectively. If number of source IPs and destination IPs addresses is almost same at the same interval, then in most of the cases the traffic flow between source systems and destination systems are one to one communication.

In Fig. 4, number of packets is maximum for certain period. In Fig. 5, number of unique source IP is maximum during a particular time interval. This indicates that during this interval the source IPs are dispersed.

In Figs. 6 and 7 unique number of destination IP and unique number of protocol are minimum during that same interval, which indicates destination IPs and protocol are concentrated. Therefore these graphs show an indication of DDoS attack in that interval. Also, different packet features are considered in attack detection (Feinstein et al., 2003).

Attack detection is done based on dynamic threshold algorithm. This algorithm is applied for each traffic parameter. Fig. 8 show the attack detection using different attributes with some false positives. DDoS attack is confirmed if and only if the all the four attributes exceeds the threshold. Fig. 9 shows attack detection using four attributes.

Since the proposed method is not based on any time series models, its processing time is very less.

The accuracy, precision, sensitivity and specificity are used for performance evaluation of the proposed algorithm. Detection Rate or sensitivity (TPR) measures the percentage of correctly identified attacks over all the actual attacks and is computed using Eq. (9).

$$Sensitivity(TPR) = \frac{TP}{TP + FN} \tag{9}$$

Accuracy measures the percentage of true detection over the entire traffic trace and is computed using Eq. (10).

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{10}$$

Specificity(TNR) relates to the test's ability to correctly detect traffic without attack. The specificity is computed by the Eq. (11).

$$Specificity(TNR) = \frac{TN}{TN + FP} \tag{11}$$

Preci sion is the positive predictive value or the fraction of the positive predictions that are actually positive and it is computed by Eq. (12)

$$Precision = \frac{TP}{TP + FP} \tag{12}$$

where True Positive(TP) indicate the correct predictions of the DDoS attack and False Positive (FP) refers to the normal traffic incorrectly classified as DDoS attack. True Negative (TN) refers to the normal data correctly classified as normal data. False Negative (FN) refers to the DDoS attack traffic incorrectly classified as normal traffic (Elhamahmy et al., 2010).

Table 3 shows a comparative study of existing method and performance for proposed method. Here time interval (T) allotted for DARPA 98 is 1 min, DARPA 2000 and generated dataset is 3 s. In existing method (Nezhad et al., 2016) first 100 samples of DARPA 98 dataset are not considered for evaluation and hence it gives better TNR compared to proposed method for this data set.

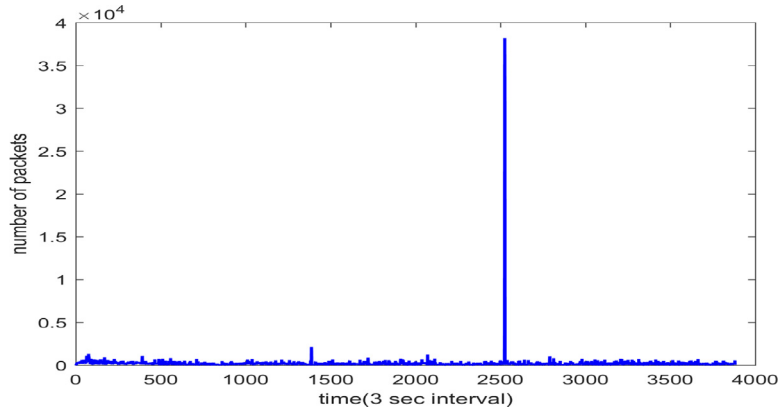

Fig. 4 – Number of packets in every three seconds.

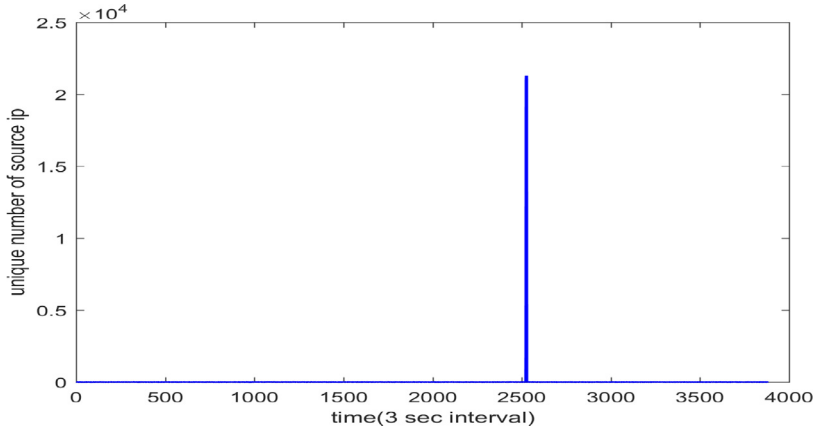

Fig. 5 – Number of unique source IP in every three seconds.

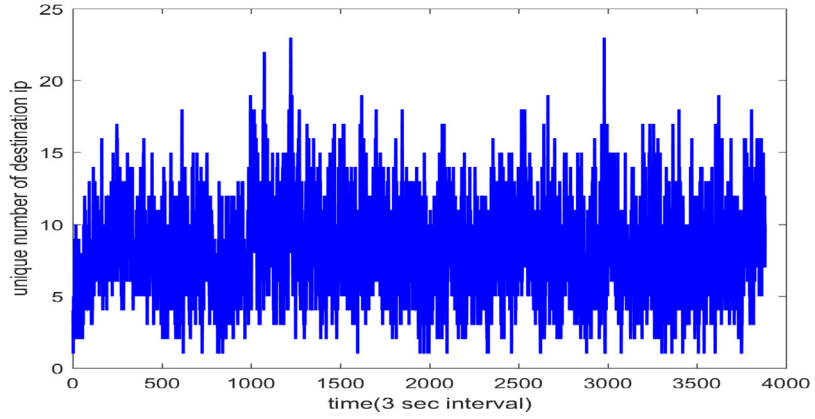

Fig. 6 – Number of unique destination IP in every three seconds.

Table 3 – Comparison between proposed method and existing method

Data Sets	Existing method (Nezhad et al., 2016)			Proposed method		
	TPR ↑	Accuracy ↑	TNR ↑	TPR	Accuracy	TNR
DARPA 98	94.4%	99.5%	99.8%	98%	99.5%	99.6%
DARPA 2000	Less than 90%	Less than 90%	Less than 90%	99.5%	99.5%	99.5%
Generated dataset	Less than 90%	Less than 90%	Less than 90%	99.5%	99.5%	99.5%

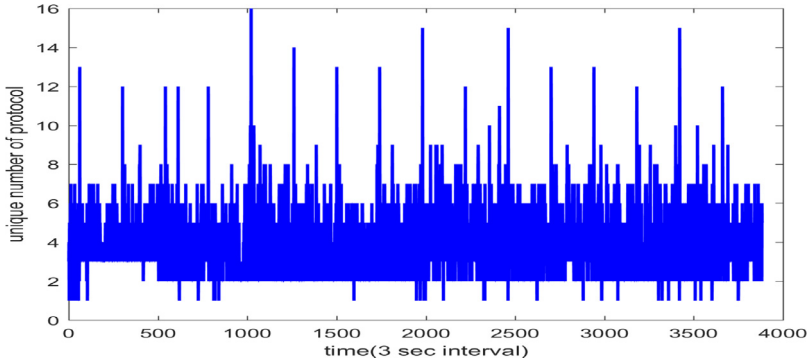

Fig. 7 – Number of unique protocol in every three seconds.

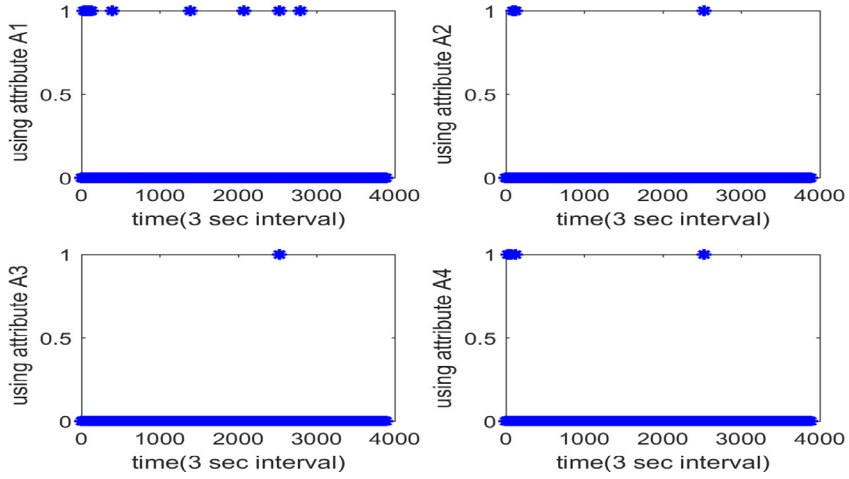

Fig. 8 – Attack detection using attributes A1-A4.

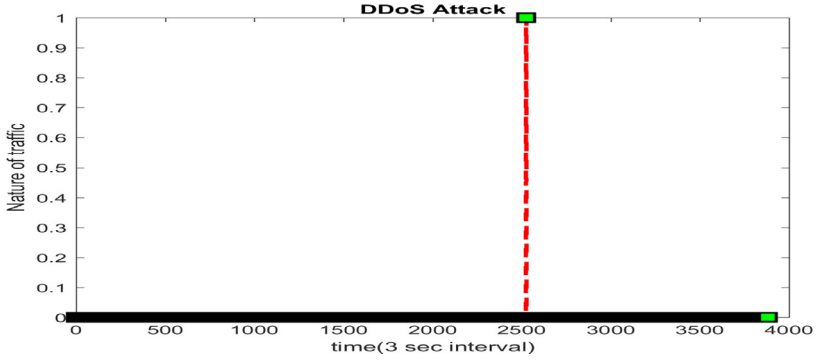

Fig. 9 – DDoS attack detection.

5. Conclusion

All statistical approaches based DDoS attack detection describes the risk of detection and false negatives, especially to complicated attacks because of considerable variability of Internet traffic and the valuable frequency of legitimate peaks. It is shown that the proposed method can successfully identify DDoS attacks with high detection rate. In the proposed method we extract different traffic features and then four attributes are calculated based on DDoS characteristics. From the observation it is seen that during DDoS attack, calculated attribute values are very high. All the four attributes are compared with threshold value and if it is exceeds the threshold DDoS attack is confirmed. This threshold values vary for different network conditions and it is updated at

regular time intervals. Experimental results demonstrate that the proposed approach is substantially more effective detection rate, accuracy and computation time compared to existing methods that uses time series model for prediction.

Supplementary material

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.cose.2019.01.002.

REFERENCES

Behal S, Kumar K. Trends in validation of DDoS research. Proc Comput Sci 2016;85:7–15.

Bhatia S, Schmidt D, Mohay G, Tickle A. A framework for generating realistic traffic for distributed denial-of-service attacks and flash events. Comput Secur 2014;40:95–107.

Bhuyan MH, Bhattacharyya D, Kalita JK. An empirical evaluation of information metrics for low-rate and high-rate DDoS attack detection. Pattern Recognit Lett 2015a;51:1–7.

Bhuyan MH, Kalwar A, Goswami A, Bhattacharyya D, Kalita J. Low-rate and high-rate distributed dos attack detection using partial rank correlation. In: Proceedings of the fifth international conference on communication systems and network technologies (CSNT). IEEE; 2015b. p. 706–10.

Braga R, Mota E, Passito A. Lightweight DDoS flooding attack detection using NOX/OpenFlow. In: Proceedings of the IEEE thirty fifth conference on local computer networks (LCN). IEEE; 2010. p. 408–15.

Cabrera JB, Lewis L, Qin X, Lee W, Prasanth RK, Ravichandran B, Mehra RK. Proactive detection of distributed denial of service attacks using MIB traffic variables-a feasibility study. In: Proceedings of the IEEE/IFIP international symposium on integrated network management. IEEE; 2001. p. 609–22.

Calvet J, Fernandez JM, Bureau PM, Marion JY, et al. Large-scale malware experiments: why, how, and so what. Proceedings of the virus bulletin conference (VB), 2010.

Chen Y, Ma X, Wu X. DDoS detection algorithm based on preprocessing network traffic predicted method and chaos theory. IEEE Commun Lett 2013;17(5):1052–4.

David J, Thomas C. DSoS attack detection using fast entropy approach on flow-based network traffic. Proc Comput Sci 2015;50:30–6.

Dong P, Du X, Zhang H, Xu T. A detection method for a novel DDoS attack against SDN controllers by vast new low-traffic flows. In: Proceedings of the IEEE international conference on communications (ICC). IEEE; 2016. p. 1–6.

Elhamahmy ME, Elmahdy HN, Saroit IA. A new approach for evaluating intrusion detection system. CiiT Int J Artif Intell Syst Mach Learn 2010;2(11).

Feinstein L, Schnackenberg D, Balupari R, Kindred D. Statistical approaches to DDoS attack detection and response, 1. IEEE; 2003. p. 303–14.

Feng Y, Guo R, Wang D, Zhang B. Research on the active DDoS filtering algorithm based on ip flow, 4. IEEE; 2009. p. 628–32.

Gillison D. Recent DDoS attack; 2016. (accessed June 7, 2018) http://www.citethisforme.com/guides/bibtex/how-to-cite-a-website.

Hick P, Aben E, Claffy K, Polterock J. The CAIDA DDoS Attack 2007 Dataset. 2012 [2015-07-10]. http://www.caida.org. 2007.

Hussain A, Heidemann J, Papadopoulos C. A framework for classifying denial of service attacks. In: Proceedings of the conference on applications, technologies, architectures, and protocols for computer communications. ACM; 2003. p. 99–110.

Jun JH, Ahn CW, Kim SH. DDoS attack detection by using packet sampling and flow features. In: Proceedings of the twenty ninth annual ACM symposium on applied computing. ACM; 2014. p. 711–12.

Kim MS, Kong HJ, Hong SC, Chung SH, Hong JW. A flow-based method for abnormal network traffic detection, 1. IEEE; 2004. p. 599–612.

Ma X, Chen Y. DDoS detection method based on chaos analysis of network traffic entropy. IEEE Commun. Lett. 2014;18(1):114–17.

Mirkovic J, Arikan E, Wei S, Thomas R, Fahmy S, Reiher P. Benchmarks for DDoS defense evaluation. In: Proceedings of the IEEE military communications conference, MILCOM. IEEE; 2006. p. 1–10.

Mirkovic J, Reiher P. A taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Comput Commun Rev 2004;34(2):39–53.

Network A. Worldwide infrastructure security report; 2015. (accessed June 7, 2018) http://www.arbornetworks.com/images/documents/wisr2016enweb.pdf.

Nezhad SMT, Nazari M, Gharavol EA. A novel dos and DDoS attacks detection algorithm using ARIMA time series model and chaotic system in computer networks. IEEE Commun Lett 2016;20(4):700–3.

No G, Ra I. An efficient and reliable DDoS attack detection using a fast entropy computation method. In: Proceedings of the ninth international symposium on communications and information technology, ISCIT. IEEE; 2009. p. 1223–8.

No G, Ra I. Adaptive DDoS detector design using fast entropy computation method. In: Proceedings of the fifth international conference on innovative mobile and internet services in ubiquitous computing (IMIS). IEEE; 2011. p. 86–93.

Nychis G, Sekar V, Andersen DG, Kim H, Zhang H. An empirical evaluation of entropy-based traffic anomaly detection. In: Proceedings of the eighth ACM SIGCOMM conference on Internet measurement. ACM; 2008. p. 151–6.

Qin X, Xu T, Wang C. DDoS attack detection using flow entropy and clustering technique. In: Proceedings of the eleventh international conference on computational intelligence and security (CIS). IEEE; 2015. p. 412–15.

Spognardi A, Villani A, Vitali D, Mancini LV, Battistoni R. Large-scale traffic anomaly detection: analysis of real netflow datasets. In: Proceedings of the international conference on e-business and telecommunications. Springer; 2012. p. 192–208.

Tavallaee M., Bagheri E., Lu W., Ghorbani A.A.. NSL-KDD dataset. Available on http://www.unb.ca/research/iscx/dataset/iscx-NSL-KDD-dataset.html), [Accessed on 28 Feb 2016] 2012.

Thomas C, Sharma V, Balakrishnan N. Usefulness of DARPA dataset for intrusion detection system evaluation. Proceedings of the data mining, intrusion detection, information assurance, and data networks security. International Society for Optics and Photonics, 2008.

Thomas C, Sharma V, Balakrishnan N. Usefulness of DARPA dataset for intrusion detection system evaluation. In: Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security 2008 (Vol. 6973). International Society for Optics and Photonics, 2008.

Wang J, Yang X, Long K. A new relative entropy based app-DDoS detection method. In: Proceedings of the IEEE symposium on computers and communications (ISCC). IEEE; 2010. p. 966–8.

Wei W, Chen F, Xia Y, Jin G. A rank correlation based detection against distributed reflection dos attacks. IEEE Commun Lett 2013;17(1):173–5.

Yu S, Zhou W. Entropy-based collaborative detection of DDoS attacks on community networks. In: Proceedings of the sixth annual IEEE international conference on pervasive computing and communications PerCom. IEEE; 2008. p. 566–71.

Zhang C, Cai Z, Chen W, Luo X, Yin J. Flow level detection and filtering of low-rate DDoS. Comput Netw 2012;56(15):3417–31.

Zhang J, Qin Z, Ou L, Jiang P, Liu J, Liu AX. An advanced entropy-based DDoS detection scheme, 2. IEEE; 2010. p. V2–67.

Zhou L, Liao M, Yuan C, Zhang H. Low-rate DDoS attack detection using expectation of packet size. Secur Commun Netw 2017;2017.

Ms. Jisa David was born in India in 1984. She has completed her B.Tech from Adi Shankara Institute of Engineering and Technology, Ernakulam, Kerala and M.Tech degrees from College of Engineering, Trivandrum, India in 2006 and 2008, respectively. She is presently working as Assistant Professor in Rajagiri School of Engineering and Technology, Kochi, Kerala, India. Her area of interests includes network security and image processing.

Prof. Ciza Thomas is currently working as Professor and Head, Electronics and Communication Department of College of Engineering, Trivandrum, India. Her area of expertise is Network Security with research interest in the fields of Information Security, Data Mining, Sensor Fusion, Pattern Recognition, Information Retrieval, Digital Signal Processing, and Image Processing. She has publications in more than 40 International Journals and International Conference Proceedings and more than 50 national conference publications. She has edited five books in the field of Sensor Fusion, Complex Systems, Ontology in Information Science and Data Mining. She has published six book chapters in the field of network security and pattern recognition. She is a reviewer of more than ten reputed International journals including IEEE transactions on Signal Processing, IEEE transactions on Neural Networks, International Journal of Network Security, International Journal of Network Management, and IEEE-John Wiley International Journal on Security and Communications Network. She is a guest editor of the IEEE Security and Privacy Magazine. She is a recipient of achievement award in 2010 and the e-learning IT award in 2014 from Government of Kerala.