(Short Paper) Effectiveness of Entropy-based Features in High- and Low-Intensity DDoS Attacks Detection

Abigail Koay[1], Ian Welch[2], and Winston K.G. Seah[2]

[1] University of Waikato, New Zealand
abigail.koay@waikato.ac.nz
[2] Victoria University of Wellington, New Zealand
ian.welch, winston.seah@ecs.vuw.ac.nz

Abstract. DDoS attack detection using entropy-based features in network traffic has become a popular approach among researchers in the last five years. The use of traffic distribution features constructed using entropy measures has been proposed as a better approach to detect Distributed Denial of Service (DDoS) attacks compared to conventional volumetric methods, but it still lacks in the generality of detecting various intensity DDoS attacks accurately. In this paper, we focus on identifying effective entropy-based features to detect both high- and low-intensity DDoS attacks by exploring the effectiveness of entropy-based features in distinguishing the attack from normal traffic patterns. We hypothesise that using different entropy measures, window sizes, and entropy-based features may affect the accuracy of detecting DDoS attacks. This means that certain entropy measures, window sizes, and entropy-based features may reveal attack traffic amongst normal traffic better than the others. Our experimental results show that using Shannon, Tsallis and Zhou entropy measures can achieve a clearer distinction between DDoS attack traffic and normal traffic than Rényi entropy. In addition, the window size setting used in entropy construction has minimal influence in differentiating between DDoS attack traffic and normal traffic. The result of the effectiveness ranking shows that the commonly used features are less effective than other features extracted from traffic headers.

Keywords: DDoS · Entropy · Traffic Features.

1 Introduction

Denial of Service (DoS) is a popular type of cyber attack that has remained a problem for users of the Internet for over twenty years. This attack is popular for its ability to effectively cripple servers and networks [6]. Now, DoS attacks are often distributed where it is called Distributed Denial of Service (DDoS) attack. In a recent case, a DDoS attack disrupted GitHub.com, a highly used site for code repository and version control using a powerful DDoS attack that peaked at 1.35Tbps [5]. The increasing severity of DDoS attacks has motivated increased efforts to develop solutions to counter the attack.

Entropy-based features are a popular measure to detect DDoS attacks [10]. Generally, entropy-based features are computed by applying entropy measures such as Shannon entropy [11] to raw traffic attributes. Entropy measures are algorithms used to calculate the uncertainty of these raw traffic attributes. Typically these attributes are packet header fields such as source and destination IP addresses, source and destination port numbers, and protocol. Entropy-based features provide a distributional view of the network traffic where it shows the variations of raw traffic attributes. For example, a high entropy value computed using the source IP address attribute indicates that there is a high variation in the origin of the traffic whereas a low entropy value indicates a smaller variation in the traffic packets' origins. This is useful for attack detection since a typical DDoS attack with a large number of attack sources targeting a single or small set of devices usually has a high variation in the source IP addresses and low variation in destination IP addresses as compared to normal traffic [7].

The usage of entropy-based features is more appealing to researchers and security professionals compared to the traditional volumetric based approaches in DDoS attack detection because they provide the following advantages: simple calculation, high sensitivity, and independence from the level of network utilisation. However, most existing approaches [4, 9, 10, 13] use a limited set of entropy-based features for detection that is only effective for specific DDoS attacks and may fail to detect different types of DDoS attacks accurately. Choosing the right set of entropy-based features to detect all types of DDoS attacks is a hard problem where it requires a deep understanding of each feature and their effectiveness in distinguishing between various attack and normal traffic. In addition, it is also important to understand the effect of entropy measures and window size used in constructing entropy-based features on the effectiveness of detecting DDoS attacks, in particularly in high- and low-intensity DDoS attacks.

The main contribution of this paper is the evaluation of a set of useful entropy-based features based upon two types of investigation: (1) exploration of the effectiveness of alternative entropy measures such as Tsallis, Rényi and Zhou as opposed to the more commonly used Shannon entropy for highlighting DDoS attack traffic patterns and (2) understanding the tradeoffs between detection window size and detection accuracy of entropy-based features to construct effective entropy-based features.

2 Related Work

Most recent existing work on DDoS Detection concentrates on using entropy-based features [4,7,10,14]. Most research focused on using a single entropy-based feature for detecting anomalies in the network rather than multiple entropy features [7]. In most entropy-based DDoS attack detection systems, Shannon entropy [11] measure is used. Gu *et al.* [2] proposed a maximum entropy and relative entropy approach based on Shannon entropy to detect network traffic anomalies in the network traffic. The reported experimental results showed that this approach is highly accurate in achieving very low false positive and

false negative rates. In another approach, Zhang *et al.* [14] proposed an advanced entropy-based method using Shannon entropy that splits variable rate attacks into different fields and treats each field with different methods to detect Low-rate DoS (LDoS) attacks. However, the method has a significantly longer response time and uses substantially more resources than prior entropy-based approaches.

Other entropy measures such as Tsallis or Rényi entropies have also been used. For example, Ma *et al.* [7] proposed a DDoS detection method using Tsallis entropy with an exponent separation detection algorithm based upon a variation of Lyapunov Exponent. Their method measures the rate of exponent separation between the source and destination IP addresses where the rate of exponent separation in attack traffic tends to be much higher than normal traffic. Bhuyan *et al.* [1] used an extended entropy metric based on Rényi entropy to calculate the entropy difference between two traffic samples taken at different times for detecting DDoS attacks. However, their method only analyses sample traffic where important information or evidence of DDoS attack might be missed, especially in low-intensity DDoS attacks.

Apart from entropy measures, DDoS attack detection approaches also adopt different window sizes to detect DDoS attack traffic. For example, Mousavi *et al.* [8] chose 50 packets as the window size by calculating the entropy of 50 new incoming packets that are sent to the software-defined network controller. Their approach is able to detect the presence of DDoS attack traffic after observing only the first five window periods. Another study [7] on the various window sizes, using a single dataset, found that 50 seconds window size yields the best result.

3 Entropy-based Features

To construct the entropy-based features, we used the UNB ISCX 2012 intrusion detection evaluation dataset (ISCXIDS2012) [12], a recent widely used dataset. This dataset contains seven days (Monday through to Sunday) of network activities which include high-. and low-intensity attack traffic. IRC Botnet DDoS attack traffic represents the high-intensity DDoS attack and HTTP Denial of Service attack traffic represents the low-intensity DDoS attack traffic. Each day has a different combination of attacks.

Entropy-based features can be constructed using two steps: (1) extract features from the raw dataset, (2) compute entropy values based on pre-defined entropy measures using a specific time interval.

3.1 Step 1 - Extract features from the raw dataset

All possible traffic features that can be extracted from packet header information (Table 1) are used to construct entropy-based features except redundant features (i.e., Absolute time, resolved/unresolved addresses) or features that contain null values (i.e., Cisco VSAN, 802.1Q VLAN id, Expert Info Severity).

Table 1. List of Regular Entropy-based Features Constructed

Regular Entropy-based Features	
Delta Time (D.Time)	Protocol Identifier (Protocol)
Source IP Address (S.IP)	Destination IP Address (D.IP)
Source Port Address (S.Port)	Destination Port Address (D.Port)
Source MAC Address (S.MAC)	Destination MAC Address (D.MAC)
Source Network Address (S.Net)	Destination Network Address (D.Net)
Packet Length (P.Length)	IP DSCP Value (DSCP)
TCP Sequence Number (Seq)	TCP Window Length (W.Length)
TCP Payload (Payload)	

3.2 Step 2 - Compute entropy values

In the second step, the entropy value of each feature is calculated based on a pre-defined entropy measure and window size. Entropy value can be calculated using several different entropy measures, namely Shannon, Tsallis, Rényi and Zhou entropies. On the other hand, the window size is defined as the distance between two time points. For example, a window size of 60 seconds means that the entropy of each feature of all packets within the 60 seconds time frame will be calculated.

Two types of entropy-based features are computed: *regular entropy-based features* (Table 1) created by calculating the entropy of a single traffic features and *entropy variation features* (Table 2) created by calculating the variation between two distinct *regular entropy-based features*.

Table 2. List of Entropy Variation Features Constructed

Entropy Variation Features	
Separation IP Address (V.IP)	Separation Port Number (V.Port)
Separation MAC Address (V.MAC)	Separation Network Address (V.Net)
Separation TCP Information (V.TCP)	

4 Influence of Entropy Measures in Traffic Patterns

This section examines the influence of different entropy algorithms on the accuracy of detecting DDoS attack traffic. We compare the traffic patterns generated using four different entropy measures, namely, Shannon, Tsallis, Rényi and Zhou entropy measures in both high- and low-intensity DDoS attack traffic. Due to space constraint, we did not show patterns of commonly used features such as S.IP, D.IP, S.Port, D.Port and Protocol.

4.1 Network Traffic Containing High-Intensity DDoS attack

The Tuesday's network activities in the ISCXIDS2012 dataset contains the IRC Botnet based DDoS attack traffic. This dataset is used as a representation of network traffic containing high-intensity DDoS attack traffic.

Fig. 1 shows entropy values generated using Shannon, Tsallis and Zhou entropy measures; Rényi entropy shows a different traffic pattern from the others. Since Tsallis and Zhou entropies are a generalisation of Shannon entropy, traffic patterns generated will be similar.

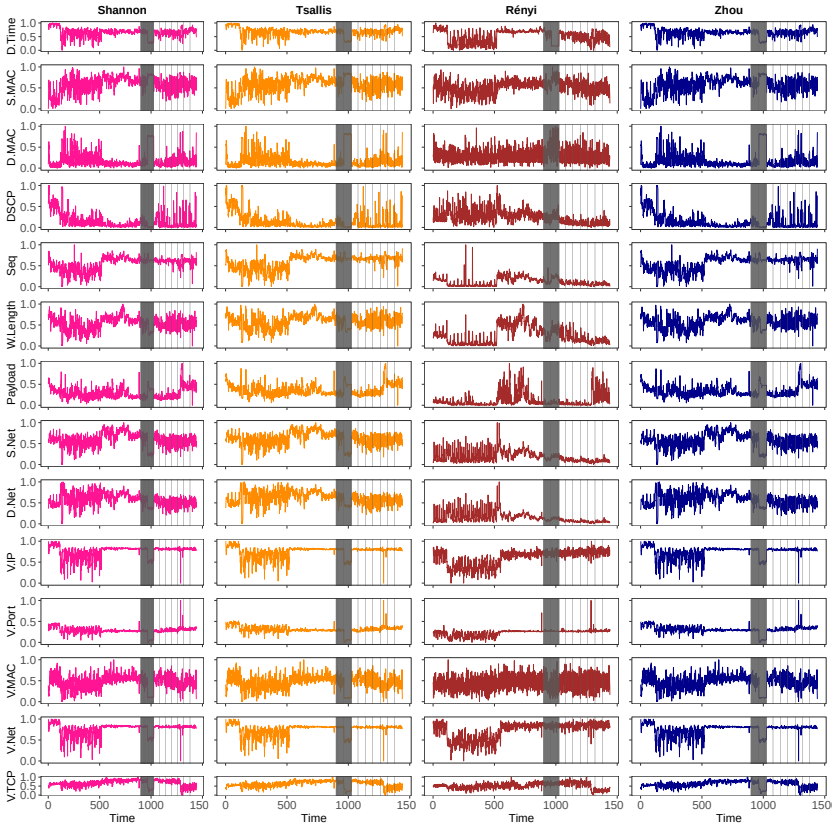

Fig. 1. Different Entropy Measures of Entropy-based Features with High-Intensity Attack Traffic; grey area shows the period of the DDoS attack.

We observe that it is possible to distinguish high-intensity DDoS attack traffic from normal traffic quite easily when entropy measures are applied to most of the traffic features except for entropy measures calculated using the Seq field as shown in Fig. 1. This is because for most of the entropy-based features generated, the entropy values of attack traffic have a much smaller range than normal traffic. For example, the attack traffic entropy values of the DSCP feature, using the Shannon entropy algorithm, lie between 0.1 to 0.35 whereas the normal traffic entropy values of the same entropy lie between 0.05 to 0.95.

The differences between these entropies represent the distributional differences between attack and normal traffic. There is not much of a difference in the distributional patterns of attack and normal traffic using entropy-based features constructed using Rényi entropy, which may not be useful in identifying stealthy DDoS attacks. This is because the differences between attack and normal traffic entropy values are too small to be noticeable and can be easily misclassified. On the other hand, Shannon, Tsallis and Zhou entropies provide clearer differences in distributional patterns and entropy values between attack and normal traffic.

Overall, Rényi entropy does not perform well at distinguishing high-intensity DDoS attack traffic from normal traffic whereas Shannon, Tsallis and Zhou entropies perform better and can identify DDoS attack traffic relatively well.

4.2 Network Traffic Containing Low-Intensity DDoS attack

The Monday's network activities in ISCXIDS2012 dataset contains HTTP Denial of Service attack traffic, an example of low-intensity DDoS attack (Fig. 2.)

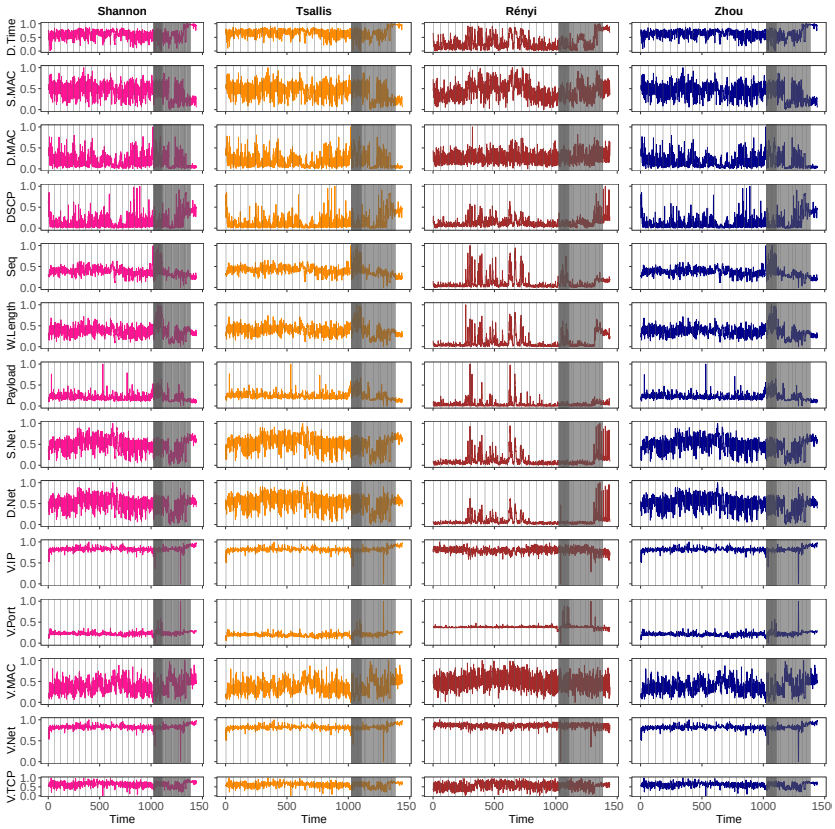

Fig. 2. Different Entropy Measures of Entropy-based Features with Low-Intensity Attack Traffic; grey area shows the period of the DDoS attack.

Unlike high-intensity DDoS attacks, it is difficult to distinguish between low-intensity attack traffic and normal traffic. Most entropy-based features such as D.Time, S.MAC, D.MAC, S.Net, D.Net, V.IP, and V.Net show the entropy values decreases during the attack. However, this is true for only a small part of the attack, specifically in the middle of the attack (i.e. around $1200 secs$). This phenomenon indicates that low-intensity attacks require some time before there are significant changes in the traffic distribution in the network. Entropy-based features such as Seq and W. Length entropies using Shannon and Zhou entropies show a clear distinction between attack traffic and normal traffic.

Similar to Rényi entropy gives almost no difference in the traffic patterns between attack traffic and normal traffic. However, Rényi entropy shows significant differences between the traffic patterns of attack traffic and normal traffic when applied to V.IP, V.Port and V.Net entropy features, in which it shows similar differences to the other entropy algorithms (Zhou, Shannon, and Tsallis) examined.

5 Effects of Window Size in Traffic Patterns

This section examines the influence of window size in calculating entropy values for DDoS detection on network traffic. If the window size is set too large, DDoS attacks that lasted for a shorter period than the window size may be hidden and the entropy value computed may not show the distinct difference between attack traffic and normal traffic. However, if the window size is set too small, entropy values generated may be too sensitive to the changes in the traffic. This means that a slight change in the network can be regarded as an attack even though it is not. In this case, a lot of false alarms may occur.

We compared six different window sizes (30, 60, 90, 120, 150, and 180 seconds) and observe the traffic patterns generated. Traffic patterns based on the entropy values of traffic features in high-intensity DDoS attack scenarios are shown in Fig. 3. We observe that all features have similar traffic patterns even though different window intervals are applied.

Furthermore, there is almost no difference in traffic patterns between these four window intervals. Entropy is being calculated more frequently in the 30-second interval compared to the 60-second interval, but both gave similar traffic patterns. The lack of differences in attack traffic and normal traffic patterns (also observed in low-intensity DDoS attack scenarios) suggest that the window size used for generating traffic feature entropy values only has a slight effect on the accuracy of DDoS attack detection.

6 Effectiveness of Individual Entropy-based Features

We analysed the effectiveness of each feature by using Pearson's Correlation, gain ratio, and information gain techniques found in the WEKA tool [3]. Table 3 shows the effectiveness ranking (correlation, information gain, and gain ratio) of entropy-based features in detecting low-intensity DDoS attacks based on 10-fold cross-validation on a single seed (seed = 1). D.Time, Protocol, W.Length, Payload, V.MAC, and V.TCP are consistently ranked within the top five in at least two out of three feature selection algorithms. These features, except for protocol, are not one of the commonly used features on most DDoS detection systems.

Table 4 shows the effectiveness ranking of entropy-based features in detecting high-intensity DDoS attacks. The top features in the high-intensity DDoS attack dataset are D.Port, D.MAC, Protocol, P.Length, Seq, V.Port and V.MAC. Unlike

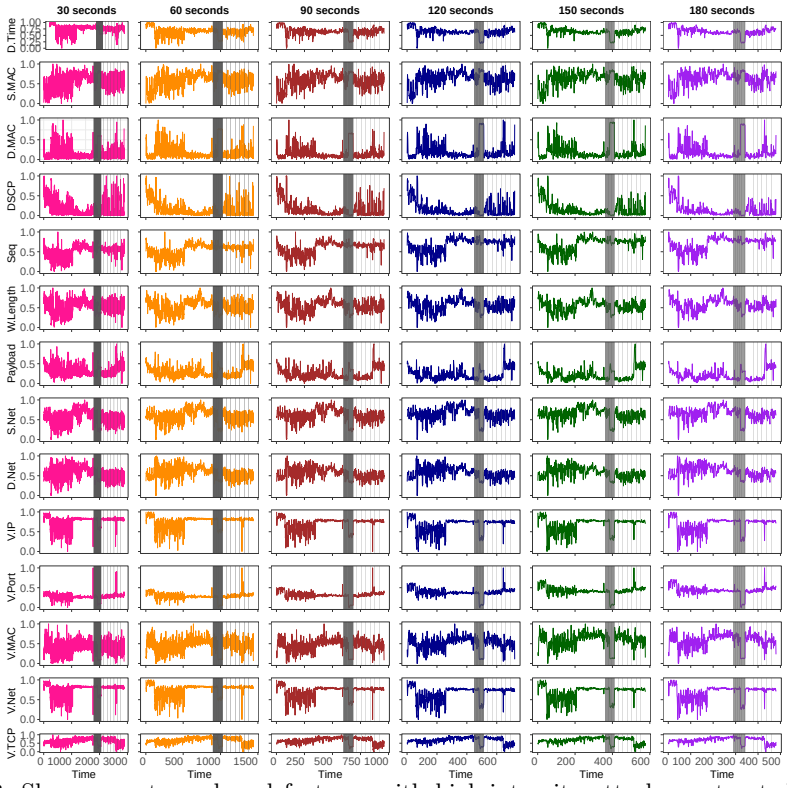

Fig. 3. Shannon entropy-based features with high-intensity attack constructed using different window sizes; grey area shows the period of the DDoS attack.

Table 3. Effectiveness Ranking in Detecting Low-Intensity DDoS Attacks

Feature	Correlation	Information Gain	Gain Ratio
D.Time	**3.5±0.5**	17.6±0.49	**3.3±2.37**
S.IP	14.4±0.66	9.9±0.83	14.4±0.66
D.IP	9.9±0.3	12.4±1.11	17.5±0.5
S.Port	16.2±0.4	6.9±0.3	6.8±0.75
D.Port	19±0	15.9±0.54	10.9±1.22
S.MAC	8.2±0.6	14.7±0.64	13.7±1.62
D.MAC	6±0	8.1±0.3	12.5±0.5
S.Net	16.8±0.4	13.5±1.96	12.1±4.04
D.Net	11±0	13±1.34	17.5±0.5
Protocol	**5±0**	6.3±0.64	**1±0**
P.Length	18±0	10.5±1.91	15±1.41
DSCP	8.9±0.3	18.5±1.02	19±0
Seq	7±0	16.6±3.93	9.2±0.6
W.Length	**3.5±0.5**	**1±0**	**2.8±0.6**
Payload	12.5±0.5	**2±0**	**5.4±0.49**
V.IP	12.7±0.78	11±1	11.3±0.46
V.Port	14.4±0.66	3.6±0.49	8.4±0.8
V.MAC	**1±0**	**3.4±0.49**	5.4±1.2
V.TCP	**2±0**	**5.1±0.3**	**3.8±0.6**

Table 4. Effectiveness Ranking in Detecting High-Intensity DDoS Attacks

Feature	Correlation	Information Gain	Gain Ratio
D.Time	15±0.77	**2±0**	**2±0**
S.IP	18.9±0.3	8.4±0.49	7.5±1.86
D.IP	12±0.77	11.7±0.9	7.2±1.4
S.Port	2.8±0.4	14.9±0.3	15.3±0.46
D.Port	**4±0**	**4±0**	**4±0**
S.MAC	14.3±0.46	8.2±0.98	9.3±1.68
D.MAC	6±0	**1±0**	**1±0**
S.Net	17±0	7±0.89	8.5±1.75
D.Net	10.9±0.83	10.6±0.8	7.9±1.37
Protocol	15.7±0.46	**3±0**	**3±0**
P.Length	5±0	11.6±1.11	13.9±0.54
DSCP	18.1±0.3	14.1±0.3	9.4±1.36
Seq	7.9±0.54	5±0	13.2±0.6
W.Length	10.9±1.04	16±0	16.7±0.46
Payload	7.2±0.4	6.4±0.49	12.2±0.4
V.IP	8.9±0.3	19±0	18.6±0.66
V.Port	1±0	12.1±1.04	**5.3±0.64**
V.MAC	2.2±0.4	17.6±0.49	18.3±0.46
V.TCP	12.2±1.08	17.4±0.49	15.8±1.54

the results for low-intensity DDoS attack dataset, the top features that are effective in detecting high-intensity DDoS attacks include one of the normally used in DDoS attack detection systems as the attack used in this dataset focused on attacking the victim using the same destination port address.

From the results, we found several features that are more effective than the commonly used entropy-based features. We also found that D.Time and Protocol are the top features for detecting both high- and low-intensity DDoS attacks.

7 Summary of the Usefulness of Entropy-based Features

In this paper, we examined the usefulness of entropy-based features in detecting DDoS attacks by analysing each entropy-based feature as shown in Figure 1 to Figure 3. We found that entropy-based features such as Protocol, and P.Length can show a more distinct difference between attack and normal traffic (refer Fig. 1). Our effectiveness ranking based on three feature selection algorithms shows that uncommon features such as D.Time, V.Port and V.MAC entropy-based features are the most effective in detecting both high- and low-intensity based DDoS attacks.

Although some entropy-based features can be effective in detecting a DDoS attack, they may not be effective for all types of DDoS attack. For example, Payload can be effective against DDoS attacks that transmit attack traffic at a low-intensity rate but may not be effective against DDoS attacks that send attack traffic at a high-intensity rate. D.IP is effective against DDoS attacks that send attack traffic to the same IP Address but may not be effective against DDoS attacks that send attack traffic to multiple IP addresses. An attacker can easily defeat the detection scheme based on single entropy features by randomising the attack traffic sending rate and IP addresses.

Also, at the earlier stage of an attack, the temporal change of a single entropy feature may be too small to be noticed by the detection scheme, especially when it is observed close to the attack source. Temporal changes are changes that could be observed over time. Entropy values before an attack and during an attack could be different based on the characteristics of attack traffic and its differences with normal traffic. These differences might not be noticeable in the early stage of an attack before the aggregated attack traffic meets at the aggregation point, but become more noticeable after some time where attack volumes are increasing over time.

8 Conclusion & Future Work

This paper evaluated a set of useful entropy-based features by exploring the effectiveness of entropy measures in detecting DDoS attacks and understanding the tradeoffs between detecting window size and detection accuracy of entropy-based features to construct effective entropy-based features. Our experiments showed that not all regular entropy-based features provide a clear distinction between attack and normal traffic patterns and window size used in entropy construction has minimal impact on overall accuracy. We also found that several uncommon features are more effective than the commonly used features in DDoS attack detection. In the future, we plan to work on the following items to further enhance the accuracy and generality of this approach:

- *Sliding window intervals.* In this paper, we only used a single fixed window interval. We plan to optimise the detection results by adopting a sliding window interval approach.
- *New machine learning classifier.* We found the top features that are effective and useful in detecting both high- and low-intensity DDoS attacks. We plan to further investigate the best machine learning classifier using those features to improve the results of DDoS detection.
- *Newer type of attacks.* Our evaluation dataset uses older types of DDoS attack. We plan to test the approach with newer and more recent of DDoS attacks such as NTP reflection attacks and DNS Amplification attacks.

References

1. Bhuyan, M.H., Bhattacharyya, D., Kalita, J.: E-ldat: A Lightweight System for DDoS Flooding Attack Detection and IP Traceback using Extended Entropy Metric. Security and Communication Networks **9**(16), 3251–3270 (2016)
2. Gu, Y., McCallum, A., Towsley, D.: Detecting Anomalies in Network Traffic using Maximum Entropy Estimation. In: Proceedings of the 5th ACM SIGCOMM Conference on Internet Measurement. pp. 32–32. USENIX Association (2005)
3. Hall, M., Frank, E., Holmes, G., Pfahringer, B., Reutemann, P., Witten, I.H.: The WEKA Data Mining Software: an Update. ACM SIGKDD Explorations Newsletter **11**(1), 10–18 (2009)
4. Jun, J.H., Ahn, C.W., Kim, S.H.: DDoS Attack Detection by using Packet Sampling and Flow Features. In: Proceedings of the 29th Annual ACM Symposium on Applied Computing. pp. 711–712. ACM (2014)
5. Kottler, S.: February 28th DDoS Incident Report. https://githubengineering.com/ddos-incident-report/ (2018)
6. Loukas, G., Öke, G.: Protection against Denial of Service Attacks: A Survey. The Computer Journal (2009)
7. Ma, X., Chen, Y.: DDoS Detection Method based on Chaos Analysis of Network Traffic Entropy. IEEE Communications Letters **18**(1), 114–117 (2014)
8. Mousavi, S.M., St-Hilaire, M.: Early Detection of DDoS Attacks against SDN Controllers. In: Proceedings of the International Conference on Computing, Networking and Communications (ICNC). pp. 77–81. IEEE (2015)
9. Nychis, G., Sekar, V., Andersen, D.G., Kim, H., Zhang, H.: An Empirical Evaluation of Entropy-based Traffic Anomaly Detection. In: Proceedings of the 8th ACM SIGCOMM Conference on Internet Measurement. pp. 151–156 (2008)
10. Özçelik, İ., Brooks, R.R.: Deceiving Entropy based DoS Detection. Computers & Security **48**, 234–245 (2015)
11. Shannon, C.E.: Communication Theory of Secrecy Systems. Bell Labs Technical Journal **28**(4), 656–715 (1949)
12. Shiravi, A., Shiravi, H., Tavallaee, M., Ghorbani, A.A.: Toward Developing a Systematic Approach to Generate Benchmark Datasets for Intrusion Detection. Computers & Security **31**(3), 357–374 (2012)
13. Zhang, C., Cai, Z., Chen, W., Luo, X., Yin, J.: Flow Level Detection and Filtering of Low-Rate DDoS. Computer Networks **56**(15), 3417–3431 (2012)
14. Zhang, J., Qin, Z., Ou, L., Jiang, P., Liu, J., Liu, A.: An Advanced Entropy-based DDoS Detection Scheme. In: Proceedings of the International Conference on Information Networking and Automation (ICINA). vol. 2, pp. V2–67 (2010)