Real-Time DDoS Attack Detection using Sketch-based Entropy Estimation on the NetFPGA SUME Platform

Yu-Kuen Lai, Po-Yu Huang, Ho-Ping Lee, Cheng-Lin Tsai, Cheng-Sheng Chang, Manh Hung Nguyen, Yu-Jau Lin[a], Te-Lung Liu[b], Jim Hao Chen[c]
Dept. of Electrical Engineering, Chung-Yuan Christian University, Chung-Li, Taiwan
Email: ylai@cnsrl.cycu.edu.tw, {10778010, 10778012, 10878030, 10778011, 10702811}@cycu.edu.tw
[a]Dept. of Applied Mathematics, Chung-Yuan Christian University, Chung-Li, Taiwan
Email: yujaulin@cycu.edu.tw
[b]National Center for High Performance Computing, Tainan, Taiwan
Email: tlliu@narlabs.org.tw
[c]International Center for Advanced Internet Research, Northwestern University, USA
Email: jim-chen@northwestern.edu

***Abstract*—With the rapid increase in network traffic and different types of attacks, real-time anomaly detection has received much attention recently. Shannon entropy can be an essential measure for identifying untypical network traffic; however, it is a time-consuming task to calculate entropy in real-time in the high-speed network environment. This work transforms the complex computations of the Shannon entropy estimation, proposed by Clifford and Cosma, into pre-computed lookup tables in the FPGA. Together with the LSTM-RNN, the proposed system on the NetFPGA SUME platform can detect DDoS attacks accurately at wire-speed of 40 Gbps throughput.**

***Index Terms*—DDoS Detection, Shannon Entropy Estimation, LSTM-RNN, Network Traffic Analysis, Sketch, NetFPGA SUME.**

I. Introduction

The IEEE's 100Gbps and 200Gbps network standards (IEEE802.3ba) [1] have been announced and approved since 2010. The industries are now deploying 400Gbps high-speed network equipment on a large scale in cloud data centers. Hence, the scale of DDoS attacks went from 40Gbps in 2008 to over 400Gbps in 2013. The number of attacks increased by more than a thousand percent, causing large-scale economic losses [2]. The empirical entropy of traffic features (e.g., the source, destination of IP addresses and TCP ports) is an essential indicator for high-speed network traffic analysis [3] [4].

The empirical Shannon entropy is defined as

$$H = -\sum_{i=1}^{n} p_i \log_2 p_i, \tag{1}$$

where $p_i = \frac{m_i}{m}$, m is the total number, n represents the distinct number, and m_i denotes the frequency of item i in the data stream.

However, computing the exact entropy value is difficult in high-speed network streams because of the limited processing and storage resources in network devices. Moreover, the entropy computations on one or more combinations of traffic features at the same time are required. Therefore, estimation techniques to speed up the complex computation of entropy value were proposed [5], [6] for high-speed anomaly detection systems.

This paper presents a hardware implementation of the Shannon entropy estimation [6] on the NetFPGA-10G SUME platform. These entropy values of selected features can be computed in real-time and sent to the Long Short-Term Memory Recurrent Neural Networks (LSTM-RNN) for DDoS attack traffic detection.

The structure of this paper is as follows. Section II, gives a general background of the related works. The proposed methodologies and system implementations concerning the design of data plane and control plane are described in Section III. Section IV discusses the setup of the data sets and overall system performance and evaluation strategy. Finally, in Section V, we summarize the work presented with future work.

II. Related Works

Artificial neural networks are extensively used to model the behavior of complex non-linear systems. It is capable of identifying intricate patterns of high-dimensional data [7].

Koay *et al.* [8] proposed a method that uses entropy-based features and multi-classifiers to detect abnormal traffic events. The paper has experimented with two types of entropy, including regular entropy and separation entropy. In particular, Separation entropy can give the variation of two distinct entropy-based features. The proposed method can utilize the rich information of multiple entropy features to improve the detection rate and reduce false alarm rates. The paper proposed a system called E3ML, which can utilize rich information of multiple entropy features, and three machine learning algorithms. It consists of a recurrent neural network, a multi-layer perceptron, and an alternating decision tree to classify

abnormal events. The E3ML system uses five separate entropy features, including TCP window size, TCP segment length, the source and destination of IP addresses, TCP ports, and layer-2 MAC addresses.

Fanzhi Meng *et al*. [9] compares the performance of LSTM with other machine learning algorithms, including SVM when classifying attack and normal instances in NSL-KDD dataset [10]. The result shows that LSTM has outperformed 99% detection rate and accuracy. In work by Behal *et al.* [11], it is mentioned that nearly half of the papers surveyed use information entropy to analyze and identify the traffic of large-scale DDoS attacks from regular flash events. The use of information entropy is also recognized as the most effective method for abnormal network behavior detection.

Based on the Mahalanobis Distance metric, Daneshgadeh *et al*. [12] proposed a methodology to detect the DDoS attack and distinguish high rate and low rate DDoS attack from a flash event. The paper utilized Shannon Entropy and machine learning algorithms to detect abnormal events in an unsupervised manner.

Xinlei Ma *et al*. [13] proposed a method to detect DDoS by analyzing the relationship between source IP and destination IP addresses with chaos theory. The method collects network traffic and calculates normalized entropy of source and destination IP addresses. The model calculates the separation rate between two related entropy series and define the threshold to detect DDoS attack. The experiment shows that the rate of separation changes significantly when a DDoS attack happens.

III. System Design

A. Data Plane

As shown in Figure 1, the module of entropy estimation is the core of the system data plane. The design is based on the methodology proposed by Clifford and Cosma [6]. The major process of this block is to make projection of incoming packets in the network traffic to the random variables $R_j(i_t)$, as illustrated in Algorithm 1, with the maximally skewed alpha-stable distribution [14]. Each packet is represented as the *key* and *value* pair (i_t, d_t). In this paper, the key i_t can be treated as any selected header field and d_t as the packet count of one.

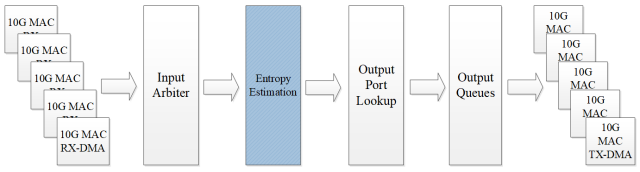


Fig. 1. The Entropy estimation module is placed in the fast dataplane pipeline of the Reference Switch project on the NetFPGA-10G SUME [15], [16] platform.

In order to avoid the time-consuming computations which involve division, logarithmic, and trigonometric functions as shown in Algorithm 2, random numbers with the maximally skewed alpha-stable distribution are pre-computed in advance.

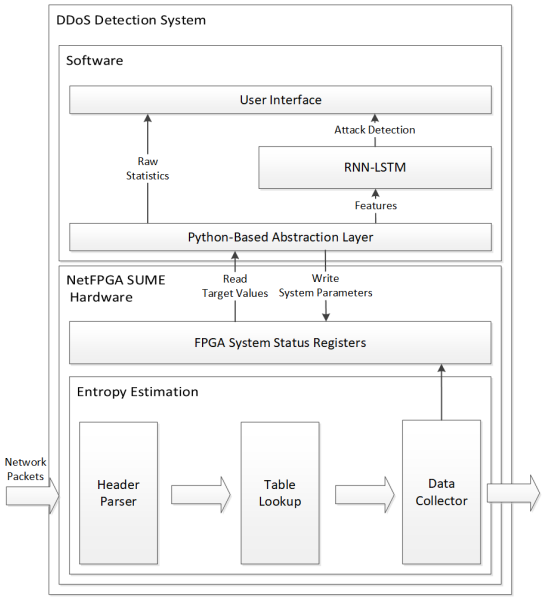


Fig. 2. The DDoS detection system block diagrams.

These values are stored in the FPGA lookup tables of size $64K$ x 20 bits.

Algorithm 1 Algorithm for estimating the Entropy of packet streams [6] .

Initialize data sketch $(y_1, \ldots, y_k) = (0, \ldots, 0)$.
Set the counter $Y = 0, d_t = 1$.
For $t = 1$ to T
  Update the counter $Y = Y + d_t$.
  Seed the PRNG with i_t.
  For $j = 1$ to k
    Generate $R_j(i_t) \sim F(x; 1, -1, \pi/2, 0)$
    Update $y_j = y_j + R_j(i_t) \times d_t$.
At time $t = T$, set $y_j = y_j/Y$ for $j = 1, \cdots, k$.
Return $\hat{H}(p) = -\log\left(k^{-1} \sum_{j=1}^{k} exp(y_j)\right)$.

For each incoming packet, the raw packet data are extracted from the packet header parser. Then, the 2-Universal hash function is used to generate k different random values based on a particular packet header, such as, the IPv4 source address. Those values are used as indexes to look up the tables for the random numbers with the alpha-stable distribution. Subsequently, the k-dimensional data sketch $(y_1, \ldots, y_k)$, illustrated as the Data Collector module in Figure 2, is updated accordingly. At the end of the observation interval, the statistic counter and data sketch are processed by the Python-based Abstraction Layer in the CPU. The choice of $k = 4$ is chose for this Proof-of-Concept design. After updating the k-dimensional data sketch $(y_1, \ldots, y_k)$ in the Data Collector,

Algorithm 2 Pseudo codes [14] to generate the random variable $R(i_t)$ with maximally skewed alpha-stable distribution of $F\left(x; 1, -1, \frac{\pi}{2}, 0\right)$.

Generate two random numbers $U_1, U_2 \sim$ Unif$(0,1)$ with seed of i_t independently.
Let $W_1 = \pi(U_1 - \frac{1}{2})$ and $W_2 = -\log U_2$.
Return $R(i_t) =$
$\tan(W_1)\left[\frac{\pi}{2} - W_1\right] + \log\left(W_2 \frac{\cos W_1}{\pi/2 - W_1}\right)$.

packet is forwarded to the egress port.

B. Control Plane

The recurrent neural network (RNN) is widely used to process sequential data streams [17]. Long short-term memory (LSTM) model is a particular variant of RNN. The LSTM cell is designed in a smarter way to overcome the vanishing gradient problem by using an input, output, and forget gate without changing the excitation function. Therefore, it is also extensively applied in the cyber security applications to detect network traffic anomaly [18], [19], [20].

The system software fetches the k-dimensional data sketch $(y_1, \ldots, y_k)$, through the *ioctl* calls. Then, these features are processed and aggregated based on the predefined observation interval $\triangle T$. The control plane CPU is in charge of computing the estimated entropy value $\hat{H}$ by using a log-mean estimator [6].

As shown in Figure 2, the system utilizes the LSTM-RNN in software as the key module for the detection of DDoS attacks. The simple LSTM model is instantiated with one input/output layer and two hidden layers. It is trained based on the selected features, including packet size distribution counters, estimated entropies of source and destination IP addresses and TCP ports, protocol, and the packet length. As shown in Figure 3, at a given time T, there are total of ten *time steps* of feature collections sent to the LSTM module.

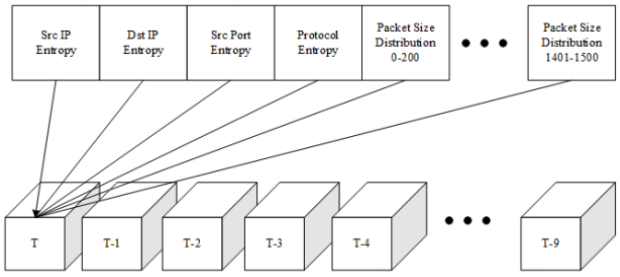


Fig. 3. At a given time T, there are total of ten time steps of feature collections sent to the LSTM module.

IV. Evaluation

A. Data Set

The evaluation is conducted based on the CAIDA 2007 DDoS [21] network traffic traces. This one-hour data set only contains attack traffic to the victim and responses from the victim. Therefore, we further take other traffic traces from MAWI Working Group Traffic Archive (MAWI 2019, 2015, and 2007) [22] as the background network traffic and merged each of them with the DDoS attack traffic for training and testing purpose. There are two sets of traces; each consists of ten 15-minute long packet files for 10-fold cross validation.

B. Performance

According to the pre-defined observation interval $\triangle T$, the raw merged packet traces are further processed to obtain four features of the estimated entropy values on selected header fields, including source, destination IP addresses, and TCP ports. Besides, statistic counters of packet numbers in eight different ranges of packet length are also provided.

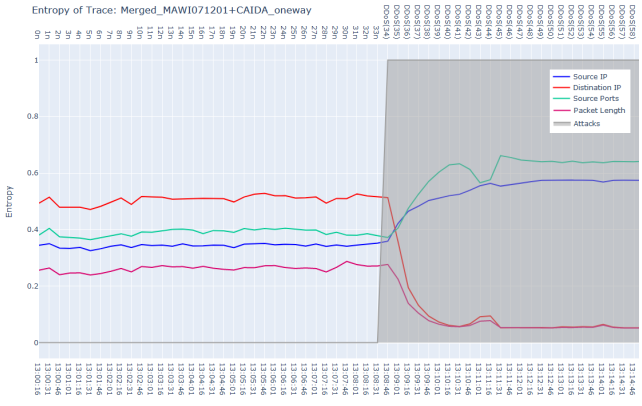


Fig. 4. The 15-minute entropy values of selected features on the merged (CAIDA DDoS 2007 and MAWI 2007) network traffic trace. The high-lighted gray area, starting at time of 13:08:31, represents the period of DDoS attack.

Figure 4 presents the 15-minute entropy values of selected features on the merged network traffic trace. The high-lighted gray area represents the period of DDoS attack.

These feature sets, arranged in a time series, are labeled with four different levels of granularity (*normal*, *likely*, *suspicious*, and *attack*) in one-hot encoding. The purpose is to avoid inaccurate detection due to the transitions from *normal* to *attack* in the time series data for the LSTM model. We adopt the 10-fold cross validation to evaluate the proposed detection system. Table I presents the evaluation results based on two different time-step configurations.

C. System Test

As shown in Figure 5, the FPGA synthesis results only consume 37% of the LUT resource. Compared to that of the original NetFPGA reference switch design, a 27% increase in the LUT is due to the lookup table needed. The data plane hardware, designed based on the system clock of 6.25ns in Verilog HDL, is capable of processing network traffic at 40Gbps wire-speed throughput. We further conduct the testing in the lab environment, as shown in Figure 6. A new set of 1-hour long packet trace (MAWI 2019) is prepared and merged with the CAIDA 2007 DDoS trace. In this traffic trace, two DDoS attacking scenarios are inserted at different times. The

TABLE I
THE PERFORMANCE OF DDOS ATTACK DETECTION BASED ON THE 10-FOLD CROSS VALIDATION WITH TWO DIFFERENT TIME STEP CONFIGURATIONS.

Time Steps	Label	Precision (%)	Recall (%)	F1 Score (%)	Accuracy (%)
6	Normal	100	97.83	98.49	94.34
	Attack	93.26	100	96.43	
10	Normal	99.65	96.69	98.14	96.63
	Attack	91.08	100	95.11	

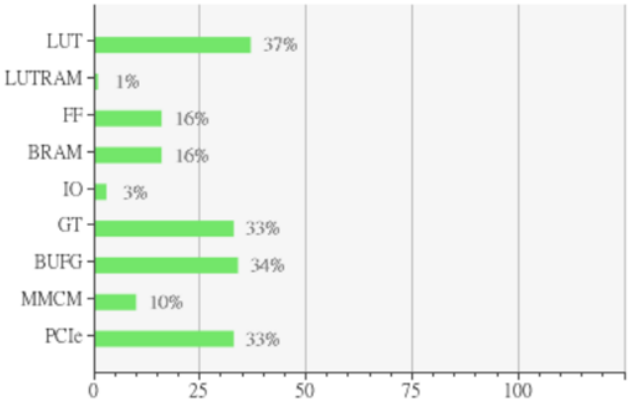
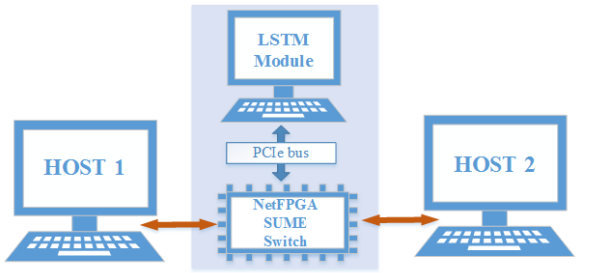


Fig. 5. The FPGA hardware utilization.



	OS	CPU	RAM
NetFPGA-10G SUME	Ubuntu 16.04 LTS	Intel i7-7700	DDR4 2400Hz 8GB×2
Host 1		Intel i7-2600	DDR3 1333Hz 4GB×1
Host 2			
10G NIC (Host1、2)	Intel 82599ES 10-Gigabit SFI/SFP+ MYRCOM 10G-PCIE-8B		

Fig. 6. The system testing configuration and network environment.

packet trace is then replayed from Host 1 and destined to Host 2 through the proposed detection system. As shown in Figure 7, the proposed system can successfully identify the attacks in two high-lighted red areas.

V. CONCLUSION AND FUTURE WORK

This paper presents an implementation of sketch-based entropy estimation with LSTM-RNN in the NetFPGA-10G SUME platform. Clifford and Cosma's method [6] is adopted by using table-lookup to estimate the entropy of selected header fields in real-time for the DDoS attack detection. The proposed system can achieve 40Gbps wire-speed packet processing capability. Several real-world traffic traces are prepared for system performance testing and verification. The results show that the proposed approach can detect the DDoS attack effectively. We plan to further explore the design space, especially on optimizing the size of the lookup table for more applications of high-speed network anomaly detection in the near future.

Fig. 7. The DDoS detection system block diagrams.

ACKNOWLEDGMENT

The work is supported in part by the Ministry of Science and Technology, Taiwan under MOST 108-2221-E-033-015 and MOST 109-2221-E-033 -032 -MY2.

REFERENCES

[1] IEEE 802.3 50 Gb/s, 100 Gb/s, and 200 Gb/s Ethernet Task Force.
[2] Bashar Ahmed Khalaf, Salama A. Mostafa, Aida Mustapha, Mazin Abed Mohammed, and Wafaa Mustafa Abduallah. Comprehensive Review of Artificial Intelligence and Statistical Approaches in Distributed Denial of Service Attack and Defense Methods. *IEEE Access*, 7:51691–51713, 2019.
[3] Haiquan (Chuck) Zhao, Ashwin Lall, Mitsunori Ogihara, Oliver Spatscheck, Jia Wang, and Jun Xu. A data streaming algorithm for estimating entropies of od flows. In *Proceedings of the 7th ACM SIGCOMM conference on Internet measurement*, IMC '07, pages 279–290, New York, NY, USA, 2007. ACM.
[4] Anukool Lakhina, Mark Crovella, and Christophe Diot. Mining Anomalies Using Traffic Feature Distributions. In *Proceedings of the 2005 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, SIGCOMM '05, pages 217–228, New York, NY, USA, 2005. ACM.
[5] Ashwin Lall, Vyas Sekar, Mitsunori Ogihara, Jun Xu, and Hui Zhang. Data Streaming Algorithms for Estimating Entropy of Network Traffic. In *Proceedings of the Joint International Conference on Measurement and Modeling of Computer Systems*, SIGMETRICS '06/Performance '06, pages 145–156, New York, NY, USA, 2006. ACM.
[6] Peter Clifford and Ioana Cosma. A simple sketching algorithm for entropy estimation over streaming data. In *Artificial Intelligence and Statistics*, pages 196–206, 2013.

[7] Yunsheng Fu, Fang Lou, Fangzhi Meng, Zhihong Tian, Hua Zhang, and Feng Jiang. An Intelligent Network Attack Detection Method Based on RNN. In *2018 IEEE Third International Conference on Data Science in Cyberspace (DSC)*, pages 483–489, June 2018.

[8] Abigail Koay, Aaron Chen, Ian Welch, and Winston K. G. Seah. A new multi classifier system using entropy-based features in DDoS attack detection. In *2018 International Conference on Information Networking (ICOIN)*, pages 162–167, January 2018.

[9] Fanzhi Meng, Yunsheng Fu, Fang Lou, and Zhiwen Chen. An effective network attack detection method based on kernel PCA and LSTM-RNN. In *2017 International Conference on Computer Systems, Electronics and Control (ICCSEC)*, pages 568–572.

[10] UNB. Datasets, Canadian Institute for Cybersecurity.

[11] Sunny Behal, Krishan Kumar, and Monika Sachdeva. Characterizing DDoS attacks and flash events: Review, research gaps and future directions. *Computer Science Review*, 25:101–114, August 2017.

[12] S. Daneshgadeh, T. Ahmed, T. Kemmerich, and N. Baykal. Detection of DDoS Attacks and Flash Events Using Shannon Entropy, KOAD and Mahalanobis Distance. In *2019 22nd Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN)*, pages 222–229, February 2019.

[13] Xinlei Ma and Yonghong Chen. DDoS detection method based on chaos analysis of network traffic entropy. 18(1):114–117.

[14] V. M. Zolotarev. *One-dimensional stable distributions*. Number v. 65 in Translations of mathematical monographs. American Mathematical Society, Provindence, R.I, 1986.

[15] Gianni Antichi, Charalampos Rotsos, and Andrew W. Moore. Enabling Performance Evaluation Beyond 10 Gbps. In *Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication*, SIGCOMM '15, pages 369–370, New York, NY, USA, 2015. ACM. 00000.

[16] Jad Naous, Glen Gibb, Sara Bolouki, and Nick McKeown. NetFPGA: reusable router architecture for experimental research. In *Proceedings of the ACM workshop on Programmable routers for extensible services of tomorrow*, pages 1–7, Seattle, WA, USA, 2008. ACM.

[17] Anton Maximilian SchÃfer and Hans Georg Zimmermann. Recurrent Neural Networks Are Universal Approximators. In Stefanos D. Kollias, Andreas Stafylopatis, WÅodzisÅaw Duch, and Erkki Oja, editors, *Artificial Neural Networks â ICANN 2006*, Lecture Notes in Computer Science, pages 632–640, Berlin, Heidelberg, 2006. Springer.

[18] Daniel Berman, Anna Buczak, Jeffrey Chavis, and Cherita Corbett. A Survey of Deep Learning Methods for Cyber Security. *Information*, 10(4):122, April 2019.

[19] Benjamin J. Radford, Leonardo M. Apolonio, Antonio J. Trias, and Jim A. Simpson. Network Traffic Anomaly Detection Using Recurrent Neural Networks. *arXiv:1803.10769 [cs]*, March 2018. arXiv: 1803.10769.

[20] Chuanlong Yin, Yuefei Zhu, Jinlong Fei, and Xinzheng He. A deep learning approach for intrusion detection using recurrent neural networks. 5:21954–21961.

[21] The CAIDA UCSD "DDoS Attack 2007" Dataset. https://www.caida.org/data/passive/ddos-20070804_dataset.xml. (Accessed on 2019-05-04).

[22] MAWI Working Group. MAWI Working Group Traffic Archive, 2007.