http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 8 (8): 1180-1188, 2009
ISSN 1812-5638

Using Renyi Cross Entropy to Analyze Traffic Matrix and Detect DDoS Attacks

[1,2]Ruoyu Yan and [1]Qinghua Zheng
[1]Moe Klinns Lab. and Sklms Lab., Department of Computer Science and Technology,
Xi'an Jiaotong University Xi'an, Shanxi Proviance, 710049, China
[2]Collage of Information, Guangdong Ocean University, Zhanjiang,
Guangdong Proviance, 524088, China

Abstract: In this study, we propose Renyi cross entropy to analyze matrix traffic and detect anomaly rather than other entropy metrics, such as Shannon entropy, used extensively in many earlier studies. At first, we introduce a new type of traffic termed IF-flow (internal flow) collected in router. IF-flow can make the attack traffic more conspicuous in a large number of normal traffics, which makes attacks, especially DDoS attacks, spotted more easily. Then, the analysis of Renyi cross entropy of IF-flow matrix traffic, Abilene matrix traffic confirms that matrix traffic distribution has local stability in time. This conclusion provides a guidance to accurately detect anomaly. Finally, Renyi cross entropy is used to detect DDoS attacks existed in IF-flow testing data set and Abilene testing data set. The results of detection experiments show Renyi cross entropy based method can detect DDoS attacks at the beginning with higher detection rate, lower false alarm than Shannon entropy based method.

Key words: Anomaly detection, DDoS attack, Renyi cross entropy, traffic matrix, traffic analysis

INTRODUCTION

Information-theory-based measurements have been successfully used to analyze and detect specific types of malicious traffic and experiments show that with only one metric this approach returns almost an order of magnitude improvement in detection (Kumar *et al*., 2007; Lakhina *et al*., 2005; Wagner and Plattner, 2005). Applying Occam's Razor (that means among all hypotheses consistent with the facts, choose the simplest), it is hard not to conclude that information theory deserves scrutiny, at the very least (Eiland and Liebrock, 2006).

Kumar *et al*. (2007) calculated Shannon entropy on four traffic features (source IP, destination IP, source port and destination port) to detect DDoS attacks in ISP network. For accurate classifying different types of network traffic, Yuan *et al*. (2008) applied information entropy technology to a set of 15 attributes of each flow. Lakhina *et al*. (2005) calculated Shannon entropy of traffic features, such as IP addresses and ports, observed in OD (Origin-Destination) flows traces. All these methods work at the cost of lots of statistical work. When traffic records are huge, time spent to extract traffic features is a bottleneck.

Kolmogorov complexity (actually another kind of entropy metric) describes a mechanism for identifying information density of a string and is always computed by compression algorithm applied to every packet in network. The complexity is effective to detect DDoS attacks (Kulkarni and Bush, 2006) or worm attacks (Wagner and Plattner, 2005). However, these compression algorithms used to compute complexity must have higher speed and packets in network should arrive at low speed. This makes it hard to be used in high speed network.

Renyi cross entropy (later we use RCE to represent it) is first used by Eiland and Liebrock (2006) to analyze dynamic changes of the network topology. Qin *et al*. (2008) introduced a type of traffic flow termed region flow aggregated by IP prefix clustering in large scale network, then use RCE to measure dynamic changes of three traffic features in region flow. It is clear that these two literatures specially focus on network topology or traffic dynamic change and never use RCE to detect traffic anomaly. In our previous work (Yan *et al*., 2008a), we propose using Renyi cross entropy and Multi-scale entropy to detect anomaly, but concrete detection experiments and its results are not provided in detail.

Peng *et al*. (2003) proposed a method to keep a history of legitimate IP addresses appeared previously in router. The history IP database is then used to decide whether a DDoS attack has occurred at current time. The big problem is how to effectively maintain a huge history IP database in router. There are other

Corresponding Author: Ruoyu Yan, Xi'an Jiaotong University, Xi'an, Shanxi Proviance, 710049, China Tel: +86-15829630593

methods (Kumar *et al*., 2007; Yan *et al*., 2008b) used to detect DDoS attacks, but all these methods are not applied to matrix traffic but single traffic trace.

In this study we focus on how information theory, especially RCE metric is applied to detect DDoS attacks. RCE is easy to be calculated and has a strong ability to display matrix traffic distribution change. We apply RCE methods to a traffic flow model termed IF-flow in this paper. IF-flow traffic can be obtained from NetFlow records in Cisco routers. This reduces the computation and statistical work. Different from OD flow (Lakhina *et al*., 2005) and region flow (Qin *et al*., 2008), IF-flow is a Port-to-Port unidirectional traffic in a router, by which internal traffic matrix can be constructed. The amount of IF-flow created is very much smaller than that of region flow because of limited port count in a router, which makes it easer to spot anomalous flow(s). IF-flow is more convenient to collect than OD flow because we needn't consider packet routing between multiple routers. To make the RCE method understandable, we analyze the local stability of IF-flow matrix traffic and Abilene matrix traffic in time. Earlier study (Yan *et al*., 2008a) also provided two abnormal traffic cases, such as DDoS attack and device failure spotted in IF-flow matrix traffic, to illustrate how RCE is used to detect anomaly. To validate the detection performance of RCE method, we give two experiments: one is to compare DDoS attacks detection performance in two different testing data sets; the other is to compare the detection performance between RCE and Shannon entropy. These experiments show RCE method has higher detection rate, lower false alarm than Shannon entropy method.

RENYI CROSS ENTROPY

Renyi's generalized entropies were introduced by Aczel and Darciczy (1975) as family of measures that characterize the distribution of a random variable. The RCE of order α can be written as:

$$L_{\alpha}(P,Q) = \frac{1}{1-\alpha}\log\sum_{i=1}^{N}\frac{p_i^{\alpha}}{q_i^{\alpha-1}} \quad (1)$$

where, P and Q are discrete random variables, p_i and q_i are their distribution functions. The K-L distance (Kullback-Leibler) is a special case of the RCE for $\alpha \rightarrow 1$. The RCE measures how much the distribution P differs from Q in the sense of statistical distinguishability.

One of important properties of the RCE is, $L_{\alpha}(P, Q) \leq 0$, if $\alpha \geq 0$, with equality if and only if P = Q or $\alpha = 0$. Another property is the more decreasing in L_{α} (P, Q), the more information obtained from one observation for discriminating between P and Q. Our experiments show that different α ($0<\alpha<1$) affects the detection performance little and $\alpha = 0.5$ has a good result relatively. So we choose $\alpha = 0.5$ in Eq. 1 in the following experiments. The RCE is symmetric and can be rewritten in the form of Eq. 2 to make $L_{0.5}$ (P, Q) always non-negative.

$$L_{0.5}(P,Q) = -2\log\sum_{i=1}^{N}\sqrt{p_i q_i} \quad (2)$$

In general, the network traffic is stable and changes little during a short period of time and RCE is close to zero. But abnormal behaviors, such as DDoS attacks, worms and device failure, can lead to sudden changes of traffic features. To calculate RCE between two continuous traffic observations is an intuitive way to find these anomalies in network. We also can set a threshold such as 3σ criterion or an empirical constant value to pinpoint these anomalies accurately. If the RCE is larger than the threshold, it is concluded that there is an anomaly in current network traffic.

IF-FLOW TRAFFIC

Definition of three types of link traffic: For the sake of facilitating the description, at first we give definitions of three types of flow traffic.

- **IF-flow:** A group of packets traveling from one port to another port in a router per unit time
- **Input link:** A group of packets entering a router from one port per unit time
- **Output link:** A group of packets leaving a router from one port per unit time

An IF-flow traffic matrix is composed of All IF-flows. We use two port numbers to identify one IF-flow. For example, one IF-flow coming from port A and going out from port C is marked as IF-flow A-C. IF-flows are different from other link traffic such as input links, output links or OD flows, which are always associated with two router ports and can be looked on as a combination of output links and input links. In Fig. 1, as an example, IF-flow A-C builds a virtual connection between output link C and input link A. Some remarkable merits of IF-flow can be obtained.

The traffic actually observed on output links (the same for input links) arises from the superposition of IF-flows within a router, which can be seen in Fig. 1. The

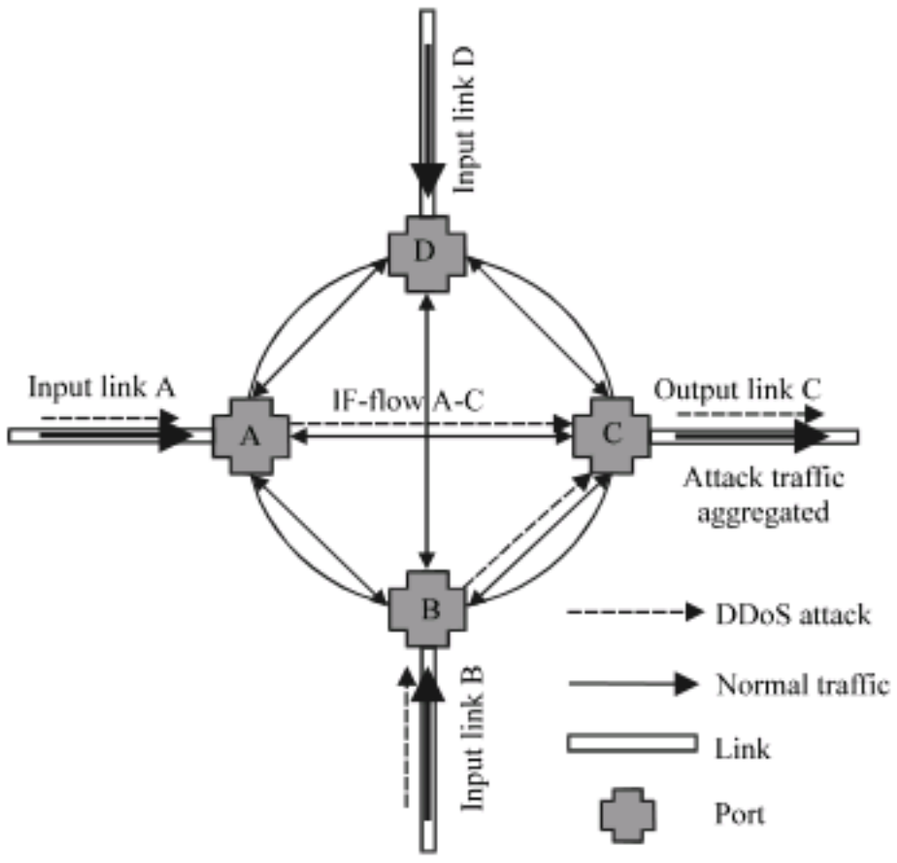

Fig. 1: DDoS attack simulation

relationship between output links and IF-flows can be concisely captured in the routing matrix A. The matrix A has size (output links count)×(IF-flows count), where, A_{ij} = 1 if IF-flow j traverses output link I and is zero otherwise. Then the vector of traffic count on output links (y) is related to the vector of traffic count on IF-flow (x) by y = Ax. In this way, the correlation between IF-flows and output links (or input links) is established. For example, in Fig. 1, the matrix A has size 4×16 and is expressed as follows:

1 0 0 0 1 0 0 0 1 0 0 0 1 0 0 0
0 1 0 0 0 1 0 0 0 1 0 0 0 1 0 0
0 0 1 0 0 0 1 0 0 0 1 0 0 0 1 0
0 0 0 1 0 0 0 1 0 0 0 1 0 0 0 1

Merits of using IF-flows to detect anomaly: Many researches in anomaly detection have focused on single-link traffic data which has limited detection ability. A router-wide view of traffic like IF-flow matrix enables detection of anomalies dwarfed in individual link traffic. We give a concrete simulation of DDoS attack as follows to illustrate IF-flow's merits in detail.

If there is a router with n ports, then it can produce n^2 IF-flows; as for n = 4, a router can produce 16 IF-flows. In order to represent the validity of our method clearly, according to the characteristic of DDoS attack path, we make some hypotheses, although the real situation is not so simple like in Fig. 1:

- Among these IF-flows, two of them are anomalous which are A-C and B-C
- Traffic count on each input links and output links is 1 and traffic count on each IF-flow is 1/3 on average (we don't consider traffic count on IF-flow A-A, B-B,C-C,D-D because of little traffic)
- Count of anomalous traffic is 1/10 respectively on input links A and B. Hence anomalous traffic counts for 10% of all on input links A and B, 20% on output links C, 30% on IF-flow A-C and B-C

Thereby, intuitively we conclude that IF-flows are more effective than input links and output links in anomaly detection. In addition, IF-flows can let us know which ports attack traffic come from and to which port they are aggregated. This port message is very useful when applying proper measures to defense attacks.

Many attackers try to distribute their DDoS attack traffic equably in large-scale network for hiding attack behaviors and avoiding being spotted at an early time. Schemes deployed on a single link, as many anomaly-based IDS systems do, are hard to spot the attacks timely. On the contrary, IF-flows based method can find this kind of attack early for IF-flows can amplify the ratio of attack traffic to normal traffic.

IF-flow data collection: Now there isn't any tools to obtain IF-flows directly and using SNMP (simple network management protocol) to access MIB (management information base) in router can only collect ports' ingress and egress traffic statistics in router. Despite IF-flows can be obtained by analyzing packet routing, but routing table in router must be used and all packets traversing router must be monitored. This consumes many time and resources.

We can conveniently aggregate IF-flow traffic in virtue of NetFlow cache (http://www.cisco.com/en/US/products/ps6601/prod_white_papers_list.html) in router. Based on flow concept, NetFlow is a technical solution proposed by Cisco Company for traffic accounting, analysis and monitoring. Flow is a unidirectional stream of packets with the same five tuples: source IP, source port, destination IP, destination port and layer 3 protocol type.

Concrete procedure is provided to obtain IF-flows statistics:

- **Step 1:** Open router's NetFlow cache, then NetFlow records are created per unit time and are encapsulated in UDP packets which are mirrored to a traffic analysis server

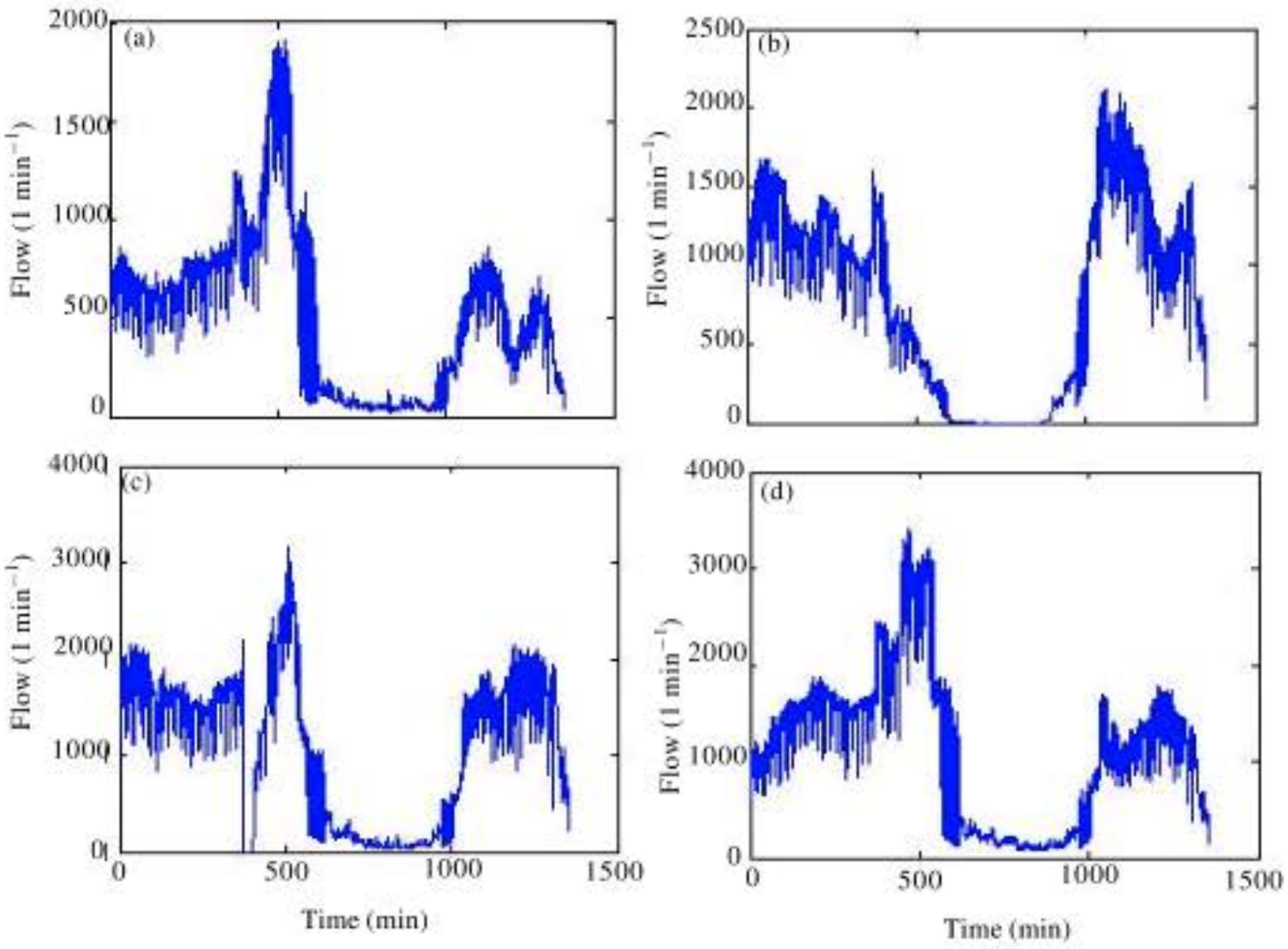

Fig. 2: Some IF-flows leaving port#7 (time from 2007.12.27 4:01 PM to 2007.12.28 2:36 PM), (a) IF-flow 1-7, (b) IF-flow4-7, (c) IF-flow 5-7 and (d) IF-flow 8-7

- **Step 2:** Traffic analysis server receives UDP packets at some UDP port; unpacks packets to extract NetFlow records; and then stores them in a database
- **Step 3:** Use SQL codes, IF-flows of byte, packet and flow count are summed up by using input and output attributes in NetFlow records per unit time

Almost one day(from 2007.12.27 4:01 pm to 2007.12.28 2:36 pm) of IF-flows traces of byte, packet and flow count are collected in a ten-port router for every one minute time bin in Xi'an JiaoTong University. All persent experiments are based on the IF-flows set. An example of 4 IF-flow traces of flow count is shown in Fig. 2a-d.

LOCAL STABILITY ANALYSIS OF TRAFFIC DISTRIBUTION IN TIME

RCE measures how much the distribution P differs from Q in the sense of statistical distinguishability, so the RCE value is the more near zero, the more close traffic distributions of the two observations are. According to the local theory that traffic in local time changes little, when traffic distribution of an observation is compared with others before or after it in time, we should have the common sense: the observations compared are the more far away in time, the more large the RCE value is; the observations compared are the more near in time, the more small the RCE value is.

In order to verify the local theory above, we compute the RCEs of real IF-flow traffic matrixes and a week of real Abilene traffic matrixes respectively. Abilene traffic is collected from the Abilene backbone (Abilene data set, 2004). For each observation, RCEs are calculated between it and 120 observations before or after it in time (the truth time is 2 h before or after it). Then the mean valueof all observations at every time point (240 time points in total) is calculated and shown in Fig. 3. Time point before the observation is set negative time and time point after it positive time. At time point zero the RCE is calculated between itself and result is also zero. We can see that the result showed in Fig. 3 meets persent expectation in the extreme. That is: time is more far away the observation, the larger RCE. Moreover, if observations compared with are in the same time distance before or after the observation, their RCEs are very close. But there are some differences between two kinds of traffic. For IF-flow traffic, entropies increase almost linearly with time distance and are higher than that of Abilene traffic. This means traffic distribution in IF-flow is more easily shifted and in Abilene shifted slowly. For Abilene traffic, there exists periodical characteristic because of diurnal feature, which makes entropies showed in Fig. 3 also change periodically.

Next we use the local stability of traffic distribution to discern anomaly in traffic. When RCE calculated is relatively higher than those nearby, we think there is an abnormity happened, because the local stability is broken.

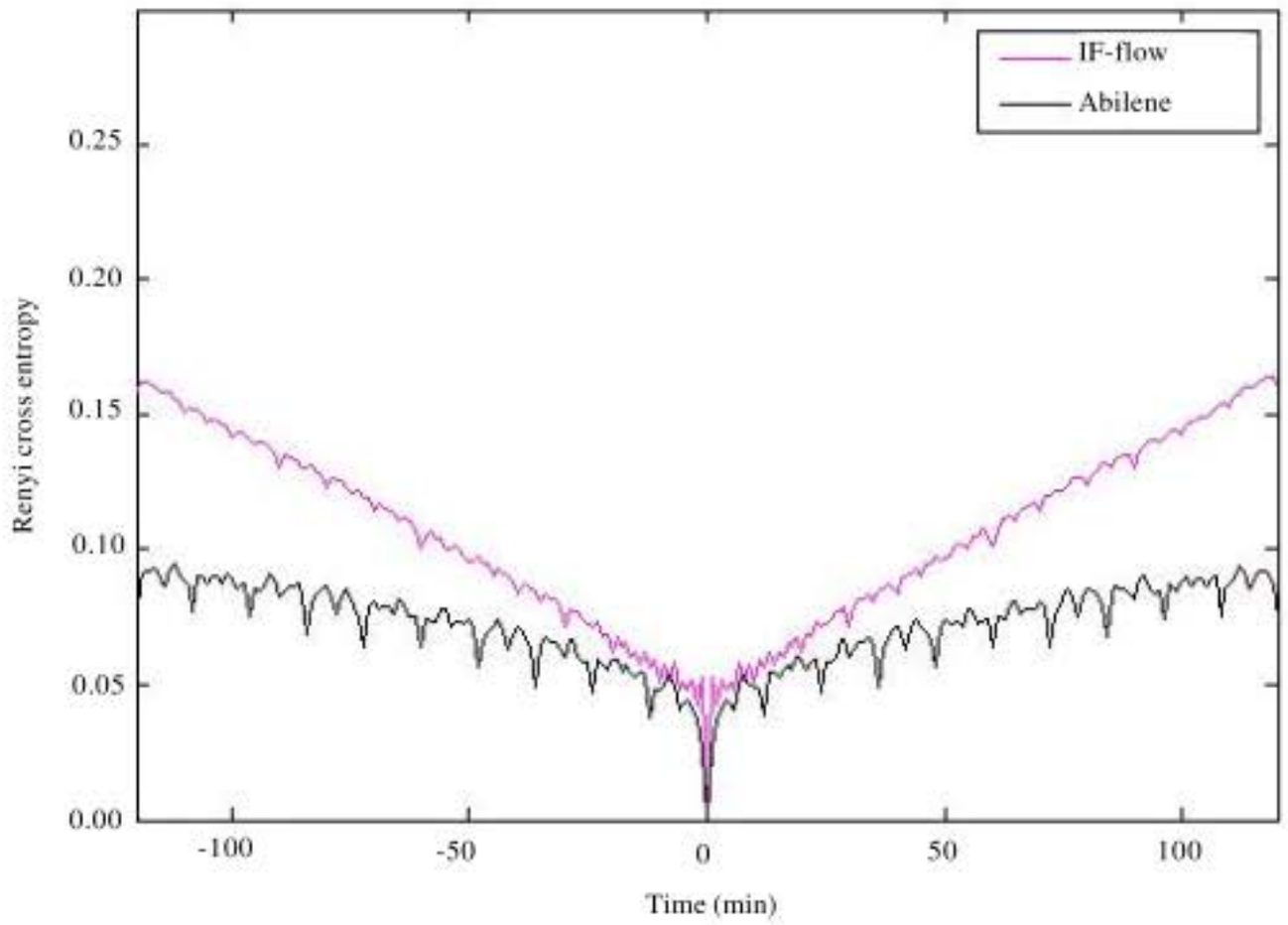

Fig. 3: The relationship between time distance and RCE of IF-flow traffic matrixes and Abilene traffic matrixes

APPLYING RCE TO DDoS ATTACK DETECTION

IF-flow traffic matrix testing data set: Figure 4 displays RCEs of whole real IF-flow traffic matrixes at every time bin. We can see there are sharp increases of RCEs from 374 to 402 time bin because of device failure. Besides, RCEs are very large from 600 to 1050 time bin (the real time is from 01:00 to 08:00 am also so) because of traffic sparse. Sparse traffic, which can bring about traffic distribution unstable in the sense of statistical distinguishability, is mainly caused by most students who can not surf internet during power control time. Real IF-flow traffics of flow count are used here as original traffics. After eliminating traffics in the two time intervals mentioned above, we use method described in literature (Soule *et al*., 2005) to generate synthetic DDoS attacks in IF-flow traffics. Detailed parameters are displayed in Table 1.

Almost, all DDoS attacks last between 1 and 30 min (Moore *et al*., 2001), although there are some outliers that only last less than 1 min. Here the attack lasting time is selected as 1 min (namely one unit time), a fixed time. Of course, the duration of attack can vary at different interval, but we only care about early detection in time which is the most important. That means attacks can be detected by method at the beginning. In Table 1, δ represents the percentage of DDoS attack traffic to normal traffic (attack intensity). The δ is a multiplicative factor which is multiple of 0.1 and multiplied by the baseline traffic to generate the attack traffic load. (Src, Dst) refers to DDoS attack coming from *Src* ports and leaving from Dst ports. Here Dst = 1 indicates DDoS attack traffics are only aggregated to one egress port. Each DDoS attack affects 1~9 IF-flows, namely (1+9)/2 = 5 IF-flows on average. For 0.1~1 attack intensity, attack traffic accounts for (0.1×5)/(9+0.1×5)) ~ (1×5)/(9+(1×5)) namely 5.3~35.7% of output link on average. It can clearly be seen that the percentage of attack traffic is very small. Shape functions are not needed, for attack duration is set fixed one unit time (1 min) (Soule *et al*., 2005).

When we generate synthetic traffic, at first traffic matrix sub-series with length of 150 unit time are extracted at random from original traffic matrixes series; after that Daubechies-5 discrete wavelet transform is used to smooth the sub-series and then a zero mean Gaussian noise is added; finally traffic of a synthetic DDoS attack is injected after attack start time is selected randomly. For each attack intensity δ we have produced 100 testing samples with DDoS attack according to the parameters showed in Table 1 and technique mentioned above.

Abilene OD flow traffic matrix testing data set: Besides, in present experiment we have used one week of public data set collected from the Abilene backbone (http://www.cs.utexas.edu/~yzhang/research/AbileneTM/X01.gz). The collection time is from 2004-03-01 to 2004-03-07. As we do to generate synthetic IF-flow traffic matrix testing data set, for each δ we have produced 100 testing samples with DDoS attack. The only difference is the Abilene backbone has 11 PoPs (Points of

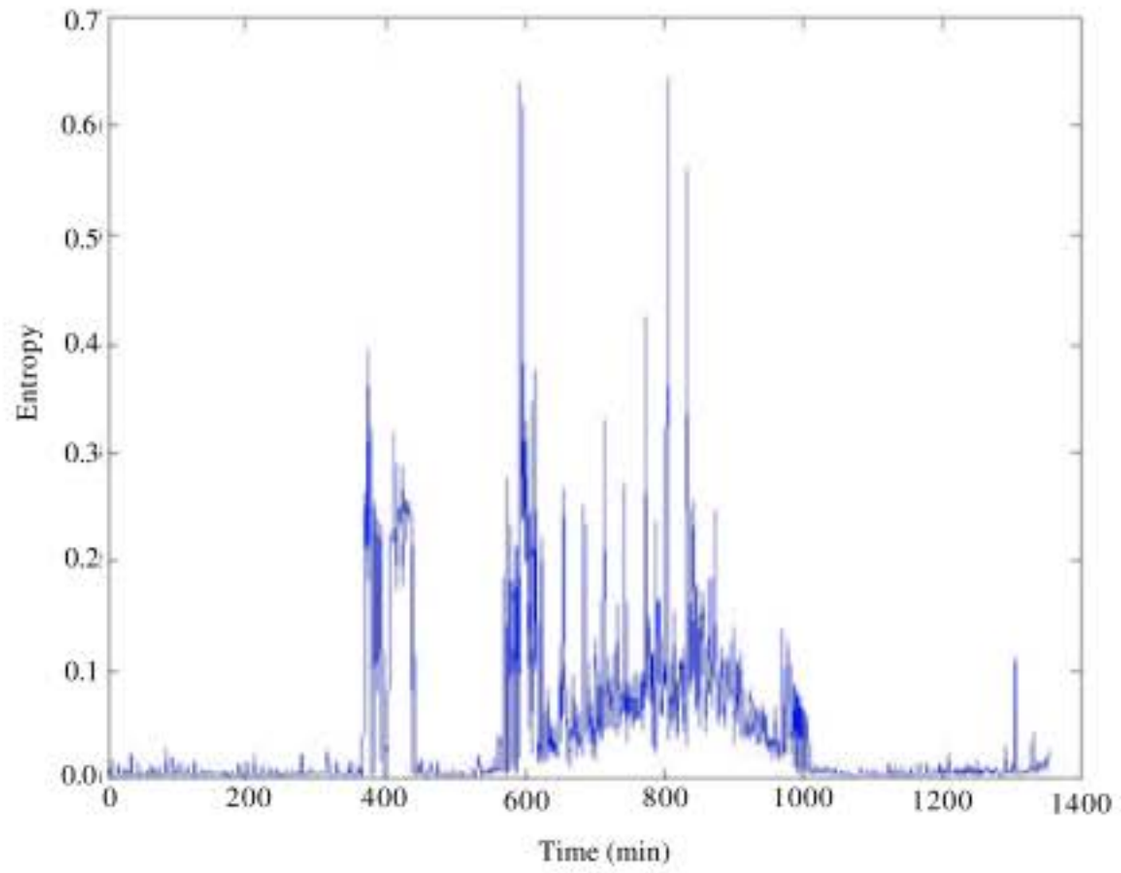

Fig. 4: The RCE of IF-flow traffic matrixes throughout the time

Table 1: DDoS attack description parameters

Parameter	Possible values
Duration (min)	1
Volume	$0.1 \le \delta \le 1$
Num (Src,Dst)	(1, 1)~ (9, 1)

Presence). Its traffic matrix dimension is 12×12 = 144 OD flows. So each DDoS attack affects 1~11 OD flows, namely (1 = 11)/2 = 6 OD flows on average.

RCE detection method: A simple rule like 3σ heuristic is adopted to make detection. The method is: according to 20 normal RCEs before detection point, compute the anomaly threshold:

$$\text{Threshold} = \bar{x} + m\sigma$$

If current RCE calculated exceeds threshold, we think the RCE is abnormal and an anomaly is determined. $\bar{x}$ is mean value of earlier 20 normal RCEs. σ is standard deviation and m is a positive value ranged from 1 to 5 in the experiment.

RESULTS AND DISCUSSION

For each value of the threshold, all the samples in IF-flow testing set and Abilene OD flow testing set are examined. One false positive percentage and one false negative percentage for each threshold configuration of a scheme are computed. The performance of the method applied to each testing data set is depicted in Receiver Operation Characteristic (ROC) curves. The ROC curve is the plot of True Positive Ratio (TPR), calculated as the percentage of DDoS attacks detected, against False Positive Ratio (FPR), calculated as the percentage of normal traffic falsely classified as DDoS attacks. In Fig. 5, one False Negative Ratio (FNR) and one FPR are average results of detecting synthetic anomaly traffic with the same attack intensity. In Fig. 6, one TPR and one FPR are average detection results at the same threshold (means the same m).

The more enormous anomalies, the easier it is to be detected and vice versa. FNR and FPR should also decrease with the increase of anomaly intensity. But as a matter of fact, Fig. 5a and b show: FNR of two testing sets decreases with the increase of anomaly intensity in the rough, however, FPR differs greatly. As for Abilene testing set, FPR increases with the increase of anomaly intensity by and large, but for IF-flow testing set, FPR shows random. One of the reason is multiple IF-flows with DDoS attack can affect the distribution of traffic each other. The traffic increase of one IF-flow not necessarily increases RCE. On the contrary, the traffic decrease of one IF-flow might increase RCE. The other reason is IF-flow original data set has lesser data samples than Abilene's. This might cause IF-flow synthetic testing samples are simplex, which leads to FPR randomly.

Figure 5a, shows under the same attack intensity, FNR of IF-flow is lower than that of Abilene and the lower abnormal traffic intensity, the lower FNR of IF-flow than that of Abilene. When the attack intensity is between 0.1~0.3, anomaly in Abilene testing data set is harder to be detected and the detection rate is

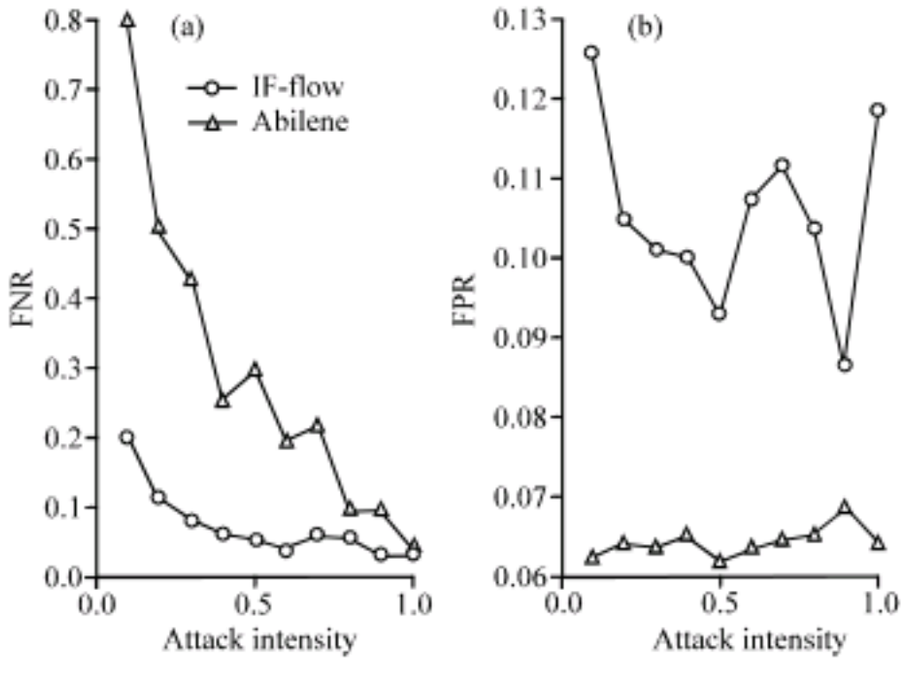

Fig. 5: (a, b) FNR and FPR as a function of the attack intensity

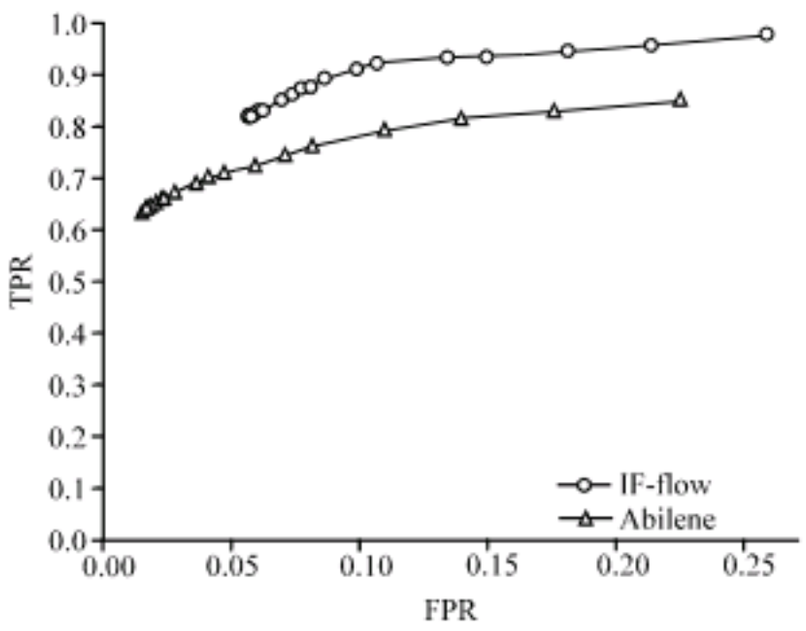

Fig. 6: ROC curves using RCE and two testing data sets

less than 60%. On the contrary, Fig. 5b shows at the same attack intensity, FPR of IF-flow is higher than that of Abilene and the FPR exceeds 10% at most of attack intensity. These show that under the same attack intensity, the method is easier to detect anomaly in IF-flow, but at the same time produces much more false alarms. Likewise, ROC curves in Fig. 6 shows that the method has much higher detection rate of IF-flow than that of Abilene. Detection rate of IF-flow is always over 80% and ten percent higher than that of Abilene.

After analyzing IF-flow and Abilene traffic, we find that IF-flow traffic is more stable most of the time, but there have some regular slump downs in the middle which cause much more violent fluctuation than Abilene traffic. This leads to detection rate and false alarm of IF-flow higher than that of Abilene. On the other hand, IF-flow traffic is measured by flow count and Abilene traffic measured by byte count. Because flow count metric is much more powerful as a measure to detect anomaly than byte count, especially in detecting DdoS attack (Lakhina *et al*., 2004). So measure is also one factor of affecting detection rate.

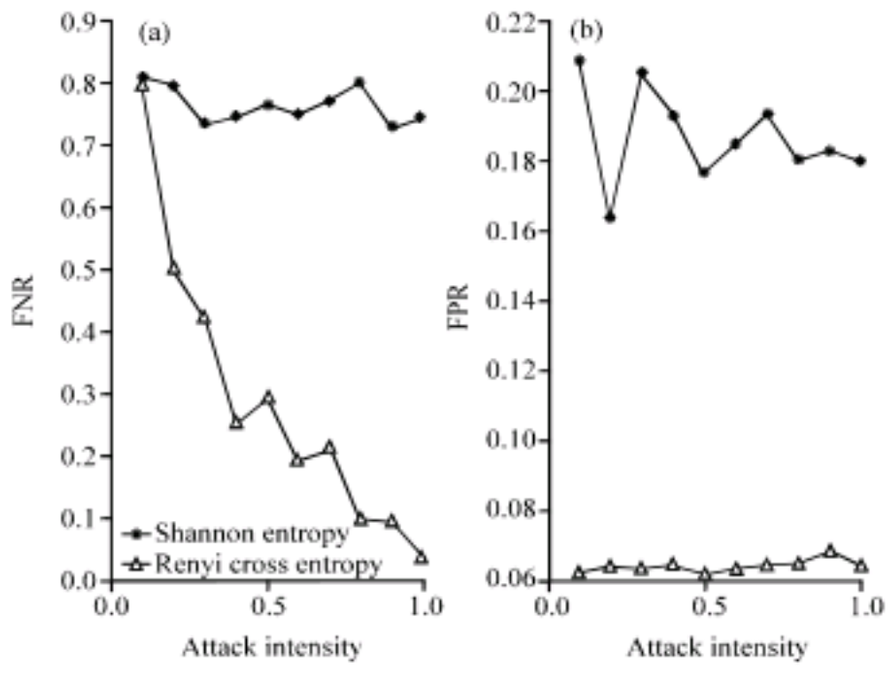

Fig. 7: (a, b) FNR and FPR as a function of the attack intensity

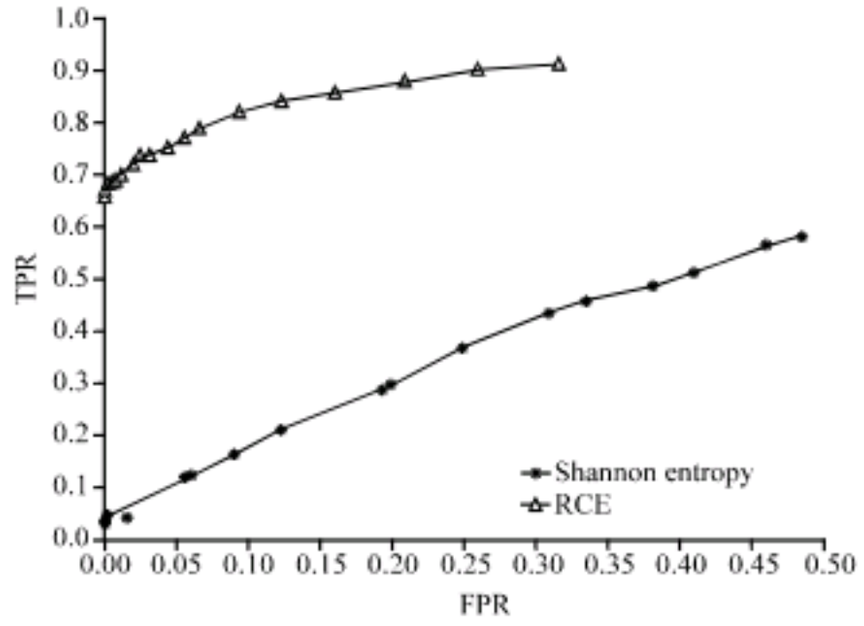

Fig. 8: ROC curves using two kinds of entropies and Abilene testing data set

Although, RCE is effective in anomaly detection, the FPR showen in Fig. 5 is a little high, especially for IF-flow. One main reason is we use threshold parameter m ranged from 1 to 5 in persent experiment. The too low of thresholds always create much false alarm. That means an improved threshold calculation method is needed to decrease false alarm. Another reason is the attack intensity is not very strong. In the output link traffic with attack, attack traffic is actually 5.3~35.7% of all on average. Besides, when an anomaly is detected, sometimes there is a false alarm accompanied (Yan *et al*., 2008b), which can not be ignored.

Next we compare the performance of RCE with that of Shannon entropy in Abilene testing data set. The Shannon entropy is widely used Kumar *et al*. (2007) and Lakhina *et al*. (2005). Detection results are showed in Fig. 7 and 8. Figure 7a, shows under the same attack intensity, FNR of RCE is very lower than that of Shannon entropy and the higher abnormal traffic intensity, the lower FNR of RCE than that of Shannon entropy. At all

the attack intensities, anomaly in Abilene testing data set is harder to be detected by Shannon entropy and the detection rate never exceeds 30%. Similarly, Fig. 7b shows at the same attack intensity, FPR of Shannon entropy is higher than that of RCE and the FPR exceeds 18% at most of attack intensities. These show that at the same attack intensity, RCE is much easier to detect anomaly in Abilene and at the same time produces much less false alarms. Likewise, ROC curves in Fig. 8 show that RCE has very much higher detection rate in Abilene than that of Shannon entropy. Detection rate of RCE is 50% higher than that of Shannon entropy. That means Shannon entropy is not suitable for DDoS attack detection here.

We think there two factors that make RCE much better than Shannon entropy in traffic anomaly detection. One is Shannon entropy is computed based on traffic matrix distribution in space, however RCE is computed not only based on space factor (traffic matrix distribution), but also the distribution change in time(because RCE considers two different observations). The local stability of traffic matrix we analyzed before makes clear that RCE method is suitable for exposing traffic anomaly in time, except for exposing anomaly like Shannon entropy does in space. The other is traffic matrix always shows local stability in spite of its extent and the more conspicuous the stability is, the more easily anomaly in traffic matrix is spotted by RCE method. Therefore, instead of Shannon entropy, the RCE can be introduced in some literatures (Kumar *et al*., 2007; Lakhina *et al*., 2005) which used Shannon entropy to detect anomaly. We expect that there will have some performance improvements on them.

CONCLUSION

This study proposes a new method based on information theory to analyze traffic within router and detect anomaly. We mainly have three contributions as follows:

- Based on internal traffic within a router, define a new type of link traffic IF-flow to construct traffic matrix, which makes malicious traffic more conspicuous
- Use RCE to analyze IF-flow traffic and Abilene traffic, which conforms that traffic distribution in time is locally stable
- Propose RCE based method to detect anomaly and DDoS attack detection experiments show that the method has higher detection performance than Shannon entropy based method

In order to further improve RCE detection performance, in the future we will do some experiments to find more powerful method of setting detection threshold; on the other hand, when anomaly is detected, how to pinpoint abnormal IF-flows responsible for the anomaly is also our future work.

ACKNOWLEDGMENTS

This study is supported mainly by National Natural Science Foundation of China (60633020, 60473136) and National High Tech. Development Plan of China (2006BAH02A24-2, 2006BAK11B02,2007AA01Z475, 2008AA01Z415).

REFERENCES

Aczel, J. and Z. Darciczy, 1975. On Measures of Information and their Characterizations. Academic Press, New York.

Eiland, E.E. and L.M. Liebrock, 2006. An application of information theory to intrusion detection. Proceedings of the 4th IEEE International Workshop on Information Assurance, Apr. 13-14, Washington, DC., USA., pp: 119-134.

Kulkarni, A. and S. Bush, 2006. Detecting distributed denial-of-service attacks using kolmogorov complexity metrics. J. Network Syst. Manage., 14: 69-80.

Kumar, K., R.C. Joshil and K. Singh, 2007. A distributed approach using entropy to detect DDoS attacks in ISP domain. Proceedings of the IEEE International Conference on Signal Processing, Communications and Networking, Feb. 22-24, Chennai, India, pp: 331-337.

Lakhina, A., M. Crovella and C. Diot, 2004. Characterization of network-wide anomalies in traffic flows. Proceedings of the 4th ACM SIGCOMM Conference on Internet Measurement, Oct. 25-27, Sicily, Italy, pp: 201-206.

Lakhina, A., M. Crovella and C. Diot, 2005. Mining anomalies using traffic feature distributions. ACM Sigcomm Comput. Commun. Rev., 35: 217-228.

Moore, D., G.M. Voelker and S. Savage, 2001. Inferring internet denial-of-service activity. Proceeding of the 10th USENIX Security Symposium, 2001, IEEE Xplore, pp: 9-22.

Peng, T., C. Leckie and K. Ramamohanarao, 2003. Protection from distributed denial of service attacks using history-based IP filtering. Proceedings of the IEEE International Conference on Communications, May 11-15, IEEE Xplore, pp: 482-486.

Qin, T., X. Guan, W. Li and P. Wang, 2008. Dynamic features measurement and analysis for large-scale networks. Proceedings of the IEEE International Workshops on Communications, May 9-23, Beijing, pp: 212-216.

Soule, A., K. Salamatian and N. Taft, 2005. Combining filtering and statistical methods for anomaly detection. Proceedings of the 5th ACM SIGCOMM Conference on Internet Measurement, Oct. 19-21, Berkeley, CA., pp: 331-344.

Wagner, A. and B. Plattner, 2005. Entropy based worm and anomaly detection in fast IP networks. Proceedings of the 14th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprise, Jun. 13-15, Washington, DC., USA., pp: 172-177.

Yan, R., Q. Zheng and W. Peng, 2008a. Multi-scale entropy and renyi cross entropy based traffic anomaly detection. Proceedings of the 11th IEEE Singapore International Conference on Communications Systems, Nov. 19-21, Guangzhou, pp: 554-558.

Yan, R., Q. Zheng, G. Niu and S. Gao, 2008b. A new way to detect DDoS attacks within single router. Proceedings of the 11th IEEE Singapore International Conference on Communications Systems, Nov. 19-21, Guangzhou, pp: 1192-1196.

Yuan, J., Z. Li and R. Yuan, 2008. Information entropy based clustering method for unsupervised internet traffic classification. Proceedings of the IEEE International Conference on Communications, May 19-23, Beijing, pp: 1588-1592.