Distributed Denial of Service Attacks Detection Method Based on Conditional Random Fields

Shi-wen CHEN, Jiang-xing WU, Xiao-long YE, Tong GUO
National Digital Switching System Engineering and Technological R&D Center
Zhengzhou, China
Email: ndsccsw@126.com

Abstract—In order to detect distributed denial of service (DDoS) attacks accurately and efficiently, a new detection model based on conditional random fields (CRF) was proposed. The CRF based model incorporates the signature-based and anomaly-based detection methods to a hybrid system. The selected features include source IP entropy, destination IP entropy, source port entropy, destination port entropy, protocol number and etc. The CRF based model combines these IP flow entropies and other fingerprints into a normalize entropy as the feature vectors to depict the states of the monitoring traffic. The training method of the detection model uses the L-BFGS algorithm. And the model only needs to inspect the IP header fields of each packet, which makes it possible for real-time implementation even on real time network traffic. The CRF based model may have the ability to detect new form of forthcoming attacks, because it is independent from any specific DDoS flooding attack tools. The experiment results show that the CRF based method has higher detection accuracy and sensitivity as well as lower false positive alarms. Experiment with KDD CUP1999, DARPA 2000 and generated attack datasets, the CRF based model outperforms other well-known detection methods such as Naïve Bayes, KNN, SVM and etc. The accuracy goes beyond 95.0% and the false alarm rate is less than 5.0%. Meanwhile, the CRF based model is robust under massive background network traffic.

Index Terms—Distributed Denial of Service, Conditional Random Fields, Feature Selection, L-BFGS Algorithm, entropy

I. INTRODUCTION

Distributed denial of service (DDoS) attacks send mass of requests to the victim through the vulnerabilities of network protocol and operating system, consume network bandwidth and host resources [1][2]. It is a significant security threat to the availability of Internet services. Because there are a multitude of compromised nodes and attack tools available, it is easy for hackers to launch DDoS attacks. The hackers can forge source IP addresses of the attack packets to escape from tracing [3]. Meanwhile, due to the DDoS attacks and flash crowds have similar behavior, attackers may mimic the behaviors just like a sudden increase of legitimate traffic. As a result, the detectors may be fooled by malicious traffic or treat the legitimate flash crowds as DDoS attacks. In other words, both of the false negative and the false positive events may happen frequently. Therefore, how to distinguish DDoS flooding attacks from flash events is a challenge for the detectors [4]. Hence, this paper focuses on how to detect flooding DDoS attacks accurately and efficiently.

Just like intrusion detection systems, the methods of DDoS attacks detection can mainly be divided into misuse and anomaly detection mechanisms [5][6][7][8]. Misuse detection relies on predefined features or fingerprints of specific DDoS attacks. It’s effective to process the definite special pattern. Unfortunately, the attack tools can mimic these features and fool the detectors, and hackers can also forge the source IP addresses of the attack packets with the real Internet IP address existing somewhere. So, it is hard for the feature-based misuse detection schemes to detect the malicious traffic from an observed massive traffic. On the other hand, anomaly detection compares the abnormal behavior of the system with normal behaviors. It’s not precise but may be effective to detect unknown intrusions.

To address the above mentioned problems, we propose a new hybrid DDoS attacks detection approach based on Conditional Random Fields (CRF) [9][14]. The major contributions of our work can be summarized as follows:

• We propose a new DDoS attacks detection model based on CRF, so we can incorporate the signature-based and anomaly-based detection methods to a hybrid system. Because CRFs have the ability to synthesize many features into a union detection vector without the demand of independence.

• We propose a concept, IP Flow Entropy (IPE) as the multi-feature vectors, to depict the states of the monitor traffic. By combining IPE, One-Way Connection Density (OWCD) [16] and other features into one metric, the model can be used to detect various DDoS attacks with high sensitivity and low false alarm rate.

• The L-BFGS algorithm [15] is used as the CRF model training method, at the same time, the detection method only needs to inspect the IP header fields of each packet, which makes it simple and possible for real-time implementation even on high speed networks.

• By comparing and analyzing with other detection methods in DARPA2000 and TFN2K real attack dataset, the experiment results show that our CRF based detection model outperforms other well-known methods such as Naïve Bayes, KNN, SVM and etc. The accuracy goes beyong 95.0%, and the false alarm rate is less than 5.0%.
The CRF model is robust under massive background traffic.

* The CRF based model is independent of any specific DDoS flooding attack tools. Therefore, on a certain extent, it has the ability to detect new form of forthcoming attacks.

The remainder of this paper is structured as follows: In Section 2 we describe the related work. In Section 3 we give the concept of the conditional random fields, then propose the CRF based detection model, including the architecture of the model, feature selection, model training and probability computation. In section 4, we evaluate the performance of the suggested method. Eventually, in section 5, we draw a conclusion on our research.

II. RELATED WORK

DDoS attacks have many characteristics such as easy to launch, massive and dormant, so how to detect DDoS attacks accurately and effectively becomes a hot research in intrusion detection systems [25][26][27][28][29][30]. At present, the main method of DDoS attacks detection is using one of the statistical properties such as bursty of the traffic [3][4], dispersibility of the source IP address [5][6], asymmetry of the traffic [7][8], TCP protocol flag and etc. There are several problems including weak adaptability, low veracity and high false alarms rate in the mono-feature based detection measures.

Conditional Random Fields (CRF)[14] is an undirected graphical model. It’s the combination of probability theory, graph theory and machine learning. CRF does not require conditional independence assumption strictly, which is similar to the self-similarity and long-range dependence features of network traffic. CRF model has been widely used in bioinformatics, Natural Language Processing and machine vision [9][10]. Gupta et al [11] proposed CRF for intrusion detection and validated the availability and the real-time character of the CRF model [12]. Liu et al [13] introduced CRF model for DDoS attacks detection, the traffic feature conditional entropy and behavior profile deviate degree were used for the detection, which improved the detection precision of TCP flood, UDP flood and ICMP flood attacks.

In this paper, an improved DDoS attack detection method based on CRF model is introduced. This approach uses IP entropies and other features as the selected union feature vector. By comparing and analyzing with different feature selection methods, the experiment result show that our DDoS attacks detection model based on CRF and fusion features outperforms other well-known methods such as KNN, SVM and etc. The accuracy goes beyond 95.0%, and the false alarm rate is less than 5.0%. The CRF model is robust under massive background traffic.

III. CONDITIONAL RANDOM FIELD MODEL

A. Definition

Definition 1.CRF definition [14]:

Consider the random variable \( X \) and \( Y \), \( P(Y \mid X) \) is the conditional probability distribution from \( X \) and \( Y \). Let the graph \( G = (V, E) \) be a Markov random fields, namely for any node \( v \),

\[
P(Y_v \mid X, Y_w, w \neq v) = P(Y_v \mid X, Y_w, w \sim v)
\]

Then \( P(Y \mid X) \) is called the conditional random field. Where \( w \neq v \) denotes all the node except the node \( v \) in graph \( G = (V, E) \), \( w \sim v \) denote the node that have edge connection with the node \( v \), \( Y_v \) and \( Y_w \) are random variable corresponding to the node \( v \) and \( w \) respectively.

Definition 2. Linear chain CRF definition:

Let the random variable sequence \( X = (X_1, X_2, ..., Y_n) \) and \( Y = (Y_1, Y_2, ..., Y_n) \) denoted by linear chain, and the conditional distribution \( P(Y \mid X) \) obeys the Markov property

\[
P(Y_k \mid X, Y_1, ..., Y_{k-1}, Y_{k+1}, ..., Y_n) = P(Y_k \mid X)
\]

Then \( P(Y \mid X) \) is a linear chain conditional random field.

Fig. 1 shows the chain-structured case of the CRF model.

![Figure 1. Chain-structured case of CRF model.](attachment:image.png)

The calculation of CRF probability define as follow: Given the certain conditional probability model, \( P(Y \mid X) \) of the label sequence \( Y \) can be computed using forward-backward algorithm according to sequence \( X \). Define the potential function \( \psi_k (y) \)

\[
\psi_k(y) = \exp \left( \sum \lambda_k f_k(c, y, c, x) \right)
\]

where \( c \) is the node of maximal clique, \( f_k \) is the eigenfunction, \( \lambda_k \) is the Lagrange multiplier. Then \( P(y \mid x) \) can be given by

\[
P(y \mid x) = \frac{1}{Z(x)} \exp \left( \sum \sum \lambda_k f_k(c, y, x) \right)
\]

where \( Z(x) \) is the normalization factor. In graph \( G = (V, E) \), the maximal clique of graph \( G \) is the edge set \( E \), therefore, for \( e = (i - 1, i) \), \( \psi_{k}(y) \) in (3) can be expressed as

\[
\psi_{k}(y) = \exp \left( \sum \lambda_k f_k(y_{i-1}, y_i, x) + \sum \mu_k g_k(y_i, x) \right)
\]

where \( f_k(y_{i-1}, y_i, x) \) is partial features of the observed sequence and its corresponding label at position \( i \) and \( i - 1 \), \( g_k(y_i, x) \) is the features of the observed and labeled sequence locating at \( i \). Then \( P(y \mid x) \) in (4) can be expressed as
\[ P(y | x) = \frac{1}{Z(x)} \exp \left( \sum_{e} \lambda_{e} f_{e}(y_e, x) + \sum_{i} \mu_{i} g_{i}(y_i, x) \right) \]  

(6)

**B. Detection Method based on CRF**

Fig. 2 shows the frame of the DDoS attacks detection based on CRF model, it consist of data preprocessing, graphical structure selection, potential function definition, model training, attack detection, output label and etc.

![Frame chart of DDoS attacks detection based on CRF model.](image)

Figure 2. Frame chart of DDoS attacks detection based on CRF model.

The detail description of Fig. 2 is shown below.

Data preprocessing extract IP packet features from offline data or real-time traffic, then compute the value of the OWCD and the IP flow entropy, which are used for model training and detection.

Graphical structure selection: use the first order linear form as the structure of CRF graphical model, and make neighbor labels meeting Markov properties, that is to say, present label is only related to the previous label neighborly. The probability distribution of label sequence is calculated through the formula (6).

Potential function definition: For a graph \( G = (V, E) \) expressed by the first order linear form, and the edge is \( e = (i-1, i) \), the potential function \( \psi_{ij}(y_i) \) can expressed as formula (5).

Model training is the parameter estimation for the CRF model. We use maximum likelihood estimation method for parameter \( \theta \) estimation according to the training dataset \( D \) (including observation sequence \( X \) and label sequence \( Y \)). The estimation is realized by L-BFGS algorithm [15], which converts parameter estimation process to an optimization question.

The attack detection judge the preprocessed monitoring traffic whether it has DDoS attacks or not. The DDoS attacks detection model is equivalent to seek the maximum conditional probability of label sequence \( y^* = (y_1^*, y_2^*, ..., y_n^*) \) under a known CRF model \( P(Y | X) \) and the sequence \( x = (x_1, x_2, ..., x_n) \). Therefore, we can use Viterbi algorithm [14] to label the traffic with normal or attacks.

**C. Feature Selection**

In the DDoS attacks detection method based on CRF model, the feature set is compose of the OWCD and the IPE, where the OWCD is the proportion of non-answer packets and total packets in IP flows. Statistical result shows that the OWCD is below 30% at normal, but it change to nearly 100% when the DDoS attacks started using forged source IP address [16]. The IPE is the entropy of some IP properties including source IP address, destination IP address, source port, destination port and protocol type. Accordingly, the IPE include the entropy of source IP address \( E_{ip} \), the entropy of destination IP address \( E_{dp} \), the entropy of source port number \( E_{sp} \), the entropy of destination port number \( E_{dp} \), and the entropy of protocol type \( E_{p} \), note that \( E_{p} \) has the expression

\[ E_{p} = -p_1 \log p_1 - p_2 \log p_2 - p_3 \log p_3 \]  

(7)

where \( p_1, p_2 \) and \( p_3 \) are the proportion of the TCP, UDP and ICMP protocol packets in all of the IP packets. The \( p_1, p_2 \) and \( p_3 \) in normal traffic is different but steadily, when DDoS attacks happened, a large number of same protocol packets would occupy the network bandwidth, and as a result, \( E_{p} \) will reduces to 0. Because the forged source IP address trend to random, and destination IP address trend to concentrated, so the \( E_{ip} \) increase and the \( E_{dp} \), \( E_{sp} \), \( E_{dp} \), \( E_{p} \) will also change obviously according to the DDoS attacks mode.

In order to validate the theory above, we use a DDoS attack dataset DARPA2000 from MIT laboratory for analysis. Firstly, we use the Windump tool for DDoS analysis and find that DDoS attack happens from the time 7574s to 7576s, then the variation of traffic is analyzed as shown in Fig. 3.

![Traffic variation of DDoS attack](image)

Figure 3. Traffic variation of DDoS attack

As presented in Fig. 3, there is a burst at time 7574s, which means that bursts of packets happens at that time, namely anomaly traffic. In order to get type of anomaly traffic, a method based on entropy was used. We first extract source IP (srcIP), destination IP (dstIP), source port (srcport), destination port (dstport) and protocol number (tranproto) from the IP header fields of each packet, then we calculate the normalized entropy. For powerful validation, the DDoS attacks data was used from the collection of both outside and inside of the link at the same time, the results as shown in Fig. 4 and Fig. 5.
Unfortunately, the parameter estimation of CRF model is difficult to realize by calculating from \( \frac{\partial L(\theta)}{\partial \lambda_k} = 0 \). The L-BFGS algorithm [15] is put forward to solve this problem. It converts the parameter estimation process to an optimization question. That is to say, now the question change to solve a large-scale unconstrained optimization question: \( \min f(x), x \in R^n \).

L-BFGS algorithm use the most recent iteration results to construct the Hessian approximation, so the method save only a few vectors instead of storing fully Hessian matrices, and as a result, the storage requirements are reduced. The update vector pairs \( \{s_i, y_i\} \) which are associated with \( x_i \) need to be stored for the following \( i = k-1,k-2,\cdots,k-m \), and the vectors have
\[
\Delta_k = x_{k+1} - x_k, \quad y_k = g_{k+1} - g_k \tag{10}
\]
where \( g_k = \nabla f_k \) means the gradient.

The BFGS optimization iteration method has the form
\[
x_{k+1} = x_k - \alpha_k H_k g_k \tag{11}
\]
where \( \alpha_k \) is the step length, and \( H_k \) is the update matrix.

The BFGS update matrix \( H_k \) has the iteration formula
\[
H_{k+1} = V_k^T H_k V_k + \rho_k s_k s_k^T \tag{12}
\]
where
\[
\rho_k = \frac{1}{y_k^T s_k}, \quad V_k = I - \rho_k y_k s_k^T \tag{13}
\]

The flow chart of the algorithm is shown in Fig. 6.

In Fig. 4 and Fig. 5, five subplots are normalized entropy named srcip, dstip, srcport, dstport and transpro. When DDoS happens, all of them have obviously changing. It confirms our hypothesis. Therefore, we can use the normalized entropy as the detection feature.

D. CRF Model Training

The training of CRF is to estimate the parameter \( \theta \). Maximum likelihood estimation method was used according to the certain training data \( D \). In this part, an improved Quasi-Newton algorithm [17] is introduced.

Training dataset is composed of the observation sequence \( X \) and the label sequence \( Y \), the empirical estimation of sequence \( X \) and \( Y \) is \( \hat{p}(x,y) \), for conditional probability \( p(y|x,\theta) \), the log likelihood function \( L(\theta) \) can be shown as
\[
L(\theta) = \sum_{x,y} \hat{p}(x,y) \log p(y|x,\theta) \tag{8}
\]

The probability distribution of CRF expressed as
\[
p(y|x,\theta) = \frac{1}{Z(x)} \exp \left( \sum_{i=1}^m \sum_{j=1}^n \lambda_k f_i(y_j,y_i,x) + \sum_{i=1}^m \mu_i g_i(y_i,x) \right) \tag{9}
\]

Denoting the right side of (8) by (9), take partial derivative of parameter \( \lambda_k \) and \( u_i \) for \( L(\theta) \), let \( \frac{\partial L(\theta)}{\partial \lambda_k} = 0 \), then \( E_{\hat{p}(x,y)} [f_i] = E_{p(y|x,\theta)} [f_i] \), we can get \( \lambda_k \). In the same way, we can get \( u_i \).

![Figure 4. Normalized entropy of DDoS attack(inside)](image)

![Figure 5. Normalized entropy of DDoS attack(Outside)](image)
E. Probability computing

Through training, we get the certain estimated parameter of the CRF model. Then, we can compute the conditional probability \( P(Y | X) \) of the label sequence \( Y \) according to the sequence \( X \). The forward-backward algorithm is used for the computation.

We define the forward vectors \( \alpha_t(x) \)
\[
\alpha_t(y_t | x) = \begin{cases} 1, & \text{if } y_t=\text{start} \\ 0, & \text{otherwise} \end{cases} \tag{15}
\]

The iteration formula is
\[
\alpha_t^+(x) = \alpha_{t-1}^+(x)M_t(x) \tag{16}
\]

Sameness, we define the backward vectors \( \beta_t(x) \).
\[
\beta_{n+1}(y_{n+1} | x) = \begin{cases} 1, & \text{if } y_{n+1}=\text{stop} \\ 0, & \text{otherwise} \end{cases} \tag{17}
\]

The iteration formula is
\[
\beta_t(x) = M_{n+1}(x)\beta_t(x) \tag{18}
\]

Then we get
\[
P(Y | y_t | x) = \alpha_t^+(y_t | x)\beta_{n+1}(y_{n+1} | x) \tag{19}
\]

\[
P(Y_{n+1}=y_{n+1}, \ldots, y_n | x) = \frac{\alpha_t(y_t | x)\beta_{n+1}(y_{n+1} | x)}{Z(x)} \tag{20}
\]

The detection of DDoS attacks based on CRF model is equivalent to get maximum conditional probability of the label sequence \( y_t = (y_1, y_2, \ldots, y_n) \), and as a result, the binary-class label between normal and attack was given to the monitoring traffic.

IV. EXPERIMENT RESULTS AND ANALYSIS

The experimental data set is given below:

Dataset1: We used the 10% KDD CUP 99 dataset [18], which contains Denial of Service (DoS), Probe, User to Root (U2R) and Remote to Local (R2L) network attacks. It includes two kinds of data: one is training data set with attack label named kddcup.data_10_percent.gz, another is testing data set without attack label named as kddcup.newtestdata.unlabel_10_percent.gz. We removed the U2R and R2L attack data, and reserved the normal data and some DoS attack data.

Dataset2: We used MIT Lincoln lab LL SDDoS2.0.2 dataset [19] as the DDoS attacks traffic.

Dataset3: The MAWI dataset [20] was used as the normal background traffic.

Dataset4: We used the tool TFN2K to generate real attack traffic. Fig. 7 shows the local environment for our DDoS attack experimentation.

The CRF++ toolkits [21] were used for the analysis of CRF model, and LibSVM toolkits [22] for the SVM algorithm. Weka toolkits [23] were used for the other machine learning methods such as Decision Tree, KNN and Naive Bayes and etc.

We define TP and TN as the packet quantities of the true detected attacks and normal packets. FP means the quantities of false alarm packets and FN means the quantities of false negative packets.

The evaluation of the performance including Precision, True Positive Rate (TPR or sensitivity), F-Value, false positive rate (FPR) and false alarm rate (FNR) are defined as below.
\[
\text{Precision} = \frac{TP}{TP + FP} \times 100\% \tag{21}
\]
\[
\text{TPR} = \frac{TP}{TP + FN} \times 100\% \tag{22}
\]
\[
\text{F - Value} = \frac{2 \times \text{Recall} \times \text{Precision}}{\text{Recall} + \text{Precision}} \tag{23}
\]
\[
\text{FPR} = \frac{FP}{FP + TN} \times 100\% \tag{24}
\]
\[
\text{FNR} = \frac{FN}{TP + FN} \times 100\% \tag{25}
\]

A. Feature Selection Effects

We used Dataset1 as the sample data. Five different schemes of the features selection were used. Among of these, scheme 1, 2, 4 and 5 selected 2, 5, 25 and all 41 features respectively according to the reference literature [24]. As for the scheme 3, it selected 4 basic network connection features and 5 flow connection features (2 seconds unit) according to the reference literature [12]. Table 1 gives the attacks detection result.

<table>
<thead>
<tr>
<th>TABLE I. ATTACKS DETECTION RESULT UNDER DIFFERENT FEATURE SELECTION SCHEMES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheme (feature)</td>
</tr>
<tr>
<td>------------------</td>
</tr>
<tr>
<td>1 (2)</td>
</tr>
<tr>
<td>2 (5)</td>
</tr>
<tr>
<td>3 (9)</td>
</tr>
<tr>
<td>4 (25)</td>
</tr>
<tr>
<td>5 (41)</td>
</tr>
</tbody>
</table>

Table 1 shows the performance of the CRF based DDoS attacks detection model under different feature selection schemes. From Table 1, we can find that different feature schemes have certain influence on the detection results. As the quantities of the features increasing, the Precision and TPR improved accordingly. But when the quantities of the features go beyond 9, there will be little improvement in Precision and TPR even if
we selected all of the 41 features, meanwhile, the training and testing time increased continuously.

Fig. 8 shows the training time of the CRF based model with different feature quantities. We can find that the spent training time increasing along with the increasing of the training packets quantities. At the same time, we can find that the training time increasing when the quantities of the selected features increasing.

From Table1 and Fig. 8, we can find that it is important to choose appropriate features for the detector, which would reduce the training time and testing time, and make good balance between the accuracy and the efficiency.

B. Model Detection Performance

In this part, multi-features vector of the CRF model is composed of the OWCD and the IPE. The dataset is sampled from Dataset2 and Dataset3 with 0.1 second interval. The methods of Decision Tree (C4.5), SVM, KNN and Naïve Bayes are adopted respectively. The experiment results as shown in Table 2.

As presented in table 2, comparing with SVM and other machine learning methods, we find that the Precision, TPR and the F-Value of DDoS attacks detection based on CRF model are superior to the others. DDoS attacks detection method based on CRF model has lower FPR (0.58%) and lower FNR (2.42%).

C. Robustness under Massive Background Traffic

We use the LLSSDDoS2.0.2 dataset [19] as attack traffic data and the MAWI dataset [20] as normal background traffic data, the training and testing sample data are mixed by 0.1s time interval sampling. Increasing the percentage of normal traffic data, then the variation of TPR and FPR are compared, the experiment results are shown in Fig. 9.

In order to test our model under realistic real-time DDoS attack traffic, we use the toolkit WinDump to catch down all of the packets at the victim host which suffered the flooding DDoS attacks from three hosts. Use TFN2K as the attack tool. The experiment results are shown in Fig. 10.

In Fig. 9 and Fig. 10, the horizontal coordinate-axis X is the ratio of normal traffic data to attack traffic data. Experimental results show that with the increasing of the background traffic proportion, the TPR of CRF method decreasing and the FPR increasing accordingly. But the detection performance of the CRF based model doesn't decrease sharply with the increasing of the background traffic. As Compared with other detection methods, the CRF model based detection method can eliminate the effect of the background traffic effectively. So the CRF based model is robustness.

V. CONCLUSION

Misuse detection methods are effective to process the definite pattern while anomaly detection methods can detect unknown intrusions, so it is a good idea to incorporate the signature-based and anomaly-based
methods into a hybrid system. But many traditional DDoS attacks detection methods only use unique feature or statistic. As a result, it is a puzzle to balance between the low precision and the high false positive rate. To solve this problem, we focused on the CRF based DDoS attacks detection method using many detection features together. Our method made use of the excellent characteristics of CRF model, that is, not need independence assumption strictly and have ability to synthesize many features into a detection feature vector.

The experiment results show that our method has higher detection accuracy and sensitivity as well as lower false positive alarms. In the same dataset and features selection scheme, the CRF based DDoS attacks detection model outperforms other well-known detection methods such as Naïve Bayes, KNN, SVM and etc. The accuracy goes beyond 95.0% and the false alarm rate is less than 5.0%. Meanwhile, the CRF based model is robust under massive background network traffic.

We use source IP entropy, destination IP entropy, source port entropy, destination port entropy, protocol number entropy and etc. as the multi-feature vectors to depict the states of the monitoring traffic. By combine the IP flow entropies into a normalize entropy including five components, we set many features into one metric. Then the model can be used to detect various DDoS attacks with high sensitivity and low false alarm rate. In addition, the L-BFGS algorithm is used as the CRF model training method, at the same time, the detection method only needs to inspect the IP header fields of each packet, both of which makes it possible for real-time implementation even on high speed networks. The CRF based model may detect new form of forthcoming attacks, because it is independent from any specific DDoS flooding attack tools. In our future we will try works to study the implementation technology taking into account the effectiveness in real time processing.

ACKNOWLEDGMENT

This work was supported in part by a grant from the National Grand Fundamental Research 973 Program of China under Grant No. 2012CB315900, and the National High-Tech Research and Development Plan of China under Grant No. 2011AA01A103.

REFERENCES


Shi-wen CHEN received the M.S. degree in signal and information processing from Zhengzhou Information Science & Technology Institute, Zhengzhou, P.R. China, in 2004. He is currently a network engineer in China National Digital Switching System Engineering and Technological R&D Center, Zhengzhou, P.R. China. He has been a member of IEEE since 2012. His current research interests include network traffic measurement, signal processing and machine learning.

Jiang-xing WU is currently a professor of China National Digital Switching System Engineering and Technological R&D Center. His interesting fields include telecommunications switching, broadband information network and etc.

Xiao-long YE is currently a M.S. candidate in communication and information system at National Digital Switching System Engineering and Technological R&D Center, Zhengzhou, P.R. China. His current research interests include network traffic anomaly detection and network traffic measurement.

Tong GUO is currently a Ph. D. candidate at the National Digital Switching System Engineering and Technological R&D Center. His research interest covers swarm intelligence, high-speed network traffic measurement and traffic prediction.