Journal of Southeast University (English Edition) Vol. 34, No. 2, pp. 191-198 June 2018 ISSN 1003—7985

Detection of P2P botnet based on network behavior features and Dezert-Smarandache theory

Song Yuanzhang Chen Yuan Wang Junjie Wang Anbang Li Hongyu

(Changchun Institute of Optics, Fine Mechanics and Physics, Chinese Academy of Sciences, Changchun 130033, China)

Abstract: In order to improve the accuracy of detecting the new P2P(peer-to-peer) botnet, a novel P2P botnet detection method based on the network behavior features and Dezert-Smarandache theory is proposed. It focuses on the network behavior features, which are the essential abnormal features of the P2P botnet and do not change with the network topology, the network protocol or the network attack type launched by the P2P botnet. First, the network behavior features are accurately described by the local singularity and the information entropy theory. Then, two detection results are acquired by using the Kalman filter to detect the anomalies of the above two features. Finally, the above two detection results are fused with the Dezert-Smarandache theory to obtain the final detection results. The experimental results demonstrate that the proposed method can effectively detect the new P2P botnet and that it considerably outperforms other methods at a lower degree of false negative rate and false positive rate, and the false negative rate and the false positive rate can reach 0.09 and 0.12, respectively.

Key words: P2P (peer-to-peer) botnet; local singularity; entropy; Kalman filter; Dezert-Smarandache theory

DOI: 10.3969/j. issn. 1003 - 7985. 2018. 02. 008

The botnet is a collection of massive malicious hosts, and the hosts of botnet are able to keep living with each other by the command and control (C&C) mechanism. With the help of the secondary injection process, the master of the botnet can update the malicious program loads of the bot hosts to launch many different types of network attacks, such as spam attacks, distributed denial of service (DDoS) attacks and so on. The new P2P botnet implements the C&C mechanism with a decentralized architecture of the P2P network. Since there is no control center in the decentralized structure, when a large number of bot hosts are eliminated, the remaining bot hosts are even able to keep living with each other, update the malicious program loads and launch network attacks. Storm is a typical kind of new P2P botnet, and the Overnet/eDonkey network is employed to construct the C&C mechanism[1]. The decentralized network structure is the development and evolution trend of the C&C mechanism, and thus how to effectively detect the new P2P botnet has turned into the hot focus of the field of network security.

Sarat et al.[2] studied the abnormal features of Storm, which lays a solid foundation for further research. For example, the distribution of peer IDs of Storm was irregular and there were a number of unreachable IPs. Steggink et al.[3] found some unique features of Storm, and then analyzed how Storm avoided the detection methods. On this basis, a new detection method based on network traffic features was proposed, such as the specific length based on the IP packet. Based on the penetrating analysis of the logic of Storm, Porras et al.[4] proposed a dialog-based detection method, which detected the P2P botnet through handling the dialog information with the pattern matching theory. Holz et al.[5] found a method to mitigate the operation and expansion of botnets, which infiltrates into the Overnet network and works as the peer of the C&C mechanism so as to publish many fake keys and affect the normal network communication among bot nodes; and finally disturb the secondary injection process and the C&C mechanism. Wang et al.[6] proposed a method to infer the botnet C&C mechanism using some inherent patterns in the bot execution trace coverage of basis blocks. The coverage analysis method is evaluated for Zeus, Sdbot and Agobot, and the result shows that the method can accurately and efficiently extract the control commands of the botnet. In the field of collaborative detection, Ref. [7] draws lessons from distributed data fusion and proposed a hierarchical collaborative detection method, and it was able to share data and cooperate under the following levels, including data, feature, and judgment. Ref. [8] proposed a coordinative running method on the basis of the Turing machine, and it was capable of analyzing the possible relationships among network attack events occurring in different geographical positions and at different times. A collaborative running system was implemented to track botnet and analyze the relationship between bot hosts and DDoS sources. Refs. [9-13] studied the development process and the evolution trend of the propaga-

Received 2017-11-15, **Revised** 2018-03-16.

Biography: Song Yuanzhang (1986—), male, master, associate research fellow, songyuanzhang@163.com.

Foundation items: The National High Technology Research and Development Program of China(863 Program) (No. 2011AA7031024G), the National Natural Science Foundation of China (No. 61133011, 61373053, 61472161).

Citation: Song Yuanzhang, Chen Yuan, Wang Junjie, et al. Detection of P2P botnet based on network behavior features and Dezert-Smarandache theory[J]. Journal of Southeast University (English Edition), 2018, 34(2): 191-198. DOI: 10.3969/j. issn. 1003 - 7985. 2018. 02. 008.

tion, attack and C&C mechanisms of botnet, and then summarized the current research, such as botnet monitoring, infiltration, analysis of botnet features, detection, disruption and so on. The limitations of the current research were discussed, and many potential instructions for future study were introduced. In brief, there are still some problems in the detection research of the new P2P botnet. Many studies have mainly focused on some certain or several unique anomalies of the P2P botnet. When a new botnet based on a new P2P network emerges, the detection accuracy of the existing detection methods will be greatly affected. Also, many detection methods need to inspect the content of packets, so they will not work effectively when the packets of P2P botnet are encrypted.

After analyzing the life cycle process and the network features of Storm, a P2P botnet detection method on the basis of network behavior features and the Dezert-Smarandache theory is proposed. Experiments verify that our method can detect a P2P botnet more accurately. The innovative points of the proposed method are as follows. First, the network behavior features are focused on in the paper, which do not change with the network topology, the network protocol or the network attack type launched by the P2P botnet, so that the network behavior features can best reflect the essential feature of the P2P botnet. This directly affects the false negative rate and false positive rate when detecting the new P2P botnet. Secondly, the local singularity and the information entropy theory are adopted to accurately describe the details of network behavior features in terms of the change of the packets and the connection features, without deep packet inspection of the content of packets. So, the detection method proposed will still work effectively when the packets of P2P botnet are encrypted. Finally, due to the complexity and variability of the features of the P2P botnet, a single network feature is not enough to accurately describe the details of the traffic changes, which will result in a high false negative rate and false positive rate. Therefore, the Dezert-Smarandache theory is adopted to overcome this problem.

1 Detection Method of P2P Botnet

Storm is a typical kind of P2P botnets, and its life cycle process is shown in Fig. 1. Several features need to be noted[5]:

1) The length of packets focus on a certain number of fixed lengths.

2) The bot node uses a certain number of fixed message types.

3) A certain number of fixed source ports are used in the C&C mechanism of Storm.

Based on the analysis of the life cycle process and the network features of Storm, a novel P2P botnet detection method based on network behavior features and the Dezert-Smarandache theory is proposed in Fig. 2. It focuses on the essential anomalies of the P2P botnet, which are the network behavior features, and they do not change with the network topology, the network protocol or the network attack type launched by the P2P botnet. First, the local singularity and the information entropy are employed to describe the network behavior features. Two detection results are obtained through the Kalman filter to detect the behavior anomalies of the above features. The final detection result is obtained by fusing the above results with the Dezert-Smarandache theory.

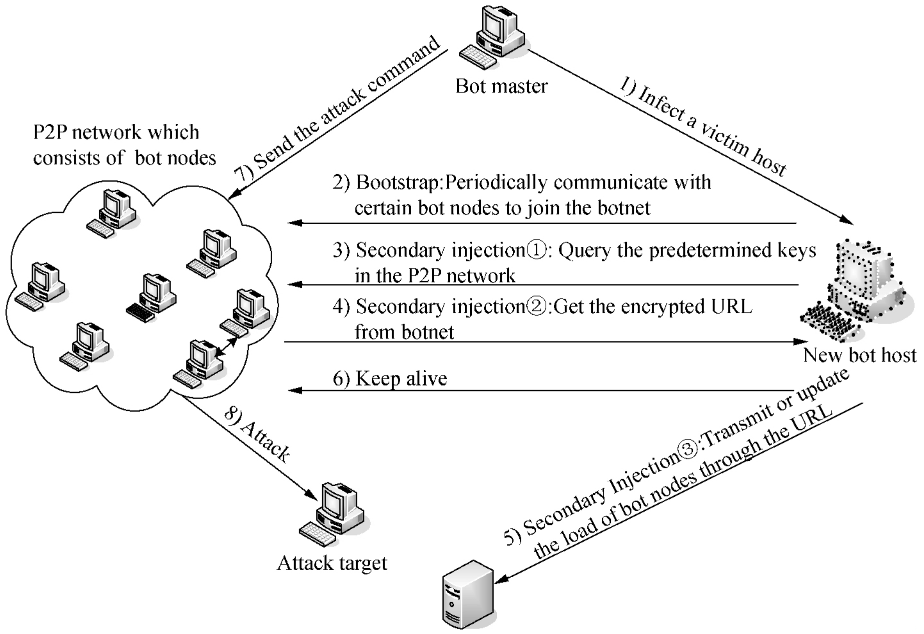
Bot master
7) Send the attack command
1) Infect a victim host
P2P network which consists of bot nodes
2) Bootstrap:Periodically communicate with certain bot nodes to join the botnet
3) Secondary injection①: Query the predetermined keys in the P2P network
4) Secondary injection②:Get the encrypted URL from botnet
New bot host
6) Keep alive
8) Attack
Attack target
5) Secondary Injection③:Transmit or update the load of bot nodes through the URL

Fig. 1 Life cycle process of P2P botnet

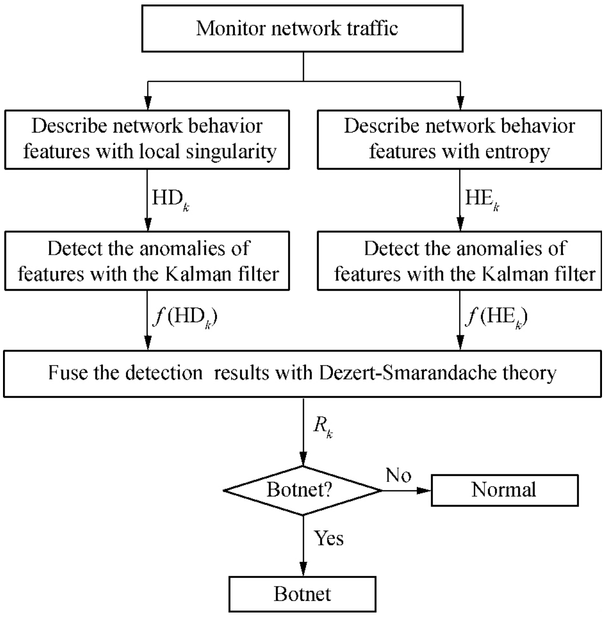
Monitor network traffic
Describe network behavior features with local singularity
Describe network behavior features with entropy
HD$_k$
HE$_k$
Detect the anomalies of features with the Kalman filter
Detect the anomalies of features with the Kalman filter
f(HD$_k$)
f(HE$_k$)
Fuse the detection results with Dezert-Smarandache theory
R_k
Botnet?
No
Normal
Yes
Botnet

Fig. 2 Process of the detection method

1.1 Network behavior features

The local singularity and the information entropy are employed to describe the network behavior features, which are the essential features of the P2P botnet.

1.1.1 Local singularity

Local singularity is the refinement and extension of self-similarity, and it is capable of flexibly describing the irregular phenomenon under the small time scale, which has little association with the self-similarity of network traffic under the large time scale.

$$X(ak)=a^{H(k)}X(k) \qquad \forall a>0 \tag{1}$$

where $H(k)$ is the Holder exponent, which is the degree of local singularity of X at a given dot k. For all $a>0$, $X(k)$ denotes a continuous-time random process and k is the current time step; for all $a>0$, $X(k)$ demonstrates the local singularity.

Let $X(k)$ denote the number of IP packets captured up to the time step k, $X(0),\dots,X(k)$ are divided into many subintervals, and the length of subinterval is d, so $H(k)$ is calculated as[14-15]

$$H(k)=\lim_{d\to 0}\frac{\log\left(\left|X\left(k+\frac{d}{2}\right)-X\left(k-\frac{d}{2}\right)\right|\right)}{\log(d)} \tag{2}$$

Without loss of generality, if the number of the subinterval is 2^n, $H(k)$ can be calculated as

$$H(k)=\lim_{n\to\infty}\left[-\frac{\log\left(\left|X\left(\frac{i+1}{2^n}\right)-X\left(\frac{i}{2^n}\right)\right|\right)}{n}\right]$$
$$i=0,1,\dots,2^n-1 \tag{3}$$

Let k denote the current time step, HD$_k$ is defined as

$$\mathrm{HD}_k=1-H(k) \tag{4}$$

As mentioned above, the botnet will make the number of IP packets increase, which leads to the improvement of the local singularity of network traffic and makes $H(k)$ decline, and thus the anomalies will be identified by detecting HD$_k$. To further improve the detection sensitivity, HD$_k$ is inputted into the Kalman filter in order to rapidly detect the anomalies of the local singularity.

1.1.2 Entropy

In the information theory, entropy is a measure of the number of specific ways in which a system may be arranged, and it is often taken to be a measure of disorder[16]. Assume that the value of a random variable $\boldsymbol{X}=\{x_1,x_2,\dots,x_n\}$, $P(x_i)$ is the probability of $\boldsymbol{X}$ values for x_i. $P(x_i)$ is the amount of information provided when the value of $\boldsymbol{X}$ is x_i. The entropy of $\boldsymbol{X}$ is calculated as

$$H(\boldsymbol{X})=-\sum_{i=1}^{n}(P(x_i)\log P(x_i)) \tag{5}$$

The greater the entropy of the random variable is, the more random its values are. Conversely, the smaller the entropy of the random variable is, the more stable its values are, which means that the random variable is more able to take some certain values.

The quadruple $q_i=(\text{length}_i,\ \text{type}_i,\ \text{srcport}_i,\ \text{dstport}_i)$ is defined to describe the features of packets. Length$_i$ denotes the length of the packet; type$_i$ denotes the message type of the packet; srcport$_i$ denotes the source port number of the packet; dstport$_i$ denotes the destination port number of the packet. Assuming that $q_i=(\text{length}_i,\ \text{type}_i,\ \text{srcport}_i,\ \text{dstport}_i)$, $q_j=(\text{length}_j,\ \text{type}_j,\ \text{srcport}_j,\ \text{dstport}_j)$, if length$_i$ = length$_j$, type$_i$ = type$_j$, srcport$_i$ = srcport$_j$ and dstport$_i$ = dstport$_j$, then it is said that q_i is the same as q_j. Assuming that p_i denotes the probability of the proposition that the quadruple q_i appears within the time interval Δt, the entropy of the quadruple to describe the features of network traffic is calculated as

$$H_{\mathrm{q}}=-\sum_{i=1}^{n}p_i\log p_i \tag{6}$$

The smaller the entropy is, the more stable the features of the network traffic are, and the greater the probability of P2P botnet appearing is. In normal scenarios and situations, the features of network traffics are in a relatively stable state, the entropy of them does not change sharply. Assuming that H_{normal} denotes the meaning of the entropy of the feature quadruple in the normal scenarios and situations and k denotes the current time step, the parameter HE$_k$ is defined as

$$\mathrm{HE}_k=|H_{\mathrm{q}}-H_{\mathrm{normal}}| \tag{7}$$

As mentioned above, the C&C mechanism of the P2P botnet makes the features of network traffic more stable than usual, which will make the entropy of the quadruple decline and make the parameter HE_k increase, and thus the anomalies will be identified by detecting the parameter HE_k. To further improve the detection sensitivity, HE_k is inputted into the Kalman filter in order to rapidly detect the anomalies of the entropy of the above quadruple.

1.2 Kalman filter

A process is estimated by using a form of feedback control in the Kalman filter shown in Fig. 3. It estimates the process state at the current time step and then acquires the feedback in the form of measurement[17-22].

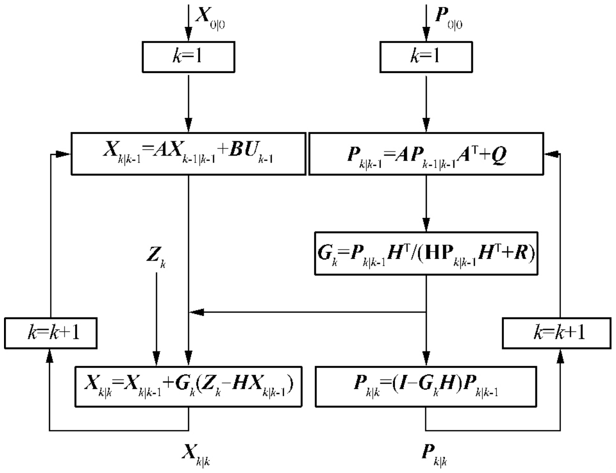
$X_{0|0}$
$P_{0|0}$
k=1
k=1
$X_{k|k-1}=AX_{k-1|k-1}+BU_{k-1}$
$P_{k|k-1}=AP_{k-1|k-1}A^{T}+Q$
Z_k
$G_k=P_{k|k-1}H^{T}/(\mathrm{H}P_{k|k-1}H^{T}+R)$
k=k+1
k=k+1
$X_{k|k}=X_{k|k-1}+G_k(Z_k-HX_{k|k-1})$
$P_{k|k}=(I-G_kH)P_{k|k-1}$
$X_{k|k}$
$P_{k|k}$

Fig. 3 Process estimated by a form of feedback control in the Kalman filter

Let k denote the current time step.

1) Time update equations

The priori estimate ($X_{k|k-1}$) is calculated based on the knowledge of the process prior to step k.

$$X_{k|k-1}=AX_{k-1|k-1}+BU_{k-1} \tag{8}$$

where $X_{k-1|k-1}$ is the posteriori estimate of step $k-1$; U_{k-1} is the control input; A and B are the system parameters.

The priori estimate error covariance is

$$P_{k|k-1}=AP_{k-1|k-1}A^{\mathrm{T}}+Q \tag{9}$$

where $P_{k-1|k-1}$ is the posteriori estimate error covariance of $X_{k-1|k-1}$; and Q is the process noise covariance.

The time update equations project forward the current state and error covariance estimates of the current time step to obtain the priori estimate for the next time step.

2) Measurement update equations

The posteriori estimate $X_{k|k}$ is calculated based on the knowledge of the measurement Z_k and $X_{k|k-1}$.

$$X_{k|k}=X_{k|k-1}+G_k(Z_k-HX_{k|k-1}) \tag{10}$$

$$G_k=\frac{P_{k|k-1}H^{\mathrm{T}}}{HP_{k|k-1}H^{\mathrm{T}}+R} \tag{11}$$

where G_k is the Kalman gain, and H is the system parameter for measurement, and R is the measurement noise covariance.

The posteriori estimate error covariance is

$$P_{k|k}=(I-G_kH)P_{k|k-1} \tag{12}$$

where I is the identity matrix.

The measurement update equations take responsibility for incorporating a new measurement into the priori estimate to acquire an improved posteriori estimate.

After each time and measurement update in pairs, the process is repeated in a way that the previous posteriori estimates are adopted to predict the new priori estimates.

As is known, Storm causes many abnormities of the network behavior features, which are described as HD_k and HE_k. After HD_k and HE_k are, respectively, when inputted into the Kalman filter, their posteriori estimates are obtained as $f(\mathrm{HD}_k)$ and $f(\mathrm{HE}_k)$.

1.3 Dezert-Smarandache theory

Due to the complexity and variability of the features of the P2P botnet, a single network feature is not enough to accurately describe the details of the traffic changes, which will result in a high false negative rate and false positive rate. Therefore, the data fusion algorithm of the decision level is employed to solve the problem.

There are many data fusion algorithms on the decision level, including the Bayesian theory, DST and DSmT. DST is a generalization of the Bayesian theory, which is capable of reducing the hypothesis set by gradually combining evidence. Although DST is very appealing, it presents many limitations, especially when the conflict between the evidence is very strong[23]. There are two categories of methods to solve the above problems. From the view point of the modification of Dempster's combination rule, the first one is to propose new rules of combination under the DST framework as alternatives to Dempster's rule of combination, such as Murphy's rule of combination, Yager's rule of combination, Dubois and Prade's rule of combination and Smets'rule of combination. From the view point of the modification of the evidence source, the second one is to put forward the new alternative rules, and DSmT belongs to the category. DSmT can be considered to be the extension of the classical DST, but there are many fundamental differences between DSmT and DST. DSmT allows formally combining any kinds of independent sources of information represented in terms of belief functions, but is mainly focused on fusing these sources of evidence, which are imprecise, highly conflicting and uncertain[24].

DSmT is on the basis of Dedekind's lattice D^{U}, which is the hyper power set of frame U. In the DSmT framework, at first U is only considered to be a set $\{\theta_1, \theta_2, \dots, \theta_n\}$ of n exhaustive elements without introducing other constraints. $m(A)$ is the generalized basic belief assignment of set A, if a function m: $\boldsymbol{D}^{\mathrm{U}} \to [0,1]$ exhibits the two properties:

$$m(\varnothing) = 0 \tag{13}$$

$$\sum_{A \in \boldsymbol{D}^{\mathrm{U}}} m(\boldsymbol{A}) = 1 \tag{14}$$

where $\varnothing$ is the universal empty set. Some subsets of $\boldsymbol{U}$ are able to contain many elements, which are known to be truly exclusive but also truly non-existing at all at a given time. Given some known integrity constraints, one must work with a proper hybrid DSm model. Under such circumstances, for $n \geqslant 2$ independent sources, the hybrid DSm rule of combination on the basis of the chosen hybrid DSm model is defined for all $\boldsymbol{A} \in \boldsymbol{D}^{\mathrm{U}}$ as[25]

$$m(\boldsymbol{X}) = \delta(\boldsymbol{A})[S_1(\boldsymbol{A}) + S_2(\boldsymbol{A}) + S_3(\boldsymbol{A})] \tag{15}$$

$$\delta(\boldsymbol{A}) = \begin{cases} 0 & \boldsymbol{A} \in \varnothing_m \\ 1 & \boldsymbol{A} \notin \varnothing_m \end{cases} \tag{16}$$

$$S_1(\boldsymbol{A}) = \sum_{\substack{\boldsymbol{X}_1\ \boldsymbol{X}_2\ \dots\ \boldsymbol{X}_n \in \boldsymbol{D}^{\mathrm{U}} \\ \boldsymbol{X}_1 \cap \boldsymbol{X}_2 \cap \dots \cap \boldsymbol{X}_n = \boldsymbol{A}}} \prod_{i=1}^{n} m_i(X_i) \tag{17}$$

$$S_2(\boldsymbol{A}) = \sum_{\substack{\boldsymbol{X}_1\ \boldsymbol{X}_2\ \dots\ \boldsymbol{X}_n \in \varnothing \\ [u(\boldsymbol{X}_1) \cup \dots \cup u(\boldsymbol{X}_n) = \boldsymbol{A}] \vee \\ [(u(\boldsymbol{X}_1) \cup \dots \cup u(\boldsymbol{X}_n) \in \varnothing) \wedge \\ (\boldsymbol{A} = \boldsymbol{\theta}_1 \cup \boldsymbol{\theta}_2 \cup \dots \cup \boldsymbol{\theta}_n)]}} \prod_{i=1}^{n} m_i(\boldsymbol{X}_i) \tag{18}$$

$$S_3(\boldsymbol{A}) = \sum_{\substack{\boldsymbol{X}_1\ \boldsymbol{X}_2\ \dots\ \boldsymbol{X}_n \in \boldsymbol{D}^{U} \\ (\boldsymbol{X}_1 \cup \boldsymbol{X}_2 \cup \dots \cup \boldsymbol{X}_n) = \boldsymbol{A} \\ \boldsymbol{X}_1 \cap \boldsymbol{X}_2 \cap \dots \cap \boldsymbol{X}_n = \varnothing}} \prod_{i=1}^{n} m_i(X_i) \tag{19}$$

where $\varnothing_m$ is the set of all elements of $\boldsymbol{D}^{\mathrm{U}}$ forced to be empty by means of the model´s constraints; $u(\boldsymbol{X})$ is the union of all singletons $\boldsymbol{\theta}_i$ that compose the set $\boldsymbol{X}$; $S_1(\boldsymbol{A})$ denotes the classic DSm rule of combination for n independent sources on the basis of the free DSm model; $S_2(\boldsymbol{A})$ denotes the mass of all absolutely and relatively empty sets transferred to the total or relative ignorance; and $S_3(\boldsymbol{A})$ transfers the sum of relatively empty sets to the non-empty sets.

The Dempster´s rule of combination is employed to fuse the above detection results. The former is $f(\mathrm{HD}_k)$ obtained by the local singularity theory and Kalman filter, and the latter is $f(\mathrm{HE}_k)$ obtained by the entropy and Kalman filter.

1.4 Process of detection method

Assume that the current time step is k, and the process of the detection method is as follows:

1) Capture network traffic with the monitor tools, and do the statistical analysis on the IP packets.

2) Detect the abnormities of network behavior features. Calculate HD_k with the local singularity theory, and then obtain the detection result $\mathrm{f}(\mathrm{HD}_k)$ after inputting it into the Kalman filter; calculate HE_k with the entropy theory, and then obtain the detection result $f(\mathrm{HE}_k)$ after inputting it into the Kalman filter.

3) Obtain the final detection results by fusing $f(\mathrm{HD}_k)$ and $f(\mathrm{HE}_k)$ with the Dezert-Smarandache theory.

4) Make the detection decision of the P2P botnet. If $R_k \geqslant T$, it is judged that P2P botnet exists, otherwise not. The threshold T is dynamically adjusted by the Kaufman algorithm[26] to adapt to different network scenarios and situations.

2 Experimental Results and Data Analysis

The experimental data are composed of two parts. One part is the network data of the normal scenarios, collected from the network server of a certain research institute. Referred to Ref. [3], the other part is the network data of P2P botnet, collected from the network scenarios which are built with the virtual machine in Fig. 4. In order to simulate a massive number of hosts, a number of virtual machines are set up with the help of Virtualbox, and a virtual machine (named as monitor VM) is selected to work as the router of the local experimental network. We choose Wireshark to be the packet analyzer, and install it on the monitoring VM. The sample packets are captured by the monitoring VM every 10 s. First, run it normally for a period of time, and then inject the bot programs of Storm into many virtual machines.

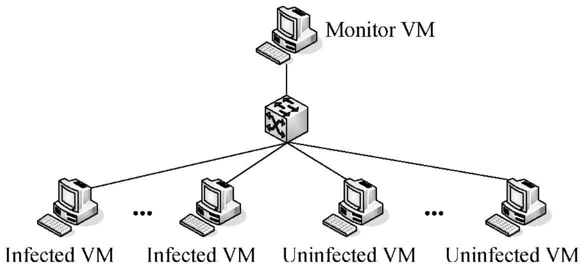

Fig. 4 Experimental environment for collecting network data of P2P botnet

2.1 HD parameter experiment

In the experiment, the change of the parameter HD is discussed, which reflects the local singularity of network traffic. In the normal scenarios and situations, the network traffic exhibits the significant local singularity, and the Holder exponent will maintain a relatively stable value interval.

From Fig. 5, after the bot programs of Storm are injected into the network, the local singularity of network traffic becomes more and more obvious and strong. HD starts to increase when $t = 340$ s, and even reaches 0.67 at the highest point when $t = 382$ s. Also, it fluctuates fiercely due to the periodic behaviors in the C&C mechanism.

2.2 HE parameter experiment

In the experiment, the change of the parameter HE is

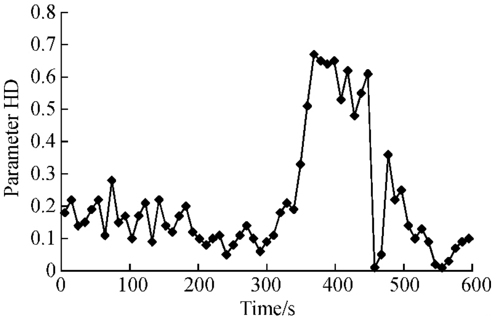

Fig. 5 Change of parameter HD reflecting the local singularity of network traffic

discussed, which reflects the entropy of the feature quadruple of network traffic. In the normal scenarios and situations, it will maintain relatively stable with little fluctuation.

From Fig. 6, along with the size of botnet as it grows larger and larger, the nodes of P2P botnet increase; the length of packets fall in some certain values; and some certain kinds of packets exist among some certain bot nodes, which make the entropy of the feature quadruple of network traffic decline, so the parameter HE increases.

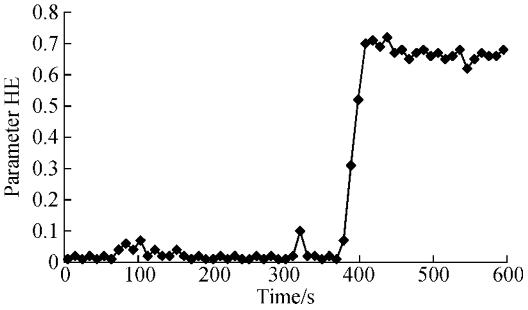

Fig. 6 Change of parameter HE reflecting the entropy of the feature quadruple of network traffic

2.3 Comparison of false negative rate and false positive rate with different detection methods

To verify the accuracy of the proposed detection method in different situations, without loss of generality, we select four groups of data to compare the false negative and false positive rate of the proposed method with other detection methods shown in Tab. 1, which use different combination of protocols and network traffic rates, particularly the variation of traffic intensity in P2P programs. The 1st and 2nd samples are in the network scenarios without bot programs, and the 2nd and 4th samples contain a number of packets from P2P programs and other web applications. With the help of the method proposed in Ref. [27], the 3rd sample is acquired by merging the 1st sample with the bot data captured from the network scenarios shown in Fig. 4, and the 4th sample is acquired by merging the 2nd sample with the bot data captured from the network scenarios shown in Fig. 4. The real attack times for the four groups of data are 0, 0, 1 000, and 1 000 in order.

From Tab. 2 and Tab. 3, only using the parameter HD and only using the parameter HE result in the high false negative and false positive rate, respectively. Due to the complexity and variability of the features of P2P botnet, a single network feature is not enough to accurately describe the details of the traffic changes. Therefore, the data fusion algorithm of the decision level is employed to solve the problem in the proposed method. These measures increase the accuracy of the P2P botnet detection to some degree. 1 018(763) in Tab. 2 denotes that the detection method detects 1 018 times of attack in total with 763 correct.

Tab. 1 Overview of different detection methods

Detection method	Description of method
MCUSUM[28]	Use the extended nonparametric CUSUM algorithm to detect the traffic anomalies of several kinds of packets
OHD	Only use parameter HD, and use the Kalman filter to detect anomalies
OHE	Only use parameter HE, and use the Kalman filter to detect anomalies
Proposed method	Focused on the network behavior features

Tab. 2 Detection result of different detection methods

Detection method	Detection result of samples			
	1	2	3	4
MCUSUM	23	121	762	1 268(784)
OHD	17	45	732	1 561(803)
OHE	29	23	871	1 284(583)
Proposed method	7	13	829	1 018(763)

Tab. 3 False negative rate and false positive rate of different methods

Detection Method	Accuracy rate	False negative rate	False positive rate
MCUSUM	0.65	0.21	0.25
OHD	0.73	0.15	0.21
OHE	0.77	0.19	0.17
Proposed method	0.89	0.09	0.12

3 Conclusion

A novel P2P botnet detection method is proposed on the basis of network behavior features and the Dezert-Smarandache theory. It focuses on the network behavior features, which are the essential abnormal features of P2P botnet and do not change with the network topology, the network protocol or the network attack type launched by the P2P botnet. First, the network behavior features are described by the local singularity and the information entropy theory, and then two detection results are acquired by using the Kalman filter to detect the anomalies of the two above features. Finally, the detection results above are fused with the Dezert-Smarandache theory. The experimental results show the superiority of our proposed method over other methods. The future work is to describe the details of the network behavior features more accurately.

References

[1] Stewart J. Storm worm DDOS attack[R]. Atlanta, GA, USA: SecureWorks, Inc, 2007.

[2] Sarat S, Terzis A. HiNRG Technical Report: 01-10-2007 Measuring the storm worm network[R]. Baltimore, ML, USA: Johns Hopkins University, 2007.

[3] Steggink M, Idziejczak I. Detection of peer-to-peer botnets[D]. Amsterdam, the Netherlands: System and Network Engineering, University of Amsterdam, 2007.

[4] Porras P, Saidi H, Yegneswaran V. A multi-perspective analysis of the storm (Peacomm) worm[R]. Menlo Park, CA, USA: SRI International Computer Science Laboratory, 2007.

[5] Holz T, Steiner M, Dahl F. Measurements and mitigation of peer-to-peer-based botnets: A case study on storm worm[C]//*1st USENIX Workshop on Large-Scale Exploits and Emergent Threats*. San Francisco, USA, 2008.

[6] Wang Z, Cai Y Y, Liu L, et al. Using coverage analysis to extract botnet command-and-control protocol[J]. *Journal on Communications*, 2014, **35**(1): 156-166. DOI: 10.3969/j.issn.1000-436x.2014.01.018. (in Chinese)

[7] Wang H L, Hu N, Gong Z H. Bot_CODA: Botnet collaborative detection architecture[J]. *Journal on Communications*, 2009, **30**(S1): 15-22. (in Chinese)

[8] Zang T N, Yun X C, Zhang Y Z, et al. A model of network device coordinative run[J]. *Journal of Computers*, 2011, **34**: 216-228. (in Chinese)

[9] Fang B X, Cui X, Wang W. Survey of botnets[J]. *Journal of Computer Research and Development*, 2011, **48**(8): 1315-1331. (in Chinese)

[10] Jiang J, Zhuge J W, Duan H X, et al. Research on botnet mechanisms and defenses[J]. Journal of Software, 2012, **23**(1): 82-96. DOI: 10.3724/SP.J.1001.2012.04101. (in Chinese)

[11] Karim A, Salleh R B, Shiraz M, et al. Botnet detection techniques: Review, future trends, and issues[J]. *Journal of Zhejiang University—Science C (Computers & Electronics)*, 2014, **15**(11): 943-983.

[12] Yahyazadeh M, Abadi M. BotGrab: A negative reputation system for botnet detection[J]. *Computers and Electrical Engineering*, 2015, **41**: 68-85. DOI: 10.1016/j.compeleceng.2014.10.010.

[13] Li K, Fang B X, Cui X, et al. Study of botnets trends [J]. *Journal of Computer Research and Development*, 2016, **53**(10): 2189-2206. (in Chinese)

[14] Maulik K, Resnick S. The self-similar and multifractal nature of a network traffic model[J]. *Stochastic Models*, 2003, **19**(4): 549-577. DOI: 10.1081/stm-120025404.

[15] Masugi M. Multi-fractal analysis of IP-network traffic based on a hierarchical clustering approach[J]. *Communications in Nonlinear Science and Numerical Simulation*, 2007, **12**(7): 1316-1325. DOI: 10.1016/j.cnsns.2005.12.004.

[16] Gu L, Yang P, Dong Y Q. A novel similarity measurement approach considering intrinsic user groups in collaborative filtering[J]. *Journal of Southeast University (English Edition)*, 2015, **31**(4): 462-468.

[17] Liu Z M, Cao S Q, Zhang Y, et al. Inverse depth parameterized attitude estimation for non-cooperative spacecraft [J]. *Optics and Precision Engineering*, 2017, **25**(2): 451-460. (in Chinese)

[18] Liu Z M, Zhang Y, Lu S, et al. Closed-loop detection and pose optimization of non-cooperation rotating target [J]. *Guangxue Jingmi Gongcheng/Optics and Precision Engineering*, 2017, **25**(4): 1036-1043. (in Chinese)

[19] Cheng L, Chen J, Chen M S, et al. Fast acquisition of time optimal sliding model control technology for photoelectric tracking system [J]. *Optics and Precision Engineering*, 2017, **25**(1): 148-154. DOI: 10.3788/OPE.20172501.0148. (in Chinese)

[20] Li Z Y, Li X M, Liu Q S, et al. Adaptive fast initial attitude estimation for inflight loitering munition[J]. *Guangxue Jingmi Gongcheng/Optics and Precision Engineering*, 2017, **25**(2): 493-501. (in Chinese)

[21] Min W D, Shi J, Han Q, et al. A distributed face recognition approach and performance optimization[J]. *Guangxue Jingmi Gongcheng/Optics and Precision Engineering*, 2017, **25**(3): 780-785. (in Chinese)

[22] Zhou J P, Chen J, Li Y, et al. Research on target prediction algorithm of shipboard photoelectric tracking equipment[J]. *Optics and Precision Engineering*, 2017, **25**(2): 519-528. (in Chinese)

[23] Mruphy C K. Combing belief function when evidence conflicts[J]. *Decision Support System*, 2000, **29**(1): 1-9. DOI: 10.1016/s0167-9236(99)00084-6.

[24] Mathon B R, Ozbek M M, Pinder G F. Dempster-Shafer theory applied to uncertainty surrounding permeability[J]. *Mathematical Geosciences*, 2009, **42**(3): 293-307. DOI: 10.1007/s11004-009-9246-0.

[25] Smarandache F, Dezert J. *Advances and applications of DSmT for information fusion* [M]. Rehoboth, USA: American Research Press, 2006.

[26] Kasera S, Pinheiro J, Loader C. Fast and robust signaling overload control[C] //*Proceedings of Ninth International Conference on Network Protocols*. Riverside, USA, 2001: 323-331.

[27] Zhao D, Traore I, Sayed B, et al. Botnet detection based on traffic behavior analysis and flow intervals[J]. *Computers & Security*, 2013, **39**: 2-16. DOI: 10.1016/j.cose.2013.04.007.

[28] Kang J, Zhang J Y, Li Q, et al. Detecting new P2P botnet with multi-chart CUSUM [C]//*International Conference on Networks Security, Wireless Communications and Trusted Computing*. Wuhan, China, 2009: 688-691.

基于网络行为特征与 Dezert-Smarandache 理论的 P2P 僵尸网络检测

宋元章　陈　媛　王俊杰　王安邦　李洪雨

(中国科学院长春光学精密机械与物理研究所，长春 130033)

摘要: 为提升对新型 P2P 僵尸的检测精度，提出了一种基于网络行为特征和 Dezert-Smarandache 理论的 P2P 僵尸检测方法. 该方法主要关注 P2P 僵尸的本质异常特征，即网络行为特征，该特征不受拓扑结构、协议和攻击类型的影响. 首先，利用局部奇异性和信息熵对网络行为特征进行多方面的描述; 然后，利用卡尔曼滤波器对网络行为特性进行异常检测; 最后，用 Dezert-Smarandache 理论对上述检测结果进行融合以得到最终检测结果. 实验结果表明: 所提方法可有效检测新型 P2P 僵尸; 相比其他方法，其漏报率和误报率较低，分别为 0.09 和 0.12.

关键词: P2P 僵尸网络; 局部奇异性; 信息熵; 卡尔曼滤波器; Dezert-Smarandache 理论

中图分类号: TP393