International Journal of Future Generation Communication and Networking
Vol. 9, No. 8 (2016), pp. 141-148
http://dx.doi.org/10.14257/ijfgcn.2016.9.8.14

Analysis of Covert Network Channel based On Two-stage Condensing Clustering of Density Multilayer

Fang Song[1], Tan Yang[1], Wang Yanxian[1], Chen Lin[1] and Liu Yan[1]

[1] *HUNAN RADIO & TV UNIVERSITY Hunan Changsha, 410004 China*
E-mail: 2348763@qq.com

Abstract

In order to improve universality of detection effect of complex network covert channel, coarsening clustering of channel is achieved, based on clustering algorithm, with hierarchical clustering in this article, then recognition detection of two-stage channel refinement is carried out in coarsening clustering results of each layer based on density clustering. Clustering method of multilayer covert channel is designed based on density, the effectiveness of proposed method is verified by carrying out contrast experiment on density clustering method, entropy method and ε evaluation method; in the end, experiments of simulation example demonstrate that such algorithm is able to quickly and accurately detect covert channel of complex network when the noise is not higher than 20%.

Keywords: *Complex network; Detection; Density clustering; clustering; coarse granularity*

1. Introduction

As the rapid development of computer & network technology, network security has gradually become a focus of people's concern, among it convert channel to invasion of network security is a very serious safety loophole and an intrusion methods, which the message is sent to one user from another user, that go against original design idea of system. Perniciousness of network convert channel reflected in the channel can be filched easily by hacker with data, which will cause serious leak matters. At the same time, this also is a basic mode for criminals to convert communication and escape from monitoring. Due to it's provided with above mentioned features, network convert channel has now become the mainstream of research in security domain. In a real world application, different types of convert channel may construct compositive covert channel with complex network, the effect of above-mentioned literature methods, which is provided with specific design, is not ideal if choose such channel to invade. In order to improve universality of detection effect of complex network covert channel, coarsening clustering of channel is achieved, based on clustering algorithm, with hierarchical clustering in this article, then recognition detection of two-stage channel refinement is carried out in coarsening clustering results of each layer based on density clustering. Such method is an unsupervised clustering mechanism, therefore, it's provided with features of realizing simplicity and auto adjustment as well as provided with actual application potential.

2. Two-stage Clustering Detection

2.1. Multilayer Condensation of Coarsening

According to the difference of design principle, clustering algorithm can be divided into five types, of which the use background of constrained clustering and

ISSN: 2233-7857 IJFGCN

high dimension clustering are particular, which is not provided with universality, the consumption issue of original data is serious and classification accuracy is worse; partitioning clustering aims at special spatial data processing; machine learning clustering is a kind of clustering method with monitoring, which focuses on process and is applied to channel detection, and it can be used as off-line detection intelligently. For this reason, this article selects another clustering method, that is, hierarchical clustering, the algorithm structure chart of it as shown in Figure 1.

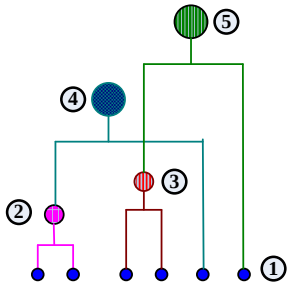

Figure 1. hierarchical clustering

In structure chart of hierarchical clustering of Figure 3, each sample is regarded as separate category at the initial stage of algorithm, then estimate and integrate the distance of individual based on Euclidean distance until the specified clustering number is satisfied. Therefore, clustering number given has important influence on iterative process of algorithm, in a real world application, owing to the lack of priori knowledge about clustering information of complex convert channel, clustering quantity setting is provided with blindness, this is the reason why hierarchical clustering is selected as coarsening clustering, it amounts to use it as preprocessing for data, then carry out refining clustering, which will effectively reduce difficulty of clustering and improves clustering accuracy, based on density clustering.

Algorithm step of traditional hierarchical clustering as follow[5]:

Step 1: (Similarity) Suppose that for N measured samples of covert channel, regard them as clustering category at initial stage, namely constitute a class by itself, then the similarity between measured samples of convert channels is:

$$\mu_{\sigma}\left(x_i, x_j\right) = e^{-\frac{\left\|x_i - x_j\right\|^2}{\sigma^2}} \tag{1}$$

In formula (1), $\sigma = \sigma_0 d$, of which d is diameter of measures samples set of convert channel.

Step 2: (Combination) Select two convert channel categories with highest similarity to combine from all individual categories of convert channel, and minus 1 from the total number of categories: $t = t - 1$.

Step 3: (Similarity) Make an updated operation to similarity of category combined according to computational formula of individual similarity of Step 1 convert channel.

Step 4: (Output) Use repeated iteration to carry out updated calculation of above Step 2 and Step 3 similarity until category number meets category number presetted, cease iteration and output coarsening clustering results of convert channel.

Viewing from executing processes of above-mentioned hierarchical clustering algorithm, such algorithm substantially is a sequential clustering process from bottom to up, such clustering method is provided with an irreversible drawback:

individual misclassification fails to restore. An improved method is designed to boost classification accuracy of hierarchical clustering and lower a proportion of error individual: for one thing, pretreat to convert channel, extract the core individual of convert channel on each layer based on core set method, in clustering process of each hierarchy, centralize the individual extracted to carry out merging cluster so as to lower probability of occurrence of error individual, algorithm steps as follow:

Step 1: Input convert channel set X and coarsening category number K of convert channel detection, and provide convert channel sample Y_K of this K category in advance;

Step 2: Compute similarity matrix $\mu^{X_\alpha^0}$ of convert channel of core X_α^0 in first-layer algorithm based on computational formula (1) of sample similarity. If x_{k+1}^* meets the conditions:

$$x_{k+1}^* = \arg\max_{x \in X} \sum_{\substack{y \in X \\ y \neq x}} \mu_\sigma \left(x_{k+1}, y \right) \tag{2}$$

Then x_{k+1}^* is called as core point of convert channel set $X \setminus \left\{ x_1^*, \cdots, x_k^* \right\}$, iterate as needed, compute subsequent hierarchical core set $\left\{ X_\alpha^2, X_\alpha^3, \cdots, X_\alpha^m \right\}$ of core set X_α^0 step by step.

Step 3: In general, regard X_α^m as top core set of sequence, the disadvantage of this kind of process mode is it will result in fundamental mistake of algorithm if top set X_α^m is an error individual of convert classification. For this reason, improving measurement adopted is to implant convert channel sample Y_K pre-given into cores set, the form is:

$$\alpha = \left\{ X_\alpha^2, X_\alpha^3, \cdots, X_\alpha^m, Y_K \right\} \tag{3}$$

Step 4: Based on formula (3), carry out hierarchical clustering successively to convert channel sample until it meets specified hierarchy, output classification result of convert channel $C = \left\{ C_1, C_2, \cdots, C_m \right\}$.

2.2. Clustering Detection of Density Refinement

The measurement method of similarity adopted is different from the one in section 3.1 in a process of density clustering, here put to use of simplified measurement method of Euclidean distance:

$$r(i, j) = \sqrt{\left(K_{1i} - K_{1j} \right)^2 + \cdots + \left(K_{mi} - K_{mj} \right)^2} \tag{4}$$

In formula (4), K is projection value of m space. Detection process of convert channel refinement using density clustering is a merging cluster through data point and its ε area., the character of it is to realize the effect of breakdown clustering to high density area by adjusting the value of neighboring parameter ε, therefore, it's very appropriate to select such algorithm as clustering algorithm of refinement. For one thing, take an random convert channel of coarsening clustering hierarchy as cluster center, then carry out similar channel search in neighborhood region given, the number of similar channel that exists is p.

Detection process of density refinement of complex convert network channel is composed of two parts: density clustering and convert channel detection. Suppose that centroid set of density clustering is $R = \left\{ R_j \right\}$, then the vector set of anticipated cluster is $\left\{ S_l \right\}$. Original state of cluster is $R = \varnothing$. Then the centroid of sector set

$\{S_l\}$ of anticipated cluster is R_j, which is denoted as $F[S_i]=R_j$, then the number, which is correspondent with centroid R_j, of convert channel sample in $\{S_l\}$ is k_j, original state $k_j=0$, then clustering process of density refinement is described as follows:

Step 1: Extract channel sample S_i, which is not correspondent with centroid R_i, from source data $\{S_l\}$ of convert channel, if an additional centroid point R_j exists in centroid set R and it meets $S_i \in N(R_j)$, then skip to Step 2; otherwise let S_i be the new centroid point, $R=R+S_i$, $R_{ju}=S_{iu}$ and $u=1,\cdots,U$, and skip to Step 3.

Where, $R_{ju}=S_{iu}$, $u=1,\cdots,U$ denotes that if S_i doesn't belong to any category, then make it as new centroid point.

Step 2: Let centroid point of convert channel S_i denote as $F[S_i]=R_j$ and update centroid count $k_j=k_j+1$.

Step 3: Skip to Step 4 if all samples in the set of convert channel are correspondent with one center point, otherwise return to Step 1 and continue carrying out a process of iterative clustering.

Step 4: Update centroid property of convert channel set:

$$R_{jk}=\sum_{A} S_{ik}/k_j \tag{5}$$

Where, $k=1,\cdots,K$, $A=\{S_i \mid F[S_i]=R_j\}$. Reset corresponding relation of sample set and centroid set of convert channel if above process fails to reach default iterations c, $F[S_i]=0$, and reset centroid count $k_j=0$, skip to Step 1 and rescan.

Step 5: Make an adjustment to effectiveness of such centroid based on relevant number k_j of convert channel contained in centroid, if it meets condition $k_j \geq p$, then such centroid will be called as invalid centroid, as to convert channel related to valid centroid, reassign valid centroid related to it with algorithm.

$$F[S_i]=R_j \Rightarrow S_i \in N_\varepsilon(R_j) \Rightarrow dist(S_i,R_j) \leq \varepsilon \tag{6}$$

Parameters adopted in above algorithm as follows: ε distance threshold, lower limit of p neighboring count, time of c default scan and quantity of U target attribute. Algorithm calculation process of detecting algorithm is:

Step 1: Suppose that convert channel m contains n attribute and sample set, then carry out a normalization processing to all attributes, the computational process is:

$$x(i,j)=\frac{x^*(i,j)-x_{\min}(i,j)}{x_{\max}(i,j)-x_{\min}(i,j)} \tag{7}$$

In formula (7), $x_{\max}(i,j)$ and $x_{\min}(i,j)$ are top and bottom limit of the j th convert channel attribute, respectively, $x(i,j)$ is the j th attribute of the i th individual, $x^*(i,j)$ is measured value of non-normalization.

Step 2: Suppose that projected sector of m dimension is a, of which $a=a_1,\cdots,a_m$, characteristic value of linear projection of x_{ij} as follows:

$$z_i=\sum_{j=1}^{m} A \times x_{ij}, i=1,2,\cdots,n \tag{8}$$

In formula (8), A is unit matrix, z_i is projection value.

Step 3: Carry out above density cluster on each dimensional space, delete inexistent clustered attribute and update attribute set $P=\{p_1,p_2,\cdots,p_k\}$, $\exists p \in P$.

After the operation of above cluster on all dimensions are completed, if no cluster exists, the convert channel is nowhere to be found, terminate and exit algorithm. On the contrary, if $l>1$ exists, the convert channel is to be found.

Step 4: If cluster exists on each weight $a_1,\cdots,a_m$ of projected vector a, then carry out the process of density clustering, if $l'>1$ cluster exists, the convert channel is to be found.

The principle of detection process of above algorithm is: for one thing, use clustering algorithm of hierarchical condensation to realize coarsening clustering of convert channel, then carry out a process of density clustering on hierarchy of target lock-on. In this process, first determine if single attribute exists multiple cluster by projecting high dimension data to realize a determination of if there exist convert channel or not, for attribute set that exists one cluster, construct multi-dimensional space and reexecute above estimation to multi-dimensional space, as a result, high dimensional data can be expanded in above algorithm.

3. Experiments and Analysis

3.1. Experimental Setup

For one thing, construct simulation experiment platform based on characteristics of complex convert network channel, as shown in Figure 2. Such network is divided into 8 subnetworks based on 6 SecPath100 routers, working mode of router is +OSPF router cooperating of static route. Five typical convert network channel in this experiment is selected for experimental subject, respectively: ACK command, ICMP Shell, Covert TCP, IPCTC and convert channel of network packet length.

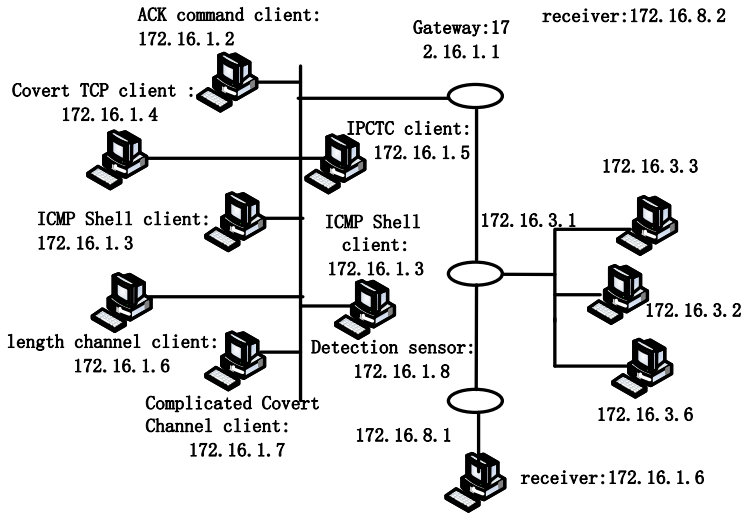

Figure 2. Simulation Environment

During the course of the experiment, hybrid sending system of convert channel is carried out to operate, the operating method mainly includes three methods below: one is convert channel of above type is received from 5 hosts with different IP address; two is carry out convert channel switch randomly to send through one host; three is add network package to convert channel in NZIX-II set as potential noise of convert channel.

3.2. Determination of Network Parameter

There's a need to set reasonable detection parameter to enhance the accuracy of convert channel detection, mainly are: selection of detection window, determination of online detection speed, neighboring parameter determination of density cluster and threshold determination of neighboring counts. Such parameters will have an influence on network performance, it however cannot be determined through experience in actual selection, as a result, first choice for this experiment is to carry out experimental measurement to the selection of network parameter. Simulation result of algorithm performance and ε distance threshold is provided in Figure 3.

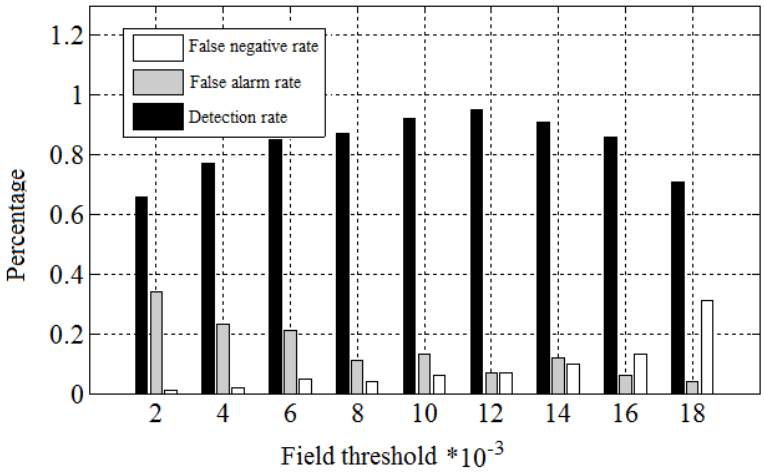

Figure 3. Parameter Influence of Neighboring Threshold

Host 172.16.1.8 is used as detector to detect covert network channel, figure 3 provides missing report of network, misinformation and change conditions of detection rate along with neighboring threshold v, and the figure shows that detection rate first increases and then decreases as the increase of neighboring threshold value, optimal result is reached at ε=0.012. Misinformation rate however presents a monotone decreasing trend, missing report rate presents a monotone increasing trend. The main reason, theoretically, is data with subtle difference will be divided into a class so as to boost missing report rate when neighboring threshold value is minor, the detection rate will be increased and the missing report rate will be decreased when neighboring threshold value is increasing. The figure shows that algorithm performance is rather preferable when neighboring threshold value is $(0.83\sim1.65)\times 10^{3}$.

As to experimental result of how the selection of lower limit p of neighboring count and additional noise amplitude will have an influence on algorithm performance, ε=0.012 is selected as neighboring threshold value, as shown in Figure 4.

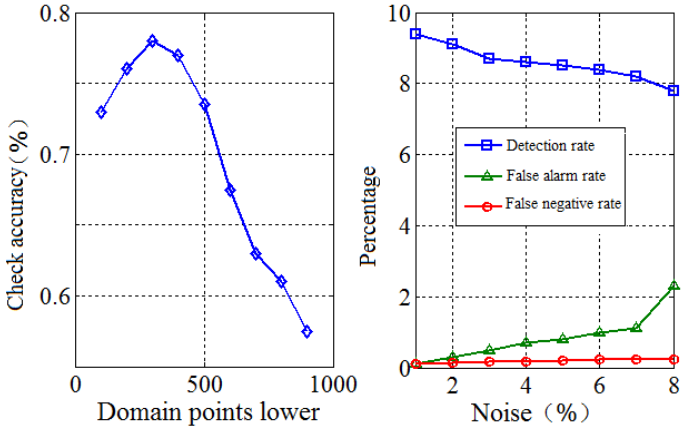

Figure 4. Influence of Lower Limit of Neighboring Counts and Additional Noise

Figure 4 represents the experimental result of how the selection of lower limit p of neighboring count and additional noise amplitude will have an influence on algorithm performance, it's observed that as an increase to quantity of lower limit p of neighboring count, the index of detection accuracy first increases and then decreases, an optimum point is reached at $p=300$. Set IP address of receiving end as: 172.16.1.6, viewing from noise influence, detection rate is decreased as an increase of noise, both misinformation and missing report rate are increased, and noise has a great influence on algorithm.

4. Conclusion

Traditional detection algorithm exists specific dead zone of convert channel or has a great pertinence to convert channel of a certain class and overlooks other issues of convert channel in solving detection problem of convert channel, starting from improving recognition accuracy of complex convert network channel, clustering method of multilayer covert channel is designed based on density, the effectiveness of proposed method is verified by carrying out contrast experiment on density clustering method, entropy method and ε evaluation method. Next, we will dedicate ourselves to test and experiment of large-scale network platform and verify the application effect of algorithm in large-scale data invasion situation.

Acknowledgement

The research is supported by Hunan Provincial Department of education in 2015 research project (15C0929).

Reference

[1] Z. Chen, W. Huang and Z. Lv, "Towards a face recognition method based on uncorrelated discriminant sparse preserving projection", Multimedia Tools and Applications, **(2015)**, pp. 1-15.
[2] D. Jiang, X. Ying and Y. Han, "Collaborative multi-hop routing in cognitive wireless networks", Wireless Personal Communications, **(2015)**, pp. 1-23.
[3] J. Yang, S. He and Y. Lin, "Multimedia cloud transmission and storage system based on internet of things", Multimedia Tools and Applications, **(2015)**, pp. 1-16.
[4] Z. Lv, T. Yin and Y. Han, "WebVR——web virtual reality engine based on P2P network", Journal of Networks, vol. 6, no. 7, **(2011)**, pp. 990-998.
[5] G. Bao, L. Mi, Y. Geng and K. Pahlavan, "A computer vision based speed estimation technique for localizing the wireless capsule endoscope inside small intestine", 36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), **(2014)**.

[6] X. Song and Y. Geng, "Distributed community detection optimization algorithm for complex networks", Journal of Networks, vol. 9, no. 10, **(2014)**, pp. 2758-2765.
[7] D. Jiang, X. Ying and Y. Han, "Collaborative multi-hop routing in cognitive wireless networks", Wireless Personal Communications, **(2015)**, pp. 1-23.
[8] J. Hu and Z. Gao. "Modules identification in gene positive networks of hepatocellular carcinoma using Pearson agglomerative method and Pearson cohesion coupling modularity", Journal of Applied Mathematics, **(2012)**.
[9] D. Jiang, Z. Xu and Z. Chen, "Joint time-frequency sparse estimation of large-scale network traffic", Computer Networks, vol. 55, no. 15, **(2011)**, pp. 3533-3547.
[10] J. Hu, Z. Gao and W. Pan, "Multiangle Social Network Recommendation Algorithms and Similarity Network Evaluation", Journal of Applied Mathematics, **(2013)**.
[11] J. He, Y. Geng, F. Liu and C. Xu, "CC-KF: Enhanced TOA Performance in Multipath and NLOS Indoor Extreme Environment", IEEE Sensor Journal, vol. 14, no. 11, **(2014)**, pp. 3766-3774.

Authors

Fang Song, he was born in Changsha, Hunan, senior engineer, lecturer, the incumbent is responsible for the network of Hunan Network Engineering Vocational College. Presided over and participated in the 5 provincial scientific research projects, the editor of the 8 textbooks.

