An Improved Solution for Multimedia Traffic in NIDS Based On Elitist Strategy

Xu Zhao, Jin Jiang, Reza Mousoli

***Abstract*—**Omission is inevitable, when the network traffic exceeds the load capacity of Network Intrusion Detection System (NIDS). In this case, dangerous packets should be given priority to processing. Since the large proportion of multimedia packets in traffic, the multithreading solution for multimedia packets has been proposed in NIDS. However, due to the use of roulette wheel selection, there is a possibility that the multimedia packets with high danger coefficient will be missed during the selection process. In this paper, the selection operator is improved by the elitist strategy, and new processing steps in the solution is proposed. When omission occurs, this improved model can choose more dangerous multimedia packets for processing within the maximum processing capacity of different threads. Experimental results indicate that this model can help NIDS to improve its detection rate for dangerous multimedia packets effectively.

***Keywords*—**Intrusion Detection, Multimedia Packets, Selection Operator; Elitist Strategy

I. Introduction

A. Background

In recent years, various new forms of attack have sprung up in cyberspace. Network Intrusion Detection System (NIDS), as an effective means of protection, can detect network attacks quickly. However, with the rapid growth of network traffic, NIDS often has performance bottlenecks under large traffic flow. Therefore, improving the detection efficiency of NIDS has been a hot topic in this field for many years.

Early research on this problem tends to improve the working mechanism of NIDS simply, for example, improving the matching efficiency of the pattern matching algorithm [1]-[2] and the detection rule [3]-[4]. With the rise of artificial intelligence [5]-[6] and big data [7]-[8], research on these technologies is increasing. In various research directions, relying on the recognition and classification of real-time network traffic to solve the performance bottleneck of NIDS, this approach is attracting increasing attention.

The existing real-time network traffic classification methods include Port Recognition, Deep Packet Inspection (DPI) and so on. Among them, Port Recognition is not reliable with the emergence of camouflage and port hopping technology. DPI detects the header and the load of the packet, so it has high classification accuracy and the fine grained network traffic classification ability [9]. But if no special processing is done in DPI, each packet needs depth inspection, so the time and space complexity is high, and it is difficult to meet the requirement of real-time in high speed network [10].

With the increasing speed of network, the proportion of multimedia packets in network traffic is increasing. Compared to other packets, because the multimedia packets are relatively safe, the NIDS has less detection rules for specific multimedia types [11]. Therefore, the recognition of multimedia packets and the separate processing according to different multimedia types will greatly improve the performance of NIDS. This advantage can solve the problem of high complexity of time and space in DPI, so the research on multimedia traffic classification has attracted more and more attention [12-14]. O.Marques of Florida Atlantic University originally proposed this idea. However, the details of the implementation are not mentioned in [15]. We have put forward a series of processing methods [3],[11],[16],[17] of NIDS for multimedia packets with good results. In the meantime, O. Marques and Pierre have also carried out follow-up studies [18], but their focus is mainly on the loopholes of streaming and non-streaming specific multimedia files. Similarly, Zander of the Murdoch University in Australia proposed the classification [19] of multimedia traffic in the firewall by machine learning technology, which provides a reference for the depth detection method of multimedia packets.

In the later study, considering the more types of multimedia packets and different security, under the limited processing capacity of NIDS, when the network traffic is too large and omission is inevitable, the multimedia packets with high risk should be selected for detection as a priority, so we set up a multi-threading solution to multimedia traffic in NIDS based on GA (genetic algorithm) [20]

Although this solution can make the NIDS's limited processing capability concentrated on a high risk multimedia packet, the selection operator in the genetic operation adopts the roulette wheel selection strategy, so the selection process is

This work is supported by National Natural Science Foundation of China (61201118), Scientific research program of the Education Department of Shaanxi Provincial Shaanxi Province (16JK1347), Xi'an science and Technology Bureau(201805030YD8CG14(8)), Xi'an Beilin District Science and Technology Bureau(GX1708).

Xu Zhao is with the Shaanxi Key Laboratory of Clothing Intelligence, School of Computer Science, Xi'an Polytechnic University, Xi'an, 710048, Shaanxi, China (corresponding author; e-mail:37274679@qq.com).

Jin Jiang is with the School of Humanities and Social Sciences, , Xi'an Polytechnic University, Xi'an 710048, Shaanxi, China.

Reza Mousoli is with the School of Law, Criminal Justice and Computing, Canterbury Christ Church University, Canterbury CT1 1QU, UK.

random. This may lead to a deviation between the number of times the multimedia package is actually selected and the expected value. This paper improves the problem through the elitist strategy and proposes a new solution.

B. Contributions Summary

The main contributions of this paper are:

(1) We propose a multi-threading solution for multimedia packets based on GA and elitist strategy. By using this solution, NIDS can focus its limited processing power on more dangerous multimedia packets when omission becomes inevitable.

(2) We propose two optimization objectives to optimize NIDS:

1) The sum of danger coefficients of multimedia packets in every threads is maximal.

2) When the above objective is achieved, the load of each thread exactly reaches the highest.

(3)We analyze the shortcomings of roulette wheel selection by examples, then improve the selection operator with elite strategy, and propose a new solution step. In addition, we also design several experiments which compare the sum of danger coefficients and the detection number of multimedia packets before and after using the solution. We also prove its effectiveness based on above-mentioned experimental results.

C. Paper Organization

The rest of the paper is organized as follows: First, A GA-based multi-threading solution to multimedia traffic in NIDS is introduced in Section 2;Section 3 discusses the shortcomings of roulette wheel selection strategies and introduces elitist strategy.; Section 4 presents the implementation of the improved solution with elitist strategy; the experiment and an analysis of the result for contrasting the differences before and after using the solution is in Section 5; Section 6 summarizes the whole paper and presents some directions for the future work.

II. The GA-based multi-threading solution to multimedia traffic in NIDS

There are 191 types of multimedia packets in network traffic according to the latest MIME protocol and each of which has a different degree of risk. For example, exe,bat,com and other types of files have relatively higher danger coefficient. According to the set-method of the danger coefficient of multimedia types in [16], the multithreading solution to multimedia traffic in NIDS can be described as following:

Definition 1: Let NIDS capture n multimedia packets $P_1, P_2, P_3, \ldots, P_n$ in a certain time slice. The load that these packets bring to the system is $L(P_i) \in (0, LT], (i = 1, 2, \ldots, n)$, and the danger coefficient of these packets is $D_k(P_i), (k = 1, 2, \ldots, 191, 1 \le i \le n)$, and the load of each thread is LT. The solution will determine the options in each time slice so that the sum of danger coefficient of multimedia packets entering each thread is the highest, and the total load caused by these packets does not exceed the load of each thread.

Definition 2: Let m be the number of all threads, $T(P_i)$ be the number of threads which load packet P_i, S_j be the sum of the loads of packets in T_j thread when the penalty function is considered, and a be the penalty factor [16] when the load of multimedia packets in a thread T_j exceeds the load of this thread. Thus, the objective function reflecting the full utilization of each thread is shown in (1):

$$f(x) = m \cdot \left\{ m - \sum_{j=1}^{m} s_j \right\} = m \cdot \left\{ m - \sum_{j=1}^{m} \left[\sum_{T(P_i)=T_j} L(P_i) - a \cdot max(0, \sum_{T(P_i)=T_j} L(P_i) - 1) \right] \right\} \quad (1)$$

Definition 3: the target function of danger coefficient of the multimedia packet in each thread is shown in (2).

$$f_1(x) = max \sum D_k(P_i), 1 \le k \le 191, 1 \le i \le n \quad (2)$$

The two objective functions in Definition 2 and 3 achieve the following two aspects of Optimization:

1) Maximize the sum of the danger coefficient of the multimedia packets selected in each thread.

2) The load which caused by the multimedia packets selected within each thread is exactly equal to or close to the maximum load capacity of that thread.

Definition 4: the fitness function is shown in the following equation (3), where $C_{\max}$ is used to adjust the fitness function to take non negative values.

$$F(x) = \begin{cases} C_{\max} - f(x), & f(x) < C_{\max} \\ 0, & f(x) \ge C_{\max} \end{cases} \quad (3)$$

III. Selection Operator of Genetic Algorithm

There are three important operations in genetic algorithm: selection, crossover and mutation. Selection is a strategy of selecting individuals from a population so that they have more chances of being passed on to the next generation. The commonly used selection strategies are proportional selection, sorting and competitive selection. Proportion selection is a common method. Proportional selection simulates the natural law of survival of the fittest in the biological world, that is, species with high adaptability to the living environment will have more chances to inherit to the next generation, and species with low adaptability will have less chances to inherit to the next generation [20]. The most commonly used strategy in proportional selection is roulette wheel selection. Roulette wheel selection strategy is used in the multi-threading solution to multimedia traffic in NIDS proposed in [17].

A. Roulette Wheel Selection Strategy and Its Disadvantages

The idea of roulette wheel selection strategy is: the probability of each individual being selected depends on its fitness $P(x_i)$. $P(x_i)$ can be expressed as follow.

$$P(\mathrm{x_i})=\frac{f(\mathrm{x_i})}{\sum_{\mathrm{j}=1}^{N} f(\mathrm{x_j})} \tag{4}$$

In the above equation, $P(x_i)$ is the relative fitness of the ith individual x_i, that is, the probability of being selected. $f(x_i)$ is the fitness of the individual x_i, and $\sum_{j=1}^{N} f(\mathrm{x}_j)$ is the cumulative fitness of all the individuals in the population.

In this solution, fitness is determined by the danger coefficient of each type of multimedia package. The higher the danger coefficient, the greater the probability of being selected. So the number of times each multimedia package is selected can also be expressed by the expected value. As shown in (5):

$$\begin{aligned} e(\mathrm{x}_i) &= p(\mathrm{x}_i)\times N=\frac{f(\mathrm{x}_i)}{\sum_{\mathrm{j}=1}^{\mathrm{N}} f(\mathrm{x}_j)}\times N \\ &=\frac{f(\mathrm{x}_i)}{\sum_{\mathrm{j}=1}^{\mathrm{N}} f(\mathrm{x}_j)/N}=\frac{f(\mathrm{x}_i)}{\overline{f}} \end{aligned} \tag{5}$$

In (5), $\overline{f}$ is the average danger coefficient of all types of multimedia packets.

There are some problems in roulette wheel selection strategy: because of the randomness in the selection and crossover operations, there may be errors between the number of individuals selected and the expected value $f(\mathrm{x}_i)/\overline{f}$, so that some individuals with high fitness may not be selected, resulting in the reduction of the group average fitness $\overline{f}$, which has a negative impact on the convergence.

Here is a concrete example to illustrate this problem in Table 1. According to the implementation of roulette selection strategy, the fitness of all individuals (the last value is 46) is accumulated, and then a uniformly distributed random number is generated in 0-46. Then the random number is compared with the cumulative value. The first individual whose fitness cumulative value is greater than or equal to the random number is selected. As you can see, the third individual with fitness 15 (second highest) in Table 1 was not selected because the random number did not happen to be between 12 and 25. So this method may cause the highly adaptive individuals to be missed.

Table 1 The Example of Roulette Wheel Selection Strategy

individual	1	2	3	4	5
fitness	7	5	15	3	18
fitness cumulative value	7	12	25	28	46
random number	32	12	9	26	41
Selected individual	5	2	3	4	5

In order to solve this problem, we can choose the elitist strategy.

B. The Elitist Strategy and Its Advantages

In order to preserve the individuals with the highest fitness to the next generation, the elitist strategy can make these individuals not participate in genetic manipulation, and directly replace the individuals with the lowest fitness after crossover and mutation in the contemporary population.

Although the elitist strategy may lead to the rapid increase of local optimal individuals and affect the diversity of the problem, but these problems are not important for this solution, because the first thing to emphasize in this solution is to ensure that the highest danger coefficient packet must be selected, there is no requirement for diversity. Therefore, the combination of elitist strategy and roulette wheel selection strategy will achieve better results.

IV. The Improved Solution Based on Elitist Strategy

A. Steps of the Improved Solution Based on Elitist Strategy

Combined with the elitist strategy, the initial multimedia packets sequence $P=\{p_1, p_2, ..., p_n\}$ in each time slice are processed as follows:

1) According to the method of setting the danger coefficient of different types of multimedia packets in reference[16], the danger coefficient of each multimedia packet is determined as $D(P_i)$;

2) find out the most dangerous multimedia package p^*, and its danger coefficient is $D(P)_{\max}$;

3) The multimedia packets in the sequence are sorted from high to low according to the danger coefficient $D(P_i)$. The sorted sequence is $P'=\{p_1', p_2', ..., p_n'\}$, where $D(P_{i-1})>D(P_i)>D(P_{i+1})$;

4) Calculate the sum of the danger coefficients of all the multimedia packets in this time slice $\sum_{i=1}^{n} D(P_i)(i=1,2,\ldots,\mathrm{n})$;

5) Calculate the probability $P(x_i)$ of each multimedia package being selected， and $P(x_i)=D(P_i)/\sum_{i=1}^{n} D(P_i)(i=1,2,\ldots,\mathrm{n})$;

6）The roulette selection algorithm is used to select n times and store the last selected multimedia packets sequence;

7) Then crossover operation and mutation operation are performed to get the new multimedia packet sequence.

8) Find out the multimedia packets $newp_{max}^*$ with the highest danger coefficient (its danger coefficient is $newD(P)_{\max}$) and the multimedia packets $newp_{\min}^*$ with the lowest danger coefficient (its danger coefficient is $newD(P)_{\min}$) in the new multimedia packets sequence;

9) Comparing the danger coefficient $D(P)_{\max}$ of the multimedia packet p^* with that of the multimedia packet $newp_{max}^*$ with the highest danger coefficient $newD(P)_{\max}$ of the new multimedia packets sequence, if $D(P)_{\max} < newD(P)_{\max}$, then $newmp_{max}^*$ is regarded as the

multimedia packet with the highest danger coefficient at present, otherwise it will remain the same;

10) Replacing multimedia packets p^* with the highest danger coefficient in the new multimedia packet sequence with multimedia packets $newp^*_{\min}$ with the lowest danger coefficient

11) Repeat the above steps to generate a new multimedia packet sequence when the number of cycles is greater than the maximum generation.

12) The new sequence of multimedia packets is arranged in descending order according to the load size, and the multimedia packets are inserted into the threads of the NIDS.

13) If the total load $\sum_{i=1}^{n} L(P_i)$ of the multimedia packets loaded in thread T_j exceeds the load capacity of this thread, the multimedia packets that exceed are loaded into thread T_{j+1}.

B. Implementation of the Improved Solutions

In order to implement the improved solution in NIDS, we added a multimedia packet preprocessor in NIDS, which has three functions:

1. Enable NIDS to distinguish multimedia packets;

2. Generate new multimedia packet sequences according to the steps of Section 3.1.

3., marking the multimedia packets in the sequence and sending them to each thread of the detection engine.

In addition, we also modify the program of the detection engine, adding the function of monitoring and adjusting the load capacity of each thread. Figure 1 shows the processing procedure of the improved solution.

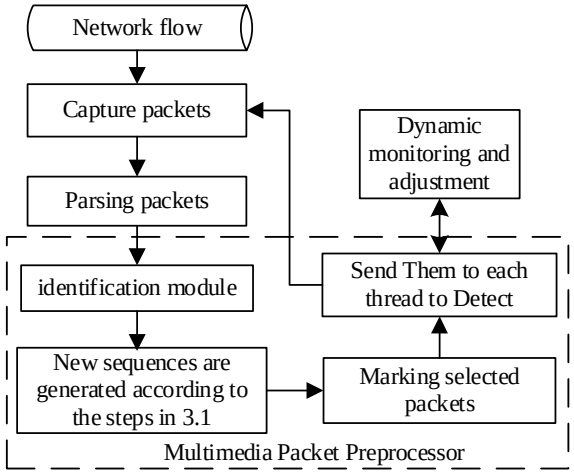

Fig. 1 The Processing Procedure Of Multimedia Packets By Improved Solutions

V. EXPERIMENTAL RESULTS AND ANALYSIS

A. Experimental Environment and Parameters

Considering that the KDD CUP 99 data set is too old, the test data is a mixture of NSL-KDD data set and background traffic with a large number of multimedia packets. The background traffic is collected by Wireshark in a LAN and transmitted to the test computer by TCPReplay on the attacking computer. Because the solution designed in this paper works when the traffic exceeds the load capacity of NIDS, the following experiments are all tested when the traffic exceeds the packet loss threshold of NIDS.

According to the danger coefficient setting method of different multimedia types in paper[16], the common multimedia packet information contained in background traffic is shown in Table 2.

Figure 2-4 are analyses of the background traffic. As can be seen from the figure, the number of documents such as ASP and ASPX is the largest, exceeding 1200. On the total data volume, the sum of JS files is the largest, reaching 3MKB. On average detection length, the SWF file is the longest, with an average of more than 200KB.

Table 2 All Kinds of Multimedia Packet Information in Background Traffic

Mime Type	File Type	Number	Total Amount Of Data (Kb)	Average Length (Kb)	Danger Coefficient
application/octet-stream	exe bin rar etc.	3	121	40	3.0
x-javascript	js	545	33245	61	2.5
text/html	htm html hts etc.	81	243	3	1.6
application/x-asap etc.	asp aspx jsp etc.	1320	22440	17	1.6
text/xml application/xml	xml	59	708	12	1.3
image/jpeg	Jpz jpg jpeg etc.	340	7140	21	1.5
image/gif	gif	728	728	1	1.5
x-shockwave-flash	swf swfi	10	**2250**	225	1.8

Figure 2-4 are analyses of the background traffic. As can be seen from the figure, the number of documents such as ASP and ASPX is the largest, exceeding 1200. On the total data volume, the sum of JS files is the largest, reaching 3MKB. On average detection length, the SWF file is the longest, with an average of more than 200KB.

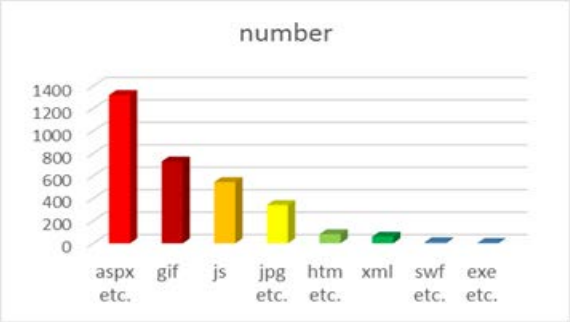

Fig. 2 The Number of Different Types of Multimedia Files

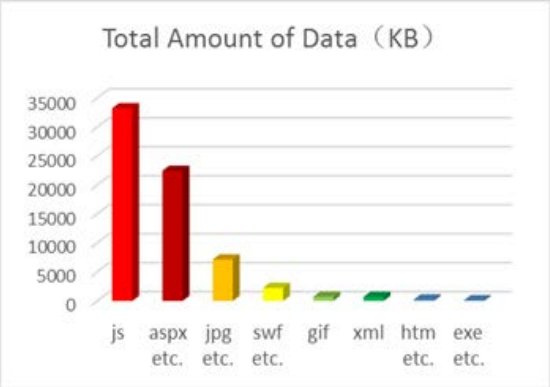

Fig. 3 The Total Amount of Data of Different Types of Multimedia Files

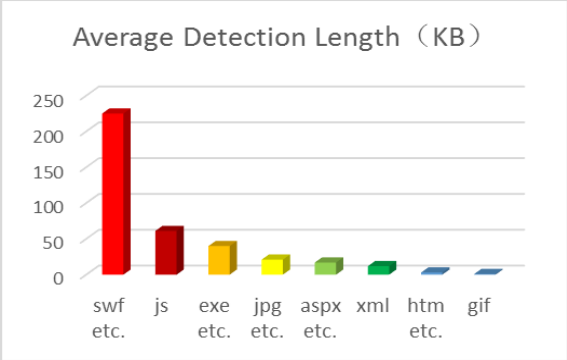

Fig. 4 Average Detection Length for Different Types of Multimedia Files

B. Detection Rates of Different Types of Multimedia Packets

As you can see in Table 3, the detection rate of different multimedia types of packets has changed before and after the use of elitist strategy. Among them, for EXE, JS, SWF multimedia packets with high danger coefficient, the number of detection improved significantly increased and reached full detection. This is mainly because the roulette wheel selection strategy is used in the former solution. Although the types with high danger coefficient are more likely to be selected, some individuals are not selected because of randomness. After adding the elitist strategy, we can ensure that individuals with high danger coefficient must be selected.

Table 3 Detection Rates of Different Types of Multimedia Packets

File Type	Total	Danger Coefficient	Detection Rates Before Improvement	Detection Rates After Improvement
aspx etc.	1320	1.6	984	879
gif	728	1.5	659	614
js	545	2.5	539	545
jpg etc.	340	1.5	325	311
htm etc.	81	1.6	75	64
xml	59	1.3	56	38
swf etc.	10	1.8	7	10
exe etc.	3	3.0	2	3

C. Detection of the Total Danger Coefficient of Selected Multimedia Packets in Different Threads

Figure 5 shows the difference in the sum of danger coefficients for selected multimedia packets in multiple threads before and after improvement in the same time slice. As shown in the figure, although the difference is not significant, the sum of danger coefficients for the selected multimedia packets in most threads is slightly higher after using the elite strategy. The main reason is that the individuals with high risk coefficient must be selected after adopting the elitist strategy. Figure 5 also shows that the objective function $max\sum D_k(P_i)$ reflecting the sum of danger coefficient in each thread has better convergence than before.

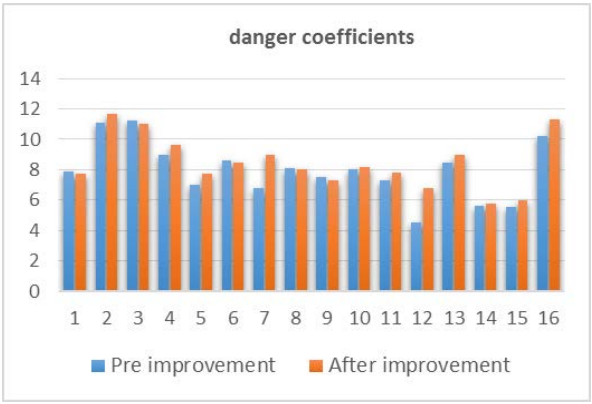

Fig. 5 The Total Danger Coefficient of Selected Multimedia Packets in Different Threads at the Same Time before and after Improvement

VI. CONCLUSIONS AND FUTURE WORK

With the increasing of network speed and network applications, the proportion of multimedia traffic in the network is becoming larger and larger. When the Network Intrusion Detection System detects large traffic in real time, it often loses packets because the traffic exceeds its load capacity. We have proposed a multi-threading solution based on genetic algorithm to identify and process multimedia traffic individually. However, this method has the problem of missing multimedia packets with high danger coefficient because of the roulette wheel selection strategy. On this basis, the selection operator is

improved by the elitist strategy, and a new processing step is proposed in the improved solution. By comparing the detection rate of different types of multimedia packets before and after the improvement with the sum of danger coefficients of selected multimedia packets in different threads, it is proved that the above improvement can effectively improve the detection rate of multimedia packets with high danger coefficients, and the convergence of the objective function is also strengthened.

In recent years, some new network applications have adopted evasion detection technology, so in the future we plan to adopt the method based on deep learning to improve the accuracy and efficiency of multimedia traffic identification and processing.

REFERENCES

[1] Zhang Ping, Liu Yanbing, Yu Jing, Et Al. Hashtrie: A Space Efficient Multi Pattern String Matching Algorithm [J]. Journal of Communication, 2015, 36 (10): 172-180.

[2] Zhao Guofeng, Ye Fei, Yao Yongan, Et Al. A Multi Pattern Matching Algorithm for Cloud Centric Network Intrusion Detection [J]. Information Network Security, 2018 (01): 52-57.

[3] Zhao X. Research on A Structure Of The Multimedia List Oriented Network Intrusion Detection System [J]. International Journal of Security and Its Applications, 2016, 10(12):53-68.

[4] Cheng Dongmei, Yan Biao, Wen Hui, Et Al. Design and Implementation of Distributed Industrial Control Intrusion Detection System Based on Rule Matching [J]. Information Network Security, 2017 (07): 45-51.

[5] Gao Ni, Gao Ling, He Yiyue, Et Al. Lightweight Intrusion Detection Model Based on Dimensionality Reduction of Self Encoded Network [J]. Acta Electronica Sinica, 2017, 45 (3): 730-739.

[6] Li W, Yang Z M, Chang Y P, et al. A Clustering Algorithm Oriented to Intrusion Detection[C]// IEEE International Conference on Computational Science and Engineering. IEEE, 2017:862-865.

[7] Buczak A L, Guven E. A Survey Of Data Mining And Machine Learning Methods for Cyber Security Intrusion Detection[J]. IEEE Communications Surveys & Tutorials, 2016, 18(2):1153-1176.

[8] Zuech R, Khoshgoftaar T M, Wald R. Intrusion Detection And Big Heterogeneous Data: A Survey [J]. Journal of Big Data, 2015, 2(1):3.

[9] Vijayanand R, Devaraj D, Kannapiran B. Intrusion detection system for wireless mesh network using multiple support vector machine classifiers with genetic-algorithm-based feature selection[J]. Computers & Security, 2018.

[10] Bai Jun, Xia Jingbo, Wu Jixiang, Et Al. Summary of Real Time Network Traffic Classification Research [J]. Computer Science, 2013, 40 (9): 8-15.

[11] Zhao Xu. Dynamic Adaptive Multimedia Data Processing Method Based on Snort [J]. Computer System Application, 2011, 20 (4): 211-213.

[12] Wei Shuning, Chen Xing, Tang Yong, Liu Hui.AR-HELM Algorithm Applied In Network Traffic Classification [J]. Information Network Security, 2018(01):9-14.

[13] Zaijianwang, Yuningdong, Shiwenmao, Et Al. Internet Multimedia Traffic Classification from Qos Perspective Using Semi-Supervised Dictionary Learning Models [J]. China Communications (English Edition), 2017, 14(10):202-218.

[14] Khammassi C, Krichen S. A GA-LR Wrapper Approach for Feature Selection in Network Intrusion Detection[J]. Computers & Security, 2018.

[15] Marques O, Baillargeon P. Design of A Multimedia Traffic Classifier for Snort[J]. Information Management & Computer Security, 2007, 15(3):241-256.

[16] Zhao X. Optimization of Dynamic Programming to The Multimedia Packets Processing Method for Network Intrusion Detection System [J]. International Journal of Security and Its Applications, 2015, 9(11):35-46.

[17] Zhao X. The Optimization Research of The Multimedia Packets Processing Method in NIDS with 0/1 Knapsack Problem [J]. International Journal of Network Security, 2015, 17(3):351-356.

[18] Marques O, Baillargeon P. A Multimedia Traffic Classification Scheme for Intrusion Detection Systems[C]// International Conference on Information Technology and Applications. IEEE Computer Society, 2005:496-501.

[19] Zander S, Armitage G. Practical Machine Learning Based Multimedia Traffic Classification for Distributed Qos Management[C]// Local Computer Networks. IEEE, 2015:399-406.

[20] Zhao Xu, Wang Wei. Genetic Algorithm Based NIDS Multimedia Package Multithread Processing Model [J]. Computer Engineering and Application, 2016, 52(14):115-118.

Xu Zhao was born on Jan.14 1978. He is a PhD student in information management and information system from Xi'an University of Architecture &Technology of China. He is also an associate professor in the School of Computer Science, Xi'an Polytechnic University, and Shaanxi, China. He received the M.S. degree from Xi'an Electronic Technology University, Xi'an City, and Shaanxi Province, China in 2007. He has developed several methods to deal with multimedia packets for network intrusion detection systems and is currently working on new optimization method with the help of artificial intelligence. His research interest is Cyber Security.

Jin Jiang is a Lecturer in the Xi'an Polytechnic University, Shaanxi, China. She received the M.E. degree from Xi'an Technological University, Xi'an City, Shaanxi Province, China in 2010. She has some projects in research supported by provincial funds. Her research interest is Network Security.

Reza Mousoli was born on April 20, 1961. He is a School Director of Stakeholder Engagement of School of Law, Criminal Justice and Computing of Canterbury Christ Church University of UK. His research Interests include Cyber Security, e-safety, Privacy and Confidentially.