Research on Automatic Intrusion Detection Method of Software-Defined Security Services in Cloud Environment

Xingjie Huang*, Jing Li, Jinmeng Zhao, Beibei Su, Zixian Dong, Jing Zhang
State Grid Information and Telecommunication Branch, Beijing, 100053, China

***Abstract*—In a cloud environment, software defined security services are highly vulnerable to malicious virus attacks. In response to software security issues, this project plans to use machine learning technology to achieve automated detection of software security services in a cloud environment. Firstly, study the intrusion characteristics of software defined security services in cloud environments based on piecewise sample regression, and establish their statistical feature quantities. Then, using the method of decision statistical analysis, achieve its fixed identification. Finally, the intrusion characteristics of software defined security services in the cloud environment are studied and compared with the data in the cloud environment to obtain its power spectral density. On this basis, machine learning methods are used to extract features from software security services in the cloud environment, in order to achieve the goal of automatic extraction and optimization of software security services in the cloud environment. Through simulation experiments, the credibility of the proposed algorithm for software defined security services in the cloud environment was verified, and the attack characteristics of software defined security services in the cloud environment were effectively patched.**

***Keywords*—Cloud environment; software; security services; invasion; detection; machine learning**

I. INTRODUCTION

Software Defined Network (SDN) is a new network innovation architecture first proposed by the Clean-Slate research group of Stanford University in the United States. Its design idea is to separate the data layer from the control layer, in which the control layer is a programmable central controller, which can obtain global network information, status, etc., which is convenient for operators and researchers to manage and configure the network, and can deploy customized new protocols. The data layer includes routers, switches and other packet forwarding devices, which focus on providing simple data forwarding functions and can quickly process matching packets to meet the growing needs of users in the network. SDN has a wide range of application scenarios, such as big data analysis, cloud computing, Internet of Things, and car networking. However, like traditional networks, the new features brought by SDN architecture are also threatened by cyber-attacks [1].

Network intrusion detection technology refers to identifying and filtering abnormal traffic in the network through effective technical means, which is the basic method to ensure network security. Identifying abnormal traffic in time and accurately can effectively reduce the impact of malicious attacks on the network and users [2]. At present, machine learning algorithm has attracted much attention in the field of network security, and intrusion detection technology based on machine learning has become a hot spot for researchers [3,4]. The study [5] proposes an intrusion detection system model by using different machine learning algorithms for different application scenarios. Autoencoder (AE) shows the advantages of the algorithm based on unsupervised learning in the task of feature extraction, feature reduction and classification, which promotes the progress of network attack traffic detection. The combination of automatic encoder and one-class support vector machine (OCSVM) algorithm can improve the anomaly detection rate and effectively reduce the training time of OCSVM algorithm, thus improving the performance of intrusion detection system. Therefore, it is of great theoretical and application value to study machine learning SDN intrusion detection technology based on automatic encoder and one-class support vector machine. Effectively detect the intrusion data of software-defined security service in cloud environment, and combine the statistical feature analysis and feature extraction methods of software-defined security service intrusion in cloud environment to fix the features and collect samples of software-defined security service intrusion in cloud environment. In research [6], an intrusion feature extraction method of software-defined security services in cloud environment based on blind balanced scheduling is proposed. Combined with the backtracking control method of intrusion nodes, the intrusion feature extraction of software-defined security services in cloud environment is realized, which improves the intrusion detection ability, but the optimization control ability of this method is not good, and the real-time performance of intrusion detection is not good. In study [7], an intrusion feature extraction method of software-defined security services in cloud environment based on spectral peak correlation search is proposed, which combines the autonomous positioning technology of intrusion nodes to realize intrusion feature extraction of software-defined security services in cloud environment, but the active optimization ability of this method is not strong. The most important feature of software-defined network is that it can program the network behavior, but the original software-defined network architecture is only limited to the programmability of the control plane, and the function of its forwarding plane is still limited by the fixed function hardware supported by the equipment provider. P4 can instantiate customized pipelines and stateful objects, support the implementation of complex

workflows, user-defined protocols and finite state machines, and use P4 switch to realize a reliable attack detection system to protect edge node resources from malicious network attacks, thus maximizing network utilization and effectively ensuring service quality [8].

Aiming at the above problems, this paper proposes a software-defined security service intrusion detection method in cloud environment based on machine learning algorithm. The statistical feature quantity of software-defined security service intrusion characteristics in cloud environment is constructed by using piecewise sample regression analysis method, and the intrusion characteristics of software-defined security service in cloud environment are fixed and identified by combining decision statistical analysis method. Combined with the feature fusion analysis method of classified intrusion samples, a big data distribution model of software-defined security service intrusion features in cloud environment is constructed, and the power spectral density feature quantity of software-defined security service intrusion features in cloud environment is extracted. The machine learning algorithm is used to adaptively optimize the extraction process of software-defined security service intrusion features in cloud environment, so as to realize automatic extraction and optimization of software-defined security service intrusion features in cloud environment. Finally, the simulation experiment analysis shows the superior performance of this method in improving the intrusion feature extraction ability of software-defined security services in cloud environment [9].

II. Software-defined Security Network Intrusion Node Distribution Model and Information Sampling

A. Cloud Software Defined Security Network Intrusion Distribution Structure Model

The data forwarding layer is located at the bottom of SDN architecture, and contains thousands of interconnected switches, which are responsible for forwarding data packets. If the switch is damaged, the message flowing through the switch will not be forwarded normally. In addition, the switch is the direct entrance for end users to access the network, and attackers can attack the switch by simply connecting to the switch port. Man-in-the-middle attack is a typical network intrusion method. Its main principle is to insert a proxy node between the source node and the target node, intercept the communication data, and tamper with the communication data without being discovered. The specific attack methods of man-in-the-middle attack include session hijacking, DNS spoofing and port mirroring. Man-in-the-middle attack between controller and switch is an ideal way to attack SDN network [10]. It can intercept and tamper with the forwarding rules of messages sent to switch, so as to control network forwarding. After that, attackers can carry out further attacks, such as black hole attacks. In addition, there may be no direct physical connection between the controller and the switch, that is, the data packet from the switch to the controller may pass through several other switches, so in the man-in-the-middle attack, all the switches and hosts directly connected to it on the communication path can easily be converted into proxy nodes. In order to realize the optimization of intrusion feature extraction of software-defined security service in cloud environment, it is necessary to construct a distributed sensor model of software-defined security network in cloud environment under intrusion. Combined with the distributed design method of directed graph, blind forensics and intrusion node location are carried out for intrusion feature extraction of software-defined security service in cloud environment. Combined with feature distributed sampling technology [5], the intrusion node distribution model of software-defined security network nodes in cloud environment is constructed by using packet forwarding control technology, as shown in Fig. 1.

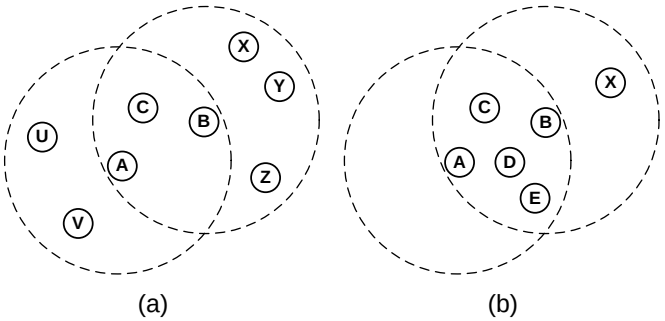


Fig. 1. Intrusion node distribution model of software-defined security network in cloud environment.

In the software-defined secure network node distribution model in the cloud environment shown in Fig. 1, when new data traffic in the network enters the OpenFlow switch for the first time, the OpenFlow switch will generate and process a Packet_In message to the control plane. By looking at the Packet_In message, the control plane will install the flow rules (dropping, forwarding and enqueuing) into the flow table and then send them to the OpenFlow switch. There is no authentication mechanism in this communication process if there is an incorrect traffic flow in the network [10].

Data plane refers to the interconnection infrastructure composed of hardware or software-based devices, which have basic packet forwarding functions, and these functions manage the received packets according to the flow rules set by the controller through the southbound interface. Each rule entry in the flow table consists of three fields: operation, counter and mode. The mode field defines the flow mode, and the flow mode is basically a collection of field values in the packet header. When a packet is received, the switch will search for a rule matching the field in its flow table. Once the switch matches such a rule, the counter of the rule will be incremented and the operation corresponding to the specific rule will be executed. Otherwise, the switch will inform the controller to ask for help or directly discard the packet.

The control plane is an independent and logically centralized server, also called the controller, which is used to handle the flow table installation of forwarding rules and monitor the status of data plane devices and links to integrate the global network view. Its main purpose is to manage the distributed forwarding devices of data plane in the network and provide operators with a simpler API, namely the northbound interface. SDN controller communicates with the switch through southbound API, such as OpenFlow protocol, and has a global view of the whole network topology. The originally

designed OpenFlow protocol promotes the decoupling of control plane and data plane. OpenFlow provides a southbound interface for the controller to establish a secure communication channel to manage forwarding device rules and receive status updates. These rules are the operations (such as forwarding, flooding and dropping) of the data packet determined according to the header information of the data packet (such as Ethernet /IP address and TCP/UDP port). The status includes the information discovered by the link layer, and the data packet and byte counters related to the flow table, which are used to support the global network view on the control plane [11].

The application plane is composed of a group of network applications, which provides users with quick response and various business requirements, such as network virtualization, topology discovery, traffic monitoring, security, load balancing and so on. The application communicates with the controller through the northbound API, such as RESTAPI, and the control layer provides the abstraction of physical network resources for the application layer, which enables the user to give the SDN controller other functions through the application and change the data flow rules without reconfiguring all the physical switches, so as to better manage and control the network behavior.

Under the network structure of SDN, equipment suppliers can focus on designing forwarding equipment for efficiently processing data packets, and network operators can easily test and deploy customized network management applications from a higher abstract level [12].

B. Software-defined Security Service Intrusion Information Sampling

Construct a node distribution model for extracting intrusion characteristics of software-defined security services in cloud environment, and use a binary directed graph to represent $G=(V,E)$, and the node's intrusion location is $\eta_n \in \Omega_\eta, n=1,2,...,N$. Construct a packet link forwarding protocol for network intrusion, and design a node directed graph model for network intrusion, and obtain a link forwarding control protocol for software-defined security services intrusion in cloud environment, which is expressed in the following form:

$$E(p)=[\underbrace{0,0,...,0}_{i-1},\frac{\gamma_{th}\sigma^2}{h_i[G-(n-k-1)\gamma_{th}]},\ldots,\frac{\gamma_{th}\sigma^2}{h_i[G-(n-k-1)\gamma_{th}]}]^{\mathrm{T}} \tag{1}$$

Set $f(p_i)=\frac{-L_i}{2}\log(1+p_i)$, by calculating the cross-correlation coefficient between different categories of the hidden layer, according to the priority $\boldsymbol{E}=\boldsymbol{E}_1\cup\boldsymbol{E}_2\cup\boldsymbol{E}_3$ of connecting to the software-defined security service intrusion node in the cloud environment, and combining with the correlation detection method, obtain the statistical probability distribution statistics of the software-defined security service intrusion neighbor node in the cloud environment as follows:

$$\boldsymbol{V}t(k)=\left\{a_{s+t}...a_{t+1}a_t...a_1 1\,|\,\overline{a_{s+t}...a_{t+1}}=k,\ a_i\in\{0,1\},0\le k<2^s\right\} \tag{2}$$

Assume $a_1,a_2\in V$, $b_1,b_2\in V'$, for Sink nodes $\boldsymbol{EH}s(j)$ and $\boldsymbol{EH}t(k)$ with software-defined security service intrusion feature distribution in the cloud environment, learn quickly and generalize the method, and get the associated feature quantity of intrusion feature detection as follows:

$$T_{l1}=\sqrt{{F_{p1}}^2+{F_{q1}}^2} \tag{3}$$

According to the number of hidden layers of the structure, the feature validity of node intrusion is analyzed, and the reliability evaluation model of intrusion feature detection is $F_{i1}=\frac{1}{P_{i1}}$, thus the feature link distribution model of software-defined security service intrusion nodes in cloud environment is constructed. The hidden layer and the output layer form a complete feature chain, which is expressed as $W(p)=G_T p^2-Cp+\alpha T$, which $W(p)$ is a quadratic function of the software-defined security service intrusion feature link set SD in cloud environment. Combined with the decision statistical analysis method, the intrusion feature of software-defined security service in cloud environment is fixed and sample identified, which improves the effectiveness of feature extraction.

C. Information Sampling of Intrusion Characteristics

A big data distribution model of software-defined security service intrusion characteristics in the cloud environment is constructed by combining the classified intrusion sample feature fusion analysis method, and the power spectral density of software-defined security service intrusion characteristics in the cloud environment is extracted, and the statistics of blind forensics judgment of software-defined security service intrusion characteristics in the cloud environment are obtained as follows:

$$\mu(n)=\begin{cases}\beta_1\left[1-\exp(-\alpha_1|e_{MCMA}(n)|^2)\right], & E\left[(|e(n)|^2)\right]>K\\ \beta_2\left[1-\exp(-\alpha_2|e_{MCMA}(n)|^2)\right], & \cdots\cdots\end{cases} \tag{4}$$

Wherein, K is the decision threshold for successful attack $\alpha_1>0$, $\alpha_2>0$, $\lambda_{\max}$ is the intrusion decision thresholds for software-defined security network in cloud environment, $0<\beta_1<\frac{1}{\lambda_{\max}}$ $0<\beta_2<\frac{1}{\lambda_{\max}}$. When the root mean square error of one-step attack in each variable set is satisfied as $MSE=E[(|e(n)|^2)]>K$, take smaller α_2

and β_2 to sample the characteristic information of intrusion characteristics. The fuzzy decision algorithm for sampling the characteristic information of intrusion characteristics is described as follows:

ROUTE_2 (Route $u = u_{s+1}...u_{t+1}u_t...u_1 0$, $v = v_{s+t}...v_{t+1}u_t...u_1 0$)

{

$x = u_{s+1}...u_{t+1}$; $y = v_{s+t}...v_{t+1}$; $\boldsymbol{I}(x,y) = \varnothing$;

For each e_i, if ($u_i \neq v_i$) $\boldsymbol{I}(x,y) = \boldsymbol{I}(x,y) + e_i$;

While ($\boldsymbol{I}(x,y) \neq \varnothing$){ $e_i = firstselect(\boldsymbol{I}(x,y))$; //

Set the success probability of feature extraction.

$y = y_{n-1}y_{n-2}...y_0$ //

Forwarding control protocol for variable sets form x to $x + e_i$; $x = x + e_i$; $\boldsymbol{I}(x,y) = \boldsymbol{I}(x,y) - e_i$;}

}

According to the above algorithm design process, an intrusion detection system ML-SDNIDS based on machine learning is designed under the SDN network architecture. The overall architecture is mainly divided into two parts: the control plane and the data plane. The control plane is mainly responsible for the feature processing of the data set, the algorithm training of the intrusion detection model, the creation of the flow table and the centralized management of the data plane. The data plane is composed of multiple P4 switches connected with each other, and is mainly responsible for malicious traffic detection and packet forwarding decision. The control plane uses the existing IDS data set in the network, inputs the data set into the feature extraction module, and then the feature extraction module processes the data packet to effectively select the original features. Then the feature mapping module selects the features with strong correlation, and maps different features to the automatic encoder network. The automatic encoder calculates the root mean square error (RMSE) between the new data and the fitting data, and then uses OCSVM classification algorithm to classify the RMSE to realize anomaly detection.

III. Optimization of Intrusion Detection for Software-defined Security Services

A. Fixed Handling of Intrusion Characteristics of Software-defined Security Services

Intrusion detection system mainly includes three modules: information collection, data analysis and emergency response. The information collection module is the foundation of the whole system, which mainly collects host log information, network segment protocol datagram information and user behavior status. The data analysis module is the core module of the whole system, which mainly uses some means such as statistics, pattern matching and anomaly detection algorithm to quickly analyze the data collected in the information collection stage and judge whether there is abnormal behavior in network activities. The emergency response module is to take corresponding protection measures in time to prevent further damage when intrusion is detected in the previous stage.

The control plane uses the existing IDS data set in the network, inputs the data set into the feature extraction module, then the feature extraction module processes the data packet, selects the effective features of the original features, then the feature mapping module selects the features with strong correlation, maps different features to the automatic encoder network, and the automatic encoder calculates the root mean square error (RMSE) between the new data and the fitting data. Then, RMSE is classified by OCSVM classification algorithm to realize anomaly detection, and the intrusion features of software-defined security services in cloud environment are fixed and optimized. This paper proposes an intrusion detection method of software-defined security services in cloud environment based on machine learning algorithm. The statistical analysis model is adopted to construct the feature spatial distribution structure model of software-defined security service intrusion characteristics in cloud environment, and the nonlinear time series of software-defined security service intrusion characteristics in cloud environment is obtained as follows:

$$x_i(t) = x_i^1(t) + x_i^2(t) + x_i^3(t) \tag{5}$$

Wherein,

$$x_i^1(t) = \sum_{k=1}^{p} \varphi_{k0} x_i(t-k) - \sum_{k=1}^{q} \theta_{k0} \varepsilon_i(t-k) + \varepsilon_i(t) \tag{6}$$

$$x_i^2(t) = \sum_{k=1}^{p} \sum_{l=1}^{2} \varphi_{kl} [w_{i1}^l, \cdots, w_{in}^l][x_1(t-k), \cdots, x_n(t-k)]^T \tag{7}$$

$$x_i^3(t) = -\sum_{k=1}^{q} \sum_{l=1}^{2} \theta_{kl} [w_{i1}^l, \cdots, w_{in}^l][\varepsilon_1(t-k), \cdots, \varepsilon_n(t-k)]^T \tag{8}$$

When the intruder attacks the target network, combining with the piecewise linear test method, the statistical characteristics of software-defined security service intrusion detection in cloud environment are obtained as follows:

$$DS = \{(x_0, t_0), (x_1, t_1), \ldots, (x_i, t_i), \ldots\} \tag{9}$$

Combining machine learning and genetic evolution methods, the feature set of software-defined security service intrusion features in cloud environment is automatically clustered, and the fuzzy fit degree of software-defined security service intrusion feature detection in cloud environment is obtained as follows:

$$\begin{aligned} O(LOF_k(p)) &= O(lrd_k(p)) + O(N_{k-dist(p)}) \\ &\quad + O(lrd_k(o_i \in N_{k-dist(p)})) \\ &= O(m * n) \end{aligned} \tag{10}$$

In the spatial distribution area of software-defined security service intrusion characteristics in cloud environment, the adaptive scheduling of software-defined security service intrusion characteristics in cloud environment is carried out by combining genetic evolution and statistical feature analysis methods.

B. Automatic Extraction and Optimization of Intrusion Characteristics of Software-defined Security Services in Cloud Environment

Combined with the decision statistical analysis method, the intrusion features of software-defined security services in cloud environment are fixed and identified, and the process of extracting intrusion features of software-defined security services in cloud environment is adaptively optimized by machine learning algorithm to realize automatic extraction and optimization of intrusion features of software-defined security services in cloud environment. The implementation steps are described as follows:

Step 1: Constructing a nonlinear feature sequence distribution set $k, k = 1, 2 \cdots, p$ and an information weighting coefficient w_{i1}^{l}, $\cdots$, w_{in}^{l} of software-defined security service intrusion features in a cloud environment, and performing node initialization operation to meet the requirements.

Step 2: Calculate the spectral density of the cluster head node of the software-defined security service intrusion feature chain in the cloud environment, and calculate the formula of information sampling time delay in the storage space of the software-defined security service intrusion feature in the cloud environment. $\tau^{*}(p) = \dfrac{\theta(p.d, q.d)}{1 + \alpha \cdot \delta(p.l, q.l)}$, construct the first route detection protocol under network intrusion.

Step 3: Machine learning algorithm is used for optimization control, and the coverage point set of intrusion feature distribution is obtained.

Step 4: Reconstruct the intrusion characteristics of software-defined security services in cloud environment in the dimension distributed feature space, and get the structural mapping output of the feature chain.

$$\Omega_i(t) = \frac{\gamma_{th}\sigma^2}{h_i[G - (N(l) - 1)\gamma_{th}]}$$

Step 5: Using the fuzzy optimization control method, the iterative formula of intrusion feature extraction is $p_i(l+1) = \min(p_{\max}, \Omega_i(l+1))$. If the software defines the security service intrusion feature storage spectrum component gain value $h_i \neq h_{\min}(l)$ and $\Omega_i(l) > 0$ in the cloud environment, the partial derivative of intrusion feature location output is obtained:

$$\frac{\partial u_i}{\partial p_i} = \frac{Gh_i}{\sum_{j \neq i} h_j p_j + \sigma^2}\left(\frac{1}{1+\gamma_i} - \beta_{C_1}\right) \tag{11}$$

Step 6: According to the improved machine learning algorithm, the adaptive iteration is carried out until the convergence criterion is met, the coverage of intrusion feature distribution of software-defined security services in cloud environment is calculated, and the intrusion feature is extracted according to the coverage, and the end is over.

The implementation process of extracting and fixing intrusion features of software-defined security services in cloud environment is shown in Fig. 2.

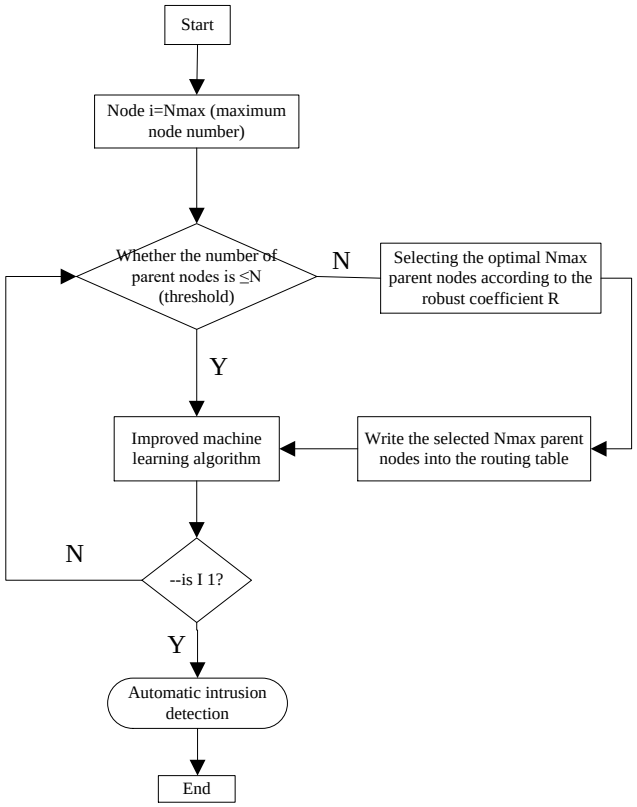


Fig. 2. Flow chart of network intrusion detection implementation.

IV. Simulation Experiment Analysis

In Matlab 7 simulation environment, the simulation experiment of automatic extraction of intrusion characteristics of software-defined security services in cloud environment is carried out. Four P4 switches and four terminal hosts are adopted. The four switches are connected with each other to form a data forwarding plane, switch s1 is connected with hosts h1 and h2, and switch s2 is connected with hosts h3 and h4, and the hosts can communicate with each other. The configuration file describes in detail the network information configuration of each host (such as IP address, MAC address and default gateway), the configuration file path of P4 switch, and the connection path between the host and the switch. CIC-IDS2018 data set is dedicated to the analysis, testing and evaluation of network-based intrusion detection systems. The

data set is generated based on the creation of a user information file, which contains abstract expressions of events and user behaviors browsed by users in the network. The data set contains seven different attack scenarios: Brute-force, Heartbleed, Botnet, DenialofService(DoS), Distributed Denialofservice (DDOS), Webattacks and Infiltration of Modern WorkFrominside. The basic attack facility includes 50 computers as attack nodes, and the attack target includes 420 computers and 30 servers. The final data set includes the captured network traffic and system logs of each machine, and 80 features extracted from the captured traffic using CICFlowMeter-V3. The running environment of ML-SDNIDS is shown in Fig. 3.

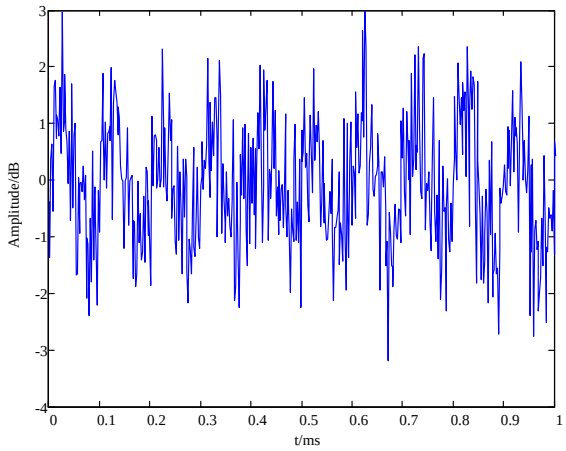
```
p4@ubuntu:~/P4/tutorials/ML-SNDIDS/P4-NIDS$ make run
mkdir -p build pcaps logs
p4c-bm2-ss --p4v 16 --p4runtime-files build/basic_nids.p4.p4info.txt -o build/ba
sic_nids.json basic_nids.p4
sudo python ../../utils/run_exercise.py -t pod-topo/topology.json -j build/basic
_nids.json -b simple_switch_grpc
Reading topology file.
Building mininet topology.
Configuring switch s3 using P4Runtime with file pod-topo/s3-runtime.json
 - Using P4Info file build/basic_nids.p4.p4info.txt...
 - Connecting to P4Runtime server on 127.0.0.1:50053 (bmv2)...
 - Setting pipeline config (build/basic_nids.json)...
 - Inserting 8 table entries...
 - MyEgress.swid: (default action) => MyEgress.set_swid(swid=3)
 - MyIngress.ipv4_lpm: (default action) => MyIngress.drop()
 - MyIngress.ipv4_lpm: hdr.ipv4.dstAddr=['10.0.1.1', 32] => MyIngress.ipv4_forwa
rd(dstAddr=08:00:00:00:01:00, port=1)
 - MyIngress.ipv4_lpm: hdr.ipv4.dstAddr=['10.0.2.2', 32] => MyIngress.ipv4_forwa
rd(dstAddr=08:00:00:00:01:00, port=1)
 - MyIngress.ipv4_lpm: hdr.ipv4.dstAddr=['10.0.3.3', 32] => MyIngress.ipv4_forwa
rd(dstAddr=08:00:00:00:02:00, port=2)
 - MyIngress.ipv4_lpm: hdr.ipv4.dstAddr=['10.0.4.4', 32] => MyIngress.ipv4_forwa
rd(dstAddr=08:00:00:00:02:00, port=2)
```

Fig. 3. ML-SDNIDS operating environment.

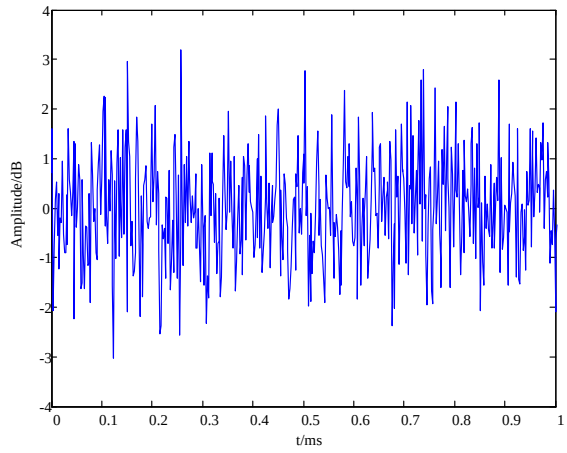
The fundamental frequency of software-defined security service intrusion feature collection in cloud environment is 20KHz, the coverage range of software-defined security service intrusion feature in cloud environment is 200*400, the spectral feature detection of software-defined security service intrusion feature in cloud environment is set to 12, the normalized termination frequency of information collection is 0.68Hz, and the modulation frequency of intrusion information detection varies between [120Hz and 1024Hz]. The intrusion characteristics of software-defined security services in cloud environment are extracted with signal-to-noise ratios of -5dB, 5dB and 20dB, respectively. CIC-IDS2018 data set is used. Due to the limited experimental environment, some data sets in CIC-IDS2018 total data set are selected for this test. The statistical information is as follows, including the total number of samples, the number of normal samples and the number of abnormal samples in each sub-data set. According to the above simulation environment and parameter settings, the intrusion characteristics of software-defined security services in cloud environment are extracted, and the original intrusion data collection is shown in Fig. 4.

Taking the data collected in Fig. 4 as input, the intrusion feature extraction of software-defined security service in cloud environment is carried out, and the extraction result is shown in Fig. 5.

From the analysis of Fig. 5, it is known that the intrusion feature extraction of software-defined security services in cloud environment by this method has strong detection ability for the distribution of intrusion areas. The accuracy of different methods for intrusion feature extraction of software-defined security services in cloud environment is tested, and the comparison results are shown in Table I. From the analysis of Table I, it is known that the intrusion feature extraction of software-defined security services in cloud environment by this method has high accuracy and good detection performance.



(a) Test sample.



(b) Training sample.

Fig. 4. Time domain waveform of software-defined security service intrusion characteristic sampling data.

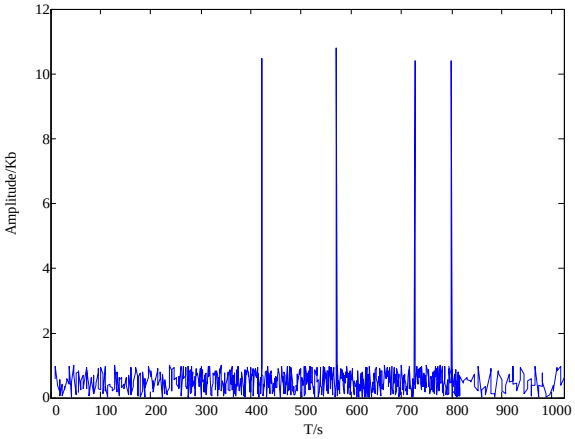


Fig. 5. Extraction results of intrusion characteristics of software-defined security services in cloud environment.

TABLE I. COMPARISON OF DETECTION PERFORMANCE

Iterations	The method in this paper	Neural network detection	Block matching detection
200	0.914	0.846	0.826
400	0.955	0.889	0.892
600	0.992	0.923	0.926
800	1	0.944	0.965

V. CONCLUSIONS

In this paper, the intrusion data of software-defined security service in cloud environment is effectively detected, combined with the statistical feature analysis and feature extraction method of software-defined security service intrusion in cloud environment, the feature fixation and sample collection of software-defined security service intrusion in cloud environment are carried out, and the software-defined security service intrusion forensics in cloud environment is realized according to the sample categories of software-defined security service intrusion in cloud environment. In this paper, an intrusion detection method of software-defined security service in cloud environment based on machine learning algorithm is proposed. The statistical feature quantity of software-defined security service intrusion characteristics in cloud environment is constructed by piecewise sample regression analysis method, and the intrusion characteristics of software-defined security service in cloud environment are fixed and sample identified by combining decision statistical analysis method. Combined with the feature fusion analysis method of classified intrusion samples, a big data distribution model of software-defined security service intrusion features in cloud environment is constructed, and the power spectral density feature quantity of software-defined security service intrusion features in cloud environment is extracted. The machine learning algorithm is used to adaptively optimize the extraction process of software-defined security service intrusion features in cloud environment, so as to realize automatic extraction and optimization of software-defined security service intrusion features in cloud environment. The research shows that this method has high accuracy in extracting intrusion features of software-defined security services in cloud environment, good reliability in network intrusion detection and strong ability in fixing intrusion features.

Finally, under the software-defined network structure, the control plane realized the intrusion detection model based on the combination of automatic encoder and support vector machine, and the data plane realized the intrusion detection system based on machine learning with P4 programming language. Feature extraction is carried out on the data plane, and the packet features are classified in the matching action pipeline, and finally the decision classification of the packet is realized in the export pipeline. The final experimental results show that, in most cases, the accuracy of attack detection is higher than that of ninety-seven percent. Although the packet processing delay is increased by about five times, its efficiency is still millisecond.

ACKNOWLEDGMENT

The study was supported by Science and Technology Project of The State Grid Information and Telecommunication Branch “Research and design of key technologies for security intelligent detection and automation arrangement in a heterogeneous cloud environment” (NO. 529939220003).

REFERENCES

[1] YANG Jianxi, ZHANG Yuanli, JIANG Hua, ZHU Xiaochen. Detection method of physical-layer impersonation attack based on deep Q-network in edge computing. Journal of Computer Applications, 2020, 40(11):3229-3235.

[2] EBTEHAJ I, BONAKDARI H, ES-HAGHI M S. Design of a hybrid ANFIS-PSO model to estimate sediment transport in open channels. Iranian Journal of Science and Technology-Transactions of Civil Engineering, 2019, 43(4):851-857.

[3] GHASEMI M, AKBARI E, RAHIMNEJAD A, et al. Phasor particle swarm optimization:a simple and efficient variant of PSO. Soft Computing, 2019, 23(19):9701-9718.

[4] KHALILI A, SAMI A. SysDetect: a systematic approach to critical state determination for industrial intrusion detection systems using Apriori algorithm. Journal of Process Control, 2015, 2776:154-160.

[5] Mernik M, Liu S H, Karaboga M D, et al. On clarifying misconceptions when comparing variants of the Artificial Bee Colony Algorithm by offering a new implementation. Information Sciences, 2015, 291(10):115-127.

[6] MORADI M, KEYVANPOUR M R. An analytical review of XML association rules mining. Artificial Intelligence Review, 2015, 43(2):277-300.

[7] BACH S H, BROECHELER M, HUANG B, et al. Hinge-loss Markov random fields and probabilistic soft logic. Journal of Machine Learning Research, 2017, 18:1-67.

[8] FARNADI G, BACH S H, MOENS M F, et al. Soft quantification in statistical relational learning. Machine Learning, 2017, 106(12):1971-1991.

[9] YUAN Chi. Identity-based dynamic clustering authentication algorithm for wireless sensor networks. Journal of Computer Applications, 2020, 40(11):3236-3241.

[10] Yongmin LIU, Yujin YANG, Haoyi LUO, et al. Intrusion detection method for wireless sensor network based on bidirectional circulation generative adversarial network. Journal of Computer Applications, 2023, 43(1):160-168.

[11] MOZAFFARI M, SAAD W, BENNIS M, et al. A tutorial on UAVs for wireless networks: applications, challenges, and open problems. IEEE Communications Surveys & Tutorials, 2019, 21(3):2334-2360.

[12] YUAN X, HE P, ZHU Q, et al. Adversarial examples: attacks and defenses for deep learning. IEEE Transactions on Neural Networks and Learning Systems, 2019, 30(9):2805-2824.