Research on distributed network attack source tracking method based on interference suppression

PG Hu and XQ Chen
Hunan Railway Professional Technology, Zhuzhou, Hunan, 412001, China
E-mail: zhisong@mls.sinanet.com

Abstract. In order to improve the security of distributed network operation, a distributed network attack source tracking method based on interference suppression is proposed. According to the structural characteristics of distributed network, the signal expression relationship between different distributed hosts is constructed, and the generalized cross-correlation weighting function is constructed to suppress the interference of distributed network. Based on this, particle swarm optimization algorithm is used to collect a sufficient number of attack marking information packets through multiple iterations. The interference signal of the separated signal is obtained through blind source separation. After signal separation, the tracking results of different attack source signals are obtained. The experimental results show that compared with the traditional attack source tracking method, this method not only reduces the tracking time, but also greatly improves the tracking accuracy.

Keywords. Interference suppression; Distributed network; Attack source tracking

1. Introduction

Among the various security problems faced by distributed networks, the high-precision tracking of attack source tracking is the most serious problem. If the attack path of attack source cannot be accurately determined, it will pose a serious threat to various privacy information in distributed networks [1-3]. If the attack source cannot be tracked for a long time, the distributed network host will lose the function of providing security services for legitimate users. The initiators of various attacks will also make a large number of puppet hosts, and use the puppet hosts to launch malicious attacks on users, resulting in serious economic losses [4]. Compared with the Internet, hosts in distributed networks are connected more frequently, which makes it more difficult to track distributed network attack sources.

Reference [5] proposes an attack source tracking method based on behavior analysis, which uses stochastic Petri nets to build a distributed network attack source behavior detection model and extract the attack characteristics of attack behavior. The extracted attack characteristics are matched with the historical attack behavior characteristics, so as to judge the attack type. According to the judgment result of attack type, the intrusion location of the attack is detected, and then the tracking detection of attack source is completed. However, the tracking results of this method are quite different from the actual results, so it is difficult to ensure the integrity of distributed network operation. Reference [6] proposes an attack source tracking method based on knowledge map. This method uses knowledge map to model the traffic communication process between multiple hosts in distributed network, judge whether the target host is the initiator of the attack, if it is the initiator of the attack, locate the host as the attack source and track the attack source. However, this method needs to judge multiple hosts in the distributed network, so
the tracking time of this method is long. Reference [7] proposes an attack source method based on isolated forest algorithm. This method shunts the cloud center model training tasks through edge nodes. After shunting, judge whether a single data stream contains attack data stream. If an attack data stream is detected in a node, judge that the node is the attack source node. Although this method can track the attack source, it has the problem of low tracking.

In order to solve the problems of low tracking accuracy and long tracking time of the above traditional methods, a distributed network attack source tracking method based on interference suppression is proposed.

2. Distributed network attack source tracking

2.1. Distributed network interference suppression

Since it is difficult to track attack sources in distributed networks, in order to improve the effectiveness of attack source tracking, it is necessary to suppress interference factors in distributed networks [8-10].

The distributed network is a network structure with \( N \) transceiver hosts. The signal transmitting and receiving hosts are scattered in the distributed network area. It is assumed that the location set of the receiver and transmitter is \((x_0, y_0), (x_1, y_1), ..., (x_N, y_N)\), the location of the jammer is \((x_j, y_j)\), the interfered host is \((x_r, y_r)\), and all transmitters are within the interference signal coverage of the jammer. If the jamming signal sent by the jammer is \( s(t) \) and the transmitting signal of the transmitter is \( x(t) \), the received signal of the \( i \)-th host in the distributed network can be expressed as:

\[
r_i(t) = \alpha_s(t - R_{ji}/c) + \beta_i(t - R_{ji}/c) + \eta_i(t), i=1, ..., N
\]

In the formula, \( \alpha_s \) represents the signal amplitude of the \( i \)-th host, \( \beta_i \) represents the interference signal amplitude, \( \eta_i(t) \) represents Gaussian white noise, \( R_{ji} \) represents the distance between the interference host and the receiving host, and \( R_{ji} \) represents the distance between the signal transmitting host and the signal receiving host [11]. The calculation formulas of \( R_{ji} \) and \( R_{ji} \) are:

\[
R_{ji} = \sqrt{(x_j - x_i)^2 + (y_j - y_i)^2}
\]
\[
R_{ji} = \sqrt{(x_r - x_i)^2 + (y_r - y_i)^2}
\]

The expression of cross-correlation function \( R_{nx} (\tau) \) between receiver signals \( r_n(t) \) and \( r_i(t) \) is:

\[
R_{nx}(\tau) = \mathbb{E} [r_n(t-\tau)]
\]
\[
= \mathbb{E} [\alpha_s(t - R_{ini}/c) + \beta_i(t - R_{ini}/c) + \eta_i(t)](\alpha_s(t - R_{ini}/c - \tau) + \beta_i(t - R_{ini}/c - \tau) + \eta_i(t - \tau))] + \beta_i(t - R_{ini}/c - \tau) + \eta_i(t - \tau)]
\]
\[
= \mathbb{E} [\beta_i(t - R_{ini}/c - \tau) + \eta_i(t - \tau)]
\]

In the formula, \( E \{\cdot\} \) represents the mean operation function, \( R_i(\tau) \) represents the autocorrelation function of the target host signal, and \( R_i(\tau) \) represents the autocorrelation function of the interfering host signal. Therefore, when \( \tau = R_{ini} \), \( R_{nx} (\tau) \) has a maximum. The relationship between cross-correlation function and cross power spectrum can be obtained as follows:

\[
R_{nx}(\tau) = \frac{1}{2\pi} \int_{-\pi}^{\pi} G_{nx}(\omega)e^{-j\omega \tau} d\omega
\]

In the formula, \( G_{nx}(\omega) \) represents the cross power spectrum.
The expression of the generalized cross-correlation function of the two receiver signals $r_m(t)$ and $r_n(t)$ is:

$$R_{mn}^e(\tau) = \int_0^\pi \psi_{mn}(\omega)G_{mn}(\omega)e^{-j\omega\tau}d\omega$$

(6)

In the formula, $\psi_{mn}(\omega)$ represents the generalized cross-correlation weighting function. The generalized cross-correlation weighting function $\psi_{mn}(\omega)$ can be weighted in the frequency domain, so as to suppress the interference in the distributed network host and improve the security and stability of the distributed network.

2.2. Distributed network attack source tracking based on interference suppression

Through the above calculation, after the interference suppression of the distributed network is completed, the particle swarm optimization algorithm is used to track the distributed network attack source.

Particle swarm optimization algorithm is a kind of bionic algorithm, which calculates the global optimal solution according to the cooperative predation mechanism between groups by simulating the predation behavior of birds [13-15]. The specific process of distributed network attack source tracking using particle swarm optimization algorithm is as follows.

The search space for defining the global optimal solution is $D$-dimensional space, which contains $m$ particles, and each particle has three constraint vectors, respectively:

(1)Current position of particles: $X_i = (x_{i1}, x_{i2}, ..., x_{im})$;

(2)Historical optimal location: $Y_i = (y_{i1}, y_{i2}, ..., y_{iD})$;

(3)Running speed: $V_i = (v_{i1}, v_{i2}, ..., v_{iD})$.

In the process of searching each particle, the change between the optimal position of a single particle and the optimal position of other particles in the space needs to be considered. Therefore, the expression of particle swarm optimization algorithm can be obtained:

$$v_{id} = wv_{id} + c_1 \cdot \text{rand}() \cdot (y_{id} - x_{id}) + c_2 \cdot \text{rand}() \cdot (v_{id} - x_{id})$$

(7)

$$x_{id} = x_{id-1} + v_{id}$$

(8)

In the above formula, $w$ represents inertia weight, which can balance the global search ability of particle swarm optimization algorithm, $c_1$ and $c_2$ maintain the self-learning ability of particles, and $\text{rand}()$ represents random function.

In the search space, the mapping function of particle velocity is:

$$s(v_{id}) = \frac{1}{1 + \exp(-v_{id})}$$

(9)

The binary expression for particle position update is:

$$x_{id} = \begin{cases} 1 & \text{rand}() \leq s(v_{id}) \\ 0 & \text{otherwise} \end{cases}$$

(10)

The relevant parameters of the particle swarm optimization algorithm calculated above are applied to the distributed network attack source tracking. Through multiple iterations, the attacked host collects a sufficient number of attack marking information packets to track the attack source.

The representation matrix of the marked packet probability in the attacked host is:
The particle swarm optimization algorithm is used to obtain the optimal path of particles through multiple iterations. Therefore, the attack path of the attack source can be constructed to obtain the ideal assignment of the marking probability matrix:

\[ A = \begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 
\end{bmatrix} \quad (11) \]

The calculation process of signal \( r(t) = [r_1(t), r_2(t), ..., r_N(t)]^T \), false attack source data separation and attack source tracking is as follows:

1. The covariance matrix \( C_r = E(r(t) r^H(t)) \) is designed, the eigenvalue of the covariance matrix is decomposed \( C_r = U \Lambda U^H \), and the whitening signal \( z(t) = W r(t) \) is obtained according to the whitening matrix \( W = U \Lambda^{-1} U^H \).

2. Calculate the product matrix \( \{M_1, M_2\} \) of the whitening signal \( z(t) \).

3. The product matrix \( \{M_1, M_2\} \) is approximately joint diagonalized by the unitary matrix \( V \).

4. Separation signal:

\[ y(t) = V^H z(t) \quad (13) \]

The interference signal of the separated signal is obtained through blind source separation, and the other target signal is the superimposed signal under the action of different time delays. The expression is:

\[ y_1(t) \approx s(t-R_{1j1}/c) + s(t-R_{1j2}/c - (R_{j1}/c - R_{j2}/c)) + \cdots + s(t-R_{1jN}/c - (R_{j1}/c - R_{jN}/c)) \]

\[ y_2(t) \approx j(t-R_{1j1}/c) \quad (14) \]

In the formula, \( y_1(t) \) and \( y_2(t) \) separate the estimated value of the signal.

After signal separation, assuming that there are \( N \) attack sources and targets, the tracking results of different attack source signals are obtained:
\[
\hat{s}_1(t) = s(t - R_{1l_1} / c) + s(t - R_{1l_2} / c - (R_{1j_1} / c - R_{j_2} / c)) + \cdots \\
+ s(t - R_{j_2} / c - (R_{j_1} / c - R_{j_2} / c)) \\
\hat{s}_2(t) = s(t - R_{2l_2} / c - (R_{j_2} / c - R_{j_1} / c)) + s(t - R_{1j_2} / c) + \cdots \\
+ s(t - R_{j_2} / c - (R_{j_1} / c - R_{j_2} / c)) \\
\hat{s}_3(t) = s(t - R_{3l_1} / c - (R_{j_2} / c - R_{j_1} / c)) \\
\] (15)

3. Experimental verification

In order to verify the practical application performance of the proposed distributed network attack source tracking method based on interference suppression, simulation and comparative verification experiments are carried out.

In this experiment, the parameters of the distributed network system are: the number of attack sources is 100, the number of source IP ports and destination IP ports are set to 20 respectively, and the number of distributed network packets is 200.

The parameters of the simulation experiment platform are shown in Table 1.

| Table 1. Experimental platform parameters |
|------------------------------------------|
| project                  | parameter               |
|--------------------------|-------------------------|
| Simulation experiment    | Windows platform        |
| Dominant frequency       | 2.13GHz                 |
| Simulation software      | MATLAB 7.0              |
| programing language      | C++, Otcl               |

The overall experimental scheme is set as follows: Taking the attack source tracking accuracy and tracking time as the experimental comparison index, the method in this paper is compared with the methods in reference [5] and reference [6].

Attack source tracking accuracy: attack source tracking accuracy refers to the consistency between the attack source tracking results of different methods and the actual attack source location. The higher the attack source tracking accuracy, the stronger the attack source tracking performance of the method.

Attack source tracking time: attack source tracking time refers to the time consumed by different methods to complete all attack source tracking under the set experimental environment. The shorter the time, the stronger the tracking performance of the method.

3.1. Attack source tracking accuracy

The comparison results of attack source tracking accuracy of the three methods are shown in Figure 1.
Figure 1. Comparison results of attack source tracking accuracy

From the comparison results of attack source tracking accuracy shown in Figure 1, it can be seen that the attack source tracking accuracy of this method will not decrease with the increase of iteration times, but maintain the trend of rising first and then stable, indicating that this method can accurately track attack sources in distributed networks. Although the attack source tracking accuracy of the methods in reference [5] and reference [6] continues to rise, the attack source tracking accuracy of the two traditional methods is always less than 90% until the end of the number of iterations.

3.2. Attack source tracking time consuming

Since malicious attack sources will pose a serious threat to the operation of distributed networks, the time-consuming of attack source tracking has become an important indicator to verify the performance of attack source tracking methods. The shorter the time-consuming of attack source tracking, the higher the tracking effect, which is conducive to ensuring the data transmission quality of distributed networks. The comparison results of attack source tracking time of this method with reference [5] and reference [6] are shown in Figure 2.

Figure 2. Comparison results of attack source tracking time
4. Conclusions

In order to improve the tracking accuracy of distributed network attack sources and reduce the tracking time, a distributed network attack source tracking method based on interference suppression is proposed, and the performance of the method is verified from both theory and experiment. This method has high tracking accuracy and low tracking time when tracking distributed network attack sources. Specifically, compared with the attack source tracking method based on behavior analysis, the tracking accuracy of this method is significantly improved, and the maximum value is 98%; Compared with the attack source tracking method based on knowledge map, the tracking time of this method is greatly reduced, and the maximum tracking time is no more than 3 min. Therefore, it fully shows that the proposed tracking method based on interference suppression can better meet the requirements of distributed network attack source tracking.

5. References

[1] Chang ZP 2018 Simulation of Traceable Marker Method for Controllable Attack Sources in High Speed Network Computer Simulation 35(02) pp 287-290+424
[2] Yuan G and Wen SJ 2020 Design of short time-delay network attack path detection system based on cloud computing architecture Modern Electronics Technique 43(21) pp 72-75
[3] Zhang L and Wang JS 2019 DDoS Attack Detection Model Based on Information Entropy and DNN in SDN Journal of Computer Research and Development 56(05) pp 909-918
[4] Wang T, Wang N, Cui YP and Li H 2020 The Optimization Method of Wireless Network Attacks Detection Based on Semi-Supervised Learning Journal of Computer Research and Development 57(04) pp 791-802
[5] Zhang ZQ, Liu SM and Cao M 2020 Research on DDoS Attack Source Tracking Technology Based on Behavior Analysis Journal of Shanxi Police College 28(01) pp 120-123
[6] Chen J 2020 DDoS Attack Detection Based on Knowledge Graph Journal of Information Security Research 6(01) pp 91-96
[7] Chen J, Ouyang JY and Feng AQ 2020 DoS Anomaly Detection Based on Isolation Forest Algorithm Under Edge Computing Framework Computer Science 47(02) pp 293-299
[8] Wu CX, Ma SL and Shi B 2020 Traceability of network attack based on electronic fingerprint Computer Engineering and Design 41(11) pp 44-49
[9] Wang XR, Zhuang L and Hu Y 2018 DDoS attack detection based on BPNN in software defined networks Application Research of Computers 35(3) pp 911-915
[10] Liu BZ 2018 Virus Tracking Optimization Detection in Network Information Transmission Process Computer Simulation 35(03) pp 123-126
[11] Ma X 2020 A defense algorithm against an active network attack with minimum cost Journal of Harbin Engineering University 41(09) pp 161-166
[12] Di C and Li T 2020 Network Unknown Attack Detection with Deep Learning Computer Engineering and Applications 56(22) pp 115-122
[13] Chen DM 2018 Research on DDoS attack source tracking technology based on packet marking Hunan University 15 pp 543-556
[14] Liu LM, Li QY and Hao CL 2019 Intelligent Tracking Technology for Communication Network Attack Path Based on Abnormal Traffic Visualization Science Technology and Engineering 19(11) pp 235-240
[15] Sun ZW and Zhu Y 2019 Location of Sybil Attack Source under Heterogeneous IWSN Chinese Journal of Sensors and Actuators 32(02) pp 120-126