Modeling of malicious code propagation in the industrial control network

Wei Yang[1,*], *Chao* Liu[2] , *Hongwei* Yan[2] , and *Yu* Yao[2]

[1]Northeastern University, Software College, 110819 Heping District, Shenyang, China
[2]Northeastern University, College of Computer Science and Engineering, 110819 Heping District, Shenyang, China

Abstract. With the development of digitalization, industrial control network have more connections and open to external network, which breaks their "isolation" from Internet and makes them more vulnerable to be attacked especially by malicious code. To model and analyze the impact of different containment strategies for attacks by malicious code in the industrial control network, the SUIQMR model is established to simulate malicious code propagation. Since the industrial control network is often coupled with Internet, industrial control coupling network is also considered in the SUIQMR model and the containment strategies of quarantine,benign worms and honeypot are added into the model to evaluate their effect against malicious code propagation.The simulation results show the effectiveness of our model.

1 Introduction

Industrial Control Network is a comprehensive integrated network applied in the industrial field and is the key information infrastructure for the development of industrial intelligence. The security of industrial control network is related to the country's key infrastructure and economic and social stability, and is an important part of the country's construction and development process[1]. However, in recent years, the frequency of security incidents occurring in industrial control system has been increasing year by year, and the destructive losses caused are also increasing.

The boundary of industrial control network has surpassed the limitation of geographical space and extended to the Internet. Since the industrial control network is often coupled with other external public networks to form a more complex network[2],it breaks their "isolation" from Internet and makes them more vulnerable to be attacked especially by malicious code.

Some researchers have build the malware propagation model to simulate the propagation of malicious code in industrial control network. But facing the coupled industrial control network which is connected to the Internet, those models cannot accurately describe the propagation behavior[3]. Therefore, how to establish a reasonable propagation model to describe the propagation behavior of malware in complex coupled

* Corresponding author: yangw@swc.neu.edu.cn

industrial control networks has become an urgent problem to be solved, which is of great significance to the security of industrial control systems.

The reliability of traditional passive defense methods against network intrusions is greatly reduced[4] and is not feasible to be applied in industrial control network. The containment strategies of quarantine,benign worms and honeypot are be adjusted to fit the industrial control systems and they are also added to the model to evaluate their effect against malicious code propagation.In this paper, the SUIQMR model is established to simulate malicious code propagation under feasible containment strategies in industrial control network.

2 Related works

As a proactive security protection technology, intrusion detection provides real-time protection against internal attacks, external attacks and misoperation. It can intercept and respond to intrusions before the network system is compromised. It is still a good way to protect industrial control network. Zhu Q etc. uses a dual intrusion detection method to detect malware attacks in industrial control coupling networks[5].Quarantine is another method to protect susceptible hosts. Once a susceptible hosts is found, it is quarantined to install patches or antivirus to make them immune to malicious code[6]. Benign worms is also a active defense technology. Through the mutual confrontation between benign worms and malware, the spread of malware can be effectively suppressed[7].

A honeypot is a specially designed trapping tool to attract potential attackers[8]. It lures attackers to attack by impersonating one or more services or devices. Its advantage is that it can capture and analyze attack behavior. The defense of honeypot can clearly understand the security threats we're facing, and enhance the security protection capabilities of the actual system through technical and management means.Therefore, this paper applies quarantine, benign worms and honeypot technology to protect the industrial control equipment in the industrial control networks, thereby inhibiting the spread of malware in the industrial control network.

3 Modeling of malicious code propagation

3.1 SUIQMR propagation model

This paper proposes a malware suppression strategy-based SUIQMR propagation model to analyze the propagation behavior of malware in industrial control coupling networks. At the beginning, the hosts are Susceptible hosts represented as S states,S_A represents the Susceptible hosts in Internet,S_B represents the Susceptible hosts in Industrial Control Network. If the susceptible host is infected, the state of the host will transfer to I states,I_A represents the Susceptible hosts in Internet,I_B represents the Susceptible hosts in Industrial Control Network. As we know,in Internet there will exist benign worms, the state of the host with benign worm will turn into U_A state.

Once an infected host in Internet is found, the intrusion detection system will immediately take measures such as powering off the host to isolate it, thus effectively preventing it from continuing to infect other hosts and industrial control equipment. So the infected host in Internet will transfer its state to Q state which means the host is quarantined. However, this isolation method is not suitable for industrial control network, because isolation will cause the equipment to stop running, which will affect the normal operation of the industrial production process. Therefore, this paper proposes a whitelist-based filtering method for filtering port traffic of industrial control equipment, which produces an

effect similar to isolation.The infected host in Industrial Control Network will transfer its state to M state.

At the same time, the honeypot device is used to protect the industrial control device, and the honeypot device is disguised as a real industrial control device. When a host in Industrial Control Network is infected, the honeypot device can replace the protected industrial control device and be infected, so that the industrial control device node is "fake infection" to deceive malware attacks and thus achieve the effect of suppressing its spread. The state of the host will transfer to the state of U_B state. The host no matter in Internet or in Industrial Control Network in R state means it has been patched and the malicious code has been removed.The model state transition diagram is shown in Fig.1.

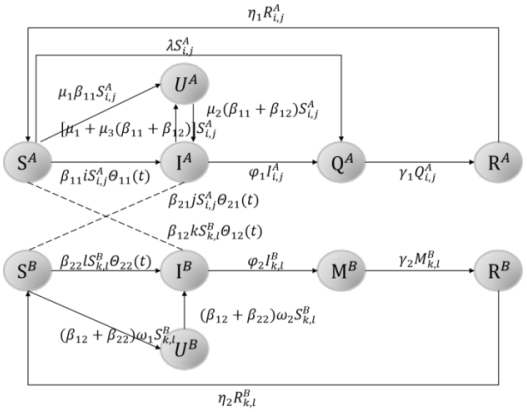

Fig. 1. State transition diagram of SUIQMR model.

The state transition process of the model is expressed as a mathematical formula, and the differential equation expression of the SUIQMR model is obtained:

$$
\begin{cases}
\frac{dS^A_{i,j}(t)}{dt} = -\beta_{11}iS^A_{i,j}(t)\Theta_{11}(t) - \beta_{12}jS^A_{i,j}(t)\Theta_{12}(t) - \mu_i iS^A_{i,j}(t)\Theta_{13}(t) - \lambda S^A_{i,j}(t) + \eta_1 R^A_{i,j}(t) \\
\frac{dU^A_{i,j}(t)}{dt} = \mu_i iS^A_{i,j}(t)\Theta_{13}(t) - \mu_2(\beta_{11}+\beta_{12})iI^A_{i,j}(t)\Theta_{13}(t) + [\mu_1+\mu_3(\beta_{11}+\beta_{12})]\mathrm{i}U^A_{i,j}(t)\Theta_{11}(t) \\
\frac{dI^A_{i,j}(t)}{dt} = \beta_{11}iS^A_{i,j}(t)\Theta_{11}(t) + \beta_{12}jS^A_{i,j}(t)\Theta_{12}(t) - [\mu_1+\mu_3(\beta_{11}+\beta_{12})]\mathrm{i}U^A_{i,j}(t)\Theta_{11}(t) + \mu_2(\beta_{11}+\beta_{12})iI^A_{i,j}(t)\Theta_{13}(t) - \varphi_1 I^A_{i,j}(t) \\
\frac{dQ^A_{i,j}(t)}{dt} = \lambda S^A_{i,j}(t) + \varphi_1 I^A_{i,j}(t) - \gamma_1 Q^A_{i,j}(t) \\
\frac{dR^A_{i,j}(t)}{dt} = \gamma_1 Q^A_{i,j}(t) - \eta_1 R^A_{i,j}(t) \\
\frac{dS^B_{k,l}(t)}{dt} = -\beta_{21}kS^B_{k,l}(t)\Theta_{21}(t) - \beta_{22}lS^B_{k,l}(t)\Theta_{22}(t) - (\beta_{21}+\beta_{22})\omega_1 S^B_{k,l}(t) + \eta_2 R^B_{k,l}(t) \\
\frac{dU^B_{k,l}(t)}{dt} = (\beta_{21}+\beta_{22})\omega_1 S^B_{k,l}(t) - (\beta_{21}+\beta_{22})\omega_2 U^B_{k,l}(t) \\
\frac{dI^B_{k,l}(t)}{dt} = \beta_{21}kS^B_{k,l}(t)\Theta_{21}(t) + \beta_{22}lS^B_{k,l}(t)\Theta_{22}(t) + (\beta_{21}+\beta_{22})\omega_2 U^B_{k,l}(t) - \varphi_2 I^B_{k,l}(t) \\
\frac{dM^B_{k,l}(t)}{dt} = \varphi_2 I^B_{k,l}(t) - \gamma_2 M^B_{k,l}(t) \\
\frac{dR^B_{k,l}(t)}{dt} = \gamma_2 M^B_{k,l}(t) - \eta_2 R^B_{k,l}(t)
\end{cases}
\tag{1}
$$

3.2 Existence of disease-free equilibrium

When the whole system reaches the state of disease-free equilibrium point, the number of infected hosts in Internet and infected devices in industrial control Network is 0, and the disease-free equilibrium point of the SUIQMR model is solved. The disease-free equilibrium point of the model obtained from the solution is as follows.

$$
E^0\left(S^{A^0}_{i,j}, U^{A^0}_{i,j}, I^{A^0}_{i,j}, Q^{A^0}_{i,j}, R^{A^0}_{i,j}, S^{B^0}_{k,l}, U^{B^0}_{k,l}, I^{B^0}_{k,l}, M^{B^0}_{k,l}, R^{B^0}_{k,l}\right) \tag{2}
$$

In equation (2), the following parameters has the following values representing in equation (3).

$$U_{i,j}^{A^0}=0,\ I_{i,j}^{A^0}=0,\ \mathrm{S}_{i,j}^{A^0}:Q_{i,j}^{A^0}:R_{i,j}^{A^0}=1:\frac{\lambda}{\gamma_1}:\frac{\lambda}{\eta_1}$$
$$\mathrm{S}_{\mathrm{k,l}}^{B^0}=N_{k,l}^{B},U_{\mathrm{k,l}}^{B^0}=0,I_{\mathrm{k,l}}^{B^0}=0,M_{\mathrm{k,l}}^{B^0}=0,R_{\mathrm{k,l}}^{B^0}=0, \tag{3}$$

3.3 Stability of the disease-free equilibrium point

Let $f=(f_1,f_2,\cdots,f_n)$ represent the change function of the infected population in the network, let $x=(x_1,x_2,\Lambda,x_n)$, Therefore, the rate of change of the infected population is $\frac{dx(t)}{dt}=f(x(t))$ Obviously, there exists a disease-free equilibrium satisfying E^0 ,satisfying $x_i=0$ in $i=1,2,...,n$ .According to the article[9], The basic reproduction number can be obtained from the characteristic spectrum of the reproduction matrix $\mathbf{r}$, $R_0=\rho(\mathbf{\Gamma})$ According to the method[10] used in the article, the calculation formula of the regeneration matrix is: $\mathbf{\Gamma}=\mathbf{F}\mathbf{V}^{-1}$ .The regeneration matrix $\mathbf{r}$ is expressed as follows.

$$\mathbf{\Gamma}=\begin{bmatrix}\frac{\beta_{11}<k^2>_{11}}{\varphi_1<k>_{11}} & \frac{\beta_{11}}{\varphi_1}<k>_{12} & 0 & 0\\ 0 & 0 & \frac{\beta_{21}<k^2>_{21}}{\varphi_2<k>_{21}} & \frac{\beta_{21}}{\varphi_2}<k>_{22}\\ \frac{\beta_{12}}{\varphi_1}<k>_{11} & \frac{\beta_{12}<k^2>_{12}}{\varphi_1<k>_{12}} & 0 & 0\\ 0 & 0 & \frac{\beta_{21}}{\varphi_2}<k>_{21} & \frac{\beta_{22}<k^2>_{22}}{\varphi_2<k>_{22}}\end{bmatrix} \tag{3}$$

Solving the eigenvalues of the regeneration matrix $\mathbf{r}$, the four eigenvalues of the malware regeneration matrix $\mathbf{r}$ are obtained as:

$$\xi_{1,2}=\frac{1\pm\sqrt{1-4C_1}}{2}-\frac{p_3}{4},\quad \xi_{1,2}^{'}=\frac{-1\pm\sqrt{1-4C_2}}{2}-\frac{p_3}{4} \tag{4}$$

The basic reproduction number R_0 is as follows.

$$R_0=\max\{|\lambda_i|\quad i=1,\cdots,4\}=\max\{|\xi_1|,|\xi'|\} \tag{5}$$

4 Simulation experiments

The experiment is based on the case of Wannacry ransomware to fit the propagation hyper-parameters, which is more realistic and instructive. The hyper-parameters is set to make R_0<1. The propagation trendency of hosts in Internet is shown in Fig.2.

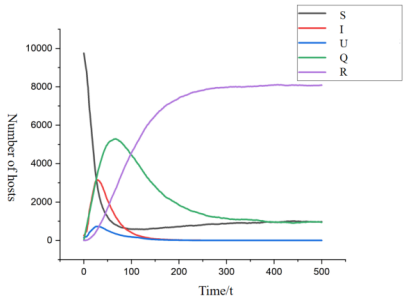

Fig. 2. Propagation trendency of hosts in Internet.

The propagation trendency of hosts in Industrial Control Network is shown in Fig.3. At the beginning, due to the rapid spread of malware, the number of infected hosts in Internet and in industrial network increased rapidly, and reaches its peak and then, due to the effectiveness of the malware suppression strategy, the number of infected hosts decreased rapidly, and finally the number decreased to 0 and the whole system reached a disease-free equilibrium state and a balanced state.

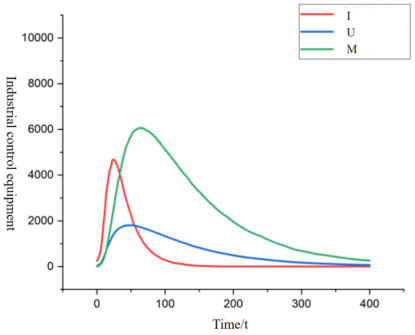

Fig. 3. Propagation trendency of hosts in industrial Control Network.

5 Conclusion

In this paper, the SUIQMR model is established, and the dynamics of the model are analyzed theoretically, and the disease-free equilibrium point of the model is obtained. Then, the basic reproducible number R_0 of the SUIQMR model is solved. When $R_0<1$, the model can reach a disease-free equilibrium state and remain stable; when $R_0>1$, the disease-free equilibrium point is unstable. Finally, the simulation experiment verifies the correctness of the theoretical analysis of the SUIQMR model and the effectiveness of the malware suppression strategy.

This work was supported by National Key R&D Program of China NO.2021YFB3101700.

References

1. dLe D T, Dang K Q, Nguyen Q L T, et al, Electronics, 10(19): 2403(2021).
2. Ojha R P, Srivastava P K, Sanyal G, et al, Wireless Personal Communications, 116: 2525-2548(2021).

3. Masood Z, Majeed K, Samar R, et al, Fundamenta Informaticae, 161(3): 249-273(2018).
4. Masood Z, Raja M A Z, Chaudhary N I, et al, Mathematics, 9(17): 2160(2021).
5. Zhu Q, Zhang G, Luo X, et al, Information Sciences, 630: 546-566(2023).
6. Pan Jie, Ye Lan, Zhao He, Zhang Xinlei, Journal of Network and Information Security, 8(03):169-175(2022).
7. Li Yan, Zhang Hongyu, Control Engineering, 27(09):1603-1607(2020)
8. Franco J, Aris A, Canberk B, et al, IEEE Communications Surveys & Tutorials, 23(4): 2351-2383(2021).
9. Wang Ruiling, Xue Yakui, Journal of Central China Normal University (Natural Science Edition):1-9(2023).
10. Yu Z, Gao H, Wang D, et al, Physica A: Statistical Mechanics and its Applications, 597: 127207(2022).