*Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023)*
*Edited by* Mário P. Brito, Terje Aven, Piero Baraldi, Marko Čepin and Enrico Zio
 *Published by* Research Publishing, Singapore.
doi: 10.3850/978-981-18-8071-1_P267-cd

# Propagation Process of Information Physical Attack in Oil and Gas Intelligent Pipeline System Based on SEIRS

Yuhuan Li

*College of Safety and Ocean Engineering, China University of Petroleum (Beijing), China. Key Laboratory of Oil and Gas Safety and Emergency Technology, Ministry of Emergency Management, China. E-mail: liyuhuan20212021@163.com*

Jinqiu Hu*

*College of Safety and Ocean Engineering, China University of Petroleum (Beijing), China. Key Laboratory of Oil and Gas Safety and Emergency Technology, Ministry of Emergency Management, China. E-mail: hujq@cup.edu.cn,(corresponding author)*

Laibin Zhang

*College of Safety and Ocean Engineering, China University of Petroleum (Beijing), China. Key Laboratory of Oil and Gas Safety and Emergency Technology, Ministry of Emergency Management, China. E-mail: cupanquan@163.com*

The normal operation of oil and gas intelligent pipeline systems depends on the coordination of sensor and control components. Incorrect sensor data and logic errors of control components will lead to an incorrect response of the system. However, the impact of an attack on a system varies depending on the importance of a component, and the attacker usually does not attack only once. To study the propagation mechanism of information physical attack in the oil and gas intelligent pipeline system and improve the security of the system, the SEIRS model of the components in the oil and gas intelligent pipeline system is constructed by using the propagation dynamics method, and the security of the system is analyzed from two aspects: attack detection and attack defense. Firstly, the SEIRS model is constructed for the components with attack detection and attack defense in the system to describe the propagation process of the attack in the system. Secondly, the numerical simulation of the model is realized by setting the time and initial parameters of the attack in Matlab. Finally, the system security under different parameters is studied.

*Keywords*: .Oil and Gas Smart Pipeline System;Information Physical Security;SEIRS model; Attack propagation.

## 1. Introduction

With the development of information technology, the intelligent pipeline system composed of the network layer, information layer, and physical layer faces new risks. The oil and gas intelligent pipeline system consists of a variety of sensors and control components, and the normal operation of the system depends on the coordination of sensor components and control components. Sensor data is used to analyze and monitor the situation of the intelligent pipeline field area. Incorrect sensor data may mislead the terminal to provide wrong control information, so incorrect sensor data and logic errors of control components. This will result in an incorrect response from the system.

The attack on the information layer of the industrial control system often has strong concealment. Once an attack spreads from the information layer to the physical layer, it can wreak havoc on the production process(Bologna et al. 2013). Secondly, the importance of components varies, and the impact on the system after being attacked is different, and the attacker

usually does not attack only once. Therefore, it is particularly important to explore the transmission process of information through physical attack between components.

By analyzing the typical information physical architecture of ICS, The literature proposed to construct a fault propagation model based on the probability of failure occurrence, matrix transformation, construct attack graph and evaluate the faulted edge of system vulnerability(Xia et al. 2023). The literature proposed a fault propagation model based on the influence of network partial node interruption on the electrical physical system. The propagation diagram and attack diagram are constructed to reveal the propagation mechanism of physical faults, and the attack strength of different communication node combinations is analyzed(Zang et al.2019). The literature proposed a new method for assessing the direct and indirect effects of attacks on network physical systems (CPS). This method studies the dynamic behavior of the system under normal conditions and security attacks and evaluates the propagation of the consequences of attacks(Orojloo et al.2017). The literature took multimodal transport networks as the research object and proposed a quantitative method of risk propagation based on improved seepage theory(Guo et al.2021). The literature established the attack-defense game model and malware propagation model of WSN( Zhou et al.2020 ).

The literature proposed a Susceptible – Exposed – Infected1 – Infected2 – Removed (SEI2RS) model with different infection rates to study malware propagation in CPSs(Yu et al. 2022). The literature proposed a compartmental model called SIIDR that accurately captures the behavior observed in real-world attack traces. (Chernikova et al. 2022).In this paper, a susceptibility - Exposure - Infection - Recovery - susceptibility (SEIRS) epidemic model is proposed to dynamically study the spreading behavior of malware in scale-free networks (SFNs)(Hosseini et al.2014).In this paper, a time-delay SIRS model is proposed to predict the dynamic behavior of mali malware propagation(Feng et al. 2013).

The above methods do not consider the importance of components in the system and give equal attack probability to each component. However, in the practical industrial field, such as oil and gas intelligent pipeline systems, the possibility of attacking critical equipment components is much higher, especially the key components that can have a significant impact on the physical layer. Therefore, from the perspective of infectious disease prevention and control, this paper proposes an information physical attack propagation model based on SEIRS, aiming at exploring the transmission process of information physical attack among key components of the oil and gas intelligent pipeline system, to determine the state of the system and analyze the security of the oil and gas intelligent pipeline system.

## 2. SEIRS

The mathematical model of the "transmission process of infectious diseases" is implemented by controlling vulnerable populations. Because infectious disease has an important significance to studying new cases, the use of mathematical knowledge with practical problems, to make the corresponding brief answer and treatment. The transmission process of a disease is a very complex process, which is subject to many social factors, such as the number of infected people, the number of vulnerable infected people, the birth and death rates of the population, the length of the incubation period, the prevention of disease publicity and individual differences. To establish a mathematical model, obviously, not all factors can be taken into account, so we should grasp the main factors, remove the secondary factors, simplify the problem, and establish the corresponding mathematical model.

The basic mathematical model of infectious diseases studies the transmission speed, spatial range, transmission path, and dynamic mechanism of infectious diseases, to guide the effective prevention and control of infectious diseases(Grassly et al.2008). The common infectious disease models are divided into SI, SIR, SIRS, SEIR models, etc., according to the infectious disease types, and are further divided into different types based on the ordinary differential equation, partial differential equation, and network dynamics according to the transmission mechanism(Andrei et al.2007).SI, SIR, SIRS, and SEIR describe the transmission process of infectious diseases, analyze the changing rules of the number of susceptible

people, latent people, infected people, recovered people, etc., forecast the moment of the climax of infectious diseases, and establish the mathematical model of the impact of infectious diseases on healthy people in the process of infectious diseases.

The SEIR model is one of the common infectious disease models. SEIR model assumes that the population can be divided into four types of hy photic tables: SUSCEPTIBLES and potential susceptibles; EXPOSED: A person who has been infected but does not show it; Ie ves: those who are infected, those who show symptoms of an infection; RESISTANCES: People who get resistance after an infected person recovers.

SEIR models the flow of people between four states: susceptible (S), latent (E), infected (I), and recovered (R). Vulnerable people undergo an incubation period at first, with symptoms appearing after some time; Susceptible persons can be infected by latent and infected persons; Those who are dormant develop symptoms and become infected; The infected are cured and become rehabilitated.

SEIRS still models the flow of people between four states: susceptible (S), latent (E), infected (I), and recovered (R). Compared with the SEIR model, the SEIRS model increased the case fatality rate of infected persons, that is, the probability of infected persons dying from infectious diseases, excluding the probability of natural death among infected persons.

## 3. Build the System SEIRS Model

### 3.1. *Feasibility analysis of the model*

The operation of oil and gas intelligent pipeline systems depends on the interaction of sensing and control components. The network structure is formed between the vertical network layer, the information layer, the physical layer, and the horizontal components of each layer. An attack spreads through a system, as a virus spreads through a population, at random, especially among highly correlated components; Detection and defense between components, as symptoms of a virus and whether it can heal itself. Therefore, it is feasible to study the spread of attacks in especially intelligent pipeline systems by establishing an epidemic transmission dynamics equation.

### *3.2.Model construction*

1. Determine component attributes

The key components (including attack detection and defense functions) are divided into four categories: vulnerable components (s), which are vulnerable to attacks; latent components (e), which are attacked but have not detected attack data; infected components (i), which are attacked and have detected attack components; and rehabilitated components (r), which are successfully defended.

2. Determine component relationships

Susceptible elements may be attacked but not detected and turn into latent elements; An infected component detects an attack and is converted to an infected component. An infected component detects an attack and defends against it. If successful, it is converted to a rehabilitated component. The rehabilitative element becomes susceptible again after successful defense. Recovery components are attacked, and even if the defense is successful, some components will be attacked again and turn into dormant components. The components of an oil and gas smart pipeline system do not change, so the model assumes a constant total number of components.

3. Determine the transmission process

Assume that the element is attacked with probability a, the attack is detected with probability b, and the defense succeeds with probability c. The probability that the element will be attacked again is d. The probability that the rehabilitative element becomes susceptible again is e. The propagation process of the model is shown in Figure 1.

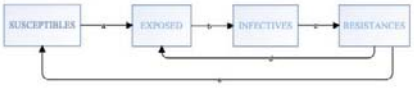



Fig.1 Model flow chart

According to the above propagation process, differential equations are established as follows:

$$\frac{dS(t)}{dt} = -aS + eR$$
$$\frac{dE(t)}{dt} = aS + dR - bE$$
$$\frac{dI(t)}{dt} = bE - cI$$
$$\frac{dR(t)}{dt} = cI - dR - eR$$

S(t), E(t), I(t), R(t) are the numbers of susceptible components, latent components, infected components, rehabilitative components and critical components at time t, respectively; S(t), E(t), I(t), R(t) are continuously differentiable functions of t with range of [0,1], and the value ranges of a, b, c, and d are all [0,1].

## 4. System Simulation of Attack Propagation

Based on Matlab numerical simulation analysis of the number of four types of components. Assume that the number of key elements is 1000 and the time is 1 minute. Judge the changes in the number of components within 20 minutes to explore the safety of the oil and gas intelligent pipeline system. Through the investigation of the oil and gas intelligent pipeline system, the model parameters are initialized as the probability a of the element being attacked is 0.5, the probability b of the element detecting the attack is 0.9, and the probability c of successfully defending the element is 0.7. Because there are attack defense data in the database after the successful defense of the element, the probability of being attacked again decreases. The probability d that the component will be attacked again is 0.4, and the probability e that the component will become susceptible again after successful defense is 0.6. It is assumed that the system is initially in a secure state, with no attacked components. The simulation results are shown in Figure 2.

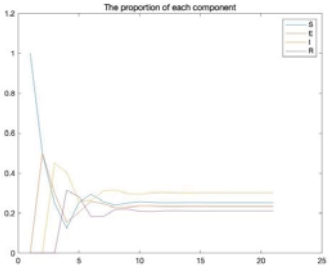



Fig. 2 Component ratio diagram

According to the simulation results, the susceptible element dropped rapidly in the first 3 minutes, the latent element, the infected element, In the first 3 minutes of rapid rise, no recovery element, this is due to the susceptible element to the rapid transformation of other; For three to 15 minutes, the four components oscillate and transform into each other; After 15 minutes, the ratio of the four components leveled off and the system reached a stable state. To better explore the overall security of the system, the key components are divided into unsafe components and security components, latent components under attack but not detected, there are security risks, classified as unsafe components, infected components belong to unsafe components, susceptible components and rehabilitation components belong to safety components. The results of the proportion of the two components in the key components are shown in Figure 3.

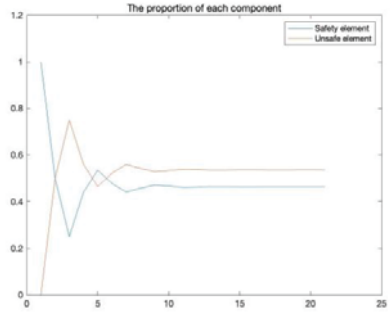
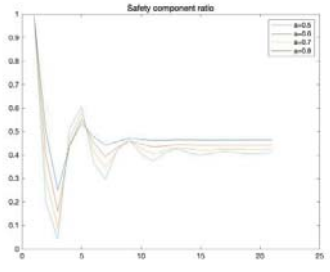



Fig.3 Ratio of safe components to unsafe components

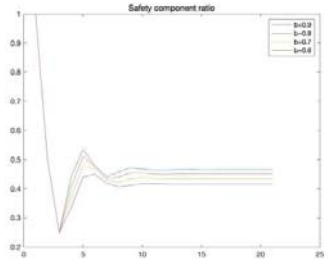
## 5. System Security Analysis

For the model, the variable parameters are probability a that the component is attacked, probability b that the attack is detected, and probability c that the defense is successful. The probability d that the component will be attacked again. Probability e that the rehabilitative element becomes susceptible again. Therefore, the security of the system is measured from the attack probability, detection success rate, and defense success rate. Since physical information attacks break through the network layer, the attack probability of the information layer reflects the defense performance of the network layer. By changing the attack probability, the

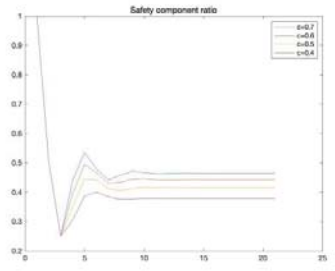
proportion of security components in key components is studied. As shown in Figure 4(a), the higher the attack probability, the weaker the network layer defense, the lower the system security, the higher the attack probability, the more time it takes for the system to stabilize, and the greater the system security fluctuation. By changing the detection success rate, the proportion of safety components in key components is studied, as shown in Figure 4(b). The higher the detection success rate is. The higher the system security is, the detection success rate is not sensitive to time, and the system security fluctuation is not obvious. By changing the defense success rate, the proportion of security components in key components is studied. As shown in Figure 4(c), the higher the defense success rate is. The higher the system security is, the defense success rate is not sensitive to time, and the system security fluctuation is not obvious.




(a)




(b)




(c)

Fig.4 Proportion of safety components under different parameters

## 6. Conclusions

This paper constructs an information physical attack model based on SEIRS to describe the transmission process of information physical attack among key components of oil and gas intelligent pipeline systems. Through Matlab simulation, it is concluded that the security of the system fluctuates in the first 9 minutes. The security intervention of the system and timely security measures within the time can better improve the security of the system. By changing different parameters, it is concluded that the attack probability is sensitive to time. Therefore, the defense of the network layer should be timely. The success rate of detection and defense is almost the same as system security. Therefore, detection and defense are equally important, but both are not sensitive to time. Therefore, the probability of success of detection and defense can be improved by sacrificing the time of detection and defense.

**Acknowledgment**

This work was supported by the Natural Science Foundation of China (52074323).

**References**

Bologna S, Fasani A,Martellini M. (2013). Cyber Security and Resilience of Industrial Control Systems and Critical Infrastructures. In: Martellini,M.(eds)Cyber Security. SpringerBriefs in Computer Science.

Xia Weifu, Wang Yanhui, Hao Yucheng(2023) . Modeling failure propagation to analyze the

vulnerability of the complex electromechanical systems under network attacks[J]. Physica A: Statistical Mechanics and its Applications, 2023, 613: 128514.

Zang Tianlei, Gao Shibin, Liu Baoxu, et al(2019). Integrated fault propagation model based vulnerability assessment of the electrical cyber-physical system under cyber attacks[J]. Reliability Engineering & System Safety, 2019, 189: 232-241.

Orojloo H, Azgomi M A(2017). A method for evaluating the consequence propagation of security attacks in cyber–physical systems[J]. Future Generation Computer Systems, 2017, 67: 57-71.

Guo Jingni, Xu Junxiang, He Zhenggang, et al(2021). Research on risk propagation method of multimodal transport network under uncertainty[J]. Physica A: Statistical Mechanics and its Applications, 2021, 563: 125494.

Zhou Haiping, Shen Shigen, Liu Jiajia(2020). Malware propagation model in wireless sensor networks under attack–defense confrontation[J]. Computer Communications, 2020, 162: 51-58.

Yu Zhenhua,Gao Hongxia ,Wang Dan,et al(2022). SEI2RS malware propagation model considering two infection rates in cyber-physical systems. [J]. Physica A: Statistical Mechanics and its Applications, 2022, 5C97: 127207.

Chernikova A, Gozzi N, Boboila S, et al. (2022). Cyber network resilience against self-propagating malware attacks. In: Computer Security-ESORICS 2022: 27th European Symposium on Research in Computer Security, Copenhagen, Denmark, September 26-30, 2022, Proceedings, Part I. Cham: Springer International Publishing, 2022, 531-550.

Hosseini S, Azgomi M A, Rahmani A T. (2014). On the global dynamics of an SEIRS epidemic model of malware propagation. In: 7th International Symposium on Telecommunications (IST'2014). IEEE, 2014, 646-651.

Feng Liping, Liao Xiaofeng, Han Qi,et al. (2013). Dynamical analysis and control strategies on malware propagation model. Applied Mathematical Modelling, 2013, 37(16-17): 8225-8236.

Grassly N, Fraser C(2008). Mathematical models of infectious disease transmission. Nat Rev Microbiol 6, 477–487 (2008).

Andrei Korobeinikov(2007). Global Properties of Infectious Disease Models with Nonlinear Incidence. Bull. Math. Biol. 69, 1871–1886.