IMPACT: International Journal of Research in Engineering & Technology
ISSN(P): 2347–4599; ISSN(E): 2321–8843
Vol. 8, Issue 3, Mar 2020, 1–8
© Impact Journals

RESEARCH ON CYBER SECURITY RISK MANAGEMENT

Zhang Jingshi

Research Scholar, Department of Management Science and Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing, China

Received: 26 Feb 2020 **Accepted:** 07 Mar 2020 **Published:** 31 Mar 2020

ABSTRACT

In the current age of globalism, the issue of cyber security is increasingly prominent. Hacker attacks, virus outbreaks and other hidden dangers seriously harm the network system. Cyber security risk has become one of the most important risks facing contemporary society. The management of cyber security risk is an important guarantee for the healthy development of network information technology. From the perspective of network system, this paper reviews the research status of epidemic threshold, risk propagation model and immune strategy, and introduces some research results and methods in the field of cyber security risk management.

KEYWORDS: *Cyber Security; Epidemic Threshold; Risk Propagation; Management*

INTRODUCTION

At present, computer and network technology is widely used in various industries and fields, greatly promoting the development of national economy. With the continuous progress of science and technology, the development of computer network has become more and more mature and perfect. Due to the openness, sharing and complexity of the computer network, it has not only brought many conveniences to people's life, work and study, but also brought severe challenges to network security. In recent years, there have been a number of major cyber security incidents, such as the Stuxnet virus that attacked an Iranian nuclear power plant in 2010 and the Wanna Cry virus in 2017. Cyber security risk has become one of the most important risks facing contemporary society. Therefore, how to effectively manage cyber security risks has become one of the most urgent problems faced by all kinds of network users, including individuals, enterprises and governments.

CYBER SECURITY RISK MANAGEMENT

Cyber security risk management is a system engineering that contains multiple links, including the research and management of risk sources, epidemic threshold, transmission process and other links.

The early definition of risk mainly refers to the probability of the occurrence of uncertainty between the investment purpose and the expected return, which can be divided into two categories: narrow sense risk and broad sense risk. Narrow sense risk mainly refers to the uncertainty of loss. Broad sense risk includes both uncertain attribute of loss and gain. The cyber security risk with the nature of propagation belongs to the narrow sense risk.

Cyber security risk can be defined as all risks related to network information including virtual reality, such as malicious attacks, data theft, service interruption, etc. There are significant differences between cyber security risks and traditional risks (auto insurance). Cyber security risk is systematic and global. Among them, the characteristic of systematizes and correlation of cyber security risk is particularly important. These characteristics are the key and difficult points of cyber security risk management. Although there is no strict definition of systemic risk in the literature, it is generally believed that this kind risk starts from a trigger event and then causes a series of adverse subsequent reactions, which is also commonly referred to as the domino effect. Therefore, the concept of systemic risk can be understood as the chain reaction of the initial attack, while the chain reaction is usually interpreted as the consequence of the spread or contagion of risk [ ]. In this way, the spread of risk in the network has become the key to the study of cyber security risk management.

The components of risk propagation in network include risk source, transmission node, transmission medium and so on. Risks may originate from inside or outside the network, thus forming endogenous and exogenous risks. All nodes in the network have the capability of risk propagation. When the risk breaks through the propagation threshold and is combined with the specific network structure, a specific risk propagation network is formed accordingly. In order to evaluate and reduce the destructiveness of network risk, it is necessary to study the transmission process of risk. After mastering the law of risk propagation, certain methods can be used to intervene and avoid risks, so as to achieve "immunity" to the network system and achieve the effect of cyber security risk management.

In the field of systematic risk transmission, since the carrier nodes of risk propagaton are often connected to form a network, researchers on risk problems tend to combine system theory and network theory with risk problems to overcome the limitation of calculation conditions and make the analysis results more widely applicable.

THE EPIDEMIC THRESHOLD

The problem of epidemic threshold is the focus of network risk propagation. Researchers hope to clearly understand the characteristics of network structure related to virus outbreak, so as to adopt effective strategies to suppress virus propagation. Hethcote proposed concepts related to the basic regeneration number R0 and viral transmission threshold. For the first time, Wang et al. built a discrete time SIS virus propagation model under the general network topology. Under this model, the author mainly discusses the threshold of virus outbreak in network, and establishes the threshold of virus outbreak based on the spectral radius of adjacency matrix and effective infection rate, which provides a theoretical basis for the phase transition phenomenon of virus behavior in network. Chakrabarti et al. proposed the precise expression of the epidemic threshold, that is, the virus transmission threshold is equal to the reciprocal of the maximum eigen value of the network adjacency matrix. At the same time, they point out, when transmission rates fall below the threshold, the virus dies at an exponential rate. Ganesh et al. extended Wang's work to the continuous time case and established a continuous time Markov virus propagation model. In the continuous time model, the concept of virus outbreak threshold is strictly defined, and the threshold is successfully obtained by means of probabilistic coupling. Draief et al. further studied that in the SIR model, if the ratio of cure rate to infection rate is greater than the spectral radius of the figure, and the number of initial infection nodes is small, the final infection scale is also small. If the ratio is less than the spectral radius, the final infection scale is larger in some specific graph structures.

The epidemic threshold is not only related to the level of infection but also closely related to the network structure. The topological characteristics of different networks have different effects on risk propagation. Risk propagation threshold exists in regular network and random network. In scale-free network, no obvious propagation threshold can be found, and the risk propagation threshold of scale-free network of limited size will decrease to zero with the increase of network scale [ ]. In a small-world network, the spread of network risk is easier and faster than in a regular network. Based on the discrete Markov SIS model, Kocarev et al. divided the transmission process of virus into reaction process and contact process and gave the upper and lower bounds of node infection probability. The dependence of propagation process on network topology is evaluated according to the difference of bound. It is found that the size of node infection probability boundary is related to the average degree of node.

In addition, the community structure in the network also has an impact on the epidemic threshold. Liu et al. found that the community structure in the network has a great influence on risk propagation. The threshold of risk propagation will be reduced due to the existence of network communities and further reduce the ultimate scale of virus transmission. Salathé et al. finds that the propagation rate of network risk increases in community structure networks due to the decrease of propagation threshold. The infection density of the node is stable at a fixed equilibrium point or presents periodic and unstable oscillations [ ]. Some other scholars have studied the transmission dynamics on scale-free networks based on different viral transmission models, such as SEAIR model and SIR model considering the randomness of transmission process.

RISK PROPAGATION MODEL

Propagation Model Based on Stochastic Process

There are abundant researches on network risk propagation in the literature, which involve many different fields and theoretical methods. Virus propagation model based on stochastic process theory and its extension are important risk propagation models. Such models played an important role in early human understanding and response to infectious diseases and laid the foundation for the study of viral propagation. The transmission of epidemic diseases is closely related to the network and to some extent similar to the transmission characteristics of computer viruses. Therefore, the following studies on network risk propagation mainly focus on viruses.

Pastor-Satorras et al. has done a lot of pioneering work in this area. They started with the simplest form of SI model, and then some improved models appeared successively, including SIR model, SIS model, SIRS model, SEIR model and so on. These models mainly describe the behavior of a virus that continues to spread (erupt) or disappear over the network.

There are some related extended models including inhomogeneous models of infection rate and recovery rate, dynamic network structure models, dependent virus transmission models and so on. Xu et al. described the interdependence of network attack events by introducing the copula theory into the virus propagation model and gave the corresponding equilibrium threshold and the bounds of equilibrium infection probability and non-equilibrium infection probability. Boguna et al. proposed an algorithm for non-Markov discrete stochastic processes and gave precise analytical solutions. The influence of time distribution of non-exponential events in the SIS model under the condition of virus attack event independence and dependence is studied by this algorithm. Da et al. proposed a viral propagation model that could describe coordinated attacks with different infection probabilities. The upper bound of infection probability is given when the network system enters the equilibrium state.

Propagation Model Based on Probability Model

Another important network risk propagation model is a static risk propagation probability model developed based on the propagation model first proposed by Kunreuther and Heal. In this model, it is assumed that the network faces two types of attacks direct attack and indirect attack. Direct attack is an attack that a network node obtains from outside the network. Indirect attack is an attack caused by successful external attacks propagating among network nodes.

Kunreuther and Heal first proposed such models in the context of optimal strategy development for cyber security investments. They assume that each node has a probability of being directly attacked. The node that is successfully (directly) attacked will attack its neighbor (indirectly) with some probability, but the node that is successfully indirectly attacked will not attack its neighbor again. That means indirect attacks are no longer contagious. This model is called the one-hop model. Subsequently, the one-hop model has been further extended by many scholars, such as the one-hop model considering the specific distribution of attack probability and the one-hop model considering the strategic attack.

Lelarge, Bolot, Laszka et al. extended the one-hop model, called the multiple-hop model, by assuming the existence of sustained infectivity of indirect attacks under different research backgrounds. For this model, Lelarge and Bolot used the average field method commonly used in statistical physics to conduct approximate analysis on the model, and analyzed network security risk strategies such as network security technology and network security insurance application effect. Laszka et al. considered the problem of network security risk assessment, calculated the distribution of the number of nodes successfully attacked in the network under the one-hop model, and gave an explicit expression of the distribution. For the multiple-hop model, the author does not provide an accurate calculation method for the above distribution, but only approximates the distribution of the number of nodes of the final successful attack through Monte Carlo simulation, and discusses the difference between this distribution and the binomial distribution (ignoring the propagation effect), so as to understand how the propagation effect affects the network risk.

Propagation Model in Other Areas

Existing research on network risk propagation has been extended to other fields, such as information transmission in brain network, risk transmission in transportation system and so on. In addition to the two important risk propagation models mentioned above, there are also some risk propagation models applied to specific problems or scenarios in the literature. For example, in the research of public security management investment management, supply chain security risk investment management, network security insurance and other issues, some specific risk models are proposed.

Aspones et al. proposed a model describing how to select nodes to set safeguards to control the spread of viruses in the network, and proved that the ratio between cost and optimal value is linear with the total number of nodes. They hypothesized that each infected node would eventually infect all of its unprotected neighbors, and that the cost of setting up safeguards and getting infected would be known. Infected nodes can observe which nodes tend to set protective measures and adjust their infection strategies accordingly. Johnson et al. proposed a network security investment model to solve the problem of choosing between the hybrid product of collective protection and individual mitigation and the external market insurance, and found several complete market insurance equilibria. Simon et al. built a model to analyze the optimal network security investment level of cooperative supply chain and the network security investment level of node independent supply chain. When the attacker has no discrimination attack, the node independent supply chain security is lower than the optimal level. When an attacker attacks strategically, the optimal investment level of the supply chain varies greatly, while the expected damage to each node is similar.

IMMUNIZATION STRATEGY

Based on the network risk propagation model, the risk propagation process is studied, and the propagation law is mastered. The purpose is to control the risk propagation more effectively and reduce the loss of the network system as much as possible. Taking the corresponding node protection measures to the network, the network system can be immune to the risk, in order to achieve the purpose of network security risk management. The classical immunization strategies in complex networks include random immunity, target immunity and acquaintance immunity.

The random immunization strategy refers to the random selection of some nodes in the network with a certain probability for immunity. The degree, position and other attributes of the node will not affect the selection of the node. Moreover, there is no priority order when immunizing nodes. This method has better immune effect in regular network and random network. However, in scale-free network, due to its unique structural characteristics, it cannot play a good immune effect.

In order to avoid the limitation that random immunization strategy cannot be applied to scale-free network, the researchers proposed a targeted immunization strategy. Target immunization strategy refers to selecting some key nodes in the network for immunization. This immunization strategy is suitable for scale-free networks, and the more heterogeneous the network topology, the better the effect of the immunization strategy. This also indicates that the network topology has a certain influence on the dynamic behavior of virus transmission. However, this strategy needs to know the overall information of the network, which is difficult to implement for some large-scale actual networks. In order to improve immune efficiency, scholars proposed the strategy of acquaintance immunity.

The strategy of acquaintance immunity refers to randomly selecting some nodes in the network with a certain probability, and then randomly selecting nodes from the neighbors of selected nodes for immunity. In scale-free networks, nodes with large degrees are much more likely to be selected after two steps than nodes with small degrees. This immune strategy is more efficient and requires only partial knowledge of the network.

Many subsequent studies have been based on these classical immune strategies. Gallos et al. improved the strategy of acquaintance immunity and significantly reduced the immune threshold. Gomez-Gardenes et al. proposed a more flexible immunization strategy that falls between local and global immunization. And the model is applied to real network to verify its high practical value. In order to achieve the best immune effect with less cost, Chen et al. proposed an immune strategy based on graph segmentation theory. It can reduce the cost by 5 to 50 percent to achieve the same immune effect as a targeted immunization strategy. Wang et al. proposed an incomplete target immunization strategy in order to solve the situation that important nodes may be ignored. Moreover, it is found that there is a linear relationship between the reciprocal of transmission threshold and immunity rate. Based on the theory of explosive seepage, Clusella et al. proposed a two-fraction attack network strategy for targeted destruction of network connectivity. It can be understood in reverse to immunize network nodes.

CONCLUSIONS

In the research field of cyber security risk management, scholars have done a lot of effective work. However, there are also some works to be further expanded and deepened:

- Important nodes in the network have greater influence on the scale of cyber risk propagation. So how to identify the important nodes in the network is very important. In the future, we can consider how to identify important nodes in different networks to better manage cyber security risks, such as dynamic networks, networks with overlapping community structures, and so on.
- When studying the risk transmission process, we can explore the key factors and specific methods to reduce the risk transmission probability by analyzing the risk transmission conditions.

The spread of network risks has always been an important part of cyber security risks. Both the research on the propagation threshold and the propagation process is to grasp the propagation law of risk, predict the trend, and better realize the management of cyber security risk. Due to the similarity between network and system in many aspects, the thought and method of system theory can be further used to study related risk management problems in the future. It is believed that these studies will better promote the research on cyber security risk management.

REFERENCES

1. *De Bandt, Olivier, & Hartmann, Philipp. (2000). Systemic risk: a survey. Social Science Electronic Publishing.*
2. *Martin, Eling, Werner, & Schnell. (2016). What do we know about cyber risk and cyber risk insurance? The Journal of Risk Finance.*
3. *Meyers, Lauren A., M. E. J. Newman, Stephanie Schrag. (2003). Applying Network Theory to Epidemics: Control Measures for Mycoplasma Pneumoniae Outbreaks. Emerging Infectious Diseases, 9(2), 204–210.*
4. *Hethcote, H. W. (2000). The mathematics of infectious diseases. SIAM Review, 42(4), 599–653.*
5. *Wang, Y, Chakrabarti, D, Wang, C, & Faloutsos, C. (2003). Epidemic spreading in real networks: An eigen value viewpoint. Reliable Distributed Systems.*
6. *Deepayan, Chakrabarti, Yang, Wang, Chenxi, & Wang, et al. (2008). Epidemic thresholds in real networks. ACM Transactions on Information and System Security, 10(4), 1–26.*
7. *Ganesh, A. J, Laurent Massoulié, & Towsley, D. F. (2005). The effect of network topology on the spread of epidemics. IEEE Computer and Communications Societies, 13–17.*
8. *Draief, M, Ganesh, A, & Massoulié, Laurent (2008). Thresholds for virus spread on networks. The Annals of Applied Probability, 18(2), 359–378.*
9. *Boguá, Marián, & Pastor-Satorras, R. (2002). Epidemic spreading in correlated complex networks. Physical Review E, 66(4), 047104.*
10. *Pastor-Satorras, R, & Vespignani, A. (2002). Epidemic dynamics in finite size scale-free networks. Physical Review E, 65(3), 035108.*

11. *Ljupčo Kocarev. (2012). Influence of the network topology on epidemic spreading. Physical Review E, 85(2), 016114.*
12. *Liu, Z, & Hu, B. (2005). Epidemic spreading in community networks. Europhysics Letters (EPL), 72(2), 315–321.*
13. *Salathé, Marcel, Jones, J. H, & Fraser, C. (2010). Dynamics and control of diseases in networks with community structure. PLoS Computational Biology, 6(4), e1000736.*
14. *Zhang, J. P, & Jin, Z. (2012). Epidemic spreading on complex networks with community structure. Applied Mathematics and Computation, 219(6), 2829–2838.*
15. *Zhang, H, Guan, Z. H, Li, T, Zhang, X. H, & Zhang, D. X. (2013). A stochastic sir epidemic on scale-free network with community structure. Physica A: Statistical Mechanics and its Applications, 392(4), 974–981.*
16. *Kephart, J. O, & White, S. R. (1991). Directed-Graph Epidemiological Models of Computer Viruses. IEEE Computer Society Symposium on Research in Security & Privacy.*
17. *Kephart, J. O, & White, S. R. (1993). Measuring and Modeling Computer Virus Prevalence. IEEE Computer Society Symposium on Research in Security & Privacy.*
18. *Pastor-Satorras, R, Vázquez, Alexei, & Vespignani, A. . (2001). Dynamical and correlation properties of the internet. Physical Review Letters, 87(25), 258701.*
19. *Pastor-Satorras, Romualdo, Alessandro Vespignani. (2002). Immunization of Complex Networks. Physical Review E, 65(3), 036104.*
20. *B. R. R. Brooks, C. L. Brooks Brooks, A.D. Jr. Mackerell, L Nilsson, & M. J. Karplus. (2009). CHARMM: The biomolecular simulation program. Journal of Computational Chemistry, 30(10), 1545–1614.*
21. *Pastor-Satorras, R, Castellano, C, Van Mieghem, P, & Vespignani, A. (2015). Epidemic processes in complex networks. Reviews of modern physics, 87(3), 925–979.*
22. *Xu, M. , Da, G. , & Xu, S. (2015). Cyber epidemic models with dependences. Internet Mathematics, 11(1), 62–92.*
23. *Boguná, Marian, Lafuerza, L. F, Toral, Raúl, & Serrano, M. ángeles. (2014). Simulating non-markovian stochastic processes. Physical Review E, 90(4), 042108.*
24. *Da G, Xu M. Zhao P. (2019). Modeling Network Systems under Simultaneous Cyber-Attacks. IEEE Transactions on Reliability, 68, 971–984.*
25. *Kunreuther H, Heal G. (2003). Interdependent Security. The Risks of Terrorism.*
26. *Heal G, Kunreuther H. (2004). Interdependent Security: A General Model. National Bureau of Economic Research.*
27. *Johnson, B, Grossklags, J, Christin, N, & Chuang, J. (2010). Uncertainty in Interdependent Security Games. International Conference on Decision and Game Theory for Security. Springer-Verlag, 234–244.*
28. *Chan H, Ceyko M, Ortiz L. (2012). Interdependent Defense Games: Modeling Interdependent Security under Deliberate Attacks. In Proceedings of the Twenty-Eighth Conference on Uncertainty in Artificial Intelligence, 152–162.*

29. *Lelarge M, Bolot J. (2008). A local mean field analysis of security investments in networks. International Workshop on Economics of Networked Systems, 25–30.*

30. *Lelarge M, Bolot J. (2008). Network externalities and the deployment of security features and protocols in the internet. International Conference on Measurement and Modeling of Computer Systems, 37–48.*

31. *Laszka A, Johnson B, Grossklags J. (2018). On the assessment of systematic risk in networked systems. ACM Transactions on Internet Technology, 18(4): 1–28.*

32. *O'Dea, Reuben, Crofts, Jonathan J, Kaiser, Marcus. (2013). Spreading Dynamics on Spatially Constrained Complex Brain Networks. Journal of the Royal Society Interface, 10(81), 20130016.*

33. *Meier, J., Zhou, X., Hillebrand, A., Tewarie, P., Stam, C. J., & Van Mieghem, P. (2017). The Epidemic Spreading Model and the Direction of Information Flow in Brain Networks. Neuroimage, 152, 639–646.*

34. *Aspnes, J, Chang, K, & Yampolskiy, A. (2006). Inoculation strategies for victims of viruses and the sum-of-squares partition problem. Journal of Computer and System Sciences, 72(6), 1077–1093.*

35. *Benjamin Johnson, Rainer Böhme, & Jens Grossklags. (2011). Security Games with Market Insurance. Decision and Game Theory for Security, 117–130.*

36. *Simon J, Omar A. (2019). Cybersecurity investments in the supply chain: Coordination and a strategic attacker. European Journal of Operational Research, 282, 161–171.*

37. *Pastor-Satorras R, Vespignani A. (2002). Immunization of complex networks. Physical Review E, 65(3): 036104.*

38. *Cohen, R. , Havlin, S. , & Ben-Avraham, D. . (2003). Efficient immunization strategies for computer networks and populations. Physical Review Letters, 91(24), 247901.*

39. *Gallos, Lazaros K., Liljeros, Fredrik, Argyrakis, Panos, Bunde, Armin, & Havlin, Shlomo. Improving immunization strategies. Physical Review E Statistical Nonlinear & Soft Matter Physics, 75(4), 045104.*

40. *J. Gómez-Gardeñes, Echenique, P, & Moreno, Y. (2006). Immunization of real complex communication networks. The European Physical Journal B: Condensed Matter and Complex Systems, 49(2), 259–264.*

41. *Chen, Y, Paul, G, Havlin, S, Liljeros, F, & Stanley, H. E. (2008). Finding a better immunization strategy. Physical Review Letters, 101(5), 058701.*

42. *Wang, Y., Xiao, G., Hu, J., Cheng, T. H., & Wang, L. (2009). Imperfect targeted immunization in scale-free networks. Physica A: Statistical Mechanics and Its Applications, 388(12), 2535–2546.*

43. *Clusella, P, Grassberger, P, Perez-Reche, F. J, & Politi, A. (2016). Immunization and targeted destruction of networks using explosive percolation. Physical review letters, 117(20), 208301.1-208301.5*