Finding the Weakest Link in the Interdependent Security Chain Using the Analytic Hierarchy Process

Chongxia Pan, Weijun Zhong, and Shue Mei

***Abstract*—with the rapid development of network finance and electronic commerce, the network and information security problems are more complex and prominent, and economics of information security has also become a hot research topic. This paper uses AHP (analytic hierarchy process) method to find the weakest link in the interdependent security chain. And the result can help information security investment decision-making. This paper firstly introduces research background including current research situations about interdependent security and the weakest link in network security. Then it introduces problems about the information system security in corporations' security chain, finally modeling the AHP method to find the weakest link in interdependent security chain and gives a conclusion at last.**

***Index Terms*—Information security economics, AHP, the weakest link, interdependent security.**

I. Introduction

With the Internet scaling up, network users are getting more and more, network finance and electronic commerce are developing at a rapid speed, but at the same time, network and information security problems have become more frequent and complex, so network and information security are required to have a more high security. At present, the problems of network and information security have become a hot research topics and they are no longer regarded as simple technical problems, but more complex systems that need to consider the technology, management, economy and so on. Economics of information security is becoming the cutting-edge research and interdependent security investment is an important part of it.

Interdependent security investment involves two or more than two information systems or networks, that is, one corporation's information security investment is affected by that of another corporation. These problems concerns the Interdependent security of a computer network: it is generally the case that once a hacker or virus reaches one computer on a network, the remaining computers can be more easily compromised because of increasing possibility of contamination. The attackers tend to attack poorly defended information systems, therefore, the information security chain depends on everyone's effort and the strength is decided by the "the weakest link". How to find "the weakest link" in the information security chain and aids decision making is the main goal of this paper.

This paper uses AHP method to find the weakest link in interdependent security chain, that is to find the weakest-protecting information systems of interdependent corporations and aids decision making of information security investment. Lawrence Gordon has used the AHP method to evaluate levels of information security investment in 2005 [1]. Lawrence Bodin, Saul I. Gass analysizes successful applications about AHP in business for the graduate students major in business in 2003 [2].

The rest sections of this paper is arranged as the follows: firstly it introduces the present research situation of interdependent security investment, secondly describes the weakest link in network security , then introduces AHP method in a brief, finally gives a conclusion.

II. Research Background

A. Interdependent Security

Interdependent security investment involves two or more than two information systems or networks and one corporation's security investment affects another corporation's investment. This interdependent security investment is based on the economic externality of information security investment. Anderson introduced the microeconomics concept "externality" into information security research and pointed out that "externality" is the inherent attribute of information security in the first time in the literature [3].

In information security chain, each corporation's computers connects to each other, frequently transmitting information and information sharing, interacting and influencing each other, with the same or similar operating systems and application programs, having the same or similar vulnerabilities, so virus easily transmit from one computer to another computer. If one corporation increases information security investment, the investment not only improves the security level of their own information systems and makes their computers network not easy to be breached, and also secure partners more security environment, this is the positive externality to their partners; however, their investment may also affect the attackers strategy at the same time and causes attackers to attack the weakest-protecting system, so this is the negative externality to their partners.

Therefore, the externality is divided into positive externalities and negative externalities. Positive externalities: increasing security investment will benefit the partners. Negative externality: increasing investment will make the attacker turn to attack the weaker-protecting information systems and thus indirectly increase the risk of partner, so increasing investment has a negative externality on their partners.

Manuscript received on June 4, 2015; revised November 23, 2015.

The authors are with Southeast University, Nanjing, China (e-mail: panchongxia@163. com, zhongweijun@seu.edu.cn, meishue@seu.edu.cn).

doi: 10.18178/jacn.2015.3.4.190

In the literature [4], Kjell Hausken supposes the externality as negative externality under which the hacker tends to attack the weakest-protecting information systems. And the paper establishes a model to analyses how the substitution effects affecting incentives for security investment companies with different sales. The literature [5] introduces two investment models about the negative externality: the weakest-target model and target slightly above the lowest protection level. In the first model, the attacker can always successfully breach the protection system, because there are always some weaker-protecting information systems. In the second model, the attacker has a limit capacity and his successful breach depends on the minimum investment of protector. The literature [6] discusses the impact of network externality incentive on security investment, and points out that positive externalities can improve the survival probability of network security and a negative externality easily produces "free rider", and these two effects influence network security investment decision-making.

From 2002 to 2007, Howard Kunreuther and Geoffrey Heal have published several articles about interdependent security problems and laid a theory foundation. In February 2002, they published the literature utilizing the airline security problem to illustrate how the incentive by one airline to invest in baggage checking was affected by the decisions made by others. And they carried out a numeral simulation finally; In December 2002, they published the literature characterizing the Nash equilibria for the interdependent security (IDS) problem and developing an IDS model by first focusing on airline security and comparing the structure of this problem with other IDS examples such as computer security, fire protection, vaccinations, protection against bankruptcy, and theft protection. They found when agents are identical, there are two Nash equilibria for a wide range of cost and risk parameters: either everyone invests in protection or no one does. In 2003's literature [7], they extends their earlier analysis of interdependent security issues to a general class of problems involving discrete interdependent risks with heterogeneous agents. In 2005's literature [8], they applied an earlier analysis of interdependent security issues to a general class of problems involving discrete interdependent exposure to terrorist risks. In 2006, in literature [9], they modeled tipping as a game-theoretic phenomenon and investigate the connection between super-modular games, tipping of equilibria and cascading, and apply the results to issues that arise in the context of homeland security and computer security. The research showed that tipping and cascading can occur in super-modular games and that 'increasing differences' is a sufficient condition for tipping. Super-modularity and tipping of equilibria are closely related. In 2007's literature [10], under considering that expectations about others' choices will influence investments in risk management and the outcome can be suboptimal for everyone, they modeled that as the Nash equilibrium of a game and give conditions for such a suboptimal equilibrium to be tipped to an optimal one. They also characterized the smallest coalition to tip equilibrium, the minimum critical coalition.

B. The Weakest Link in Network Security

In the interdependent information security systems, network security is the most typical example. The complexity of network security, on the one hand, is because the computer network has various weaknesses, such as system software and application software, hardware configuration, the initial development strategy and so on, and these weaknesses have made the network security management become a more difficult thing [11]. On the other hand, there exists a known dilemma "the defender's dilemma", that is, when facing with more complicated and systematic attacks, the defenders find it very difficult to ensure that the system does not exist any vulnerabilities. "The defenders dilemma" problem is similar to "the weakest link" problem whose strength depends on its weakest link. That is, the smallest piece of board determines the quality of the whole barrel. The weakest link has become a breakthrough easily to be breached for attackers in interdependent information security.

About the "the weakest link" research, the literature [12] pointed out that the security system is determined by the strength of its weakest link, from the mainframe, the personal computer, the networked organization, the human factor to the new vulnerability indicator, all have illustrated this viewpoint. This paper also proposed that information security strategy can only succeed if it incorporates workstations and their users into an overall picture that today is dominated by network and server security paradigms. The literature [13] describes the voluntary provision of public goods and pointed out that there are two situations about the number of public goods provided by the private: "the weakest link (minimum)" and "the best shot (maximum)" that happen in various social conditions.

By developing a hypothetical example, Andrew R. Bearlin, E. S. G. Schreiber, Simon J. Nicol, A. M. Starfield and Charles R. Todd simulated the entire adaptive management (AM) process of the reintroduction of a threatened fish to determine the consequences of reevaluating program objectives, release strategies, and measurement indicators and to identify any weak links in the process that would limit the capacity of the AM program to facilitate "learning by doing" [14].

III. Modeling

A. The Problem

In the interdependent security chain, there exist many information systems. For example, the well know Electronic Data Interchange (EDI) and the more recent Continuous Replenishment Program that link manufacturers, distributors, and retailers within a supply chain [15].

In the interdependent security chain, one organization's security influences its neighbor's security. Junjie Lu, Wanhua Qiu and Yuanzhuo Wang take the transmission of the virus between enterprises as an example, modeled the information security investment game in consideration of interdependency and types of the threats between companies. And discusses the Nash equilibrium solutions of information security investment for many companies [16]. In literature [17], R. Ann Miura-Ko and Benjamin Yolken develop a matrix model for security decision-making in interdependent organizations described by a linear influence network. Using the matrix, this paper presents how one organization's investment influences its neighbor's investment. Michael Kearns, Luis E. Ortiz pointed out that all interdependent security problems share the following important properties: (1). There is a 'bad event' to be avoided, and the opportunity to reduce the risk of it via some kind of investment. (2). The cost-effectiveness of the security investment for the individual is a function of the investment decisions made by the others in the population [18].

There exists the fact that all other things being equal, rational attackers motivated by potential financial gains tend to direct their effort toward less-protected targets. The attackers evaluate potential targets to identify poorly defended information systems to attack. "The weakest link" refers to the most poorly protected system. "The weakest link" system has become a key factor to determine the security level of chain. If these corporations want to improve the security level of the whole information systems and optimize security chain integration, they must improve the security level of "the weakest link".

However, how to find "the weakest link" and how to evaluate the security level of systems are main problems. The following sections analyses the main indexes influencing the information system security and then give an evaluation using the AHP method.

The United States Department of defense proposed "information assurance (IA)" concept in 1995, compared with the previous concept of information security, IA has more broader scope than the concept of information security, in addition to emphasizing protection ability of the information security system, it also proposes that people should pay more attention to the ability of intrusion detection system, the ability of the accident response and the ability of recovery quickly from damage. IA pays attention to the defense and recovery of the whole life cycle of information systems.

Also, these four abilities of information security are self-protection ability, intrusion detection ability, accident response ability, quick recovery ability and these four abilities are not only applicable to measure the security level of national defense information system, can also be used to measure the security level of information system of a corporation. For the information system of a corporation, the four kinds of abilities stand for different meanings.

The self-protection ability of information system refers to the ability to respond to the invasion of automatic protection information system. "The computer information security classification standards" divides the self-protection ability into 5 levels: the first level, user's self-protection level; the second level, system audit protection; the third level, the labeled-protecting level; the fourth level, structure- protecting level; the fifth level, accessing-verified protection. The level of information system security protection is gradually increased from the low level to high level. And each level division has strict standards. Intrusion detection is to detect the network breach in case of not affecting the network performance and it is a network security technology to protect the system from being attacked. Intrusion detection ability is the main ability of intrusion detection system. The main function of the intrusion detection system includes: network traffic monitoring, identifying attackers' characteristics, abnormal behavior analysis, system vulnerability warning, customized response etc. [19]. Accident response ability reflects the ability of emergency response when faced with emergency accident, emergency response refers to preparations to deal with unexpected major security incidents and measures taken by the organization in the accident. Quick recovery ability: learning lessons from security accidents, system vulnerabilities timely patched, recovery and recovery of systems etc. [20].

The four abilities reflect the total security level of information systems of a corporation. So this paper establishes the following AHP model to find "the weakest link" after a comprehensive comparison.

B. AHP Introduction

The Analytic Hierarchy Process (referred to as AHP) is the decision method based on qualitative and quantitative analysis. It is used to decision-making and is always divided into objectives, criterions, alternatives and other levels. This method is developed in in the early 1970s by USA operational research experts Sarti who is a professor in Pittsburgh University, for American defense research "power distribution to industrial sectors according to their various contribution to the national welfare" project. The method uses proposed the theory of network application system and multi-objective comprehensive evaluation method and is a decision method of analyzing weights and hierarchy.

The building steps of AHP is as follows: the first step: identifying AHP tree; the second step: establishing hierarchical structure; the third step: pairwise comparisons; the fourth step: consistency test; the fifth step: scores ranking. Finally, to obtain the total scores ranking and choose the best alternatives or worst alternatives.

C. Modeling to Find the Weakest Link

1) The first step: Identifying AHP tree

The four abilities of information system are self-protection ability, intrusion detection ability, accident response ability and quick recovery ability. In order to evaluate the security level of information system of a corporation in the interdependent security chain, it needs to identify AHP tree.

The goal of this model: evaluate the security level of information system.

The four indexes are used: (1). Self-protection ability; (2). Intrusion detection ability; (3). Accident response ability (4). Quick recovery ability.

Self-protection ability is divided into 5 levels: the first level, user's self-protection level; the second level, system audit protection; the third level, the labeled-protecting level; the fourth level, structure-protecting level; the fifth level, accessing- verified protection.

Intrusion detection ability is the main ability of intrusion detection system that include network traffic monitoring, identifying attackers' characteristics, abnormal behavior analysis, system vulnerability warning, customized response etc.

Accident response ability reflects the ability of emergency response including preparations to deal with unexpected major security incidents and measures taken by the organization in the accident.

Quick recovery ability includes learning lessons from security accidents, system vulnerabilities timely patched, recovery and recovery of systems etc.

The AHP tree is as Fig. 1:

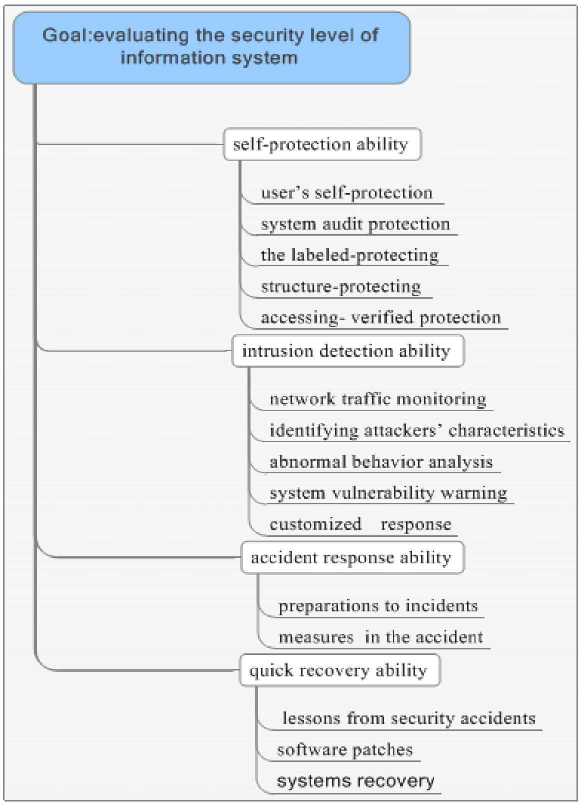
Goal:evaluating the security level of information system
self-protection ability
user's self-protection
system audit protection
the labeled-protecting
structure-protecting
accessing- verified protection
intrusion detection ability
network traffic monitoring
identifying attackers' characteristics
abnormal behavior analysis
system vulnerability warning
customized response
accident response ability
preparations to incidents
measures in the accident
quick recovery ability
lessons from security accidents
software patches
systems recovery

Fig. 1. The AHP tree.

2) *The second step: Establishing hierarchical structure*

Suppose there are three corporations and their information systems are named as C1, C2, C3 respectively. Goal node A: evaluating the security level of information systems. The criterion includes: B1. The self-protection ability; B2. The intrusion detection ability; B3. The accident response ability; B4. The quick recovery ability. The AHP hierarchical structure is as Fig. 2:

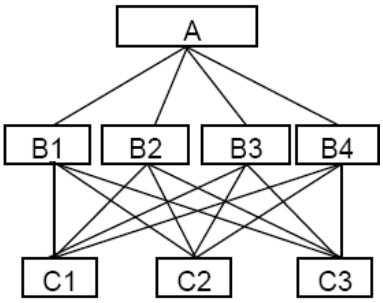

Fig. 2. AHP hierarchical structure.

3) *The third step: Pairwise comparisons*

Notations: figures in the tables mean intensity for each criterion or sub-criterion as following, 7: extremely high,5: very high, 3: reasonably high, 4: between very high and reasonably high,1: equally high.

According to the evaluation of information systems of three corporations, hypotheses are as follows: information system 1 reasonably high than information system 2, information system 2 equally high than information system 3 in self-protection ability as the following Table I:

TABLE I: PAIRWISE COMPARISONS FOR THE THREE SUB-CRITERION FROM THE SELF-PROTECTION ABILITY NODE

B1	C1	C2	C3
C1	1	3	3
C2	1/3	1	1
C3	1/3	1	1
sum	1.67	5	5

About intrusion detection ability, information system 2 reasonably high than information system 1, and very high than information system 3, information system 2 extremely high than information system 3 as the following Table II:

TABLE II: PAIRWISE COMPARISONS FOR THE THREE SUB-CRITERION FROM THE INTRUSION DETECTION ABILITY NODE

B2	C1	C2	C3
C1	1	1/3	5
C2	3	1	7
C3	1/5	1/7	1
sum	4.2	1.48	13

About the accident response ability, information system 1 reasonably high than information system 3, and very high than information system 2, information system 3 reasonably high than information system 2 as the following Table III:

TABLE III: PAIRWISE COMPARISONS FOR THE THREE SUB-CRITERION FROM THE ACCIDENT RESPONSE ABILITY NODE

B3	C1	C2	C3
C1	1	5	3
C2	1/5	1	1/3
C3	1/3	3	1
sum	1.53	9	4.33

About the quick recovery ability, information system 1 reasonably high than information system 2, and very high than information system 3, information system 2 between very high and reasonably high than information system 3 as the following Table IV:

TABLE IV: PAIRWISE COMPARISONS FOR THE THREE SUB-CRITERION FROM THE QUICK RECOVERY ABILITY NODE

B4	C1	C2	C3
C1	1	3	5
C2	1/3	1	4
C3	1/5	1/4	1
sum	1.53	4.25	10

Normalizing the above pairwise comparisons matrix and getting the following Table V:

TABLE V: SCORES FOR THE FOUR ABILITIES

	B1	B2	B3	B4
C1	0.6	0.28	0.63	0.62
C2	0.2	0.64	0.11	0.28
C3	0.2	0.07	0.26	0.10

4) *The fourth step: Consistency test*

By calculating and getting the following maximum eigenvalues of four matrices respectively:

$$\lambda_1=3,\ \lambda_2=3.066$$
$$\lambda_3=3.039,\ \lambda_4=3.087$$

Calculating C.I.(consistency index) according to C.I.=(λ_{max}-n)/(n-1) as follows:

$$C.I._1=(\lambda_1-n)/(n-1)=(3-3)/2=0<0.58$$
$$C.I._2=(\lambda_2-n)/(n-1)=(3.066-3)/2=0.033<0.58$$
$$C.I._3=(\lambda_3-n)/(n-1)=(3.039-3)/2=0.19<0.58$$
$$C.I._4=(\lambda_4-n)/(n-1)=(3.087-3)/2=0.043<0.58$$

Calculating C.R. according to C.R.=C.I./R.I. as follows:

$$C.R._1=C.I.1/R.I=0<0.1$$
$$C.R._2=C.I._2/R.I=0.033/0.58=0.056<0.1$$
$$C.R._3=C.I._3/R.I=0.019/0.58=0.033<0.1$$
$$C.R._4=C.I._4/R.I=0.043/0.58=0.074<0.1$$

Generally speaking, if CI<0.1 and CR<0.1, the consistency of matrix can be accepted, or it must be compared again. By looking-up the following index Table VI, the consistency of the above four matrix is acceptable.

TABLE VI: MEAN RANDOM CONSISTENCY INDEX

order	3	4	5	6	7	8
RI	0.58	0.89	1.12	1.26	1.36	1.41
order	9	10	11	12	13	14
RI	1.46	1.49	1.52	1.54	1.56	1.58

5) *The fifth step: Scores ranking*

For an information system, self-protection ability is the most important, followed by the self-protection ability, the intrusion detection ability, the accident response ability, the quick recovery ability in descending order. Therefore, we can build the following pairwise comparisons for the three criterion from the goal node as Table VII:

TABLE VII: PAIRWISE COMPARISONS FOR THE THREE CRITERION FROM THE GOAL NODE

A	B1	B2	B3	B4
B1	1	3	5	7
B2	1/3	1	4	5
B3	1/5	1/4	1	6
B4	1/7	1/5	1/6	1

From Table VII, we can get the following weights for the self-protection ability, the intrusion detection ability, the accident response ability, the quick recovery ability:

$$W=(0.533,0.27,0.147,0.05),$$
$$W=(0.533,0.27,0.147,0.05).$$

Calculating the figures in Table V and Table VII, we get total ranking scores as in Table VIII:

TABLE VIII: SCORES RANKING

criterion		Self-protection	Intrusion detection	Acciden response	Quick recovery	Total score
weights		0.533	0.27	0.147	0.05	
alternatives	C1	0.6	0.28	0.63	0.62	0.520
	C2	0.2	0.64	0.11	0.28	0.310
	C3	0.2	0.07	0.26	0.10	0.169

From the total scores, we can know that the information system of the first corporation get the most score, the least score is for the third information systems. So the information security system of the third corporation is the weakest link in the interdependent security chain and it needs to be increased security investment.

IV. CONCLUSION

This paper uses AHP to find "the weakest link" in interdependent information security chain and the result provides a decision-making basis for investment decision makers. However, AHP is used to assist the enterprise decision-makers and cannot completely replace human behavior. And the process and analysis of weights of criterion, sub-criterion and alternatives is determined by human. teria and al level, criterion level, sub criterion layer and layer according to the information During the estimation of level of information security needs the participation of the people.

V. FUTURE RESEARCH

In the literature [21], Hal R. Varian points out, there exists three prototypical cases in the context of system reliability, they are total effort, weakest link and best shot. The total effort case means reliability depends on the sum of the efforts exerted by the individuals. The weakest link case means reliability depends on the minimum effort. The best shot case means reliability depends on the maximum effort. So the security level of information systems sometimes depend on the total effort or the maximum effort. Under these two situations, relevant research will have different results from this study.

This paper uses AHP method to find the weakest link in the interdependent security chain that is not as good as the more complex model such as game theory, mathematical differential model.

ACKNOWLEDGMENT

The author would like to thank Xing Gao for his helpful comments and suggestions that have improved the paper.

REFERENCES

[1] L. D. Bodin, L. A. Gordon, and M. P. Loeb, "Evaluating information security investments using the analytic hierarchy process," *Communications of the ACM*, vol. 48, no. 2, pp. 78-83, 2005.

[2] L. Bodin and S. I. Gass, "On teaching the analytic hierarchy process," *Computers & Operations Research*, vol. 30, no. 10, pp. 1487-1497, 2003.

[3] R. Anderson, "Why information security is hard-an economic perspective," in *Proc. 17th Annual Computer Security Applications Conference*, 2001, pp. 358-365.

[4] K. Hausken, "Income, interdependence, and substitution effects affecting incentives for security investment," *Journal of Accounting and Public Policy*, vol. 25, no. 6, pp. 629-665, 2006.

[5] J. Grossklags, N. Christin, and J. Chuang, "Secure or insure? A game-theoretic analysis of information security games," in *Proc. the*

17th International Conference on World Wide Web, 2008, pp. 209-218.

[6] C.-H. Liao and C.-W. Chen, “Network externality and incentive to invest in network security,” *Economic Modelling*, vol. 36, pp. 398-404, 2014.

[7] G. Heal and H. Kunreuther, “You only die once: Managing discrete interdependent risks,” National Bureau of Economic Research, 2003.

[8] G. Heal and H. Kunreuther, “IDS models of airline security,” *Journal of Conflict Resolution*, vol. 49, no. 2, pp. 201-217, 2005.

[9] G. Heal and H. Kunreuther, “Supermodularity and tipping,” National Bureau of Economic Research, 2006.

[10] G. Heal and H. Kunreuther, “Modeling interdependent risks,” *Risk Analysis*, vol. 27, no. 3, pp. 621-634, 2007.

[11] S. Convery, *Network Security Architectures*, Pearson Education India: Cisco Press, 2004.

[12] I. Arce, “The weakest link revisited [information security],” *Security & Privacy*, vol. 1, no. 2, pp. 72-76, 2003.

[13] J. Hirshleifer, “From weakest-link to best-shot: The voluntary provision of public goods,” *Public Choice*, vol. 41, no. 3, pp. 371-386, 1983.

[14] A. R. Bearlin *et al*., “Identifying the weakest link: Simulating adaptive management of the reintroduction of a threatened fish,” *Canadian Journal of Fisheries and Aquatic Sciences*, vol. 59, no. 11, pp. 1709-1716, 2002.

[15] T. Bandyopadhyay, V. Jacob, and S. Raghunathan, “Information security in networked supply chains: impact of network vulnerability and supply chain integration on incentives to invest,” *Information Technology and Management*, vol. 11, no. 1, pp. 7-23, 2010.

[16] J. J. Lv, W. H. Qiu, and Y. Z. Wang, “An analysis of games of information security investment based on interdependent security,” *Chinese Journal of Management Science*, vol. 14, no. 3, pp. 7-12, 2006.

[17] M.-K. R. Ann *et al.*, “Security investment games of interdependent organizations,” in *Proc. IEEE 2008 46th Annual Allerton Conference on Communication, Control, and Computing*, 2008, pp. 252-260.

[18] M. Kearns and L. E. Ortiz, “Algorithms for interdependent security games,” *Advances in Neural Information Processing Systems*, 2003.

[19] J. W. Liu, J. Mao, and R. L. Hu, *The Introduction of Network Security*, Beijing: Electronic Industry Press, 2009, pp. 161-189.

[20] X. Hong, F. Li, and B. H. Zhan, Evaluation of Information Security and Risk Assessment, 2nd ed. Beijing: Electronic Industry Press, 2014, pp. 281-312, 330-343.

[21] H. Varian, “System reliability and free riding,” *Economics of Information Security*, Springer US, 2004, pp. 1-15.

Chongxia Pan is currently pursuing the Ph.D. degree, majoring in management science and engineering at Southeast University in China. She was born in Shandong province in 1977. Her research interests include information security economics and game theory.

Weijun Zhong is a professor at Southeast University in China, whose current research interests include information security economics, management information systems, management of technology and innovation. Prof. Zhong has published research articles in various academic journals such as Journal of Management Information Systems, International Journal of Production Economics, Technological Forecasting and Social Change, Marketing Letters, Operations Research Letters.

Shue Mei works at Southeast University in China and focuses on the information security economics, management information systems, electronic commerce, management of technology and innovation. Prof. Mei has published research articles in many journals including Technological Forecasting and Social Change, Marketing Letters, Operations Research Letters, Computational Economics.

Wireless Sensor Network