Yu-Kai HUANG

Institute of Publishing and Culture Enterprise Management, Nanhua University, Taiwan

Vulnerability Analysis of 18-hour Retail Delivery Service Using by Bayesian Network

Abstract. *With the growth in electronic commerce, ordering books on the Internet is clearly becoming a significant market. Hence, logistics management exposes the formerly latent logistics system in the economic activities and reveals the inner connections between parts of logistics activities. The retail delivery system in Taiwan provides an easy on-line shopping process, safe payment method and quick delivery service for e-retailing. The main purpose of this study is to examine the retailing delivery service process of KingStone on-line book store and highlight all of the most vulnerable parts of the system through Bayesian network (BN). The Bayesian network analysis provides preliminary insights into the direction of relationship management toward maximizing effectiveness of retail delivery service.*

Streszczenie. *System sprzedaży detalicznej w Taiwanie realizuje w większości metody on-line, bezpieczne płacenie i szybką dostawę. Celem prezentowanej pracy jest analiza procesu sprzedaży detalicznej sklepu internetowego KingStone i uwypuklenie najbardziej wrażliwych części systemu z wykorzystaniem sieci bayesowskiej. (**Analiza wrażliwych punktów 18-godzinnej sieci sprzedaży z wykorzystaniem sieci Bayesa**).*

Keywords: Vulnerability, Bayesian Network, 18-hour Retail Delivery Service
Słowa kluczowe: sieć Bayesa, sprzedaż on-line

Introduction

With the growth in electronic commerce, there are more and more consumers ordering books from on-line bookstores in Taiwan. Because of the convenient online order process and low price service, ordering books on the Internet is clearly becoming a significant market. Retail delivery of e-commerce in Taiwan is about eight years old, and the e-commerce RD model is mainly employed by providers. Providers have had to improve information flow both internally and externally, and integrate their logistics services into the retail delivery service provided by convenience stores. This refers to customers shopping in an online store and then picking up the purchased goods in a convenience store. The difference between e-commerce development in Taiwan and in other countries is that there is a new logistics service called retail delivery. Taiwan has a high density of convenience stores. It is easy to find convenience stores in Taiwan. Also, most of stores in Taiwan provide 24-hours service.

One of the major on-line bookstores in Taiwan, KingStone on-line bookstore, cooperates with retail delivery (RD) providers to provide customers the 18-hour delivery service. It means books will arrive after pick-up point in 18 hours after ordering. Because RD provides an easy on-line shopping process, safe payment method, quick delivery service and self pick-up approach, RD becomes the major logistics model for on-line bookstores in Taiwan which is shopping on the Internet and picking-up at convenience store.

Vulnerability is a new concept in risk management. Because of recent increases in the frequency of hazards and catastrophes, risk management has been discussed in many different fields. The influence of systems on risk consequences has been assessed in studies on climate change and natural hazards, and is characterized by the notion of vulnerability. The definition of vulnerability varies depending on the field of study. In recent years, a growing number of studies in different fields have examined this issue, particularly because of the recent series of catastrophes and hazards that impacted global economy causing large losses. However, there are few papers focused on the concept of vulnerability in retailing logistics system with e-commerce. To analyze interrelationships among the factors of vulnerability about retail delivery service, this study examine all of the retailing delivery process used by KingStone on-line book store and highlight all of the most vulnerable parts of the system through Bayesian network.

Vulnerability of 18-hour Retail Delivery Process

In Taiwan, there are many convenience stores, and the retailing delivery (RD) services form a new retail delivery model: “Shopping on the Internet and picking up the merchandise at convenience stores.” The retailing delivery services have made remarkable successes. The procedure that combines on-line bookstores with RD system is illustrated below (see Fig. 1): (1). On-line shopping and select the pick-up point: After making an on-line purchase, customers must choose a pick-up point through e-map to receive their orders; (2). Packing and delivery process: First, after the KingStone confirms the orders, it turns over the order information to delivery center (DC), and DC should help finish the packing process and transport the orders to the delivery centre for the convenience store which had chosen. Second, the DC will collect the orders and transport them to different convenience stores, which are the pick-up points, and then it will report the finished order information to the on-line bookstore; (3). Pick-up goods: According to the information replied from delivery centre, KingStone will notify the customer by e-mail or cell phone message to pick-up their orders. KingStone on-line bookstore promises customers that books will arrive in pick-up point in 18 hours after ordering. That is, receivers might wait more days to get their goods after they click the “purchase” button on the website.

There are several strengths to retail delivery. First, in contrast to home delivery, people using retail delivery do not need to wait for their products at home, and thus have more flexibility to select the time and store that are most convenient. Second, people can pay their bill after picking up their product in the store if they are worried about the credit card safety. Third, online stores can lower costs through retail delivery. However, various risks exist when products are delivered. The KingStone.com promises customers that products will arrive 18 hours after the sender sends the product. Maintaining efficiency and security during such a short time is not that easy.

The concept of vulnerability was still vague in 1990. In general, vulnerability was considered to be the context of risk. It is the adverse reaction that occurs when something is exposed to a hazard or harmful situation. After 1990 definitions of vulnerability became more and more detailed because of increases in the number disasters around the

world. It has been discussed not only regarding environmental issues, but also social and individual issues. Vulnerability is a multidimensional concept. The characteristic of the system constitutes the degree of vulnerability. Supply chain vulnerability is a conceptual framework of supply chain risk management (SCRM). The influence of systems on risk consequences has been assessed in studies of climate change, natural hazard and is characterized by the notion vulnerability [1]-[2]. Vulnerability represents the system sensitivity to external or internal disruptive events which remove the system from its standard working conditions [3]. Supply chain disruptions can have great impact on corporate financial performance, so it is widely accepted that SCRM is necessary in today's business [4]. Supply chain is exposed not only to the risks that come from external environment but also the risks caused by suboptimal interaction between the organizations within the network. The susceptibility of the supply chain to the harm of this situation seems significantly relevant. This leads to the concept of supply chain vulnerability [5]. Even though there are different approaches to the construct supply chain vulnerability; Peck still appraises its conceptual basis as immature [6]. Svensson distinguishes between atomistic vulnerability (of a part of the supply chain) and holistic vulnerability [7]. Barnes and Oloruntoba describe vulnerability as "a susceptibility or predisposition to loss because of existing organizational or functional practices or conditions'' in their study in maritime supply chain [8]. Wagner and Bode interpret further that supply chain characteristics are antecedents of supply chain vulnerability and have impact on both the probability of occurrence as well as the severity of supply chain disruptions [9]. We define the delivery vulnerability that "the properties of the delivery system construct the sensitivity of it. The sensitivity and loss of it when product delivering suffers from risks is considered as delivery system vulnerability. "

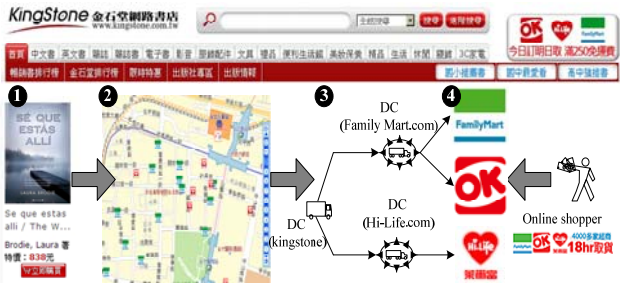

Fig.1. Concept of retail delivery service of KingStone.com

Methodology

A Bayesian Network (BN) is a probability-based knowledge representation method, which is appropriate for the modelling of causal processes with uncertainty. It is based on the Baye' theorem and can be used to denote causal inference. A BN is a directed acyclic graph (DAG) whose nodes represent random variables and whose links define probabilistic dependencies between variables (see Fig.2). The nodes with arrows directed into them are called "child" nodes; and the nodes from which the edges depart are called "parent" nodes; and nodes without arrows directed into them are called "root" nodes.

The DAG represents the structure of causal dependence between nodes and shows the qualitative part of causal reasoning in a BN. Thus, the relations between variables and the corresponding states provide the quantitative part, which consists of a conditional probability table (CPT). Diagnosis or prediction using BN is composed of fixing the values of the observed variables and computing the posterior probabilities of some of the unobserved variables.

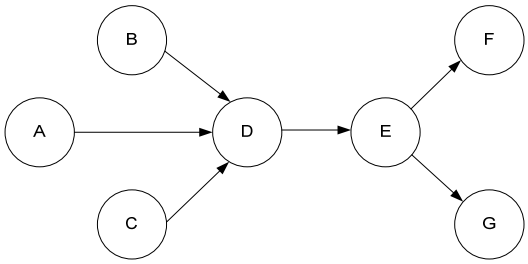

Fig.2. BN framework

There are three types of connections between variables (serial connections, diverging connections and converging connections), which facilitate the ability to infer and learn in BNs, and comprise DAGs. Many learning techniques rely heavily on data. A BN, which is a knowledge representation, can provide new knowledge by combining expert domain knowledge with statistical data. The chain rule says that a BN is a representation of the joint distribution over all the variables represented in the DAG. Marginal and conditional probabilities can be computed for each node in the network. Let BN be a Bayesian network over $U=\{X_1, X_2, ..., X_n\}$. BN specifies a unique joint probability distribution given by the product of all conditional probability tables specified in BN:

$$P(U) = \prod_{i=1}^{n} P(X_i \mid Pa(X_i)) \tag{1}$$

where $Pa(X_i)$ are the parents of X_i in BN, and $P(U)$ reflects the properties of BN. Therefore, various marginal and conditional probabilities can be computed given an evidence e, as the following shows. The evidence is information received from external sources about the possible states of a subset of the variables of the network.

$$P(X_1, X_2, ..., X_n \mid e) = \frac{P(X_1, X_2, ..., X_n, e)}{P(e)} \tag{2}$$

There are two kinds of evidence. One is called hard evidence. Hard evidence is an exact observation of the state of the variables. The other is called soft evidence. Soft evidence occurs when non-definite information is given, expressed in terms of likelihood of the states of the variable. In other words, a probabilistic inference is given that is capable of updating our belief about events given observations. It is then possible to perform a sensitivity analysis of probabilities given different subsets of evidences. A probabilistic inference is given that is capable to updating our belief about events given observations, and then it is possible to perform a sensitivity analysis of probabilities given different subsets of evidences.

Analysis and Discussion

We interview with experts to understand the whole 18-hour delivery service system well and then build the BN framework. Because BN modeling is too complicated and the prior probabilities are hard to be obtained from experts and input manually, the prior failure probabilities of root nodes are collected from experts (Tab. 1 and Fig. 3), and our study uses expression function to generate conditional probability table. There are two ways to measure the vulnerability of RD system. First, we implemented predictive analysis. This was measured by means of the difference in conditional probability of failure occurrence of the marginal probability that delay situation (A_1) when different states are given. Second, we conducted a diagnostic analysis. We computed the result of each root node when the different states of A_1 are instantiated. Finally, we examine the most vulnerable parts in the system.

Table 1. Prior failure probability of root nodes

Node	Description	Prob.
E_1	E-map information is not updated	0.48%
E_2	Personnel operational errors	0.24%
E_3	Time difference about batches issue	0.19%
E_4	Arrival notice is sent in advance	0.29%
E_5	Unusual errors during delivery	0.45%
E_6	No goods information	0.16%
E_7	Problems with system scheduling	0.19%
E_8	Unusual information system error	0.17%
E_9	No barcode label	0.51%
E_{10}	Defaced or unclear barcode	0.82%
E_{11}	Articles have the same barcode info.	0.12%
E_{12}	Problems from shift changes (DC)	0.79%
E_{13}	Wrong labels attached to goods	0.39%
E_{14}	Goods sent to the wrong store	0.55%
E_{15}	Goods sorted to the wrong container	0.61%
E_{16}	Couriers errors	0.15%
E_{17}	Sorter errors	0.21%
E_{18}	Clerk errors	0.55%
E_{19}	CS is temporarily closed	0.17%
E_{20}	Problems from shift changes	1.00%
E_{21}	Barcode not scanned on arrival	0.28%

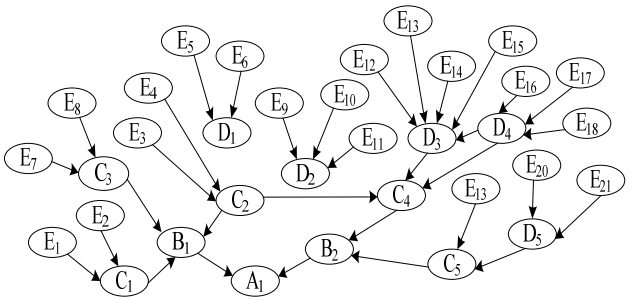

Fig.3. BN framework of the 18-hour delivery service

Table 2 and Table 3 illustrated the results of Bayesian network analysis, the marginal probability that goods delay arriving A1 occurs is 4.829%. It is slight underestimate, but quite similar to the real data, which was 5.94%, the average rate from October to December, 2010. There may be a bias in the short-term data collected. In addition, the probabilities given by experts' were based on their long-term experience, so it is more stable and close to a normal situation compared to the real data. Therefore, we considered it to be a valid result and did an analysis using this framework.

A predictive analysis was conducted on the basis of the prior probabilities of the root nodes and the conditional dependency of each node. In order to discuss the relationships between the root nodes (E_i) and *A1*, P (A_1 = *True* | *Ei= True*) and P (A_1= *True* | E_i= *False*) were calculated. "*Ture*" state is represented as failure occurrence and "*False*" state means no failure occurrence. Our study attempts to figure out the relationship between the failure probability of E_i and the result of Table 3. It is pointed out that problems from shift changes (E_{20}), e-map information is not updated in time (E_1) are considered as potential vulnerable parts because they have higher failure probabilities, and also have higher conditional probabilities variations than average when the state of E_i changes from "*False*" to "*True*". On the other hand, CVS is temporarily closed (E_{19}), problems with system scheduling (E_7), unusual information system error or breakdown (E_8), technical personnel operational errors (E_2), barcode not scanned on arrival (E_{21}), arrival notice is sent in advance (E_4) may be more vulnerable than the other ones.

Table 2. The result of BN

Description	Prob.
A_1: Goods delay arriving	4.83%
B_1: Information failures	1.79%
B_2: Physical logistics failures	3.73%
C_1: E-map is not updated	2.35%
C_2: Information is asymmetric	1.03%
C_3: Buyers not receive arrival notices	2.17%
C_4: Errors from fleets or DC	0.37%
C_5: Errors from the selected CS	3.65%
D_1: Asymmetric information occurred	2.17%
D_2: Errors from barcodes	0.81%
D_3: Redeliver goods	0.16%
D_4: Lost goods	0.64%
D_5: Goods can't be found in the CS	2.81%

A predictive analysis was conducted on the basis of the prior probabilities of the root nodes and the conditional dependency of each node. In order to discuss the relationships between the root nodes (E_i) and *A1*, P (A_1 = *True* | *Ei= True*) and P (A_1= *True* | E_i= *False*) were calculated. "*Ture*" state is represented as failure occurrence and "*False*" state means no failure occurrence. Our study attempts to figure out the relationship between the failure probability of E_i and the result of Table 3. It is pointed out that problems from shift changes (E_{20}), e-map information is not updated in time (E_1) are considered as potential vulnerable parts because they have higher failure probabilities, and also have higher conditional probabilities variations than average when the state of E_i changes from "*False*" to "*True*". On the other hand, CVS is temporarily closed (E_{19}), problems with system scheduling (E_7), unusual information system error or breakdown (E_8), technical personnel operational errors (E_2), barcode not scanned on arrival (E_{21}), arrival notice is sent in advance (E_4) may be more vulnerable than the other ones.

Table 3. Result of probabilistic inference

Predictive analysis			
P (E_i=True | A_1=True)		P (E_i=True | A_1=False)	
E_1:0.104	E_{12}:0.051	E_1:0.048	E_{12}:0.049
E_2:0.085	E_{13}:0.049	E_2:0.049	E_{13}:0.049
E_3:0.068	E_{14}:0.050	E_3:0.049	E_{14}:0.049
E_4:0.077	E_{15}:0.051	E_4:0.049	E_{15}:0.049
E_5:0.053	E_{16}:0.055	E_5:0.049	E_{16}:0.049
E_6:0.053	E_{17}:0.053	E_6:0.049	E_{17}:0.049
E_7:0.110	E_{18}:0.055	E_7:0.049	E_{18}:0.049
E_8:0.100	E_{19}:0.137	E_8:0.049	E_{19}:0.048
E_9:0.055	E_{20}:0.125	E_9:0.049	E_{20}:0.048
E_{10}:0.056	E_{21}:0.084	E_{10}:0.049	E_{21}:0.049
E_{11}:0.054		E_{11}:0.049	
Diagnostic analysis			
P (E_i=True | A_1=True)		P (E_i=True | A_1=False)	
E_1:0.010	E_{12}:0.008	E_1:0.005	E_{12}:0.008
E_2:0.004	E_{13}:0.004	E_2:0.002	E_{13}:0.004
E_3:0.004	E_{14}:0.006	E_3:0.002	E_{14}:0.006
E_4:0.005	E_{15}:0.006	E_4:0.003	E_{15}:0.006
E_5:0.005	E_{16}:0.002	E_5:0.005	E_{16}:0.002
E_6:0.002	E_{17}:0.002	E_6:0.002	E_{17}:0.002
E_7:0.004	E_{18}:0.006	E_7:0.002	E_{18}:0.006
E_8:0.004	E_{19}:0.005	E_8:0.002	E_{19}:0.002
E_9:0.006	E_{20}:0.024	E_9:0.005	E_{20}:0.009
E_9:0.001	E_{21}:0.005	E_{10}:0.001	E_{21}:0.003
E_{10}:0.01		E_{11}:0.008	

It can be found that all root nodes are potential vulnerable parts. They should be kept at low conditional probabilities if we do not want A_1 to occur and also small change in their conditional probabilities of failure occurrence will cause A1 occurrence. Combining the results of two analyses, shift changes, e-map information is not updated in time are regarded as the most vulnerable parts with

higher failure probabilities. They all have higher failure probabilities and contribute to a higher conditional probability of failure occurrence of A_1. Additionally, just small change in their conditional probabilities of failure occurrence, given the evidence of A_1, will lead to an occurrence of A_1.

The root nodes that have lower failure probabilities are worth mentioning. CVS is temporarily closed, problems with system scheduling, unusual information system error or breakdown, technical personnel operational errors, barcode not scanned on arrival, arrival notice is sent in advance are the most vulnerable parts with lower probabilities. Although these events do not happen easily, they all greatly increase the conditional probability of A_1 occurrence and even more than those that have higher failure probabilities. In addition, only a small change in their conditional probabilities of failure occurrence gives evidence that A_1 will occur.

Conclusion

Supply chain vulnerability is a new concept in risk management. In recent years, a growing number of studies in different fields have examined this issue, particularly because of the recent series of catastrophes and hazards that impacted global economy causing large losses. Supply chain risk management is no exception. Although a substantial number of studies in supply chain vulnerability have been performed to date, most of them employed qualitative analysis. In addition, relatively little research has been conducted on a specific system or company. Retailing delivery is the main logistics model for on-line bookstores in Taiwan. The study is aimed at discussing the vulnerability of the KingStone.com's 18-hour retailing delivery process, which is part of a supply chain. To do this, BN is used to conduct this research. Through predictive and diagnostic analyses, the most vulnerable parts can be classified into two categories, those which have higher failure probabilities and which have lower failure probabilities. For the former ones, KingStone's managers should pay more attention to improving staff's skills and implementing standard operation process intensively to reduce their failure probabilities. For the later ones, managers should allocate more resources to maintaining the reliability and stability of information systems. Besides, they should keep updating information of situation of convenience stores and goods as well. For further research, our study suggests that analyst should try to accumulate statistical data to evaluate the BN in order to achieve more objective results. In addition, BN allows events to include multiple states. Considering multiple states can increase the depth of the study. The conclusions obtained in this study can be used to improve the retailing delivery logistics service quality for on-line bookstores. Although the BN is a useful tool for vulnerability analysis, but we think the BN in this study has been improve as the retailing delivery process change. For future research, it is recommended to explore the vulnerability and resilience issue of the retailing delivery service system.

Acknowledgments: This work is supported by the National Science Council of Taiwan for providing the research grant (NSC 99-2410-H-343 -030 -).

REFERENCES

[1] Huang Y.K., Feng C.M., A catastrophe model for developing loyalty strategies: a case study on choice behaviour of pick-up point for online shopping, *International Journal of Services Operations and Informatics*, (2009), No. 4, 107-122

[2] Hongliang, Z., A redefinition of the project risk process: Using vulnerability to open up the event-consequence link, *International Journal of Project Management*, (2007), No. 25, 694-701

[3] Albino V., Garavelli, A.C., A methodology for the vulnerability analysis of just-in-time production systems, *International Journal of Production Economics*, (1995), No. 41, 71-80

[4] Stephan M.W., Nikrouz N., Assessing the vulnerability of supply chains using graph theory, *International Journal of Production Economics*, (2010), No. 126, 121-129

[5] Jüttner, U., Peck, H., Christopher, M., Supply Chain Risk Management: Outlining an Agenda for Future Research. *International Journal of Logistics: Research and Applications*, (2003), No. 6, 197-210

[6] Peck, H., Drivers of supply chain vulnerability: an integrated framework, *International Journal of Physical Distribution & Logistics Management*, (2005), No. 35, 210-232

[7] Göran S., A typology of vulnerability scenarios towards suppliers and customers in supply chains based upon perceived time and relationship dependencies, *International Journal of Physical Distribution & Logistics Management*, (2002), No. 32, 168-187

[8] Stephan M.W., Christoph B., An empirical investigation into supply chain vulnerability, *Journal of Purchasing and Supply Management*, (2006), No. 12, 301-312

[9] Pearl J., Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference, Morgan Kaufmann, San Mateo

***Authors**: Yu-Kai Huang is an Assistant Professor of the Institute of Publishing and Culture Enterprise Management, Nanhua University, Taiwan.*
E-mail: osilo.huang@gmail.com.