Using Social Network Analysis to Combat Counterfeiting

Abstract

Counterfeiting undoubtedly produces great harm to companies and the society. This paper presents a study on the application of Social Network Analysis (SNA) to combating this problem. The supply chain can be viewed as a network of parties involved in delivering value to consumers. Normally, SNA is used to analyze relationships between people. In this study, it is utilized to analyze supply chains for identification of parties that are likely to be involved in counterfeiting activities. After identifying the suspects in a supply chain, the company can deter and detect counterfeiting by tightening surveillance on these parties. The feasibility of using SNA as an anti-counterfeiting tool is investigated in a case study, the findings of which indicate that SNA can effectively help companies to prevent sources of counterfeit products from infiltrating into the supply chain. Problematic parties can be identified by characterizing the following features: high degree of centrality, high closeness of centrality and high betweenness of centrality.

Keywords: Anti-counterfeiting, RFID, Social Network Analysis, Supply Chain Management

1. Introduction

In recent years, counterfeiting has become a serious economic problem around the world. Counterfeiting is the act of imitating or copying other products. The imitated or copied products are arguably the same as the original ones, but they are sold at a fraction the price of the original ones (Hung, 2003). Because of technological advances, problems of counterfeiting worsened as counterfeiters gain the advantage with the wide adoption of the Internet and customers now purchase products in a product-unseen fashion as well as a seller-unseen fashion (Henderson, 2001; Bastia, 2002). Counterfeit products affect the brand value and equity of brand owners. According to the MIT Center for International Studies, counterfeiting is estimated to be 15% to 20% of all products produced in China and such products account for around 8% of China's annual GDP (Morrison, 2012). Recent statistics indicated that counterfeit products caused global losses of about US$654.38 billion (Havocscope, 2012), a huge damage to the development of global economy.

A range of technologies has been introduced to combat counterfeiting problems (Hopkins et al., 2003). Radio Frequency Identification (RFID) based anti-counterfeiting solutions have been widely reported in literature (Ting et al., 2011; Kwok et al., 2010; Lehtonen et al., 2008; Wong et al., 2006). Generally, RFID technology combats counterfeiting in two ways: (i) item identification and (ii) traceability of an item's trail of transactions in its supply chain. However, these solutions are reactive because they can only detect fakes after the latter have infiltrated into the supply chain. In today's business environment, since companies have to deal with counterfeiting threats that have become more complex and debilitating, there is a need to shift from reactive to proactive countermeasures (Spink, 2011).

Social Network Analysis (SNA), a computational network theory in visualizing social relationships, is freshly introduced in supply chain management (Knoke and Yang, 2008). In general, supply chain data is inputted into a simulation software package and network analysis results are derived to visualize knowledge networks within the supply chain, to monitor knowledge flows and to identify the nodes of a network that accumulate knowledge (Borgatti and Li., 2009). Inspired by these approaches, SNA can arguably be applied as a proactive anti-counterfeiting strategy. By using it to analyze the transaction records of counterfeit products, SNA can assist in identifying relationships between supply chain parties so as to detect likely problematic parties.

In this study, SNA is adopted to analyze the relationship and performance of a supply chain utilizing the graphical network theory. Network analysis characterizes relationships between different nodes of a network by generating centrality coefficients of nodes and by using network diagrams to visualize the connectedness of nodes (Cockcroft, 2010). The technique is performed to identify likely problematic entities in a network, along with estimates of each party's possibility of being a counterfeit source. This study is the first of its kind in adopting SNA to combat counterfeiting. A case study is presented to illustrate the feasibility of applying SNA to visualize and analyze the logistics flow of the supply chain of counterfeit products, as well as its effectiveness for identifying suspicious parties.

2. Current Anti-counterfeiting Technologies

2.1 Counterfeit Products

Counterfeiting refers to fraudulent imitation or facsimile of something valuable. It is an offense when the producer of these imitated items has intent to defraud, passing them as genuine and to take advantage from them (Burton, 2007). Producers of counterfeit products always benefit from the fraudulent act because their products can be sold at high price while their costs are relatively low. The first cases of brand counterfeiting appeared about five decades ago. The phenomenon was a minor problem at that time because only a few manufacturers of high-value products (such as textile, jewelry and accessories) were affected in such cases (Elif, 2010). Since then, counterfeit products have proliferated and rampaged through both less and well developed countries (Matos et al., 2007).

2.2 Challenges of Preventing and Detecting Counterfeit Products

The root cause of counterfeits is the chance to earn profit and the trade-off of risk and reward that favors illegal activity (DuPont, 2010). Lax or nonexistent legislation and weak penalty enforcement of most governments are the main impediments to anti-counterfeiting. As a result, activities of counterfeit manufacturing and distribution have increased rapidly. Recently, increased counter-measures have been made in countries with serious counterfeiting problems. However, it is still challenging to detect and prevent counterfeiting; the key issues of addressing these problems are summarized in Table 1. It can be argued that tightened law enforcement and the use of anti-counterfeit technologies are the main solutions to combat counterfeiting activities.

Table 1

Key issues concerning the detection and prevention of counterfeiting

	Key Issue	Description
1.	Legislation on counterfeit products is usually imprecise and fragmented, leading to proliferation of criminal offences (Gabara and Krause, 2003)	Counterfeiting is serious in many developing countries such as Azerbaijan, Georgia, Bosnia-Herzegovina, etc, in which most of them do not understand the importance of fighting against counterfeiting, letting alone to have legislation that address the issue. In some cases, the manufacture of counterfeits is declared as criminal offence without the law being enforced, while it is even treated as a legitimate business in some of the developing counties.
2.	Few countries regard counterfeiting as a serious criminal offence because they do not recognize the full extent of the adverse economic and social impacts of the act (The Canadian Chamber of Commerce and the Retail Council of Canada, 2007)	The judiciary of many countries does not recognize counterfeiting as an “economic crime”, leading to the lax enforcement to deter and prevent the corresponding business in the countries. With the adverse economic impacts like lowering the confidence of investment made by brand owners and hampering the countries’ export to other countries, the judiciary of these countries should proclaim counterfeiting as a criminal

		act and set legislation against the issue.
3.	The customs authority does not have sufficient resources to detect and prevent counterfeit products (Gabara and Krause, 2003)	It is difficult for the law enforcement authority to detect and intercept whether the items are counterfeit or not as they are scattered after import. Thus, more resources are required to deal with the problem.
4.	Imposing high levels of import tariffs and excise taxes on luxury goods, alcohol and tobacco increases the incentive for producing counterfeit goods (Pike, 2000)	Prices of counterfeit products are often slightly lower than that of the real products. Without having to pay for taxes such as import tariffs and excise taxes, in comparison to the production of authentic goods, the marginal profit of the counterfeit manufacturing is therefore significantly higher, creating great incentive for people to engage in counterfeit business.
5.	The resources government deploys on anti-counterfeiting are often limited as a country typically emphasizes on other types of high-margin illicit issues (Henderson, 2001)	Without having enough police force resources spent on combating fraud, together with the grey areas in anti-counterfeiting laws and regulations, loopholes exists that encourages the thriving of counterfeiting business.
6.	Businesses succeed in criminal activities (Gabara and Krause, 2003)	With sophisticated industry technologies (e.g. photocopying and printing technologies) and manufacturing equipment, counterfeiters can easily imitate not only physical products in the market, but also the corresponding packaging and labels in mass inexpensively. In some cases, counterfeiters may even use genuine labels and packaging materials from authorized but unscrupulous suppliers in order to make the counterfeits look like the real products.

2.3 Existing Approaches to Prevent and Detect Counterfeit Products

Most available strategies and technologies are introduced to manufacturers and brand owners to authenticate products in order to detect counterfeits. Some of them are very simple, while others are very sophisticated and highly secure. The level of sophistication mainly depends on the cost and applications, whereas the areas of implementation range from product packaging to individual products (Power, 2009). For example, high-value collectible items, such as artworks and antiques, require more sophisticated techniques to detect fakes because of the high potential loss caused by counterfeit items.

To address counterfeiting problems, several technologies with different security measures have been developed. The primary purpose of these technologies is to facilitate product authentication; whereas their secondary purpose is to act as deterrent to counterfeiters who consider the difficulty and costs involved. Product authentication is one of the common anti-counterfeiting technologies widely adopted in industry (Lehtonen et al., 2008). It achieves the anti-counterfeiting function in a physical manner. Additional tools are available to stakeholders

ascertaining the genuineness of products. Generally, these technologies can be classified into five categories: overt (visible) technology, covert (hidden) technology, machine-readable technology, serialization / track and trace technology and forensic technology.

(a) Overt (visible) technology

Overt technology allows end users to confirm the identity of a package (Power, 2009). It can be visible and judged with naked eyes. Examples of this approach include holograms, optically variable devices, color shifting security inks and films.

(b) Covert (hidden) technology

Covert technology facilitates the brand owner to detect counterfeit items but the identifier cannot be visualized with naked eyes (Power, 2009). Special reading devices or equipment are usually required for identification and verification. Typically, the identifiers are invisible under visible spectrum, but they are visible under an excitation light. Examples of this technology include chemically altered dyes, invisible printing, digital watermarks, laser coding, ultraviolet (UV) ink, infrared (IR) ink, and synthetic molecular markers.

(c) Machine-readable technology

Machine-readable technology can be either overt or covert, but authentication must be processed by equipment. Speedy and error proof results can be expected without human intervention. Examples of this technology include RFID tag, watermark magnetic, and hologram with magnetic signature.

(d) Serialization / Track and trace technology

Serialization / track and trace technology refers to identification systems such as RFID technology and bar code systems. Normally, they provide the identification of products, assets, documents or people and thus tracking and tracing. Because of their identification functions, they are widely adopted to facilitate the operation of information system in different areas such as inventory management of manufacturing, receiving management of warehousing, distribution management of transportation and so forth (Ilie-Zudor et al., 2010). Normally, they store product information like product name, lot number, manufacture day and so on, all of which are recorded via the supply chain until they are consumed.

(e) Forensic techniques

Forensic techniques refer to high-technology solutions which need laboratory testing or other dedicated tools to test the item’s authenticity. They are classified as covert technologies, examples of which are chemical taggants, DNA taggants, and isotope ratios.

2.4 Limitations of Existing Approaches

At present, the usual approach to combat counterfeiting is to use the techniques introduced in Section 2.3 to authenticate the end product. However, these solutions are not preventive measures against counterfeiting. Moreover, with advancement of technology, many of these anti-counterfeiting methods can be easily imitated eventually, reducing their potency in combating the counterfeit problem. Table 2 summarizes the strengths and limitations of the existing anti-counterfeiting approaches.

Table 2 Strengths and limitations of existing anti-counterfeiting approaches

Approach	Strengths	Limitations
Overt technology	• Difficult and expensive to copy • Simple to implement • Smart product packaging	• Requires knowledge in detecting the visual features and distinguishing the authenticity of the item in an effective manner
Covert technology	• Requires specialist knowledge to detect or mimick	• Possible to reverse engineer the covert technology by examining specimens of the product • Possible to produce identical or similar security mark by emitting light of the same wavelength range and putting the mark on the counterfeit product
Machine-readable technology	• Eliminates the problem of inconsistent manual verification • Supports high speed and large scale detection	• Expensive • Possible to reverse engineer the technology by examining a specimens of the product
Serialization/ Track and trace technology	• Allows products to be tracked the manufacturing points to designated distribution points • Enables supply chain visualization for product authentication (Kwok et al., 2010)	• Expensive to develop the track and trace platform /infrastructure • Requires full participation of supply chain parties
Forensic technology	• Robust and effective for item identification • Relatively secure against imitation	• Not possible to broadly apply to markets and end-users because of the dedicated knowledge and equipment required and their high cost

		• Costly when licensing fees and the equipment costs are taken into consideration

Anti-counterfeiting technologies have been developed to be implemented in areas ranging from product packaging to the product itself. While some of these solutions involve using tags as identifiers of products, others use physical or chemical markers for identification. Product packaging authentication is not foolproof as the solution is easy to imitate. Security devices alone can only facilitate detection of counterfeit products, they do not prevent supply of these fake items.

Kwok et al. (2008) and Bastia (2002) suggest that tracking and tracing movements of products in a supply chain is a more effective approach to anti-counterfeiting. The traditional solutions cannot do this because using them to collect product flow is difficult and labor intensive. Moreover, some of these solutions are likely to be neutralized soon, as many of the formerly "advanced" technologies have quickly found widespread applications today.

Kwok et al. (2010) propose a more proactive solution that involves the use of a counterfeit network analyzer (CNA) based on RFID technology and EPC networks. It is an automatic information sharing network that can visualize distribution of fraudulent products by analyzing information captured in EPC networks. The CNA detects entities that are very likely to have involved in distributing suspicious items and the source of these items.

3. Methodology

3.1 Social Network Analysis (SNA)

In this study, Social network analysis (SNA) is used to analyze interactions between organizations in a supply chain so as to identify parties that are very likely to be involved in counterfeiting activities. The SNA methodology consists of three main stages: (i) describing the set of actors of the network; (ii) characterizing the matrix (or relationships) between actors; and (iii) analyzing the network structure of the data matrix.

The first step of SNA consists of describing the actors of the network. SNA studies connections among nodes in a network. In a network an actor is represented by a node and relationships between actors are represented by edges (Allesina et al., 2010; Raghavan and Viswanadham, 2010; Kerbache and Smith, 2004). Actors may refer to individuals, organizations, or even countries, whereas edges may represent transactions, communication, friendship, collaboration, or trade (Chen and Paulraj, 2004; Christopher, 1992). In identifying relationships between supply chain parties for counterfeit products distribution, the supply chain data (i.e. transaction records

of counterfeit products) can be viewed as actors in the network of an organization that delivers value from the first involved party to the end consumer in this study.

The second step of SNA consists of identifying the existence of flows of information between actors or, in other words, the demand (receiving information) and supply (providing information) of information between supply chain parties. This information can be collected through track-and-trace technology like RFID or barcode (Kwok et al., 2010). Data collected are recorded in the information flow matrix as elaborated by Brinkerhoff (2004) and Marsden (1990). With the matrix showing the supply of information between actors, the network structure can be evaluated and analyzed in the next step.

The final step of SNA is to analyze the network structure of data matrix via the measurement of degree of centrality, betweenness of centrality, and closeness of centrality. The network can help the user to understand how the counterfeit distribution is formed (i.e. which supply chain party has the highest possibility to be a counterfeiter). More discussion on construction of network structure is depicted below.

3.2 Constructing Network Coefficients

A network structure can be evaluated by attributes known as network coefficients. Two commonly used categorizes of network attributes are network-level coefficients and node-level coefficients (Benta, 2005).

3.2.1 Network-level Coefficients

Network-level coefficients are used to compare performance of networks with different structures and topologies, or to study changes in network performance over time (Kilduff and Tsai, 2003). The SNA implemented in this study does not involve measurement of network-level coefficients.

3.2.2 Node-level Coefficients

Node-level coefficients measure the relative importance, role and effects of different nodes within the network. In other words, they reflect the status (relationship) and connectivity of each node within the network. Three node-level coefficients, or centrality coefficients, are introduced below:

(a) Degree Centrality

The node that connects with the largest number of other nodes is called the central actor as it interacts with most other actors (Liu, 2011). The degree centrality of a node measures the

number of interactions (edges) the node has with others. This coefficient can be broken down into in-degree centrality and out-degree centrality. In-degree centrality measures the number of ties directed to the node (see Figure 1a), whereas out-degree centrality measures the number of ties that the node directs to others (see Figure 1b). Degree centrality can be determined using Eq. (1), in which degree centrality – $C_D(n_i)$ – of node n_i, equals the degrees of a node that refers to the number of edges – $d(n_i)$ – it connects, normalized with the maximum degrees (g – 1) of all nodes in the network.

$$C_D(n_i) = \frac{d(n_i)}{g-1} \tag{1}$$

(a) (b)

Figure 1(a) In-degree Centrality (b) out-degree Centrality

(b) Closeness Centrality

Closeness centrality is defined as the sum of distances to or from all other nodes. Distance refers to the shortest path link between two nodes (Freeman, 1979). If a node interacts easily with many other nodes, its total distance to all other nodes will be shorter. Eq. (2) shows the formula for determining closeness centrality of n_i, in which $d(n_i, n_j)$ denotes the shortest distance between node n_i and node n_j.

$$C_c(n_i) = \frac{(g-1)}{\sum_{j=1}^{g} d(n_i, n_j)} \tag{2}$$

Similar to degree centrality, closeness centrality can be decomposed into in-closeness centrality and out- closeness centrality; in-closeness centrality measures the number of ties directed to the node, out-closeness centrality measures the number of ties that the node directs to others.

(c) Betweenness Centrality

Betweenness centrality is defined as the level of control. The level of control a node has on connections (flows) in the network is determined by the node's actual or potential intermediary value to all other nodes of the network. It involves the determination of the shortest paths among all pairs of nodes. A node with a relatively high score of betweenness centrality has a high probability that it is on a randomly chosen shortest path. This type of node is more powerful than others because more parties will depend on it to have interactions with others (Freeman, 1977). Betweenness centrality is determined by Eq. (3).

$$C_B(n_i) = \sum_{n_j < n_k} \frac{P_{n_j n_k}(n_i)}{P_{n_j n_k}} \tag{3}$$

where $P_{n_j n_k}(n_i)$ refers to the number of paths which pass through node n_i and $P_{n_j n_k}$ refers to the total number of shortest paths between node n_j and node n_k.

3.3 Applying Network Coefficients of Nodes in a Supply Chain for Anti-counterfeiting

Kuglin and Rosenbaum (2000) are the first who introduced the concept of supply chain network which is the network of firms that integrates each other and coordinate together in order to produce and deliver finished goods to the end user. The nodes (in the supply chain) refer to different supply chain parties which are connected by many links, representing physical activities in the supply chain network. Applications of SNA in supply chain analysis are reported in Bezuidenhout et al. (2012), Swaminathan et al. (2002) and Lazzarini et al. (2001).

It is argued that studying and analyzing the network structure that represents a supply chain can help to detect suspected counterfeiting parties in the network (Kwok et al., 2010). This can be accomplished by using centrality coefficients to analyze the network structure. As discussed in Section 3.2 above, degree centrality measures the level of activity, hence the importance and potential influence, of a node in the network. However, the attribute only considers the direct ties an actor has with others without considering the indirect ones. If one node direct connects to many other nodes, but those other nodes, in turn, do not connect to others, the node can only be viewed as a central node in a local neighborhood. Certain nodes may be essential to some of the transactions even though these nodes are weakly connected as reflected by their relatively low value of degree centrality. Closeness centrality and betweenness centrality reflect an individual's capacity to control interactions within a network.

4. Case Study on SNA in Combating Counterfeiting

4.1 Case Study Background

To demonstrate the feasibility of using social network coefficients for nodes in a supply chain network as tools to combat counterfeits, stock in / out data of a paper product company (with an anonymous name, Midas) were collected and analyzed by SNA.

Data used in the case study were collected at the Dongguan Plant. The parties featured in the network include different functional areas including docking area, four production plants each with different functionalities and a warehouse. The physical flow of products in the case company follows one of 10 routes listed in Figure 2. The parties involved are Docking Area, Production Plants 1 to 4 (PP1 to PP4), and Warehouse. Data on problematic transactions are automatically collected by RFID at the case company (Figure 3).

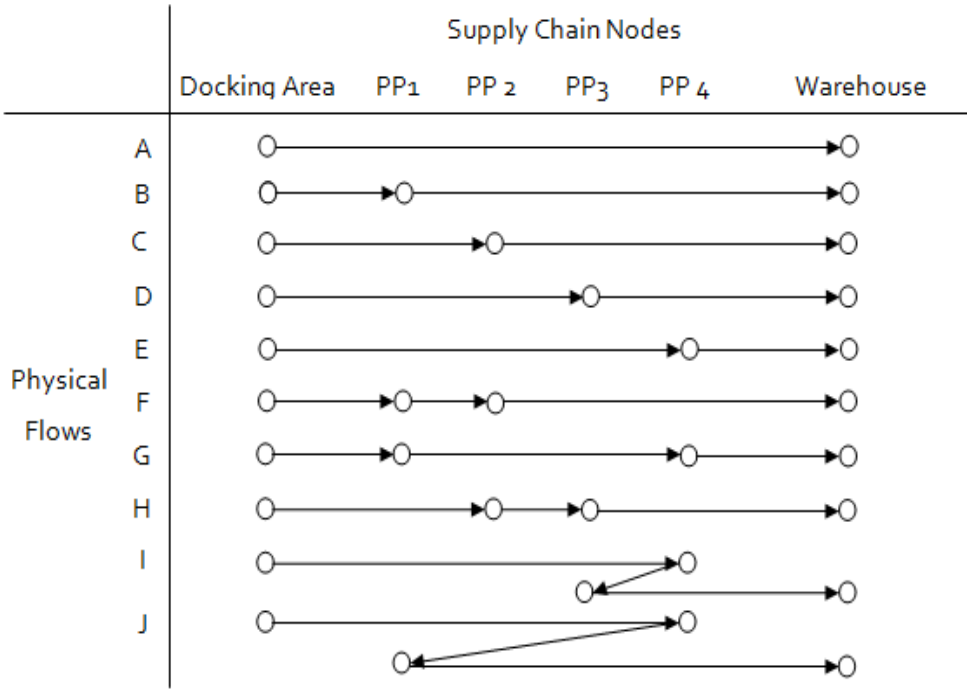


Figure 2 10 Routes of Physical Flow

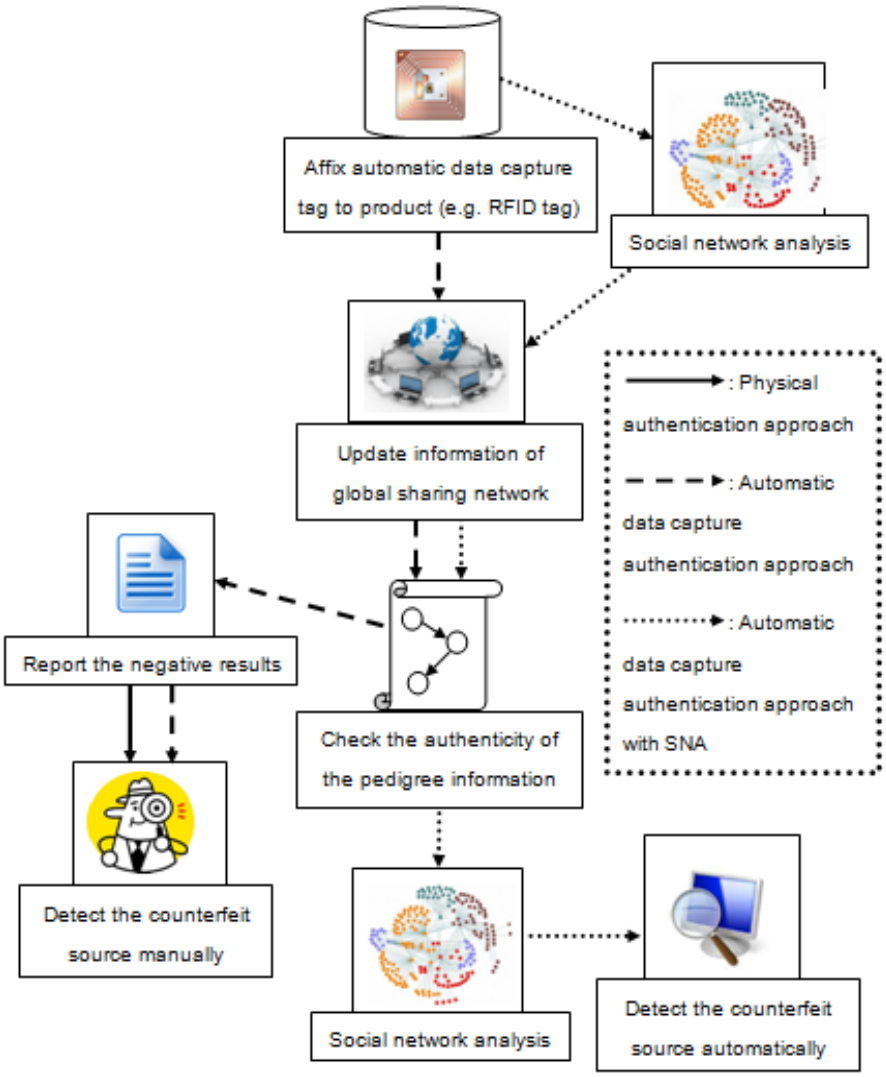


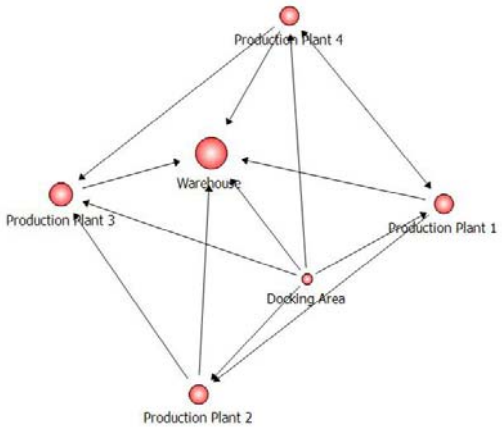
Figure 3 Procedure of Using SNA Centrality Measures to detect Counterfeits

4.2 Network Structure of the Case Study

In order to analyze the social network structure of Midas, NetMiner (NetMiner, 2006) is employed in this case study. NetMiner is a social network visualization and analysis tool which allows user to visually and interactively study the network data, and therefore helps user to find out the underlying patterns and structure of the network formed. Results of three social network coefficients including degree of centrality, closeness of centrality and betweenness of centrality are generated and discussed in the following sections.

4.2.1 Degree of Centrality

Degree of centrality measures the level of activity of each node in a network, i.e. the bigger the node size, the more active the node is. As shown in Figure 4, warehouse is the most active node, which has the highest in-degree of centrality score (i.e. 1). Among all production plants, production plant 3 has the highest in-degree of centrality score (i.e. 0.60). Other production plants have the same value of in-degree of centrality score (i.e. 0.40) whereas docking area is the least active party, in which it has the smallest node and gets the highest out-degree of centrality score. In short, the mean of both in-degree of centrality and out-degree of centrality are 0.467; in which the in-degree of centrality of both production plant 3 and warehouse are higher than the mean, while the out-degree of centrality of docking area, production plant 1 and production plant 4 are higher than the average value.

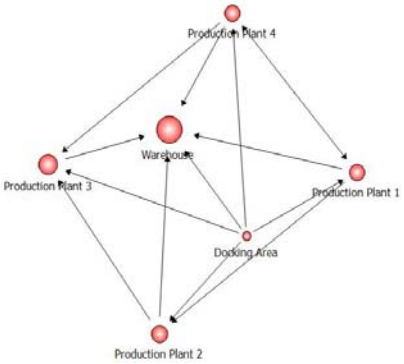


		1	2
		In-Degree Centrality	Out-Degree Centrality
1	Docking Area	0.000000	1.000000
2	Production Plant 1	0.400000	0.600000
3	Production Plant 2	0.400000	0.400000
4	Production Plant 3	0.600000	0.200000
5	Production Plant 4	0.400000	0.600000
6	Warehouse	1.000000	0.000000

Figure 4 Social network diagram and vector summary of degree of centrality

4.2.2 Closeness of Centrality

Closeness centrality measures the ease level of one party to interact with other parties, i.e. the bigger the node size, the easiest of one party to interact with other parties. As shown in Figure 5, warehouse is the easiest party (i.e. the highest in-degree of centrality score), following by production plant 3 (with 0.64 in-degree of centrality score). Production plant 1, 2 and 4 have the same node size. The most difficult to interact with other parties is docking area which the node is the smallest (i.e. 0 out-closeness of centrality is warehouse). In short, the mean of in-closeness of centrality and out-closeness of centrality are 0.482 and 0.48, respectively. The out-closeness of centrality of both production plant 3 and warehouse are higher than the mean, while the out-closeness of centrality of docking area, production plant 1 and production plant 4 are higher than the average value.

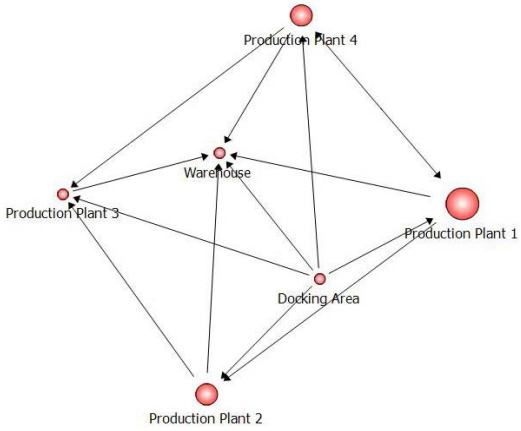


		1	2
		In-Closeness	Out-Closeness
1	Docking Area	0.000000	1.000000
2	Production Plant 1	0.400000	0.640000
3	Production Plant 2	0.450000	0.400000
4	Production Plant 3	0.640000	0.200000
5	Production Plant 4	0.400000	0.640000
6	Warehouse	1.000000	0.000000

Figure 5 Social network diagram and vector summary of closeness of centrality

4.2.3 Betweenness of Centrality

Betweenness of centrality indicates the level of control between parties over the network, i.e. the bigger the node size, the more powerful the node is. Different from the above results, production plant 1 is the most powerful node which has the largest ability to control the product flows over the network (Figure 6). Production plant 2 and 4 come to the second and is followed by docking area, production plant 3 and warehouse. Regarding the highest betweenness of centrality value of nodes is 0.050, only half of the nodes have power of control in this supply chain network. The betweenness of centrality of production plant 1 is the highest whereas the lowest betweenness of centrality is docking, production plant 3 and warehouse. In short, the mean of betweenness of centrality is 0.017. The betweenness of centrality of production plant 1, 2 and 4 are higher than the mean. Among these three parties, production plant 1 has the greatest power of control over the supply chain network.



		1
		Node Betweenness Centrality
1	Docking Area	0.000000
2	Production Plant 1	0.050000
3	Production Plant 2	0.025000
4	Production Plant 3	0.000000
5	Production Plant 4	0.025000
6	Warehouse	0.000000

Figure 6 Social network diagram and vector summary of betweenness of centrality

5. Discussions and Conclusion Remarks

5.1 Discussions

5.1.1 Degree of Centrality

5.1.1.1 In-degree of Centrality

Other parties seek to directly tie to production plant 3 and warehouse as both of them have a higher in-degree of centrality than the mean value. Furthermore, the preference to directly tie to warehouse is higher than the production plant 3 as the in-degree of centrality of warehouse is higher. As a result, warehouse is the most important and prominent party, following by production plant 3.

5.1.1.2 Out-degree of Centrality

Docking area, production plant 1 and 4 are able to interact with others and usually act as third-parties in product exchange among nodes as their out-degree of centrality is higher than the mean value. Thus, it is claimed that they are influential parties. Having the out-degree of centrality of docking area is the highest, the docking area is the most influential party, and is followed by production plant 1 and 4 (i.e. same value of out-degree of centrality).

5.1.1.3 Summary

Production docking, production plant 1 and 4 may be the potential parties to spread the counterfeiting as they have relative high influential power. Warehouse and production plant 3 may be the potential parties to receive the counterfeiting as they have relative high interaction on receiving problematic products.

5.1.2 Closeness of centrality

5.1.2.1 In-closeness of Centrality

Both warehouse and production plant 3 are the easiest parties to receive products from other nodes. They are the most powerful parties in the supply chain as values of their in-closeness of centrality are higher than the mean value. Among these two parties, warehouse has the larger chance of receiving products from other nodes than production plant 3 as the in-closeness of centrality of warehouse is higher.

5.1.2.2 Out-closeness of Centrality

Docking area, production plant 1 and 4 are easy to send products to other parties in a supply chain network as their out-closeness of centrality are higher than the mean value. Among these three parties, docking area has the largest opportunity to send products to other parties. Production plant 1 and 4 has the same opportunity to send goods to other parties which are the second highest.

5.1.2.3 Summary

Docking area, production plant 1 and 4 may be the potential parties to deliver counterfeits as they have relatively high chance to interact with other parties. Warehouse and production plant 3 may be the potential parties to receive counterfeits as they have relatively high interaction on receiving problematic products.

5.1.3 Betweenness of Centrality

Production plant 1, 2 and 4 are viewed as movers-and-shakers and the deal-makers that made things happen. They are important for the network formation and stratification. Production plant 1 is the most powerful supply chain parties in this situation.

5.1.4 Summary of the Results

The problematic parties can be obtained by finding the high degree of centrality, high closeness of centrality and high betweenness of centrality. As production plant 1 and 4 has relatively high score in these measures, they have the highest probabilities in supplying counterfeiting sources. The possibility of production plant 1 has counterfeiting sources is higher than that of production plant 4 as production plant 1 is more powerful in the control of product flows within the supply chain network (i.e. higher betweenness of centrality).

In addition, warehouse and production plant 3 has the highest probabilities in receiving counterfeiting sources as they have relatively high score in in-degree of centrality and in-closeness of centrality. The possibility of warehouse in receiving counterfeiting sources is higher as it has higher in-degree of centrality and in-closeness of centrality. In summary, Figure 7 concludes the paths of conducting counterfeiting sources and spreading along the supply chain.

To better control the counterfeit distribution within Midas, it is recommended to pay more attention to production plant 1 and 4 (which have the higher chance of spreading problematic sources). Midas is also suggested to conduct investigation on the four routes of product flows as highlighted in Figure 7.

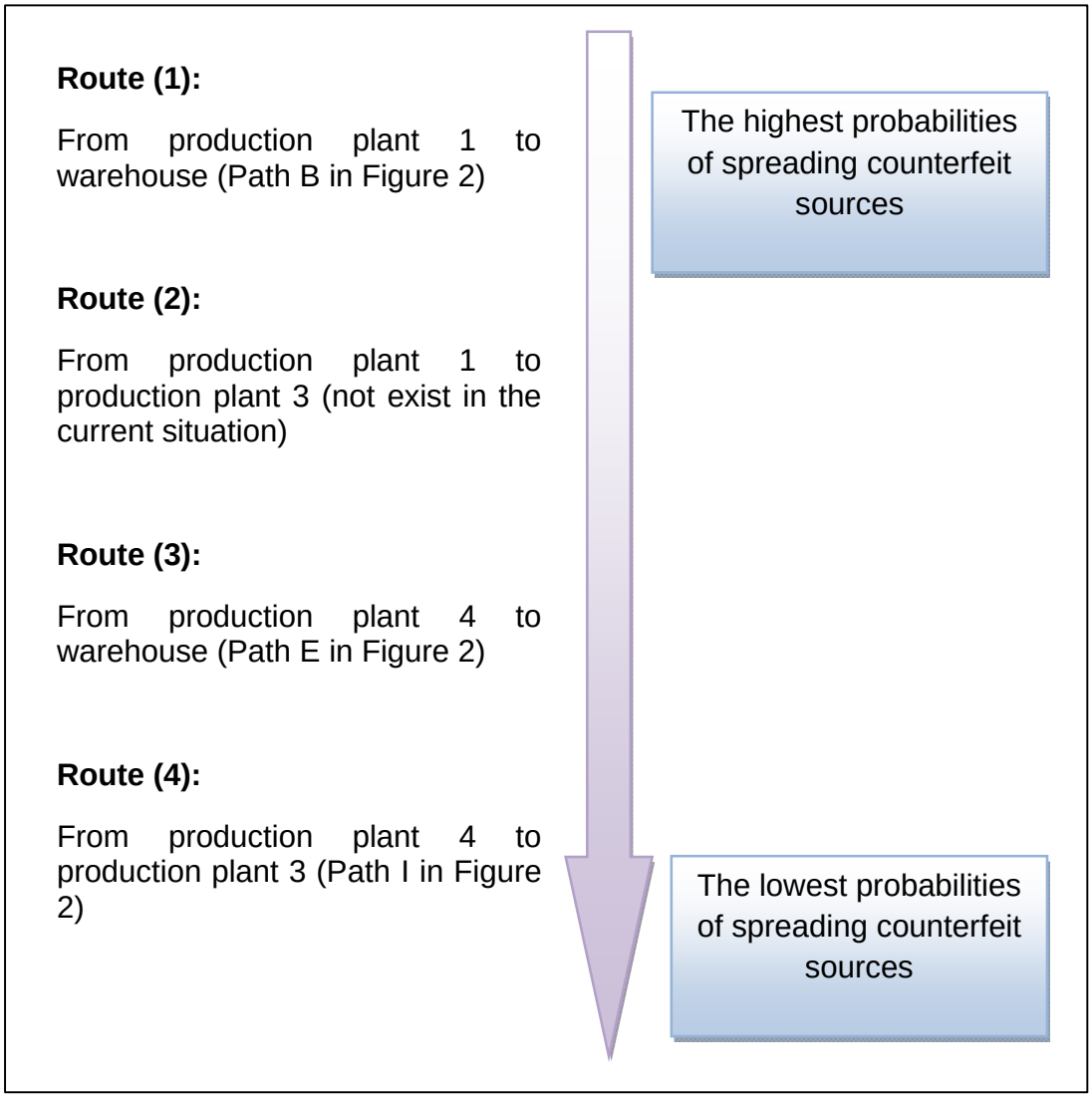


Figure 7 Likelihood of paths of counterfeiting

5.2 Conclusion

This study applies the theory of SNA to the supply chain in order to combat counterfeiting problems with accomplishment of two objectives: (i) to introduce the use of an SNA-based technique for combating counterfeiting activities; it involves visualization and analysis of the logistics flow in a supply chain; and (ii) to demonstrate the feasibility of applying the proposed technique and its effectiveness of detecting counterfeiting parties through a case study. It evaluates the effectiveness of applying three SNA measures to historical data stored in transaction records of a supply chain for detection of likely problematic parties and suspicious trails. The social network measures used include degree of centrality, betweenness of centrality,

and closeness of centrality. Results of the case study reported in this paper indicate that SNA is a method that is both effective and efficient for combating sources and channels of counterfeit products.

Comparing with traditional anti-counterfeiting techniques (listed in Table 2), SNA can analyze the logistics flow of items and perform as an intelligent detector of the source of counterfeiting (such as highlighting plant 1 and 4 as the higher chance of spreading problematic sources in the case study). At present, the usual approach to combat counterfeiting is to use the techniques (e.g. overt, covert, machine-readable, etc.) to authenticate the end product. However, these solutions are not preventive measures against counterfeiting. In contrast, by transforming the data matrix into network structure, SNA can simply identify suspicious supply chain parties that are likely to be the counterfeit distributor and notify the user if there is anomaly once a possible counterfeiting source is being detected (like plant 1 as it out-closeness of centrality are higher than the mean value in the case study). With the coefficient measurement of SNA, the attributes of the supply chain parties are visualized and presented in graphical and quantitative manner, which can further facilitate the analysis and examination of the supply chain parties' roles systemically. For example, the degree of emission and reception of the node can be used to determine whether the entity is the distributor or customer of the counterfeit items.

Although encouraging results have been achieved, there are a number of aspects that need further investigations. First, more data samples have to be collected to further ascertain the effectiveness of the proposed system in combating counterfeiting. It would be interesting if statistical estimates including more risk factors could be incorporated into the network predictions. On the other hand, the outputs from SNA could be augmented with rules to explain the rationale used to reach a prediction. In this aspect, future work on combining rule extraction techniques can be examined.

Acknowledgement

The authors gratefully thank the Department of Industrial and Systems Engineering, The Hong Kong Polytechnic University for its support of this research work.

References

Hung, C.L. (2003). The business of product counterfeiting in China and the post-WTO membership environment. *Asia Pacific Business Review*, 10(1), 58-77.

Henderson, L. (2001). Factors which allow the white collar crime problem to continue unabated. Available at: http://www.crimes-of-persuasion.com/laws/problems.htm (accessed at November 13 2011).

Bastia, S. (2002). Next generation technologies to combat counterfeiting of electronic components. *IEEE Transactions on Components and Packaging Technologies*, 25 (1), 175-176.

Morrison, W.M. (2012). China-U.S. Trade Issues. *Congressional Research Service*, Washington, DC.

Havocscope. (2010). Havocscope global counterfeit goods value. Available at: http://www.havocscope.com/counterfeit-goods-ranking (accessed at 4 March 2012).

Hopkins, D.M., Kontnik, L.T. & Turnage, M.T. (2003). Counterfeiting exposed: protecting your brand and customers. Hoboken: John Wiley & Sons.

Ting, S.L., Kwok, S.K., Tsang, A.H.C. & Lee, W.B. (2011). Critical elements and lessons learnt from the implementation of an RFID-enabled healthcare management system in a medical organization. *Journal of Medical Systems*, 35(4), 657-669.

Kwok, S.K., Ting, S.L., Tsang, A.H.C. & Cheung, C.F. (2010). A counterfeit network analyzer based on RFID and EPC. *Industrial Management & Data Systems*, 110(7), 1018-1037.

Lehtonen, M., Staake, T. & Michahelles, F. (2008). From identification to authentication – a review of RFID product authentication techniques. *In: Networked RFID Systems and Lightweight Cryptography (Book Chapter)*, pp. 169-187.

Wong, K.H.M, Hui, P.C.L. & Chan, A.C.K. (2006). Cryptography and authentication on RFID passive tags for apparel products. *Computers in Industry*, 57(4), 342-349.

Spink, J. (2011). Overview of the selection of strategic authentication and tracing programmes. *In: Counterfeit Medicines Volume I: Policy, Economics and Countermeasures (Book Chapter)*, pp. 111-128.

Knoke, D. & Yang, S. (2008). Social network analysis. Sage: Newberry Park, CA.

Borgatti, S.P. & Li, X. (2009). On social network analysis in a supply chain context. *Journal of Supply Chain Management*, 45(2), 5-22.

Cockcroft, S. (2010). The use of Social Network Analysis to explore relationships between the Medical Informatics and Information Systems literature. *AMCIS 2010 Proceedings*, 551.

Burton, W.C. (2007). Counterfeiting legal definition of counterfeiting. Available at: http://legal-dictionary.thefreedictionary.com/counterfeiting (accessed July 25 2011).

Elif, A.E. (2010). The rise in the sales of counterfeit brands: the case of Turkish consumers. *African Journal of Business Management*, 4 (10), 2181-2186.

Matos, C.A., Ituassu, C.T. & Rossi, C.A. (2007). Consumer attitudes toward counterfeits: a review and extension. *Journal of Consumer Marketing*, 24(1), 36-47.

DuPont, (2010). counterfeiting and fraud threaten consumers and businesses. Available at: http://www2.dupont.com/Authentication/en_US/assets/downloads/Counterfeit_Facts.pdf (accessed July 25 2012).

Gabara, I.I. & Krause, C. (2003). Global counterfeiting: Background Document. Available at: http://counterfeiting.unicri.it/docs/Global%20counterfeiting%20background.pdf (accessed July 25 2012).

The Canadian Chamber of Commerce and the Retail Council of Canada. (2007). The problems underlying Canada's failed IP enforcement system. *Report on Counterfeiting and Piracy in Canada: A Road Map for Change*, 25 - 41.

Pike, J. (2000). International Crime Threat Assessment. US Government Interagency Working Group, Available at: http://www.fas.org/irp/threat/pub45270chap2.html (accessed May 7 2012).

Henderson, L. (2001). Factors which allow the white collar crime problem to continue unabated. Available at: http://www.crimes-of-persuasion.com/laws/problems.htm (accessed November 13 2011).

Power, G. (2009). Anti-counterfeit technologies for the protection of medicines. International Medical Products Anti-Counterfeiting Taskforce, 1-13.

Ilie-Zudor, E., Kemény, Z., van Blommestein, F., Monostori, L. & van der Meulen, A. (2010). A survey of applications and requirements of unique identification systems and RFID techniques. *Computers in Industry,* 62(3), 227-252.

Kwok, S.K., Tsang, A.H.C., Ting, J.S.L., Lee, W.B. & Cheung, B.C.F. (2008). An intelligent RFID-based electronic anti-counterfeit system (InRECS) for the manufacturing industry. *In Proceedings of the 17th World Congress, The International Federation of Automatic Control*, Seoul, Korea, 6-11 July 2008, pp. 5482-5487.

Kerbache, L. & Smith, J. M. (2004). Queuing networks and the topological logistics of supply with systems. *International Journal of Production Economics*, 91(3), 251-272.

Christopher, M. (1992). Logistic and Supply Chain Management. Pitman: London.

Benta, M.I. (2005). Studying communication networks with Agna 2.1. *Cognition Brain Behavior*, 9(3), 567-574.

Kilduff, M., & Tsai, W. (2003). Social networks and organizations. Thousand Oaks, CA: Sage.

Liu, B. (2011). Web Data Mining. Springer.

Freeman, L.C. (1977). A set of measures of centrality based on betweenness. *Sociometry,* 40, 35-41.

Freeman, L.C. (1979). Centrality in social networks: conceptual clarification. *Social Networks*, 1(3), 215-239.

Kuglin, F.A. & Rosenbaum, B.A. (2000). The supply chain network @ Internet speed: preparing your company for the e-commerce revolution.

Swaminathan, A., Hoetker, G. & Mitchell, W. (2002). Network structure and business survival: the case of U.S. automobile component suppliers. Working Paper.

Lazzarini, S.G., Chaddad, F.R. & Cook, M.L. (2001). Integrating supply chain and network analyses: the study of netchains. *Journal of Chain and Network Science*, 1(1), pp. 7-22.

NetMiner (2006). Netminer Overview. Avaliable at: http://www.netminer.com/NetMiner/overview_01.jsp (accessed May 17 2012).

Bezuidenhout, C.S., Bodhanya, S., Sanjika, T., Sibomana, M. & Boote, G.L.N. (2012). Network-analysis approaches to deal with causal complexity in a supply network. *International Journal of Production Research*, 50(7), 1840-1849.

Allesina, S., Azzi, A., Battini, D. & Regattieri, A. (2010). Performance measurement in supply chains: new network analysis and entropic indexes. *International Journal of Production Research*, 48(8), 2297-2321

Raghavan, N.R.S. & Viswanadham, N. (2010). Generalized queueing network analysis of integrated supply chains. *International Journal of Production Research*, 39(2), 205-224.

Chen, I.J. & Paulraj, A. (2004). Understanding supply chain management: critical research and a theoretical framework. *International Journal of Production Research*, 42(1), 131-163.

Brinkerhoff D. (2004). Accountability and health systems: toward conceptual clarity and policy relevance. *Health Policy and Planning*, 19(6), 371-379.

Marsden P.V. (1990). Network data and measurement. *Annual Review of Sociology*, 16, 435-463.