Cargo Security Early Warning System
The Application of Neural Networks to Detect Cargoes with Potential Security Fraud

Final Report

METRANS Project 07318906

August 2008

Melody Y. Kiang
Information Systems Department,
College of Business Administration
California State University, Long Beach
1250 Bellflower Blvd.,
Long Beach, CA 90840

METRANS Transportation Center
USC CSULB

Disclaimer

The contents of this report reflect the views of the authors, who are responsible for the facts and the accuracy of the information presented herein. This document is disseminated under the sponsorship of the Department of Transportation, University Transportation Centers Program, and California Department of Transportation in the interest of information exchange. The U.S. Government and California Department of Transportation assume no liability for the contents or use thereof. The contents do not necessarily reflect the official views or policies of the State of California or the Department of Transportation. This report does not constitute a standard, specification, or regulation.

Abstract

Kohonen's self-organizing map (SOM) network is one of the most important network architectures developed during the 1980's. The SOM network was originally designed for solving problems that involve tasks such as clustering, visualization, and abstraction. The main function of SOM networks is to map the input data from an n-dimensional space to a lower dimensional (usually one or two-dimensional) plot while maintaining the original topological relations. In this research, we evaluate the feasibility of applying SOM networks to build a cargo security warning system that can identify cargoes with higher potential of security fraud.

The salient feature of the extended SOM network is its ability to reduce the input space to a 1- or 2- dimensional output map while maintaining the original topological relations. In other words, the data points that were close in the higher dimensional space should remain close in the reduced lower dimensional map. Therefore, when grouped into clusters, the cargoes that possess similar attributes values will be in the same cluster. Besides providing the cluster membership information, the SOM visual map clearly depicts the actual relationship among the cargoes within and among different risk groups.

Table of contents

Disclaimer i
Abstract ii
Table of contents iii
List of figures and tables iv
Disclosure v
Acknowledgement vi
Introduction 1
Background Information 4
Artificial Intelligence in Port Security 6
Contraband Detection/Fraud Prevention 8
Factors Impacting Fraud/Contraband Detection 10
Research Methodology 15
Supervised vs. Unsupervised Learning 15
Kohonen Self-Organizing Map (SOM) Network 15
Cluster Analysis using SOM 16
SOM Network Architecture 17
Weight Adaption Function 17
The Self-Organization Process 18
Conscience Mechanism 19
The Contiguity-Constrained Clustering Method 20
SOM Training Process 22
The Experimental Design 23
Sample Generation and Experiment Results 23
The Iris Plants Database 27
Conclusions and Recommendations 29
Implementation 31
References 32

List of figures and tables

Tables

Table 1. Statistical analysis of the Iris Plants sample attributes 27

Table 2. Performance comparison of the extended SOM and the three statistical clustering methods using the Iris database.....27

Figures

Figure 1 How Cargo Flows Securely to the U.S.....7

Figure 2 Bill of Lading 8

Figure 3 Cargo and Supply Chain Security Report 12

Figure 4 A *4 x 4* Kohonen Layer and neighboring nodes with radial distance (r = 1).....18

Figure 5 SOM output of the Compact data set 25

Figure 6 SOM output of the Closer data set 25

Figure 7 SOM output of the Unequal data set 26

Figure 8 Output map of the Iris Plants Data 28

Disclosure

“Project was funded in entirety under this contract to California Department of Transportation."

Acknowledgement

This research was entirely supported by Metrans Center and its funding agencies: the Department of Transportation and California Department of Transportation. I also thank my graduate assistant, Larry Kimaara, for his help in this research.

Introduction

Every year, more than 5,500 vessels carrying 4.5 million cargo containers pass through the airports and harbors of the U.S. By far the busiest of these ports are the combined docks of Los Angeles and Long Beach, where 45 percent of the nation's containers arrive. With $200 billion worth of goods flowing in and out of Los Angeles and Long Beach, these ports have a large influence on the economy, across several different industries including aerospace, electrical, consumer products, textiles, among others (Grossberg, 2006).

Given the importance of the ports of Los Angeles and Long Beach and their significant influence on the urban population, it becomes more and more important that some type of real-time monitoring/early warning system is needed to ensure the security and safety of the ports. Ever since the terrorist attacks of September 11, 2001, security has become a national epidemic. Great emphasis has been placed on securing the U.S. borders to help minimize any threat of attack. With that, it has been increasingly recognized that the country's ports represent a significant point of entry and vulnerability. For example, in 2004, customs inspectors started scanning more than double the percentage of packages compared with 2003 after recognizing the potential threat. Nevertheless, only 5.4 percent of all incoming cargo is scanned for contraband given the enormous cost and time necessary for manual inspection. Even with the advent of gamma, X-ray, and radiation detection technology, manual inspection of all cargo coming from just the ports of Los Angeles and Long Beach alone would not be practical given the processing time and financial implications, and the fact that these two ports represent 30 percent of all U.S. international sea trade.

Known that the current security controls in place at the ports are not adequate for today's environment, an information system solution to support safe movement of cargo would greatly improve safety with a minimum impact on current processes. According to Rod MacDonald, acting assistant commissioner of the U.S. Customs Border Protection's Office of Information and Technology, collecting and reviewing shipment information before arrival is the best solution to combating illegitimate cargo. Application of an information technology solution that takes into account the variability of the cargo

process and container variations would be ideal. Therefore, this paper explores the possibility of applying artificial intelligence (AI) and machine learning techniques such as neural networks to the security issue at hand. Information is one of the most valuable assets for any organization, and neural networks can exploit this advantage through in-depth analysis and informed decision-making.

There are numerous cases of successful applications of neural networks to real world problems. In terms of security, neural networks have been utilized in various industries to combat everything from terrorism to fraud. For example, the financial industry has been using neural networks to detect credit-card fraud since 1992, helping to cut fraud incidents by 50% (The Fair Issac Corporation, 2003). Traditionally, detecting fraudulent insurance claims was the responsibility of the claim's adjuster. But several insurance companies are now installing neural network fraud-detection systems to solve the problem (Balaji 2002). Using large volumes of history, the network learns patterns and trends in order to predict fraud on a larger scale, while at the same time, adapting to new criminal techniques. Using a scoring range of one to 1,000, investigators can focus their attention on those claims with the highest scores. These systems have proven effective by saving millions of dollars in fraudulent activity. For example, since December 1997, Texas Health and Human Services Commission (HHSC) has used the Medicaid Fraud and Abuse Detection System's (MFADS) neural network and learning technology to detect fraud, abuse or waste in the Texas Medicaid Program and resulted in cost savings of $72 million, in addition to the $3.4 million actual dollar amount recovered from suspected fraud in year 2000 alone (Window on State Government, 2003).

The objective of this study is to explore the possibility of applying neural networks as an early warning system to alert port authorities with cargoes of potential security fraud. In other words, when fed the appropriate data inputs regarding cargo containers, this system would "learn" the differences between potentially lawful and unlawful cargoes. Unlawful cargo would include forms of contraband such as untaxed cigarettes, infested fruit, counterfeit software, illegal immigrants, narcotics, drugs, "dirty bombs" (i.e., explosives filled with nuclear waste), weapons, and other terrorist devices. X-ray, radiation scanners, and cameras can only go so far as to detect these forms of contraband. A neural networks based early warning system will allow for port personnel

to focus their investigation efforts on cargoes that are more likely to contain contraband, which helps to improve detection efficiency and safety.

The balance of the paper is organized as follows: section two provides background information regarding the dynamics of modern day port security including potential risks and methods used by law enforcement in their efforts to mitigate high impact risks in conjunction with private business enterprise stakeholders. Different current and future potential methods of detection will also be discussed as this is a primary focus of Congress and the federal government as they seek ways to prevent another large scale attack in the country. Section three presents the basic concept of SOM network and illustrates its use as a data-reduction tool. This is followed by a discussion of the extended grouping capability. Due to the sensitivity and confidentiality of cargo data, simulated data sets will be used to demonstrate the potential of applying SOM to cargo security early warning systems. A classic real world clustering example will also be used to validate and compare the performance of SOM with three popular statistical clustering methods. Section four describes the data sets, the experimental design, and results from the SOM networks. The paper concludes with a summary of our findings.

Background Information

One of the more serious threats faced by the country today is the possibility of a nuclear device being detonated at a local port or transported from a local port further inland to another location for detonation. In a scenario analysis conducted by the Rand Corporation in July of 2006 "*a 10 kiloton nuclear explosion occurs on a pier in the Port of Long Beach causing a ground-burst explosion that would kill 60,000 people instantly, expose 150,000 more to almost certain death from hazardous levels of radiation. Infrastructure in the Los Angles & Long Beach ports would be completely destroyed including all docked ships*" (Mead and Molander, 2006). An estimated sixty million people would attempt simultaneous evacuation from the greater Los Angeles metropolitan area. Gas supplies would run critically short as one third of gas supplies west of the Rockies are supplied by refineries located at the Port of Long Beach. Port security thus ranks close to or at the very top of considerations that the federal government has in its threat assessment matrix.

AI based security systems are still relatively costly to purchase, implement, and maintain for small to medium size enterprises which comprise the bulk of the supply chain. These companies are thus reluctant to commit to them, as they would have to pass the cost on down to their customers. Only very large corporations and government agencies have the financial backing required to make the cost worth pursuing and maintain the system. The most popular applications of AI based security system are found in the financial services sector. Conventional banks, credit companies, mortgage lenders and investment companies have been using various forms of AI based systems to aid in fraud detection and prevention. Among them, the most popular AI techniques implemented is artificial neural networks.

Artificial neural networks (ANN) also known as connectionist models, parallel distributed processing models, neurocomputers, and artificial neural networks are a network of many simple highly interconnected processing units (also called neurons or nodes) operating in parallel. The processing unit responds to external inputs through dynamically change connection strengths between the nodes. The processing result is not stored or output to a specific memory location. It is represented by the overall state of the

network after it has reached some equilibrium condition. Knowledge within a neural network is acquired through a learning process. Knowledge is stored both in the way the processing units are connected and the strengths of inter-neuron connections.

For many centuries researchers have been trying to build intelligent computer systems that can perform daily routine of mankind for the purpose of replacing human from tedious tasks or hazardous work environment. Several problems have encountered in conventional artificial intelligence research. For example, human memory can store a huge amount of information and find relevant items very quickly that far exceed what the machine can do. To make intelligent computer systems requires an understanding of how human process information. The inspiration for neural network architecture originally came from studies of biological nervous systems. People have long recognized that human beings and animals are much better and faster at processing and recognizing speech and images than most sophisticated computers. The field of neural networks began as an approach to imitating human intelligence for building artificial intelligence systems that can learn from experience.

ANNs with their remarkable computational power can extract information and uncover meaningful trends from complicated and massive amount of data that are too complex to be processed by humans or other conventional computer techniques. For example, credit card companies are also able to prevent fraudulent activity on their customer's credit cards by using ANNs to map and predict a customer's purchase behavior and flag activities that are determined to be "suspicious" in nature by the ANNs. The Communications Fraud Control Association reported that fraud costs telecommunications carriers around the world $15 billion annually. NTL, the United Kingdom's No. 1 broadband company has won the fraud battle by implementing the Fraud Manager system, a neural network based system created by the Fair Isaac Corporation. According to the company, the Fraud Manager for Telecommunications installation had a direct impact on the company's bottom line, with a return on investment in just four months (The Fair Issac Corporation, 2003). Today, ANN's are used by many financial service providers in the US including American Express, Washington Mutual Bank, Wells Fargo and MasterCard. Even though success metrics are hard to come by, industry analysts all agree that the use of ANN's has enabled these firms to efficiently and

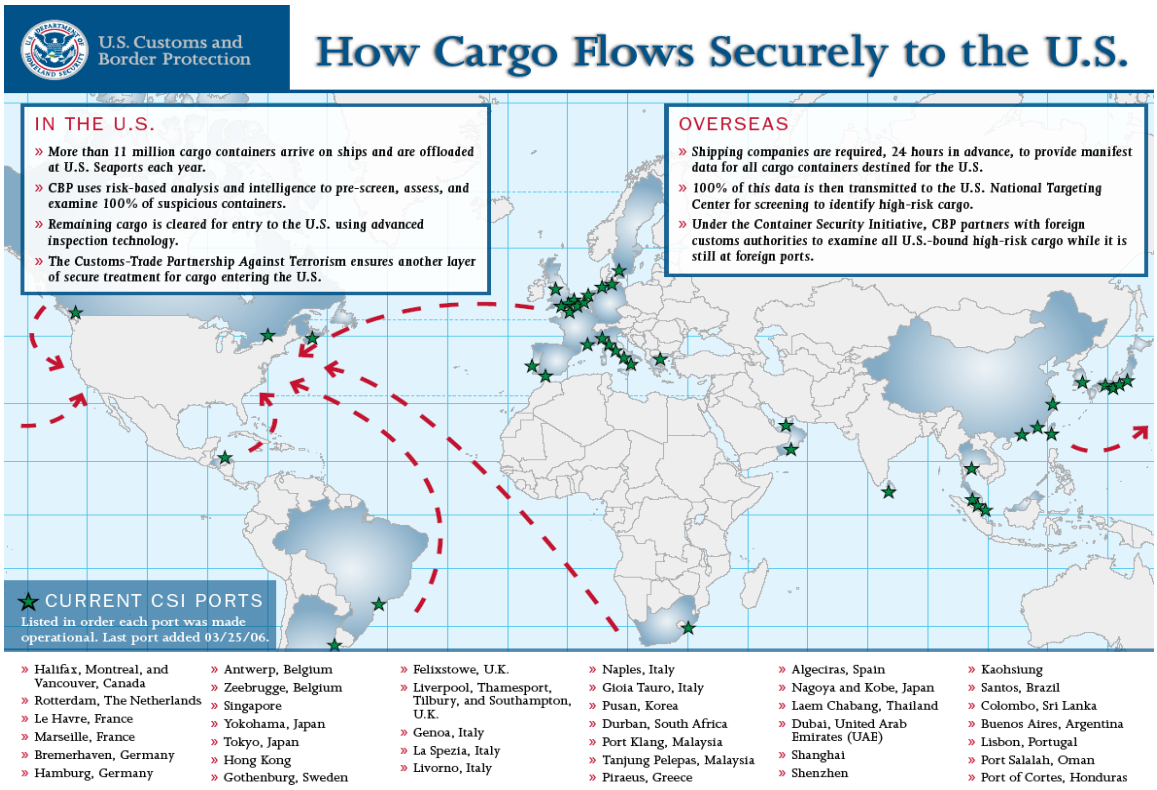
effectively cut down on fraud activity in turn realizing significant savings from losses of covering fraud charges on customer accounts (Balint 2005).

Artificial Intelligence in Port Security

It was not until after the activities of 9/11 those security analysts realized that artificial intelligence systems could greatly assist in the fight against fraud at ports. In a report published by Office of the President, the US Department of Homeland Security identified several critical mission areas where information technology can contribute 1) Intelligence and warning, 2) Border and Transportation Security, 3) Domestic Counterterrorism, 4) Protecting Critical Infrastructures and Key Assets, 5) Defending against Catastrophic Threats, and 6) Emergency Preparedness and Response (The White House, 2002).

Cargo screening presents logistical roadblocks to security analysts that are unprecedented. One only has to see the volume of cargo involved to understand how daunting the task cargo screening is. Ensuring the integrity of imported cargo is the most critical area of port security today. Nearly seven million marine containers from all corners of the globe arrive at U.S. seaports annually while eight million truckloads and about two million railcars arrive at U.S. border crossings a year. Of all this inbound cargo, only 2% is screened or searched before being allowed entry in the U.S. After 9/11 Customs and Border Protection (CBP) issued new requirements requiring freight carriers to report cargo manifests before reaching U.S. borders. Container ships must report shipment details on each container 24 hours before it is loaded at a foreign port (CBP.gov, 2008). Truckers from Canada and Mexico must report their trailers contents from 30 minutes to an hour before reaching a border crossing point. CBP analyzes the manifests and other intelligence to select certain containers and trailers to undergo physical inspection. Due to the volume of the traffic, it is not feasible to search every single cargo arrives at U.S. port. This is where the AI based screening system can come into play as the selection process is the most critical in keeping contraband from coming onshore. The AI based system can filter and identify high risk cargoes from low risk ones based on the patterns of unlawful cargoes found in historical data. Therefore, it allows the port officials to focus their attention on high risk cargoes based on certain key features. The

chart below describes the process of cargo flow highlighting the origin of cargo and processes occurring at those regions.



http://www.cbp.gov/linkhandler/cgov/import/cargo_control/cargo_flow_map.ctt/cargo_flow_map.pdf

Figure 1 How Cargo Flows Securely to the U.S.

After 9/11 U.S. law enforcement realized that they could not effectively guarantee the safety of arriving cargo and cargo in transit to and from the U.S on their own. Freight transportation is the backbone of international trade and involves a complex network of logistical and physical supply chains. Our review reveals there are no credible AI systems currently in use by either law enforcement or private sector that are specifically geared toward cargo screening. Advanced technologies such as improved screening/x-ray machines and biometric identification cards for port employees have been implemented recently to improve the port security. However, we have not seen any intelligent systems developed to help screening cargoes. Congress has taken a pro-active approach to this issue and has approved research funding through grants given by federal government agencies to research institutions to build viable AI systems that would aid in screening a much larger footprint of inbound cargo effectively.

It is important to note that fear of terrorists smuggling a dirty bomb is not the only driving concern warranting us to pay attention to port security. Every year tons of contraband is smuggled through U.S. ports by organized crime groups and shady businesses looking to make a quick buck. Popular contraband smuggled includes illegal narcotics, cigarettes, textiles, human cargo, vehicles and prescription medicines. These are only a handful of items in a list that include anything that is used by consumers.

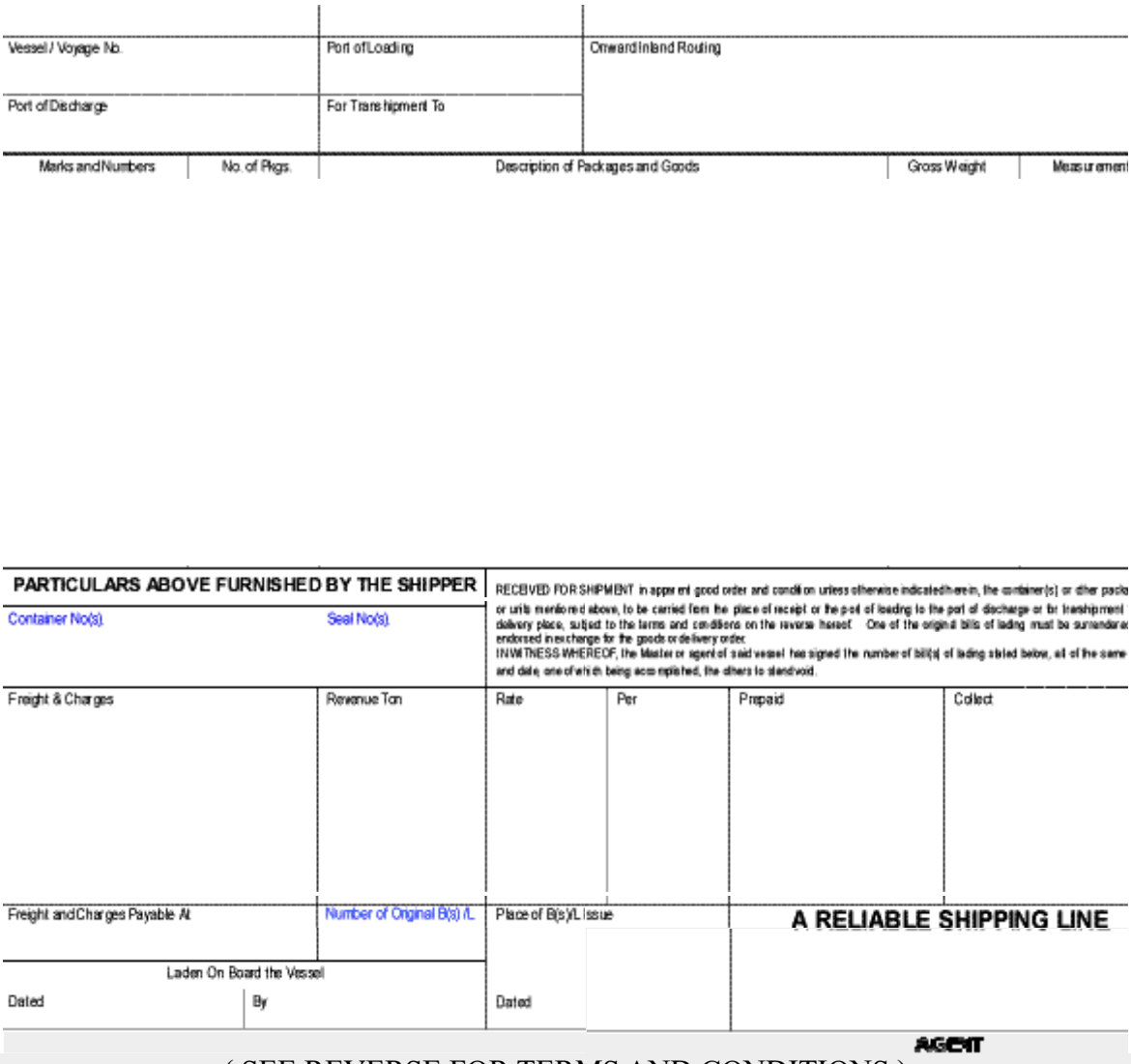
Contraband Detection/Fraud Prevention

Goods for export/import are packed into steel boxes commonly known as "containers" that measure twenty to forty feet in length. Once a container is full and goods ready to be transported, a bill of lading (BOL for ocean transport), waybill or consignment note (air, road, or rail transport), and a receipt (postal or courier delivery) must be completed. Collectively these are known as the "transport documents". The BOL must indicate that the goods have been loaded on board or shipped on a named vessel and it must be signed and authenticated by the carrier, or the agent of the carrier. A sample BOL is attached below:

A RELIABLE SHIPPING LINE

(NON-NEGOTIABLE UNLESS CONSIGNED TO ORDER)

	ORIGINAL	Bill of Lading No.
	Export References	
Consignee (Complete Name and Address)	Forwarding Agent - References	
	Point and Country of Origin of Goods	
Notify Party (Complete Name and Address)	Domestic Routing / Export Instructions (Additional Notify Party, Etc.)	
Pre-carriage By / Place of Receipt		



Vessel / Voyage No.	Port of Loading	Onward Inland Routing
Port of Discharge	For Transhipment To	

Marks and Numbers	No. of Pkgs.	Description of Packages and Goods	Gross Weight	Measurement

PARTICULARS ABOVE FURNISHED BY THE SHIPPER

Container No(s). Seal No(s).

RECEIVED FOR SHIPMENT in apparent good order and condition unless otherwise indicated herein, the container(s) or other packa
or units mentioned above, to be carried from the place of receipt or the port of loading to the port of discharge or for transhipment
delivery place, subject to the terms and conditions on the reverse hereof. One of the original bills of lading must be surrendere
endorsed in exchange for the goods or delivery order.
IN WITNESS WHEREOF, the Master or agent of said vessel has signed the number of bill(s) of lading stated below, all of the same
and date, one of which being accomplished, the others to stand void.

Freight & Charges	Revenue Ton	Rate	Per	Prepaid	Collect

Freight and Charges Payable At	Number of Original B(s) /L	Place of B(s)/L Issue	A RELIABLE SHIPPING LINE

Laden On Board the Vessel

Dated By Dated

AGENT

(SEE REVERSE FOR TERMS AND CONDITIONS)

http://www.export911.com/e911/ship/docBL.htm

Figure 2 Bill of Lading

Every shipping container has a container number. This container number is entered on the BOL. The shipper or the shipper's agent must seal the container before transferring it to the carrier. Each metal seal contains a number which is also entered on the BOL. If a seal is broken for customs purposes, a customs inspector must supervise the breaking of the seal and the resealing of the container. The new seal number replaced the previous seal number that was entered into the BOL. The "Notify Party" is the party that the carrier must notify when the goods at their destination port. The carrier issues an arrival notice informing the party that the goods have arrived including number of packages and discharge point. Some of the cargo security systems available today

include a monitor system that monitors individual container doors electronically where a security system sends an alarm once a container has been breached while in transit. To implement this on a large scale is currently not feasible as additional cost to carriers per container would be in the hundreds of dollars. All commercial lines on the high seas broadcast identification information to one another every 30 seconds by radio frequency. In 2005, the U.S. Coast Guard contracted with a private satellite communications company to relay the transmissions to them in real time from as far as 3,200 miles away for the possibility of early warning and prevention of any security fraud (Ianotta 2004).

The current cargo screening process still heavily relies on the port official's own knowledge and experiences. Due to the sensitivity of the task and the difficulty of transforming expert knowledge directly into rules that can be process by the computer, we believe the use of artificial intelligent system that can learn from historical data as well as incorporate existing expert knowledge possess high potential for developing cargo early warning systems. Based on the review of current port operation in screening cargoes, we have identified the following important factors that have been used as key indicators for potential security fraud:

Factors Impacting Fraud/Contraband Detection

1. Port of Origin

The port of origination of a shipping container is important as cargo can be traced back to the port of origination or loading, if a particular container causes concern while en-route to its destination port.

2. Shipping Line/Forwarder

The shipping company used to transport the goods to a destination port is important because shippers are a critical part of the supply-chain and the potential for collusion with criminal elements is real. Un-vetted and relatively new shipping firms should attract more scrutiny initially to ensure that they do not become the weak link in the chain.

3. Shipper/Exporter and Consignee

The two parties on the both ends of the shipping transaction are the main stakeholders in the transaction. If any contraband will be moved from one location to another, one or both of these parties would probably be aware of such a ploy. Law enforcement would carefully review the companies/individuals involved in the transaction to further ensure the integrity of the process.

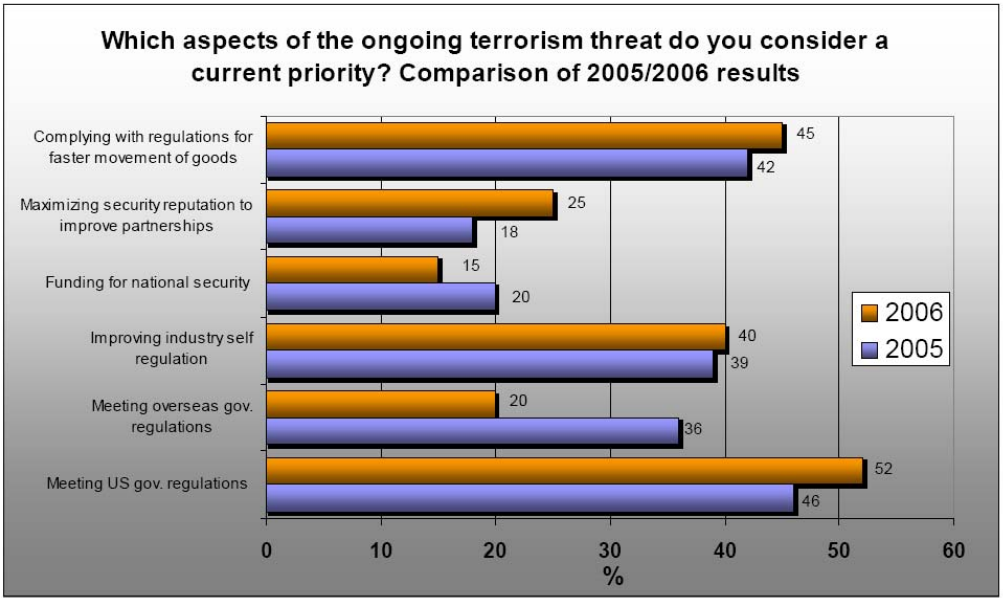
4. Nature of goods on manifest

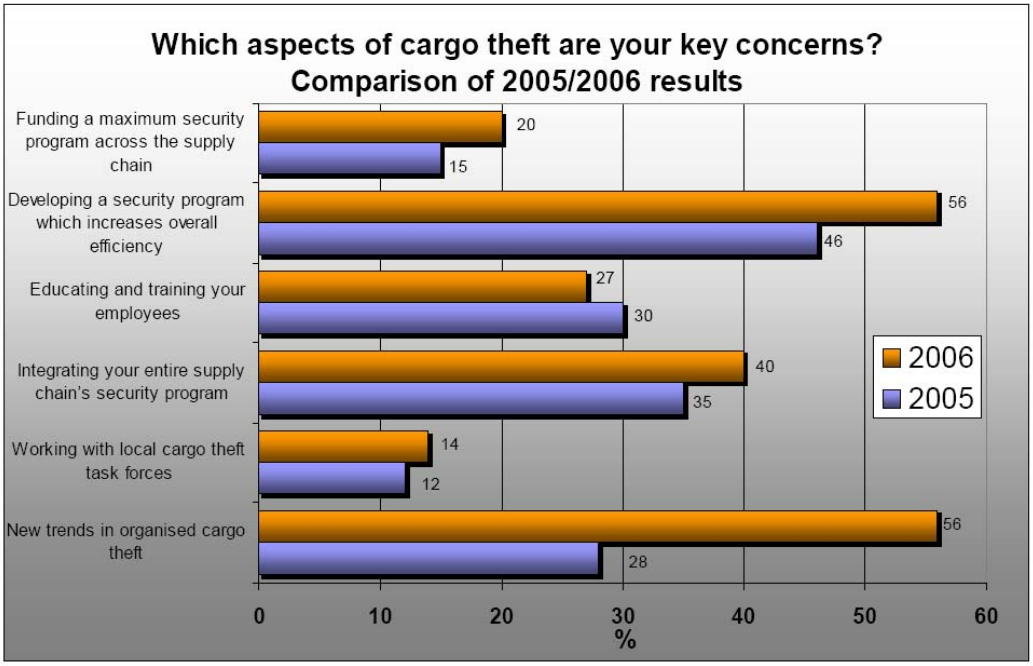
The actual goods being shipped would help in determining if a shipment should be flagged for inspection. Certain goods such as electronics, vehicles & medicines have a higher rate of theft/fraud and as such parties involved in exporting/importing such goods should be scrutinized carefully.

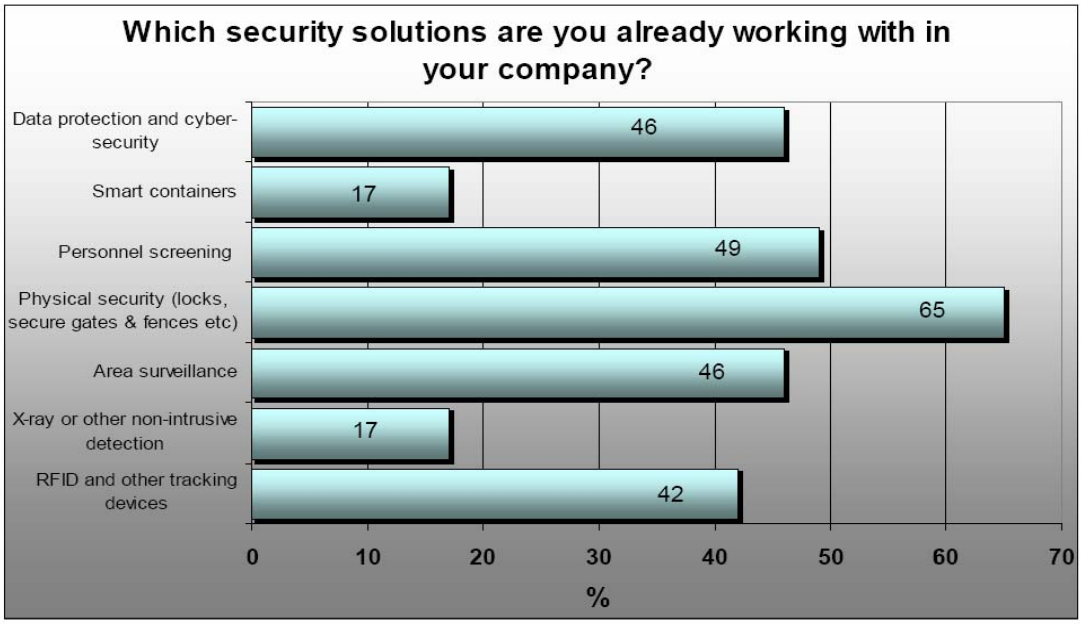
5. Nature of paperwork filed/filled out

The export/import process involves nearly 25 different pieces of documents and numerous parties in the supply chain. Companies/individuals that have been in the business are pretty proficient at having the requited paperwork. Missing documents and incorrectly filled out paperwork could possibly point to suspicious persons/companies trying to infiltrate the supply chain for criminal purposes.

There is clearly an awakening in port security considerations from both governmental organizations and the private sector. Traditionally, private sector was not actively involved in the security supply chain and preferred to leave this responsibility in the hands of the federal government. This has clearly changed as more and more companies realize that to have workable and comprehensive port security, all facets of the supply chain will have to be revamped in order to adapt to the new threats and increase efficiencies in the security apparatus. The following graphs, adopted from (Thomas 2006) were compiled from a survey of stakeholders in the supply chain excluding law enforcement and compares responses for 2005 and 2006.


Which aspects of the ongoing terrorism threat do you consider a current priority? Comparison of 2005/2006 results
Complying with regulations for faster movement of goods
45
42
Maximizing security reputation to improve partnerships
25
18
Funding for national security
15
20
Improving industry self regulation
40
39
Meeting overseas gov. regulations
20
36
Meeting US gov. regulations
52
46
2006
2005
0
10
20
30
40
50
60
%


Which aspects of cargo theft are your key concerns? Comparison of 2005/2006 results
Funding a maximum security program across the supply chain
20
15
Developing a security program which increases overall efficiency
56
46
Educating and training your employees
27
30
Integrating your entire supply chain's security program
40
35
Working with local cargo theft task forces
14
12
New trends in organised cargo theft
56
28
2006
2005
0
10
20
30
40
50
60
%



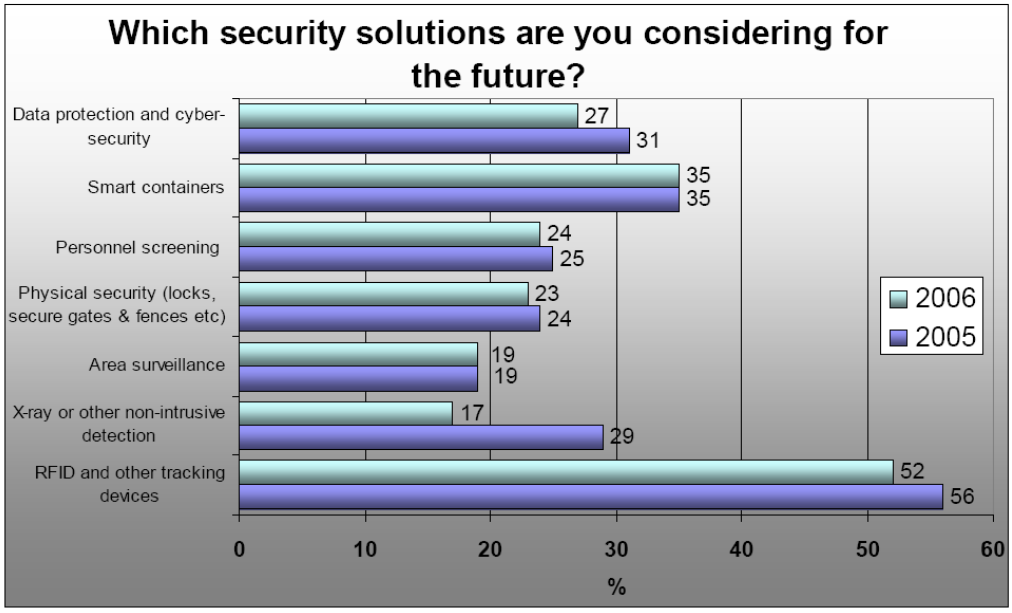


Figure 3 Cargo and Supply Chain Security Report

We have observed the following from the survey results shown above:

- There has been a 13.04% increase among transit companies in meeting U.S. government regulations concerning cargo security and transportation.

- When asked what aspects of cargo theft concerned them, there was a 100% increase in consensus that there were new trends in organized cargo theft. This realization that the "bad guys" have a new face and are using new and improved methods is a positive indicator as it will lead to increased security awareness and a willingness to invest in better cargo security measures.
- The survey shows that even though companies recognize the advanced methods of fraud, they are still using traditional methods of detection. Fewer than 20% of all surveyed are incorporating technology in their security systems, instead relying on manual screening and traditional physical security such as locks.
- On a more positive note, about 60% of those polled are considering technologically advanced security measures such as RFID tracking and smart containers.

On October 13th 2006, President Bush signed into law the SAFE Port Act. Security and Accountability For Every (SAFE) Port Act is a law that is designed to be pro-active in all aspects of port security. It addresses numerous current issues with port security and recommends remedies for them. But more importantly, it mandates that there be funding for more research & development going towards funding of AI projects and other types of contraband/fraud detection programs in addition to training exercises to be conducted at the ports. This will be a great incentive towards private sector technology firms in the design and creation of security systems as well as aligning everyone involved in port security to be on the same page – so to speak – when it comes to efficiency and readiness.

Research Methodology

Supervised vs. Unsupervised Learning

The two primary categories of learning algorithms for neural networks are supervised and unsupervised. In supervised learning, the network acquires knowledge by comparing the generated output with the known correct output. A set of training cases consisting of input data and corresponding output has to be available. The connection strengths are adjusted to tune the network over a number of training cycles. An example of supervised learning is a network being trained to recognize handwritten characters. On the other hand, in unsupervised learning, the network does not require the knowledge of corresponding output for comparison and learning. Input data presented to the network consists of the complex characteristics of the entities of interest. Through repeated training cycles the learning algorithm adjusts the connection strengths and causes the network to represent a simplified feature map of the characteristics from which meaningful information can be identified. An example of unsupervised learning is a network being trained to group customers into different market segments based on their purchasing behaviors.

Kohonen Self-Organizing Map (SOM) Network

SOM Network is a special type of neural network that can learn from complex, multi-dimensional data and transform them into visually decipherable clusters. The theory of the SOM network is motivated by the observation of the operation of the brain. Various human sensory impressions are neurologically mapped into the brain such that spatial or other relations among stimuli correspond to spatial relations among the neurons organized into a two-dimensional map (Kohonen 1995). The main function of SOM networks is to map the input data from an n-dimensional space to a lower dimensional (usually one or two-dimensional) plot while maintaining the original topological relations. The physical locations of points on the map show the relative similarity between the points in the multi-dimensional space.

Kohonen's SOM networks have been successfully applied as a classification tool to various problem domains, including speech recognition, image data compression, image or character recognition, robot control and medical diagnosis. It has also been

successfully applied to clustering problems such as market segmentation (Kiang et al., 2006).

The physical locations of points on the map show the relative similarity between the points in the multi-dimensional space. Each node on the map can be considered as a cluster by itself. An extension of SOM has been developed and tested by Kiang (2001) to further group the nodes into smaller number of clusters. This is especially useful when the number of output nodes is more than the number of desired clusters. The purpose of maintaining a reasonable size output map is to help the decision maker visualize the relationship among the input data in a less abstract manner. The fewer nodes we have on the map, the more abstract the output. The extended SOM technique enables the map to depict more detailed membership relationships between and within clusters while maintaining the capability of deriving any desired number of clusters.

Cluster Analysis using SOM

In cluster analysis, we try to identify similar elements by their attributes. We form groups, or clusters, that are homogeneous but are different from other groups. SOM networks combine competitive learning with dimensionality reduction by smoothing the clusters with respect to an a priori grid and provide a powerful tool for data visualization. Kohonen's SOM networks have been successfully applied to clustering problems such as gene research (Gibbons & Roth 2002; Herrero et al., 2001), text mining (Ciesielski et al., 2005), market segmentation (Kiang et al., 2006), MBA school selection (Kiang et al., 2008) and web search tools (Turetken and Sharda, 2005).

Cluster analysis is a technique for grouping subjects into groups of similar elements. In cluster analysis, we try to identify similar elements by their attributes. We form groups, or clusters, that are homogeneous and different from other groups. SOM networks combine competitive learning with dimensionality reduction by smoothing the clusters with respect to an a priori grid and provide a powerful tool for data visualization.

Unlike other neural network approaches, the SOM network performs unsupervised training; that is, during the learning process the processing units in the network adjust their weights primarily based on the lateral feedback connections. The more common approach to neural networks required supervised training of the network (i.e., the network is fed with a set of training cases and the generated output is compared

with the known correct output). Deviations from the correct output result in adjustment of the processing units' weights. On the other hand, unsupervised learning does not require the knowledge of target values. The nodes in the network converge to form clusters to represent groups of entities with similar properties. The number and composition of clusters can be visually determined based on the output distribution generated by the training process.

SOM Network Architecture

The SOM network typically has two layers of nodes, the input layer and the Kohonen layer. The input layer is fully connected to a two-dimensional Kohonen layer. During the training process, input data are fed to the network through the processing elements (nodes) in the input layer. An input pattern $\boldsymbol{x_v}$ (v = 1, … , V) is denoted by a vector of order m as: $\boldsymbol{x_v} = (x_{v1}, x_{v2}, \ldots, x_{vm})$, where x_{vi} is the *i th* input signal in the pattern and m is the number of input signals in each pattern. An input pattern is simultaneously incident on the nodes of a two-dimensional Kohonen layer. Associated with the N nodes in the n x n ($N = n$ x n) Kohonen layer, is a weight vector, also of order m, denoted by: $\boldsymbol{w_i} = (w_{i1}, w_{i2}, \ldots, w_{im})$, where w_{ij} is the weight value associated with node i corresponding to the *j th* signal of an input vector.

As the training process proceeds, the nodes adjust their weight values according to the topological relations in the input data. The node with the minimum distance is the winner and adjusts its weights to be closer to the value of the input pattern. In this study, Euclidean distance, the most common way of measuring distance between vectors, is used.

Weight Adaption Function

A Gaussian type of neighborhood adaptation function, which decreases both in the spatial domain and the time domain, has been proposed (Lo and Bavarian 1991). Lo and Bavarian (1991) have shown that an algorithm that uses the Gaussian type function will enforce ordering in the neighborhood set for every training iteration, yielding faster convergence. They modified Kohonen's adaptation rule to include the amplitude of neighborhood adaptation $A_i(t)$ as follows:

$\boldsymbol{w_i}(t+1) = \boldsymbol{w_i}(t) + \alpha(t)\, A_i(t)[\boldsymbol{w_i}(t) - \boldsymbol{x_v}]$, for $i \in N_i(t)$, $0 <= r <= R$

$\boldsymbol{w_i}(t+1) = \boldsymbol{w_i}(t)$, otherwise.

Figure 1 shows the architecture of a *4 x 4* Kohonen layer and the definition of neighboring nodes with radial distance (r) = 1. In general, the farther a node is from the winner, the lower is the amplitude A_i and hence the lower is the update rate of the node's weight vector. For $\alpha(t)A_i(t)$ above, we use a Gaussian type neighborhood adaptation function $h(t, r)$, similar to the one used by Mitra and Pal (1994). This function decreases in both spatial and time domains. In the spatial domain, its value is the largest when node i is the winner node and it gradually decreases with increasing distance from i.

$$h(t,r) = \frac{\alpha(1 - r * f)}{\left[1 + \left(\frac{t}{cdenom}\right)^2\right]}$$

where r is the radial distance from the winner node i. Nodes within a radius R are considered for adaptation at time t. Hence, $0 <= r <= R$ if $i \in N_i(t)$. R itself decreases over time and thus fewer and fewer neighbors are updated every iteration. Parameter α determines the initial value of $|h|$. The parameter f ($0 < f < 1/r$) determines the rate of decrease of $|h|$ in the spatial domain. In the time domain, t controls the value of $|h|$ whereas the parameter *cdenom* determines the rate of its decay.

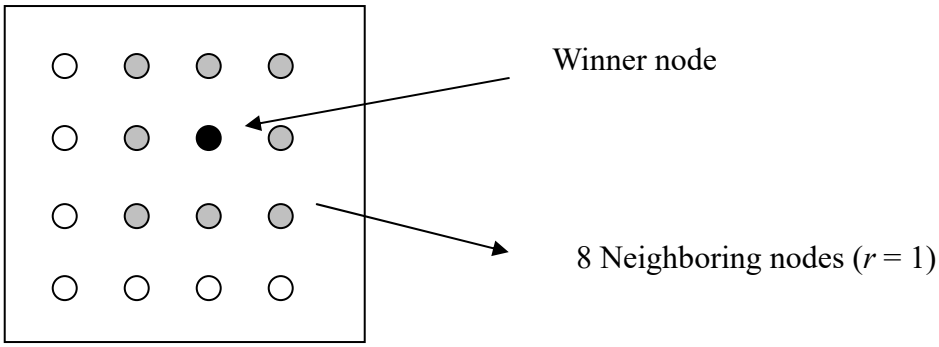


Figure 4. A *4 x 4* Kohonen Layer and neighboring nodes with radial distance (r = 1)

The Self-Organization Process

The network undergoes a self-organization process through a number of training cycles, starting with randomly chosen $\boldsymbol{w}_i$'s. During each training cycle, every input vector is considered in turn and the winner node is determined. The initial value of R is determined by trial and error and is influenced by the size of the network. Kohonen suggests that the initial size of the neighborhood should be the size of the network itself in order to minimize the effect of initial random weights assigned to the nodes. We

followed his recommendation and always set the initial value of R large enough to cover the whole network. The training is conducted in many stages; at each stage, we reduce R by one. Note that R affects the number of nodes in the set N_i. To determine the number of training cycles to be run at each stage, we use the index of disorder D proposed by [Mitra and Pal 1994]. Essentially, D measures the "improvement" in the "state" of the network at discrete time intervals. The state of the network is denoted by the mean-squared-distance, *msd,* between the input vectors and the weight vectors of the nodes in the set N_i.

$$msd = \frac{1}{|trainset|} \sum_{x \in trainset} \left[\sum_{r=0}^{R} \left\{ \left(\frac{1}{|Nr|} \sum_{i \in Nr} \|x - m_i\|^2 \right) * (1 - r * f) \right\} \right]$$

where *trainset* is the training set number and N_r is the number of the set of nodes that are distance r away from the winner node. Note that the nodes closer to the winner node contribute more to *msd*. Due to the converging property of the weight adaptation mechanism, the value of *msd* decreases monotonically with proper choices of α, *f,* and *cdenom* parameters. *msd* is measured at an interval of every k cycles. The index of disorder D is simply the improvement in *msd* between two consecutive measurements. When this index falls below a certain threshold ($D <$ *convergence coefficient* δ), the next stage of training begins with a reduced R value. Reader may refer to (Mitra and Pal 1994) for the detailed algorithm.

Conscience Mechanism

In a self-organized map, a few nodes may end up representing too much of the input data due to the effect of the initial random weight values assigned to them. To avoid this, we use a “conscience” mechanism that prevents the nodes with higher winning frequency from winning repeatedly and makes the nodes with lower winning frequency more likely to win. The purpose of this mechanism is to give each node in the Kohonen layer an opportunity to represent approximately equal information about the input data.

The conscience mechanism that we use is proposed by DeSieno (1988). It adjusts the Euclidean distance between a node's weight vector and the input vector $||\boldsymbol{x}_v - \boldsymbol{w}_i||$ by a bias B_i. B_i is proportional to the difference between the node’s winning frequency and the average winning frequency:

$$B_i = \gamma\left(\frac{1}{N} - F_i\right).$$

F_i is the winning frequency of node i and is updated at every iteration of the training process. Initially, F_i is assigned the average value 1/N; thus $B_i = 0$. The γ coefficient starts at a large value and decreases over time. The winning frequencies are updated as:

for the winning node: $F_{i,t+1} = F_{i,t} + \beta\ (1.0 - F_{i,t})$,

for all other nodes: $F_{i,t+1} = F_{i,t} + \beta\ (0.0 - F_{i,t})$,

where β is a small positive fraction. In this study, we set the value of β fixed at 0.1, a number in the range of appropriate values suggested in previous research.

The Contiguity-Constrained Clustering Method

The output from SOM networks is a two-dimensional map (Kohonen layer). Each node on the map may represent zero to many input data. The input data that are similar in higher dimension should be close to each other on the output map. We can consider each node on the output map as one group and cluster the input data accordingly. However, this type of Kohonen network usually has many nodes in the output layer. For example, a network of size 10x10 will have total 100 nodes in the output layer. When the number of nodes on the map is more than the number of clusters we desire, additional procedure to further group the nodes into fewer number of clusters is required. One way to do it is to manually group the points into clusters. Often times it is hard to visually group the output from SOM especially when the map is highly populated. Hence, a more scientific approach that can help user to group the output from SOM network based on certain objective criteria is needed. In this research, the extended SOM network method developed by (Kiang 2001) will be implemented to automate the segmentation process to complement the usage of the Kohonen SOM networks. The method groups the output from SOM based on a *minimal variance criterion* to merge the neighboring nodes together. The rationale is that the SOM networks will maintain the original topological relations; therefore the nodes that are closely located on the representational grid should have similar cluster centers. We start with each node in the map representing one group, and calculate the centroid of each group. Then we try to merge two neighboring groups

so that the result of the merger will maintain the global minimal variance for that number of clusters. The merge process is repeated until a user specified number of clusters has derived or when only one cluster remains. The detailed process is described in the following (adopted from Kiang 2001):

Step 1. For each $node_i$, calculate the centroid (C_i) of $node_i$ as

$$C_i = \frac{1}{|node_i|} \sum_{x \in node_i} \vec{x} .$$

where | $node_i$| is the number of input vectors associated with the node.

Step 2. Assign a group number (G_k) to each $node_i$ if $|node_i| > 0$, and update the corresponding centroid value G_k.

Step 3. Calculate the overall variance of the map:

a) Sum the square distance between input vector x and the group centroid C_k for all x in G_k.. Calculate for every group k.

$$V_k = \sum ||x - C_k||_2, x \in G_k .$$

b) Total the variances from all groups. This will give us the global variance of the map:

$$V_{Total} = \sum V_k .$$

Step 4. For each pair of neighboring groups, calculate the total variance of the map if the two groups were merged. Merge the two groups that result in the minimum global variance.

a) Calculate the new centroid for G_{pq} if G_p and G_q were merged:

$$G_{pq} = (|G_p| * \vec{G}_p + |G_q| * \vec{G}_q) / |G_p| + |G_q| .$$

b) Calculate the new variance if G_p and G_q were merged (modified from [Murtagh 1995]):

$$V_{pq} = \sum ||x - C_{new}||, \text{ for all } x, x \in G_p \text{ or } x \in G_q .$$

c) Calculate the new global variance for merging G_p and G_q:

$$V_{pqTotal} = V_{Total} + V_{pq} - V_p - V_q .$$

d) Calculate the $V_{pqTotal}$ for every pair of p and q on the map. For each iteration, groups p and q must be within a fixed radial distance on the grid. We start with radial distance = 1, hence for each node there are

eight neighboring nodes within that distance (see Figure1). We increase the radial distance by one each time if there is no neighboring group within current radial distance for all groups k. Finally, we merge the two groups that result in global minimal variance.

e) Update V_{Total} and the group number and group centroid of the two newly merged groups.

Step 5. Repeat step 4 until only one cluster or the pre-specified number of clusters has been reached.

SOM Training Process

During the training process, many features and characteristics of the cargo containers will be collected for evaluation. In this research, we have identified the following important features: 1) port and country of origin, 2) shipping line/forwarder, type, 3) shipper/exporter and consignee, 4) nature of goods on manifest, and 5) nature of paperwork files/filled out. This information is available through existing documents such as the shipper's Letter of Instructions, commercial invoices, the Certificate of Origin, and the carrier's Bill of Lading. Once these data points are captured for a sample of containers, they will be flagged as containing suspicious or safe cargo based on historical records where illegal substances were found. The data will then be used to train the neural networks to group legitimate and illegitimate cargoes. As the system becomes more accustomed to recognizing the differences, it can better perform clustering and classification functions, which can later be validated through physical inspection. Once implemented, the early warning system will have the ability to profile high-risk shipments that will warrant physical inspection. Major advantages of neural networks include the ability to learn, self-organize, make generalizations, and avoid mistakes that maybe more likely through human intervention. The learning capability of the neural networks allows the model to automatically adjust itself according to the new data, thus can substantially reduce the budgets and personnel that would normally require in maintaining the system.

The Experimental Design

Because this study is a preliminary investigation of the applicability of SOM to cargo security warning system, we decided to first focus on artificially constructed data. Knowledge of the true data generating mechanisms (the correct cluster membership for each observation) is essential for valid comparisons with respect to the accuracy with which SOM recovers the true cluster structures. To test the effectiveness of SOM on problems with data of different characteristics and distribution, we randomly generated three data sets: compact, closer, and unequal. Compact data set contains data with well-separated compact clusters; Closer data set contains data with poorly-separated compact clusters; and Unequal data set contains data with compact clusters of unequal size. Next, we compare the performance of SOM with three statistical clustering methods to further validate the applicability of SOM to real world clustering problems using a classic clustering analysis data set, the Iris plants database.

Samples Generation and Experiment Results

Compact Data Set

A total of 150 random observations were generated that contains 5 observed variables, to match with the 5 important factors impacting fraud/contraband detection we identified, are equally distributed among the three segments (clusters), low, medium, and high risk. We fixed the initial values of all parameters in the network to simplify the network tuning process (Mitra and Pal 1994). Previous research has shown that the performance of SOM networks is less sensitive to changes in the parameter settings relative to other types of neural networks (Kohonen 1995). Based on our experience with SOM, the network parameters we selected consistently perform satisfactorily (with data samples from various problem domains) on the following criteria: the ability to converge properly and the ability to produce meaningful clusters or maps. Proper convergence is characterized by a monotonically decreasing value of a measurement of the mean square distance between the input vectors and the weight vectors of the nodes in the set N_i, such that the network does not keep oscillating between a set of states and never converging to a final state. A too sudden convergence may indicate the possibility of a sub-optimal state attained by the network. Meaningful maps are those that do not exhibit problems

such as one or a few nodes representing too many entities, or a majority of winning nodes bunching into a small portion of the map, prohibiting any meaningful clustering.

In this study, we implemented the algorithm in C++. This language was selected for its object-oriented approach and its generality to other object-oriented algorithms. The code was verified by independently testing specific components and comparing computer-generated results with hand calculations. Each processing unit in the network and each input pattern were implemented using objects. All calculations are performed through message passing between objects in the program. Small networks were used to verify the overall program, again, by comparing computer-generated results with hand calculations. Version 9.1 of the SAS Statistical package was used to generate the data set.

Experiment Result for Compact Data Set

An initial set of experiments is conducted to determine an appropriate configuration for the SOM network. During this stage, various network configurations were tested. The final values of the network parameters set for the SOM network are: network size 9 x 9, $\alpha = .25$, and starting r = 4.0 and decreasing over time along with the neighborhood size (R). Figure 5 is the output map from SOM network that shows the distribution of cargoes and their corresponding risk levels. We grouped the cargoes into three risk levels: high, medium, and low risks. The cargoes fall in the high risk area have higher risk of security fraud based on historical information and need to be monitored more closely. For the cargoes in the medium risk group, the ones that are closer to the high risk areas also need to be monitored more closely than the ones near the low risk area. The cargoes in the low risk area will require least attention. The output map can assist the port officials in determining how to best allocate their limited resources while not scarifying the security and safety of the port and its nearby metropolitan area.

After the network is trained, every time when there is new cargo data available, it can be input to the trained network to calculate the location of the new cargo. If the cargo falls in the “High Risk” area, the system will send a warning signal to alert the port official for the possibility of security fraud. The system can continue to learn and adapt itself to the new data presented to the system.

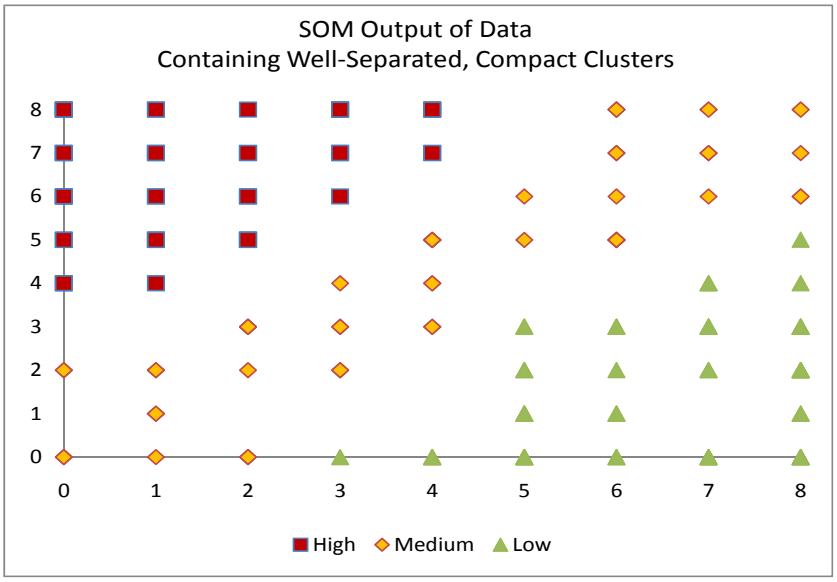


Figure 5 SOM output of the Compact data set

Closer Data Set

Again, a total of 150 random observations were generated that contains 5 observed variables, to match with the 5 important factors impacting fraud/contraband detection we identified, are equally distributed among the three segments (clusters), low, medium, and high risk. However, the data sets are poorly separated. The same network parameters were implemented and the results are shown in Figure 6.

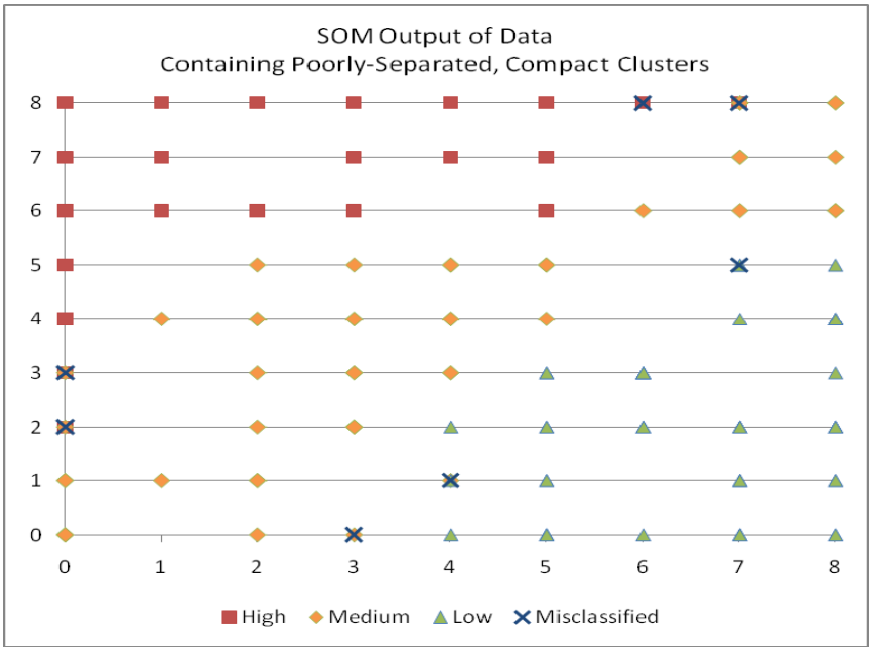


Figure 6 SOM output of the Closer data set

The map shows that some of the data points at the borders are overlapping between two groups. However, the map still provides a very good picture of the distributions of different risk cargos and can assist decision makers in determining cargo risk level when given new cargo information.

Unequal Data Set

Last, a total of 140 random observations were generated that contains 5 observed variables, to match with the 5 important factors impacting fraud/contraband detection we identified. The distributions of the observations are 20 high-risk, 40 medium-risk, and 80 low-risk. The same network parameters were implemented and the results are shown in Figure 7.

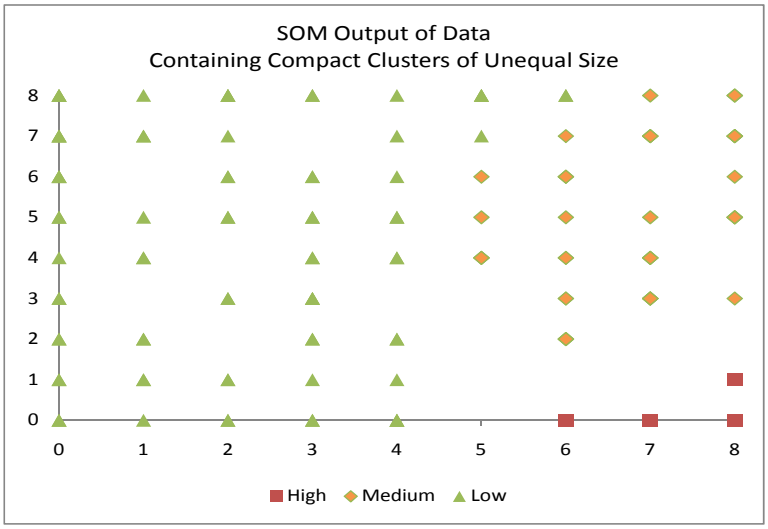


Figure 7 SOM output of the Unequal data set

It shows that SOM can successfully separate data points from the three different risk groups when there is unequal distribution in the data set. In real world situation, the number of high risk cargos is usually much smaller than the number of low and medium risk cargos. The result shows that unlike some statistical tools that require adjustment to data when unequal sample sizes are presented, SOM network can work well with unequal size sample without any additional steps for data preprocessing or adjustment.

In the following, we compare the SOM network with three statistical clustering methods, both parametric and nonparametric approaches, using a classic clustering analysis data set, the Iris plants database. The three statistical clustering methods are: *k*-

means analysis, a popular clustering method based on the least squares criterion, the Ward's minimum variance cluster analysis, and a nonparametric (or distribution-free) method supported by SAS MODECLUS procedure.

The Iris Plants Database

The database was created by R. A. Fisher [Fisher 1936] and has been since widely used in subsequent research in pattern classification [Duda & Hart 1973, Dasarathy 1980]. The data set contains three classes of 50 instances each, where each class refers to a type of iris plant. The three classes are: Iris Setosa, Iris Versicolour, and Iris Virginica. The first class is linearly separable from the other two; the latter are not linearly separable from each other. There are four numeric attributes and no missing value. The four attributes are: 1) sepal length in cm, 2) sepal width in cm, 3) petal length in cm, and 4) petal width in cm. Table 1 is a brief statistical analysis of the sample attributes.

Table 1. Statistical analysis of the Iris Plants sample attributes

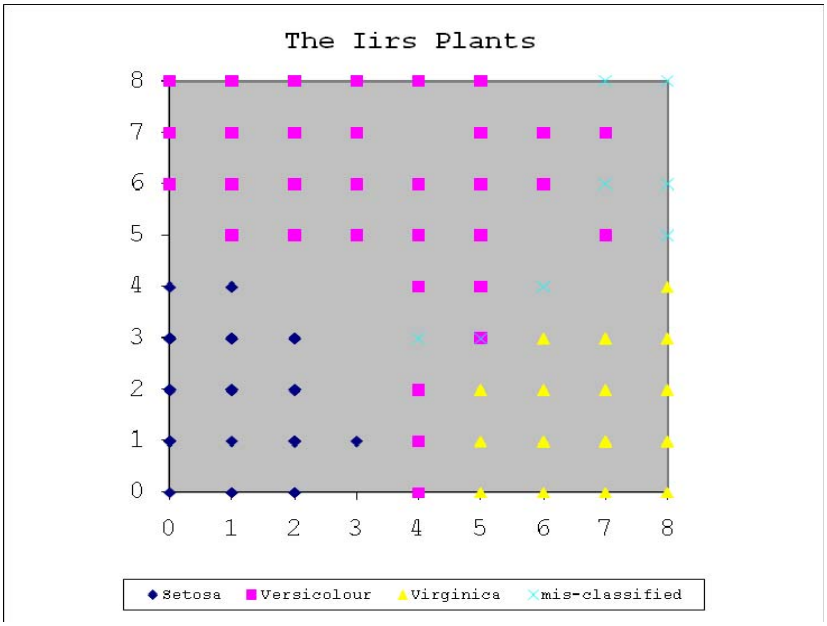
Attribute	Min	Max	Mean	Standard Deviation
sepal length	4.3	7.9	5.84	0.83
sepal width	2.0	4.4	3.05	0.43
petal length	1.0	6.9	3.76	1.76
petal width	0.1	2.5	1.20	0.76

For this experiment, the network size of 9 x 9 was used and the result was compared with that of the other three statistical approaches. Table 2 summarizes the experiment results.

Table 2. Performance comparison of the extended SOM and the three statistical clustering methods using the Iris database

Method	Rate of Correctness
SOM	90.34%
k-means Analysis	88.67%
Ward's	88.67%
MODECLUS	88.67%

The results show that the performance of the extended SOMS method is better than that of the three statistical methods. Figure 8 shows the output map of the Iris Plants.



*Each point in the figures represents one or more observations.

Figure 8 Output map of the Iris Plants Data

One of the reasons that Iris plants database was selected was because it contains three clusters similar to the three groups of cargo risk levels we attempt to identify. Although the three types of Iris plants does not possess the same ordinal relationship of low, medium, and high risks, the output map does help us to understand how to use the map to identify three clusters and the possibility of fuzzy cluster membership of the data points on the borderlines separating two groups. For example, some of the data points belong to Virginica were misclassified as Versicolour as shown in Figure 5. For cargo security early warning system, the borderline cases won't be a problem since we are not interested in identifying three distinct groups of low, medium, and high risk cargoes. We are more interested in screening and focusing attention on higher risk cargoes. Different colors representing different security risk can be assigned to each cargo to alert the port official of potential cargo security threat.

Conclusions and Recommendations

In this study, we explore the possibility of applying neural networks as an early warning system to alert port authorities with cargoes of potential security fraud. The system will allow port personnel to focus their investigation efforts on cargoes that are more likely to contain contraband and helps to improve detection efficiency and safety. We first presented background information regarding port security. It includes current practice and technology development in the port security contraband detection and fraud prevention. Five important factors were identified as key features to determine the potential of cargo security fraud. They are: 1) port and country of origin, 2) shipping line/forwarder, type, 3) shipper/exporter and consignee, 4) nature of goods on manifest, and 5) nature of paperwork files/filled out. Both simulated data set and the classic Iris plants database are used to demonstrate the potential of applying SOM network to separate high risk cargoes from low risk ones.

Predictive models based on statistical techniques have been widely adopted and some techniques perform reasonably well in terms of rate of correctness in their predictions. However, all methods require complex and advanced analytical skill to explain and interpret the output from the prediction model. In this study, we introduce a special type of neural networks, the Self-Organizing Map (SOM) Network that can learn from complex, multi-dimensional data and transform them into visually decipherable clusters on an output map. A salient feature of using SOM method over the other approaches is the added visual map. The 2-dimensional plot provides an easy-to-read graphical interface that does not require specialized analytical knowledge to interpret the results. It is a valuable decision support tool that helps the port personnel visualizes the relationships among inputs. Therefore, the port personnel can interactively determine the composition of the clusters using the output map of SOM and incorporate subjective criteria when desired. .

Due to the scarcity/confidentiality of historical cargo data with contraband found at Long Beach Port, we were not able to test our system using real-world data. However, the simulated data sets allow us to know the true cluster membership of the data points hence can validate the accuracy of the cluster outcome from SOM. A classic real world

case of Iris plants database is also used to compare the clustering performance of SOM to three popular statistical clustering techniques. In our future research, we would like to collaborate with the port officials and seek the possibility of obtaining cargo data to train and test the proposed cargo security early warning system.

We have seen that current port security is improving and more effort will be needed going forward to reduce the risk threshold. This process however must not lose focus of reality. There is no "fail safe" solution to port security. We must understand that ports cannot be protected 100% and security breaches will always occur. However, artificial Intelligence systems are much more efficient and accurate than human experts alone and will also enable ports to conduct security operations without halting or seriously disrupting the flow of cargo which could very well doom the ports and the country's economy. Neural networks are but one of many technological solutions being sought today to combat the issue of port insecurity, theft and contraband entry into the country.

Implementation

We recommend the following phases to implement the port early warning system:

Phase I - Data Identification

Phase I of the implementation requires input and expertise from port officials and support staff at the Long Beach Port. Time will be spent at the port to understand more about the problems and relevant factors. This is an evolving and iterative process. More key factors may be identified and analyzed in later phases.

Phase II - Data Collection and Analysis

Phase II involves further exploring of the data sources for collecting the key factors identified during Phase I of the project. Data will be collected and analyzed for its quality before used for network training. This includes checking for percent of missing data and chances of entry errors. It may require transforming the data into proper format before it can be further processed. Once the data have been validated, the importance of each factor collected will be tested and data characteristics be analyzed.

Phase III – Training and Testing of the System

The SOM networks will be trained and tested with real world data. Preliminary training and testing cases will be generated to determine the SOM network configuration. Data will be pre-processed if needed. Complete training and testing cases will be developed and implemented toward the end of this phase.

Phase IV – Result Analysis

Finally, output maps derived from SOM networks will be evaluated and analyzed. The SOM system may be put into practice using new data in order to effectively predict outcomes related to contraband detection. These predictions may need to be manually validated using historical data and human oversight.

References

Balaji, Laki, "Insurers tackle fraud with technology," Risk Management, Oct 2002, http://findarticles.com/p/articles/mi_qa5332/is_200210/ai_n21319223, last visited on June 11, 2008.

Balint, Kathryn, "Fraud fighters, Fair Isaac Corp. products protect consumers, companies," SignOnSanDiego.com, the Union-Tribune, Feb. 18, 2005.

CBP.gov, "C-TPAT: Customs-Trade Partnership Against Terrorism," U.S. Customs and Border Protection- Securing America's Borders, *http://www.cbp.gov/xp/cgov/import/commercial_enforcement/ctpat/,* retrieved on March 12, 2008.

Ciesielski, K., M Dramiriski, MA Klopotek, M, "On Some Clustering Algorithms for Document Maps Creation," *Intelligent Information Processing and Web Mining,* 2005.

DeSieno, D., "Adding a Conscience to Competitive Learning ," *Proceedings of the International Conference on Neural Networks*, IEEE Press, New York, Vol. I, July 1988, pp. 117-124.

Gibbons, F.D., Roth, F.P., "Judging the Quality of Gene Expression-Based Clustering Methods Using Gene Annotation," *Genome Research,* 2002, Cold Spring Harbor Lab.

Grossberg, J.," No safe harbor for smugglers," *Daily Breeze*: A1, A8, April 9, 2006.

Herrero, J., A Valencia, J Dopazo, "A hierarchical unsupervised growing neural network for clustering gene expression patterns," *Bioinformatics*, 2001, Oxford Univ Press.

Ianotta, Ben, "Satellites Could Help Identify and Track Threats From Sea," *Space News Correspondent*, http://www.space.com/spacenews/archive04/seaarch_083004.html, 30 August 2004.

Kiang, M.Y., "Extending the Kohonen Self-Organizing Map Networks for Clustering Analysis," *Journal of Computational Statistics and Data Analysis (CSDA),* 38(2001) pp. 161-180.

Kiang, Melody Y. and D. Fisher "Selecting the Right MBA Schools -- An Application of Self-Organizing Map Networks," *Expert Systems With Applications*, 2008.

Kiang, Melody Y., M. Hu, and D. Fisher "An extended self-organizing map network for market segmentation—a telecommunication example," *Decision Support Systems*, Vol.42, No.1, Oct 2006, pp.36-47.

Kohonen, T. (1995). *Self-Organizing Maps*, Springer.

Meade, Charles and Roger C. Molander, *"Considering the Effects of a Catastrophic Terrorist Attack,"* The Rand Corporation, July 2006.

Mitra, S. and S.K. Pal, Self-Organizing Neural Network as a Fuzzy Classifier, *IEEE Transactions on Systems, Man, and Cybernetics*, Vol. 24, No. 3, pp. 385-399, March 1994.

Murtagh, F. "Interpreting the Kohonen self-organizing feature map using contiguity-constrained clustering," *Pattern Recognition Letters*, Vol. 16, April 1995, pp. 399-408.

Lo, Z.-P. and B. Bavarian, "On the rate of convergence in topology preserving neural networks," *Biol. Cybern.,* Vol. 65, 1991, pp. 55-63.

The Fair Issac Corporation, *"*Leading UK Telecom Company winning fraud battle with neural network," *View Points, News, Ideals, and Solutions from Fair, Issac,* March/April 2003.

The White House, "The National Strategy for Homeland Security: Office of Homeland Security," Office of the President, http://www.whitehouse.gov/homeland/book/, July 2002.

Thomas, David, "Summary and analysis of eyefortransport's survey: Cargo and Supply Chain Security Trends," http://www.loginstitute.ca/files/pdfs/cargo_sec_2006_report.pdf, July 2006.

Turetken, Ozgur and Sharda, Ramesh, "Clustering-Based Visual Interfaces for Presentation of Web Search Results: An Empirical Investigation," *Information Systems Frontiers,* 7, 3, July 2005, pp. 273-297.

Window on State Government, Susan Combs Texas Comptroller of Public Accounts, Special report, March 2003, (http://www.window.state.tx.us/specialrpt/hcc2003/section1/2activities.html#fn24), last visited June 11, 2008.