AirSIMS: A Simulator and Executor for a Safer Airport Environment

Felix Keng Fong Cheong
Kelly Jung
Scott Moura
Wai Leung William Wong

December 9, 2005

Abstract

The 9-11 tragedy has raised the attention to improve airport security. Looking into four specific areas of potential terrorist attacks, we propose a comprehensive airport security system called AirSIMS. Our goal is to provide a complete solution to airport security that is cost effective, adaptable, and immediately responsive to terrorist attacks. AirSIMS is composed of four modules: E-Passport identification, structural-health monitoring, population mobility monitoring, and counter bio-terrorism. These modules make use of the Smartcard technology, cryptography, sensors, and cameras. Gathered data is sent to AirSIMS' central processing system through a wireless sensors network. The system analyzes the data and optimizes the airport operations accordingly. Specifically AirSIMS calculates the safest possible evacuation route. The details of wireless sensors, algorithms, and actions taken by AirSIMS are explained in this paper. Synchronizing the four modules as a whole, AirSIMS is the all-in-one solution to airport security which minimizes highly organized terrorist attacks.

Table of Contents

Table of Figures

AirSIMS: A Simulator and Executor for a Safer Airport Environment

Introduction

Airport security has become one of the biggest security concerns for the US government since the September 11 attack, and improving airport security has become top priority. We propose a system called AirSIMS that simulates and monitors activity within an airport in order to create a more secure environment. AirSIMS is a reliable network which best suits today's requirements consisting of four modules: E- Passports, Structural Health Monitoring, Population Movement, and Bio-terrorism. AirSIMS divides these modules into Sensors, Diagnostics, Simulation Algorithms, and Actions. Figure 1 shows the processes that AirSIMS follows for our modules.

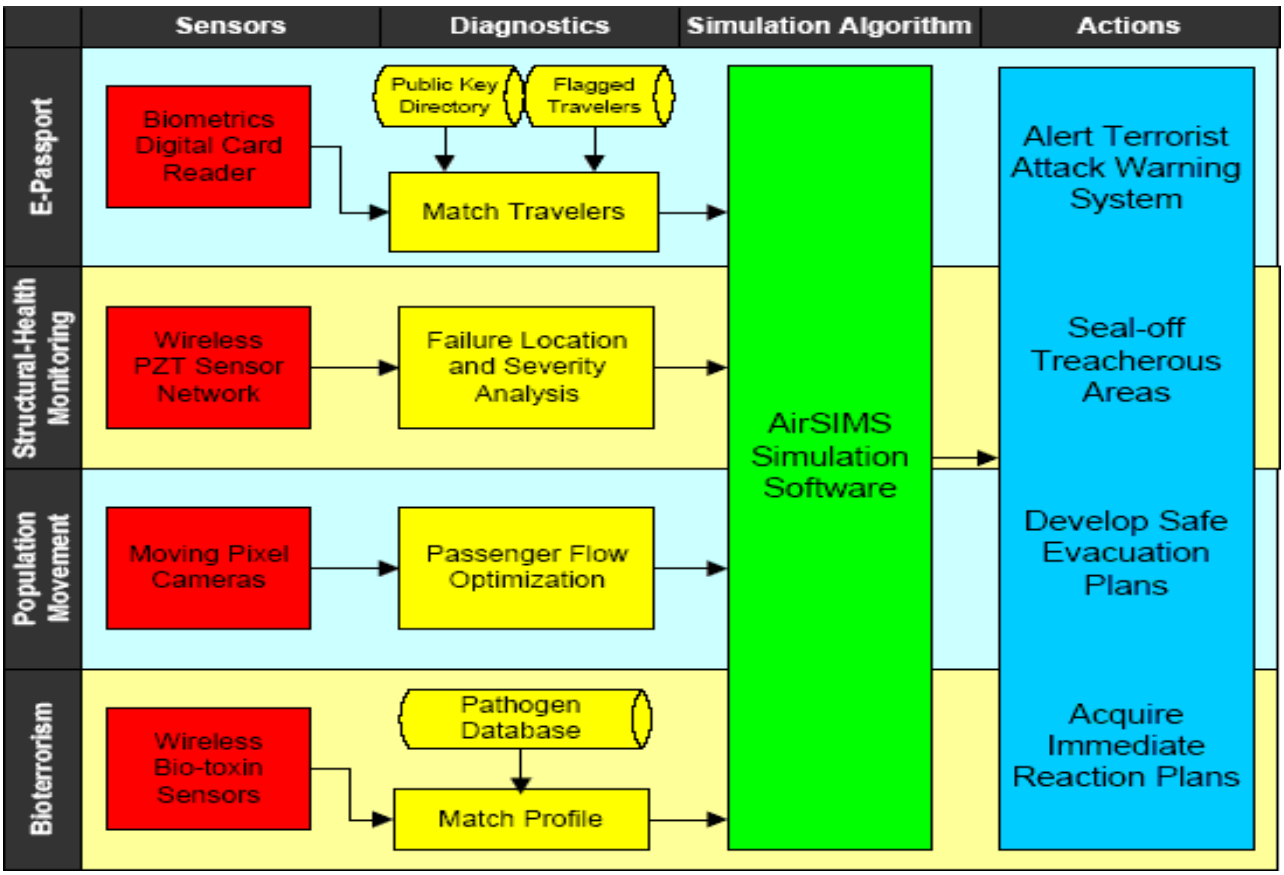

Fig 1. Organizational Flow Chart for the proposed AirSIMS

In order for us to show how AirSIMS can be implemented we will introduce a scenario that consists of a cell of four terrorists on a mission. Terrorist A is thwarted by AirSIMS E-Passport System. The other three in the group, somehow slip past the tracking system. Terrorist B is out to destroy the airport's structure while Terrorist C plans to trap passengers within the building. Lastly Terrorist D's undertaking is to release hazardous gas in the terminal.

E-Passport Component

One of the most important reasons why the September 11 attack on both the world trade center and the pentagon could take place "successfully" was because the hijackers were allowed into the United States unnoticed. If the US Customs could have identified them when they entered the country, they would have been all arrested and the whole catastrophe could have been prevented. How did they manage to get into the country as being identified as potential terrorists by security agencies such as Central Intelligence Agency (CIA), and/or Federal Bureau of Investigation (FBI)? The answer lies on the fact that their true identities were not known to those visa issuing agencies and the US customs. They could have used (or faked) other people's identities as well, which made checking even more difficult.

Having identified the problem, the key point is to make sure that everyone is really who say they are and that we must know before hand if they are (potential) terrorists. To achieve that, we need to check everyone's identity against the database in our AirSIMS system which contains all the necessary information to identify any person. E-Passport would be an ideal choice for such application for such purpose. If a terrorist (Terrorist-A) again would like to enter America with a

faked identity, he would never succeed under the new E-Passport system. We will explain how the E-Passport system works in the following sections.

Smartcard Technology

What is an E-Passport? It is a new generation passport that is currently under development. It looks just like a traditional passport (see figure 2) but contains more information in digital form. A proposed idea for E-Passport is to integrate new technologies such as:

- **Smartcard**,
- Fingerprints, and
- **Digital signature**

into current passports. Among this three technologies, smart card and digital signatures are the two that employ cryptography.

Figure 2: An example of E-passport [1]. It looks just like an ordinary passport since the chip is embedded on the back cover.

Cryptography is traditionally used in communication and computer applications to ensure data confidentiality or for identification purposes. How does it work for our purpose here exactly? It is used here to provide identification primarily. For example, many government agencies or national labs have security clearance, only authorized personnel could enter the facility with proper identification (could be a badge, a magnetic ID card, or other things). In fact, our Cal IDs are also smart cards, contactless smartcards actually; but all it stores is just our student ID in unencrypted form. E-Passport is similar in idea, except that is more advanced and secure by its nature.

Implementation

How does the new E-Passport work? To summarize, a micro computer chip will be built into the passport (the smart card part); digital signature and **biometrics** information will be stored inside the chip. To identify people who hold such a passport, we will have to follow the steps below:

1. The E-Passport issuer issues passports with appropriate digital signature and locks it in the chip with the passport holder's fingerprint (see figure 3). The issuer must release the corresponding **public key** (they are stored in the public key directory in our AirSIMS system) for the public to verify the digital signature.

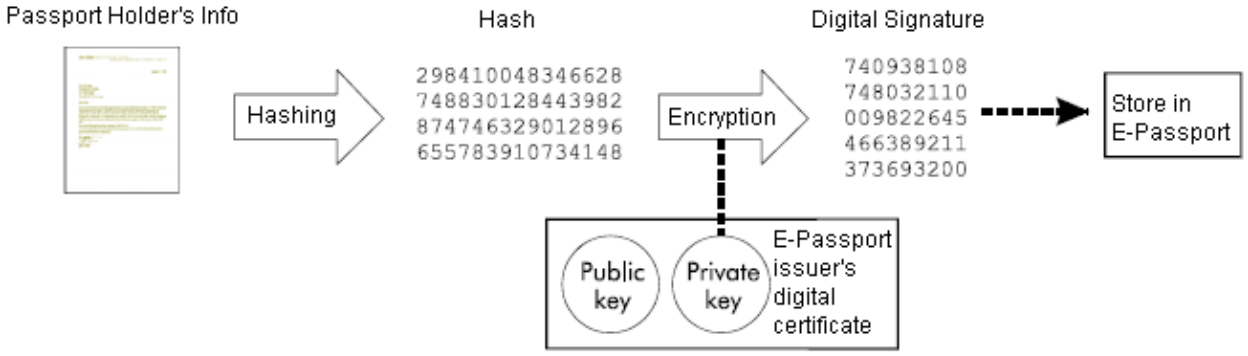

Figure 3: E-Passport Issuing Process (modified from Banjo^{TM} Verify user menu) [2].

2. We will need to take a fingerprint sample from each passenger on the airport.
3. Then we will use the fingerprint sample to unlock the digital signature stored inside the chip. The digital signature could only be unlocked if there is a match between the fingerprint sample taken and the fingerprint data stored in the chip.
4. Once the digital signature is unlocked and extracted from the chip, we will verify the digital signature using the corresponding public key from the public key directory in our AirSIMS system (see figure 4).

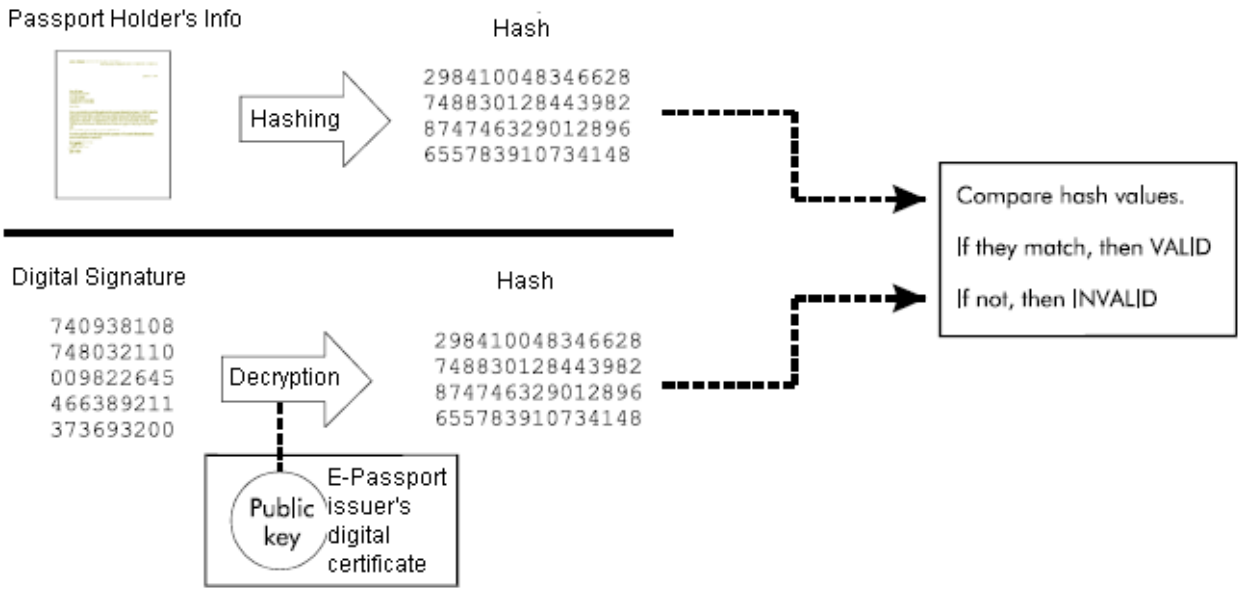

Figure 4: E-Passport Verification Process. [2]

5. Finally we will compare the **hash value** from the digital signature to the known correct hash value which generated with the passport holder's information.

If the generated hash value matches the hash value from the digital signature, then we could be pretty sure that the person is really who he or she claims is. However, in cases where things don't match up, we should at least be suspicious about that passport holder's true identity.

This proposed E-Passport is as secure as it could get compare to the current version and other ideas. Because of its cryptography feature, it is nearly impossible to duplicate. It also provides greater protection against fraudulent misuse and tampering and reduces the risk of identity fraud; but most importantly, it helps enhance the protection of border through speedy and secure verification of incoming E-passport holders. In fact, Japan has tested a primitive prototype, and it was of great success. Australia and Canada are already issuing E-passports. Also, the US government is investing money on such systems and trying to make it work with Axalto as stated in the document "Axalto e-Passport Technology Selected by the U.S. Government"[3]. However, in order to achieve compatibility of different E-Passports issued by different countries, perhaps the United Nations could help establish a standard for such passports. Also, since different countries issue their own passports, if they decide to use E-Passport, they must publish the generated public key to the rest of the world so that other countries would be able to check it. Because the generated public key cannot be reverse engineered (at least there is no known method to do it now), we don’t have to worry about private personal information being illegitimately used by other countries.

With the information of the U.S. E-Passport, I interviewed Chris Tam, one of the developers of smartcard enabled applications, for his professional expertise. "It is a smart choice to use **GlobalPlatform** compliant smartcards rather than file system cards which Hong Kong government did for their smart identity card. However, as I know, response **APDU**s of GlobalPlatform compliant smartcards (Cyberflex Access series) from Axalto Technologies are not encrypted. Since Global Platform is application based, software developers can patch this

defect by encrypting the response APDUs in their **cardlet**. Although the product they choose is not perfect, it is still repairable." Chris said [4].

E-Passport can stop a terrorist from faking his or her identity. It is impossible for any terrorist (say Terrorist-A) to enter America holding a falsified passport. Although an unidentified terrorist (a new terrorist whose data is not in AirSIMS's terrorists database) may pass through security checks, E-Passport system would still make tracking and investigation much easier than the current system once a new terrorist is identified. Implementing E-Passport is worth much more than what it costs.

Structural-Health Monitoring

Suppose Terrorist B attempts to plant an explosive device somewhere inside the airport terminal. If they somehow pass the security checkpoint, what security measures exist to protect the travelers and employees? Until now, nothing does exist. AirSIMS addresses this shortcoming by implementing a reliable and cost-effective solution to protect terminal populace.

AirSIMS utilizes a **structural-health monitoring** (SHM) module to protect travelers and airport employees. Sensors immediately detect structural failures and assess the extent of damage. This data is used to signal a terrorist attack warning system. Then, information about structural damage is combined with the other system inputs to develop an instant evacuation plan and seal-off treacherous sections of the terminal. By considering how each system inside an airport interacts with each other, AirSIMS provides a comprehensive and robust security solution, unlike anything before.

SMART Layer® Technology

There are a variety of methods available to obtain vital information concerning damage within critical airport structures. The most feasible and readily available solution for structural-health monitoring has already been designed and developed into an off-the-shelf product manufactured by Acellent Technologies called SMART Layer™. SMART Layer™ is a thin, flexible layer with a network of miniature **piezoelectric transducers** that can be embedded inside or mounted onto metal and composite assemblies to acquire information on structural integrity [5]. A schematic of an embedded SMART Layer® is provided in Figure 5.

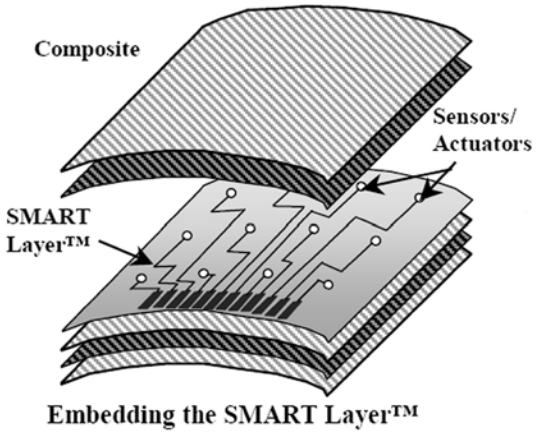

Figure 5: Acellent Technologies SMART Layer™ [6].

AirSIMS employs this technology by embedding SMART Layers® into an airport's most critical structures. These structures include, but are not limited to, the following

- Control Towers
- Terminals
- Parking Structures
- Bridges
- Airline Jets
- Airplane Hangers

Data acquisition software captures the signals emitted and sensed by the piezoelectric transducers in order to determine the structure's condition. This information is provided to AirSIMS, along with the other inputs, to optimize the best evacuation plan and seal off areas of the airport that are deemed unsafe.

SMART Layer® Diagnostics

To perform this task Acellent Technologies has developed diagnostic software that analyzes the information obtained from the sensors. This information is acquired through two methods: active and passive sensing. Each piezoelectric transducer can both actuate and sense **strain** waves inside the structure. In active sensing, **actuators** in one location emit wave signals that propagate through the material to sensors in another location. By comparing the emitted and captured wave signals, diagnostics software determines the location and severity of damage existing between the transducers. This is the method used for routine inspections. However, in the event of an explosion, SMART Layer® uses passive sensing to attain structural damage data. Piezoelectric sensors detect strain waves created by explosive impacts and determine its properties using diagnostic software. Consequently, critical information about the damage caused by an explosive device is acquired immediately.

Wireless Sensors and Network Architecture

A typical SHM sensor network application contains three drawbacks that must be addressed: cost, scalability, and reliability. In order to monitor every critical structure, construction crews must install and cable thousands of sensors. Implementing such a system is probably beyond the means of most airports. Additionally, wired instrumentation lacks the ability to add a variety of

sensors and risks damage to the wired connections. For those reasons, AirSIMS employs a network of wireless sensors, consisting of many low power nodes. Wireless technology is a viable, low-cost solution due to its excellent development over the past decade, exemplified by **IEEE 802.11** and **Bluetooth**.

The concept of applying wireless technology to structural-health monitoring was first envisioned and proposed by Straser and Kiremidjian [7]. Since, researches have developed numerous variations and improvements. However, every system is characterized by the same basic architecture, as represented in Figure 6. Each sensor unit transmits a signal to the monitoring station. For wireless links, the signal is **digitized** at the sensor unit for higher performance.

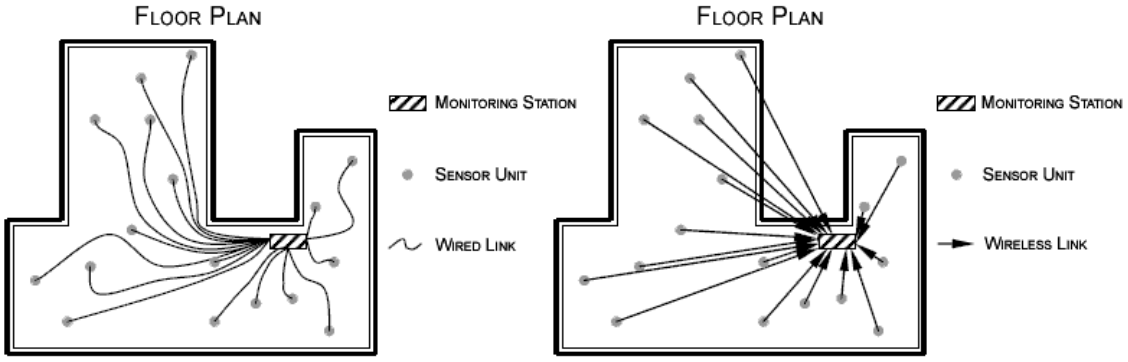

Figure 6: Basic Wired and Wireless Sensor Network Architecture [8].

The first-generation of wireless network architectures were designed and developed by research teams using a **star topology**, illustrated in Figure 6. In such topologies, each sensor unit acquires data from a single on-board sensor and transmits a digital signal to a central monitoring system. Since the initial designs were developed purely to test the function of wireless networks, architecture design was not taken into account. Star topology limits scalability because each central monitoring station can only support a limited number of sensors. Moreover, each sensor

is connected directly to the sensor unit, thus requiring more cabling than alternative topologies. Finally, other architectures optimize electrical power consumption more efficiently than star topology.

To address the issues, Stanford researcher Mastroleon suggests a two-tiered design architecture, depicted in Figure 7 [8]. Groups of sensor units (SUs) transmit data to a Local Site Master (LSM), forming the lower-tier, called a cell. The upper-tier consists of a network of LSMs that broadcast data from each cell to the Central Site Master (CSM). Each SU is battery-operated and designed for low power consumption. The LSMs require a regular power supply, but power consumption is relatively small. Additionally, multiple sensors can be embedded into each SU, allowing for more comprehensive and robust monitoring. The end result is a network architecture that is considerably more cost effective, scalable, and reliable.

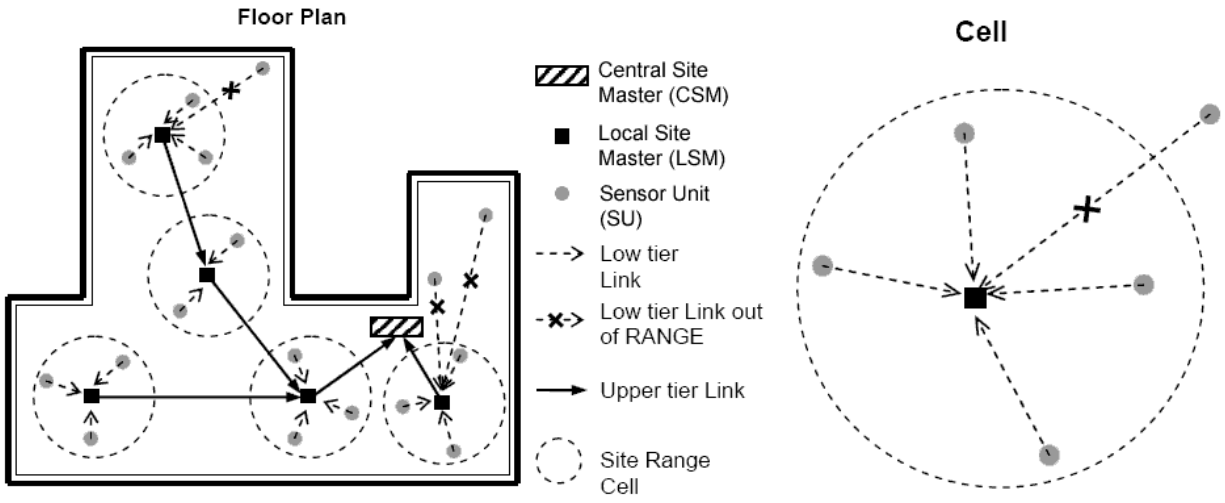

Figure 7: Two-Tier Wireless Network Architecture [8].

Protective Actions

Terrorist B might have thought that the explosive device would magnify the destruction and confusion caused by each attack. However, the AirSIMS structural-health monitoring sensor network provides a robust and cost effective protection system against such a malicious act. Combined with information gathered from other AirSIMS modules, quick and safe evacuation routes are developed. This objective is achieved through the use of SMART Layer^{TM}, developed by Acellent Technology. The sensor layers are either embedded inside or mounted onto the critical structural components. These sensors communicate via wireless two-tier network architecture, using either Bluetooth or IEEE 802.11 technology. The overall design optimizes cost, reliability, scalability, and power consumption. Structural-health monitoring detects and analyzes damage caused by explosive attacks immediately. In the event that one of the terrorists bypasses security to plant an explosive device inside the terminal, AirSIMS will save thousands of lives and evacuate everyone safely.

Population Mobility Monitoring

Imagine that the third member of the terrorist group is planning on barricading passengers inside a terminal. How will an airport security's system thwart the terrorist's mission to obstruct critical evacuation paths trapping as many people as possible within the targeted area? The terrorist believes that he can obstruct the key points of evacuation routes, but AirSIMS proves him otherwise.

The population movement sector of AirSIMS provides simulation modeling tools to create an evacuation plan. AirSIMS uses the real time conditions of the airport in addition to a shortest

path method. In an effort to counter terrorism, AirSIMS takes data from biosensors, structural sensors and airport information to create the most efficient route to steer passengers away from the danger.

Simulations

It is important to monitor the movement of the people within an airport setting because their movement provides results such as frequent paths, social networks, and congestion spots. However because the movement of people is hard to predict, simulations such as AirSIMS are often used to facilitate the process. The reason this movement is difficult to model is because even in an airport, which seems like a more controlled environment in terms of variety of routes, people diverge in their movements at unexpected times. The purpose of AirSIMS is to create a simulation to help control the course of travelers especially in emergency situations. AirSIMS also provides the added feature of updating the flow of people. The use of simulation is beneficial because it can provide a balance between airport characteristics, passenger demand, passenger process flow, and staffing. Simulations offer an opportunity to observe the environment in a non intrusive way. In order to validate these simulations, observations with statistical analysis are necessary.

Implementation

In order to accomplish this, the population within the building must be monitored. Currently at most main airports, cameras are strategically placed in the terminals and walkways to simulated where, when, and how the passengers, staff, and others move. These results are used as inputs in an algorithm that computes usage data for gates, escalators, and walkways. These airports are

secured with a camera computer network to simulate baggage and passenger screening activity. AirSIMS will use the current modeling techniques as well as enhance the current simulation systems by obtaining information about infectious diseases, structural conditions, and passenger information. The use of the passenger flow simulation and modeling is to create an evacuation plan in the case of an emergency based on the conditions of the airport at then time of a needed evacuation. The current algorithms and programs are helping with the design and layout of airports.

In the case of our terrorist group trying to harm an airport, AirSIMS will provide alternate routes to avoid the damaged area of the building while maintaining controlled flow. Terrorist C thought that the main corridors had been blocked, but AirSIMS found alternate routes that the terrorist never thought of and lead the travelers safely away. These alternate routes will be generated by the program at the time of crisis.

Currently, airport simulations are used only to monitor congestion areas and queue wait times. Modeled airports are equipped with cameras on a secure network.

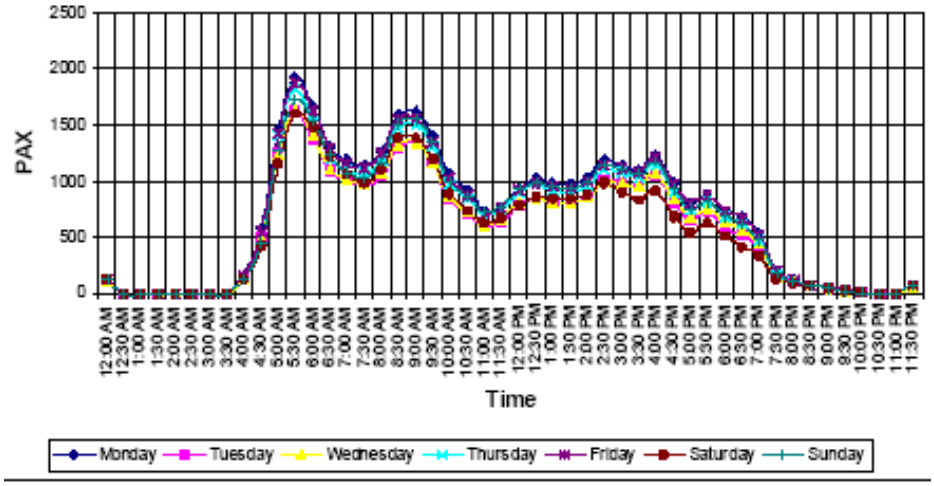

Figure 8: Passenger Arrival Times at a Checkpoint [9]

These cameras use a moving pixel method to detect motion and track it. Data from **closed circuit television** (CCTV) cameras will record where and when people move giving us more

information about the fluid nature of airport activity and note congested times and areas. Graphs are generated showing information such as the one in Figure 8. One conclusion that cam be taken from the passenger arrival time graph is that more staffing can be provide at the peak times. This result and other real-time data provide operational engineers with information to eliminate congestion and wait time.

AirSIMS will employ the series of cameras at various entry and exit and add an algorithm for updated evacuations routes. In addition to the inputs previously mentioned AirSIMS will account for structural conditions and quarantined areas.

Algorithms

There are many languages and algorithms available to use, but AirSIMS calculates the most efficient route by using a **vertex edge weight method**. Graphs such as the one below (figure 9) are made in a computer language such as **Java** [10]. Each vertex on the graph represents a door, gate, or threshold in the airport. The walkways or edges are represented by arrows connecting each vertex. These edges are assigned a weight which prioritizes the route. The priority is based on its importance and length and difficulty. In AirSIMs, one represents the shortest or easiest path and five represents the longest path. Priority can also be given to a vertex using an alphabetical order. Let's apply this to our scenario. Say that vertex B represents a doorway, while vertex F represents the emergency exit. The shortest path from B to

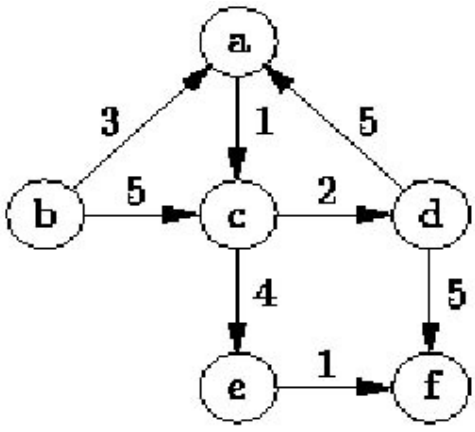

Figure 9: Vertex Edge Graph [10]

F is through C and E. However what if Terrorist B, plants a bomb in the door represented by C? AirSIMS must account for this incident and does so by redirecting traffic to D instead of C.

The use for such a program is efficient in our airport setting because of the easily geometric modeling features. These features include availability of multiple views, easy editing of geometry, and ability to make use of every location. The blueprints of the airport and area will be coded into a graph and used for evacuation plans. This makes AirSIMS flexible, allowing for layouts of different airports. In addition it can adapt to changes in peak times and delays in the schedule of airplanes. To organize all of the edges and vertices, a **heuristic** search approach can be used [11]. The organization of the data creates the shortest edges to the weighted vertices. The heuristic approach is very effective for graphing paths because it does not limit itself to the path configuration in the algorithm. Optimal paths are shown more clearly because it accounts for all vertices connected to an edge. By using a simple shortest path algorithm, effective evacuation plans can be designed.

As with every population simulation, the challenge is unpredictable nature of human activities. Hence we have to ensure the simulation is as accurate as possible. The validity of these algorithms can be proved by pure observation with statistical analysis and by using as many inputs as possible. Over a set amount of time, the airport population can be watched. Here are some input data are necessary for the proposed model:

I. Flight Schedules
- Aircraft Type
- Domestic/International Passengers and Baggage
- Total Passengers

II. Passenger Characteristics
- Online Check – In Percentage
- Passenger Group Size
- Transfer Rates
- Loading Rates

III. Facility Information
- Security Time Distribution
- Location of Services
- Facility layout and size
- Structural safety
- Ventilation Information

By using this information, flow charts such as Figure 10 are generated. These show the process of the algorithms that simulate passenger movement within an airport. These are useful to note the stage of a traveler's airport process.

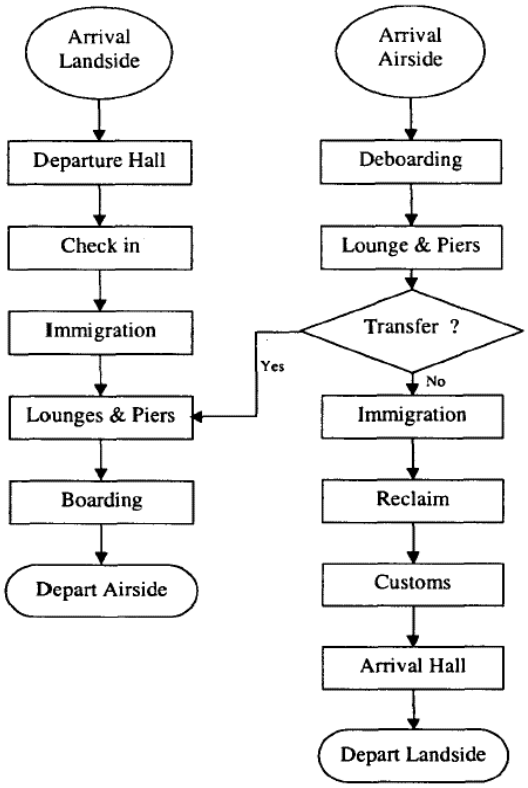

Figure 10: Processes in Passenger Handling [12]

Actions

AirSIMS Population Movement is an important decision tool for planners to maintain an organized normal flow of traffic. It also provides the necessary security to counter terrorism and provide safety. This objective is accomplished by processing inputs such as structural conditions, congestion sites, hazardous areas, population dynamics, and even construction. Routes resulting from a vertex edge algorithm maneuver people through the building, avoiding the "quarantined or damaged area." In addition, AirSIMS is easily adaptable to all airports and environments. Simulations within an airport setting are effective way to evaluate the behavior of technologies, trends, and systems to examine the environment [13]. They also eliminate bottlenecking and potential sites of congestion during an emergency. However, it is very important that our results are valid, to increase efficiency and cost effectiveness. With the implementation of AirSIMS, the airport's evacuation program and normal traffic flow will be optimized thwarting terrorist groups from completely destructing the airport and harming the innocent people. The damage created by Terrorist C will limit those exposed to the area.

"Population mobility models have been used for extremely high resolution and fidelity urban interdependencies studies of multimodal transportation, electrical power girds (including electrical markets), wireless telecommunications, and epidemiology" [14]. In AirSIMS, the tracking of diseases is another priority because of bio-terrorism. Biological agents have become a means of terrorist attacks and major threats to United States and world security. Therefore, real time and accurate detection and identification of biological agents are crucial to contain and neutralize them. Airport is one of the places that are vulnerable to biological attacks.

Counter Bio-Terrorism

In AirSIMS, extensive wireless sensors are used to detect the presence of such biological agents. Then, this information is sent to the AirSIMS central processing system and automated mechanisms of the air valves controlled by AirSIMS reduce the spread of bio-toxic gas to minimum. In addition, the information is used for developing a safety evacuation plan by simulating people's movement.

To better illustrate how the system works a scenario is developed, in which Terrorist D tries to release a poisonous gas in the airport. The poisonous gas contains an airborne virus which transmits **severe acute respiratory syndrome (SARS)**. In Hong Kong, there were 1755 cases of SARS and 299 deaths during the outbreak in 2003[15]. One of the buildings with the most severe outbreak was investigated and results showed that poor ventilation was the main reason that caused the rampant transmission among its neighborhood. Although the feasibility of using SARS virus in terrorism is not known by the meantime, we use it as an example to illustrate how AirSIMS works.

To spread the diseases, Terrorist D releases the SARS gas in highly populated area such as a lobby, a customs area, a common eating area, etc. In addition, the terrorist sneaks into the air shafts and releases the gas through the central ventilation system of the airport.

The wireless sensors installed at various locations detect bio-toxic gases released. Information such as concentrations and locations of threats is sent to the AirSIMS central processing system. By matching the profile of the gas with the bio-toxin and poisonous gas database, AirSIMS is able to identify the specific type and properties of the detected bio-toxic gas.

Protective Actions

Based on the blueprints of the ventilation system, AirSIMS closes the connecting air valves of the areas with high concentrations of bio-toxic gas to prevent further spread. In addition, the efficiency of air ventilation is adjusted to a faster than normal rate to discharge the gas outdoor from the infected area. On the other hand, information on the concentrations of bio-toxic gas monitored by the sensors and the gas flow analyzed by AirSIMS is sent to the population mobility module. Through simulation of population movement, the module analyzes different possible routes and develops the safest evacuation plan to avoid people from entering the high-risk area.

Not only does AirSIMS help to develop safe evacuation plan, it also identifies the specific bio-toxin and the movement of the infected victims, which allows medical personnel to provide medical treatment to infected victims easily. Using the wireless sensors, the blueprints, and the bio-toxin database, it identifies the locations, types, and concentrations of the bio-toxic gas.

Interacting with the population mobility module, the movement of people evacuated from the high-risk zone is monitored and medical personnel are sent to provide suitable treatments according to the bio-toxin types and concentrations provided by AirSIMS.

Biological Toxic Gas Sensors

As a wireless sensor is one of the key components of AirSIMS, the choice of sensors used directly affects the effectiveness of the system. Various gas sensors are available to detect bio-toxic gases. Reducing the number of false positives and increasing the sensitivity to bio-toxin are the major considerations of biosensors. Among those biosensors available in the market, the most popular type is the **ionization sensor**. It functions by fingerprinting the ionization characteristics of distinct gases. However, due to its huge, bulky size, and high power consumption, extensive use in airports is not cost effective. In AirSIMS, sensors with carbon **nanotubes** developed by researchers at Rensselar Polytechnic Institute at New York are used [16]. Results have shown good sensitivity and selectivity, and are undisturbed by external factors such as temperature, humidity, and gas flow.

Figure 11 shows the components of the sensor. The sensor consists of a **cathode** (an aluminum sheet), vertically aligned multiwalled nanotube (MWNT) film, and glass insulators which separates the cathode and MWNT. Controlled direct current voltage is applied between the MWNT and the cathode. The MWNTs within the film create very high nonlinear electric fields at their tips. When the gas passes through, a conducting filament of highly ionized gas surrounding the MWNT tip is formed, which is known as a “corona”. The gas itself acts as a powerful **plasma streamer** that acts as a bridge between the gap of the electrodes. Finally, the

change in electrical resistance characterized by gases with different **breakdown voltage** determines the presence of poisonous gas.

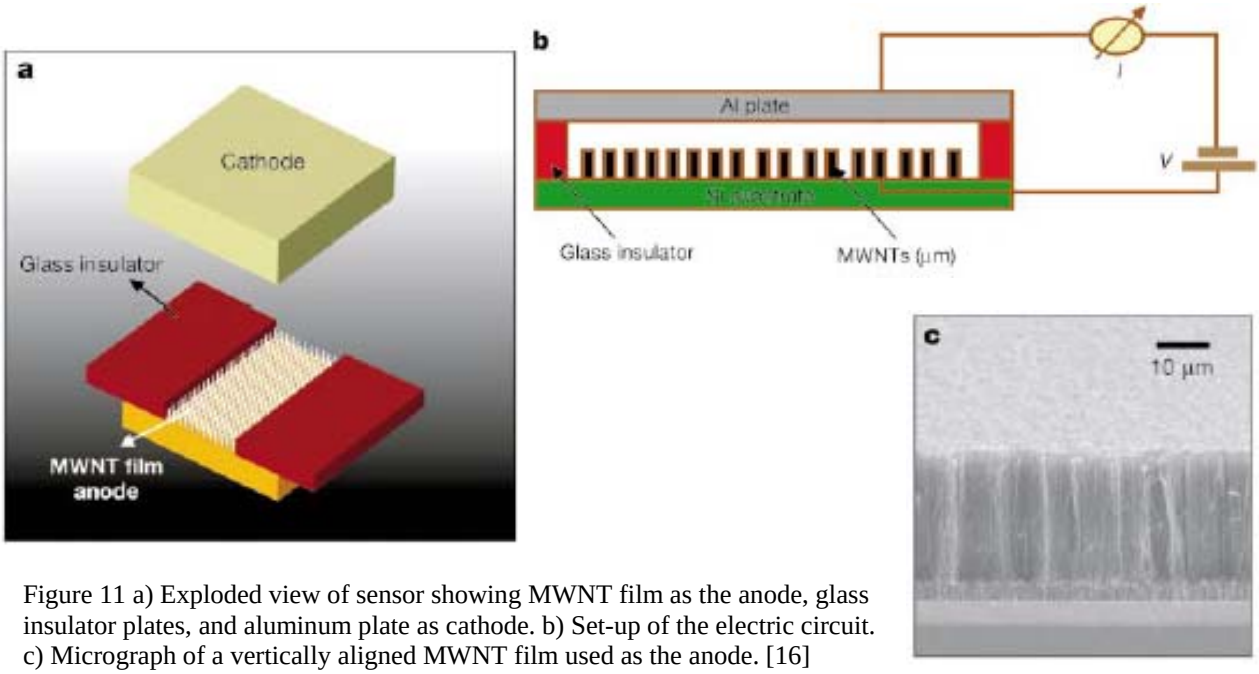

Figure 11 a) Exploded view of sensor showing MWNT film as the anode, glass insulator plates, and aluminum plate as cathode. b) Set-up of the electric circuit. c) Micrograph of a vertically aligned MWNT film used as the anode. [16]

Experiments show that the sensors provide good sensitivity and selectivity of gas detection. Figure 12 illustrates results of an experiment in which several test samples are passed through the sensors. Different gases show distinct breakdown voltages, which could be easily identified. By characterizing the profile of voltage breakdown of specific bio-toxic and poisonous gas, the gas passed through the sensors could be easily detected and identified.

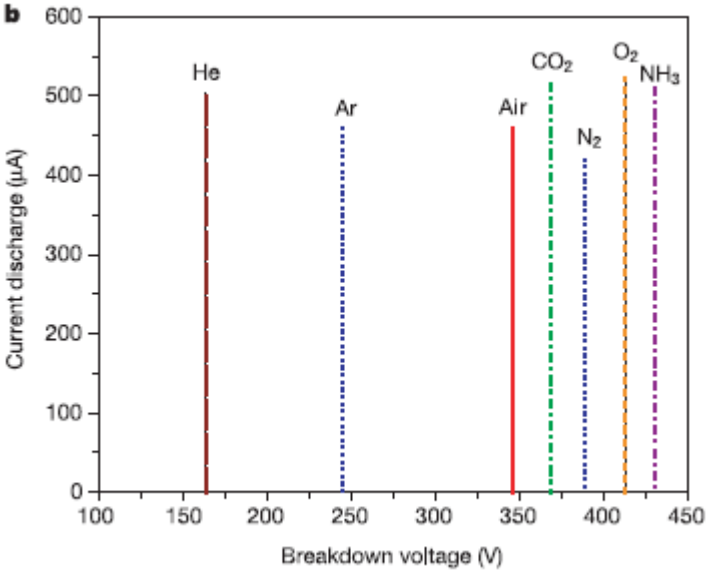

Figure 12. Different gases exhibiting distinct breakdown voltages. [16]

This technique is effective for several reasons. For one thing, the signature breakdown voltage of specific gas provides the 'fingerprint' for it to be identified and it is well established that every gas has its unique breakdown electric field at constant temperature and pressure. Second, the gas concentration can be easily determined by monitoring the self-maintaining discharge current. Last but not the least, this technique does not involve any adsorption of gas and hence it displays a fast response.

The wireless technology employed for transmitting the information detected by bio-toxic sensors to the AirSIMs central processing system is identical to that used in structural health monitoring. Further details are described in the section "Wireless Sensors and Network Architecture" above.

Conclusion

In today's increasingly dangerous world, measures must be taken to ensure our safety and security. The tragic events of 9/11 revealed critical airport security flaws that must be addressed to avoid a future attack. AirSIMS provides an efficient and comprehensive solution to this problem. As illustrated by the proposed scenario, AirSIMS protects travelers and airport employees from highly organized multi-pronged attacks. To accomplish this feat, AirSIMS contains four modules: E-Passport, Structural-Health Monitoring, Population Movement, and Biological Agent Detection. The E-Passport system represents the next generation of identification, highlighted by technologically advanced security features. Smart cards, biometrics, and digital signatures are all combined to form a digital identification method that cannot be falsified. Secondly, AirSIMS utilizes a structural-health monitoring system to detect and react to physical damage endured by critical structures. Through a wireless sensor network,

information is gathered and analyzed instantaneously, allowing the immediate development of reaction plans. The Population Movement module tracks passenger traffic within the airport terminal to determine optimum evacuation routes. If an entryway is obstructed, the software can instantly recalculate the quickest route to safety. Finally, AirSIMS counters bioterrorism by means of bio-toxin sensors and a database of toxic gas profiles. If the central processing system matches the detected gas with a toxic gas in the database, actions are taken to seal-off the infected area and adjust the ventilating system. These four modules comprise an all-in-one solution that considers the interaction between systems, rather than isolating each case. Advanced electronic technology allows this to be a continuous process, able to gather information immediately. As a result, preventive and reactive measures are taken to ensure the population's safety. AirSIMS is the most comprehensive airport security solution in today's increasingly dangerous world.

Glossary

actuators
A device responsible for actuating a mechanical device, such as one connected to a computer by a sensor link.

APDU
APDU (Application Protocol Data Unit) is the communication unit between a reader and a card. The structure of an APDU is defined by the ISO 7816 standards. There are two categories of APDUs: command APDUs and response APDUs. As the name implies, the former is sent by the reader to the card: it contains a mandatory 5-byte header and from 0 to up to 255 bytes of data. The latter is sent by the card to the reader: it contains a mandatory 2-byte status word and from 0 to up to 256 bytes of data.

biometrics
Includes characteristics of structure and of action such as iris and retinal patterns, hand geometry, fingerprints, voice responses to challenges and the dynamics of hand-written signatures.

Bluetooth
An industrial specification for wireless personal area networks (PANs) used to exchange information between devices such as personal digital assistants (PDAs), mobile phones, laptops, PCs, printers, and digital cameras via a secure, low-cost, globally available short range radio frequency.

breakdown voltage
The voltage at which the insulation between two conductors will break down

cardlet
Cardlet is a piece of running program within the smartcard chip which follows a particular life cycle that different with normal computer program.

cathode
A negatively charged electrode of an electron tube.

closed circuit television
A series of surveillance cameras connected directly through a monitor resulting in a secure network.

data acquisition software
A computer program that captures and records information acquired from sensors.

digitized
The process of converting a continuous analog signal to a digital signal consisting of either 0’s or 1’s.

digital signature
A digital guarantee that information has not been modified, as if it were protected by a tamper-proof seal that is broken if the content were altered. The two major applications of digital signatures are for setting up a secure connection to a Web site and verifying the integrity of files transmitted.

GlobalPlatform
GlobalPlatform is a cross-industry membership organization created to advance standards for smart card growth. It combines the interests of smart card issuers, vendors, industry groups, public entities and technology companies to define requirements and technology standards for multiple application smart cards. It is fully independent and democratic with priorities established by a Board of Directors. (*taken from the Global Platform FAQ - http://www.globalplatform.org*)

hash value
The fixed-length result of a one-way hash function.

heuristic
Heuristic is a technique designed to solve a problem that ignores whether the solution can be proven to be correct, but which produces the most appropriate solution by means of a trial and error method.

IEEE 802.11
A set of wireless local area network (LAN) standards used by computers for Internet access, file sharing, or printer sharing.

ionization sensor
Sensor which consists of one positive charge and one negative charge plate and ionizes the gas passed through to form an electric circuit.

Java
Java is an object-oriented programming language.

nanotube
A tiny, hollow cylinder with an outside diameter of a nanometer that is formed from atoms such as carbon. It shows different electric conductivity when aligned in different ways.

piezoelectric
The generation of electricity or of electric polarity in dielectric crystals subjected to mechanical stress, or the generation of stress in such crystals subjected to an applied voltage.

plasma streamer
An electrically neutral ionized gas in an electric discharge.

public key
An encryption key that can be made public or sent by o rdinary means in public key cryptographic system.

severe acute respiratory syndrome (SARS)
A viral respiratory illness caused by a coronavirus, called SARS-associated coronavirus (SARS-CoV).

smartcard
A plastic card with a built-in microprocessor and memory used for identification or financial transactions. When inserted into a reader, it transfers data to and from a central computer. It is more secure than a magnetic stripe card and can be programmed to self-destruct if the wrong password is entered too many times. As a financial transaction card, it can be loaded with digital money and used like a travelers check, except that variable amounts of money can be spent until the balance is zero.

star topology
An architecture in which all nodes are connected to a central node. In this network, one malfunctioning node does not affect the rest of the system and it is easy to add and remove nodes. However, they typically require more cabling than other topologies.

strain
The amount of elongation or compression that occurs in a structure at a given stress or load.

structural-health monitoring
A continuous, non-invasive method used to detect and interpret damage within a structure, thereby eliminating manual inspection.

transducers
A device, such as a piezoelectric crystal, microphone, or photoelectric cell, that converts input energy of one form into output energy of another.

vertex edge weight method
A mathematical method using vertices and edges as symbols which represent elements in a process. A weight can represent an importance or priority of the vertex or edge.

References

1. U.S. Department of State. 2005. Design of the New U.S. e-Passport. (http://travel.state.gov/passport/eppt/eppt_2501.html). Accessed Nov 27 2005.

2. LineType Software. 2005. Banjo™ Verify User Menu. 9.

3. TMCnet News. October 13th, 2004. Axalto e-Passport Technology Selected by the U.S. Government. (http://www.tmcnet.com/usubmit/2004/Oct/1082776.htm). Accessed Nov 27, 2005.

4. Tam, Chris. Personal Interview. Dec. 5, 2005.

5. Kumar, A., F. Wu, M. Lin, S.J. Beard, X. Qing, C. Zhang, M. Hamilton and R. Ikegami. Mar 16-17, 2004. Potential applications of SMART Layer® technology for homeland security. *Proceedings of SPIE - The International Society for Optical Engineering*. San Diego, CA. 5395: 61-69.

6. Lin, M., X. Qing, A. Kumar, and S.J. Beard. Mar 18-21, 2001. SMART Layer® and SMART Suitcase™ for structural health monitoring applications. *Proceedings of SPIE - The International Society for Optical Engineering*. Newport Beach, CA. 4332: 98-106.

7. Straser, E.G. and A. S. Kiremidjian.1998. A modular, wireless damage monitoring system for structures, *Report No. 128*. John A. Blume Earthquake Engineering Center, Department of Civil and Environmental Engineering, Stanford University. Stanford, CA. (Cited in [7], 52).

8. Mastroleon, L., A. Kiremidjian, E. Carryer, and K. Law. Mar 16-17, 2004. Design of a new power-efficient wireless sensor system for structural health monitoring. *Proceedings of SPIE - The International Society for Optical Engineering*. 5395: 51-60.

9. Pendergraft, D. R., C. V. Robertson, and S. Shrader. Dec. 5-8, 2004. Simulation of an Airport Passenger Security System. *Proceedings of the 2004 Winter Simulation Conference.* Washington, D.C. 878-882.

10. Priess, B. R. 1998. Data Structures and Algorithms with Object-Oriented Design Patterns in Java. (http://www.brpreiss.com/books/opus5/html/page564.html#SECTION00174100000000000000). Accessed Nov 2005.

11. Algorithmic Solutions Software GmbH. Oct. 16, 2002. Shortest Path Algorithms. (http://www.pcs.cnu.edu/~riedl/software/leda/shortest_path.html). Accessed Nov 2005.

12. Gatersleben, M. R., and S. W. van der Weij. Dec 5-8, 1999. Analysis and Simulation of Passenger Flows in an Airport Terminal. *Proceedings of the 1999 Winter Simulation Conference*. Phoenix, AZ. 2: 1226-1231.

13. Wilson, D.L. Oct 11-14, 2004. Use of Modeling and Simulation to Support Airport Security. *38th Annual 2004 International Carnahan Conference.* Albuquerque, NM. 20, 81: 247-251.

14. Rinaldi, S. M. Jan 5-8, 2004. Modeling and Simulating Critical Infrastructures and Their Interdependencies. *Proceedings of the 37th Hawaii International Conference on System Sciences.* Big Island, HI. 37: 873-880.

15. Department of Health, Hong Kong. April 17, 2003. Health, Welfare & Food Bureau SARS Bulletin. (http://www.info.gov.hk/dh/diseases/ap/eng/bulletin0417.htm). Accessed Nov. 28, 2005.

16. Modi, A., N. Koratkar, E. Lass, B. Wei, and P.M. Ajayan. 2003. Miniaturized gas ionization sensors using carbon nanotubes. *Nature.* 424:6945:171-174