Chapter 1

Introduction

Due to an alarming increase in terrorist activities targeting the United States in general, and the United States commercial airline industry, in particular, aviation security has become of paramount importance to all travelers. The constant threat of terrorism requires that the Transportation Security Administration (TSA), the airports, and the commercial airlines closely inspect passengers and baggage for threats. These threats are typically in the form of explosives and firearms. A single explosive device passing through airport security undetected has the potential for major damage and loss of life. Moreover, the negative effects caused by such a disaster for an airline, in both monetary and public relations, are incalculable. Government agencies, including the TSA, responsible for dealing with the continuing problem of terrorist threats are in constant search of new solutions to address this problem. Identifying these *entities* (i.e. any passenger, baggage, or other items that are examined by a security device) as threats requires an efficient and effective coordinated effort between all parties involved.

These *threat entities* (i.e., any entity that is introduced to the system that contains an explosive or firearm threat) can be classified into two categories: explosive threats and firearm threats. Each of these categories has a particular set of characteristics, which indicate when the threat is present. For example, the presence of certain kinds of wires and synthetics can suggest the presence of explosives. Likewise, the presence of certain metals may suggest the presence of firearms. Furthermore, since not every *security device* (i.e., any machine or procedure that has the ability to ascertain if an entity poses a threat) can detect every possible type of threat entity, a variety of devices must be deployed. The detection capabilities of each security device are known. For example, a security device may be able to detect explosives with a high probability, but it may not be capable of detecting firearms. In such cases, if only one device is deployed, firearm threats would likely pass undetected. One solution is to add a second security device that detects firearms to the *detection system* (i.e., the structure of the security devices that determines if a particular entity should be considered a threat entity). Adding these new devices to the system raises several questions.

- How should the security devices interact?
- What is the proper path to route the entities that must be examined by the system?
- How is a *system response* (i.e., the action or response that is determined necessary by the overall detection system of security devices. In this case, either an alarm or a clear.) determined?
- In what order should the security devices be arranged?

The TSA has already determined that the devices contained in the detection system should produce independent responses. Furthermore, the response of the individual security devices shall determine the path a specific entity takes through the detection system. This thesis will examine the order in which the

devices should be arranged within the system structure, to maximize the detection of threat entities.

Currently, the TSA has no standardized detection system deployed at airports in the United States. The same is true for airlines; each airline has different procedures for detecting threats to their aircraft. This approach has certain drawbacks, in that many of the current systems are ineffective in detecting threat entities. By standardizing and optimizing the detection system of every American airport and every airline, the TSA can better guarantee that a threat entity will not reach an aircraft.

Security systems consist of a set of security devices. The TSA currently assumes that while the individual device responses are independent of one another; the routing of entities through the system is dependent. That is, an entity is scanned by a device, which responds with is an alarm or a clear. It is the device response of an alarm or a clear determines where the entity will be routed next. It is the routing of the entity that determines the overall system response. That is the route of the entity through the system determines if the overall system will declare the entity alarm or a clear. This concept is further developed and discussed in Chapter 3.

“One important aspect of designing the detection system is managing the tradeoff between the two types of errors that can occur. A detection system can allow a *false clear* (i.e., allow a threat entity to pass through undetected), or the detection system can allow a *false alarm* (i.e., not allow a non-threat entity to gain access). Because these errors are dependent on one another, it is impossible to minimize both simultaneously” Jacobson, et.al. [5]. Both the false alarm error and the false clear error can have a disabling effect on the aviation industry. A high false clear rate would result in numerous aircraft being destroyed by explosive devices. While, a high false alarm rate might result in passengers being unnecessarily delayed and eventually missing flights. These

missed flights and disgruntled passengers would create a ripple effect, with significant human and economic implications.

The question faced by the TSA can be stated as follows:

> *how can the TSA improve the performance of their threat detection system?*

The answer to this question is to identify detection systems that minimize the overall associated costs of implementation and operation. These costs include the costs of false alarms, false clears, and system operating costs. An optimal detection system minimizes the total system cost. The objective of this thesis is to explore and design tools and algorithms for identifying an optimal performance for aviation security detection system.

The thesis is organized as follows. Chapter 2 contains a literature review of access control security systems, including previous work focusing on the false alarm / false clear tradeoff. Chapter 3 presents the methodology used in this research. The development of the Secure Air Flight Effectiveness (SAFE) Model is discussed. The SAFE Model uses a Generalized Hill Climbing (GHC) Algorithm to minimize the costs of the aviation security detection system. Chapter 4 presents the results of the SAFE Model and their implications. Finally, Chapter 5 discusses the implications of these results and suggestions for future research.