Airport Runway Security Risk Evolution Model Based on Complex Network

Xianli Zhao

School of Management, Wuhan University of Technology, Wuhan 430070, China

Abstract

Airport runway security risk assessment and safety testing is of great significance in fields like risk control, navigation and traffic monitoring. An airport runway risk evolution mathematical model and risk evolution topology model based on complex network is individually proposed. In the model, nodes represent every possible risk factor, edges represent risk induced process. The airport runway risk evolution mathematical model is described from clustering coefficient, average path length and degree distribution. The risk evolution topology model is analyzed from in-degree and out-degree, the number of nodes and the number of branches, and the risk broken chain control scheme is proposed. The results indicated that security management system vulnerabilities, lack of staff safety training, lack of safety awareness of the ground staff and illegal operations, bad weather are key nodes of airport runway security risk evolution model.

Keywords: complex network, risk evolution model, airport runway, safety and security.

1. INTRODUCTION

Airport security refers to the techniques and methods used in protecting passengers, staff and planes which use the airports from accidental/malicious harm, crime and other threats. Airport runways are safer today than they were in the past. Oster appearing before the US Senate Commerce subcommittee on aviation safety issues said that “three year average commercial accident rate is 0.017 accidents per 100,000 departures” meaning accident rate is the equivalent of one fatal accident for every 15 million passenger carrying flights (Oster et al., 2013). In today’s world intelligence, security partnering and information sharing has help to reduce incidents and accidents at the airport runways.

Figure 1. The Block Diagram of SHELL Model

In spite of all of the activities that the airports have undertaken to reduce runway incursions, the human factor remains the most valuable and the most vulnerable asset in the aviation environment. The first human factors...
models in aviation is SHELL model which is proposed by Elwyn Edwands (1972). The SHELL model is a conceptual model of human factors that clarifies the scope of aviation human factors and assists in understanding the human factor relationships between aviation system resources or environment (the flying subsystem) and the human component in the aviation system (the human subsystem).

The model is named after the initial letters of its components (software, hardware, environment, liveware) and places emphasis on the human being and human interfaces with other components of the aviation system (Johnston et al., 2001). The SHELL model adopts a systems perspective that suggests the human is rarely, if ever, the sole cause of an accident (Wiegmann and Shappell, 2003). The systems perspective considers a variety of contextual and task-related factors that interact with the human operator within the aviation system to affect operator performance (Wiegmann and Shappell, 2003). As a result, the SHELL model considers both active and latent failures in the aviation system.

The block diagram of SHELL model is shown in Figure 1.

Each component of the SHELL model (software, hardware, environment, liveware) represents a building block of human factors studies within aviation. The human element or worker of interest is at the centre or hub of the SHELL model that represents the modern air transportation system (Hawkins and Orlady, 1993). The human element is the most critical and flexible component in the system, interacting directly with other system components, namely software, hardware, environment and liveware.

However, the edges of the central human component block are varied, to represent human limitations and variations in performance. Therefore, the other system component blocks must be carefully adapted and matched to this central component to accommodate human limitations and avoid stress and breakdowns (incidents/accidents) in the aviation system. To accomplish this matching, the characteristics or general capabilities and limitations of this central human component must be understood.

The four components of the SHELL model or aviation system do not act in isolation but instead interact with the central human component to provide areas for human factors analysis and consideration (Wiegmann and Shappell, 2003). The SHELL model indicates relationships between people and other system components and therefore provides a framework for optimizing the relationship between people and their activities within the aviation system that is of primary concern to human factors. In fact, the International Civil Aviation Organization has described human factors as a concept of people in their living and working situations; their interactions with machines (hardware), procedures (software) and the environment about them; and also, their relationships with other people.

According to the SHELL model, a mismatch at the interface of the blocks/components where energy and information is interchanged can be a source of human error or system vulnerability that can lead to system failure in the form of an incident/accident (Johnston et al., 2001). Aviation disasters tend to be characterized by mismatches at interfaces between system components, rather than catastrophic failures of individual components (Wiener and Nagel, 1988).

There have been a lot of researches about airport runway security risk models, but the research on risk evolution is relatively lack. Airport runway risk is a dynamic evolving open network, the randomness and regularity co-exist. In this paper, airport runway risk evolution mathematical model and risk evolution topology model based on complex network is constructed. The model can reveal the inherent law of risk evolution, it is very useful to improve the safety management level of airport runway.

2. COMPLEX NETWORK THEORY

In the context of network theory, a complex network is a graph (network) with non-trivial topological features—features that do not occur in simple networks such as lattices or random graphs but often occur in graphs modeling of real systems. The study of complex networks is a young and active area of scientific research inspired largely by the empirical study of real-world networks such as computer networks, social networks (Kuran and Thiran, 2006; Barabási and Albert, 1999; Kossinets, 2006), brain networks and technological networks.

2.1 Topological features of complex network
Trivial networks such as lattices and random graphs have been studies extensively in the past. Lattices are regular graphs whose drawing corresponds to some grid/mesh/lattice. A random graph is a graph that is generated by a random process. Some of the more prominent graph properties will be discussed. Graph properties or invariants depend on the abstract structure only, not on the representation. They include degree, clustering coefficient, connectivity (scalars); degree sequence, characteristic polynomial, Tutte polynomial (sequences/polynomials).

Complex networks display substantial non-trivial topological characteristics, with patterns of connection between their nodes that are neither purely regular nor purely random. Such characteristics include a heavy tail in the degree distribution, a high clustering coefficient, a small average path length, hierarchical structure and community structure (Albert, 2002).

The degree of a node in a network is the number of connections or edges the node has to other nodes. The degree distribution \( P(k) \) of a network is defined to be the fraction of nodes in the network with degree \( k \). Thus if there are \( n \) nodes in total in a network and \( n_k \) of them have degree \( kk \), we have \( P(k) = n_k/n \). A network is named scale-free (Barabási, 2009) if its degree distribution follows a particular mathematical function called a power law. The power law implies that the degree distribution of these networks has no characteristic scale. In a network with a scale-free degree distribution, allowing for a few nodes of very large degree to exist, these nodes are often called “hubs”.

In complex networks, clustering coefficient is a measure of the degree to which nodes in a complex network tend to cluster together. The clustering coefficient is based on triplets of nodes. A triplet consists of three nodes that are connected by either two (open triplet) or three (closed triplet) undirected ties. A triangle consists of three closed triplets, one centred on each of the nodes. The clustering coefficient is the number of closed triplets (or 3 x triangles) over the total number of triplets (both open and closed). Watts and Strogatz defined the clustering coefficient as follows. Suppose that a vertex \( V \) has \( K \) neighbours; then at most \( K(K-1)/2 \) edges can exist between them (this occurs when every neighbour of \( v \) is connected to every other neighbour of \( v \)). Let \( C_v \) denote the fraction of these allowable edges that actually exist. Define Cas the average of \( C_v \) overall (Watts and Strogatz, 1998).”

Average path length is one of the three most robust measures of network topology, along with its clustering coefficient and its degree distribution. In a network, the distance \( d(v_i,v_j) \) between two nodes \( v_i \) and \( v_j \) is defined as the number of edges along the shortest path connecting them. Assume that \( d(v_i,v_j) = 0 \) if \( v_i \) cannot be reached from \( v_j \).

Connectivity of a graph is a measure of robustness as a network. Two vertices are connected, if there is a path between them. Otherwise they are disconnected. A graph is connected if every pair of vertices is connected.

Vertex connectivity is the smallest vertex cut of a connected graph-the number of vertexes that must be removed in order to disconnect the graph. Local connectivity is the size of a smallest vertex cut separating two vertexes in a graph. Graph connectivity equals the minimal local connectivity.

Edge connectivity is the smallest number of edge cuts that renders the graph disconnected. Local edge connectivity is the smallest number of edge cuts, which disconnect the two edges. Again, the smallest local edge connectivity in a graph is the graph edge connectivity.

The vertex- and edge-connectivity of a disconnected graph are both 0. The complete graph on \( n \) vertices has edge-connectivity equal to \( n-1 \). Every other simple graph on \( n \) vertices has strictly smaller edge-connectivity. In a tree, the local edge-connectivity between every pair of vertices is 1. Edge connectivity is bounded by vertex connectivity and the latter is bounded by the minimum degree of the graph.

Assortativity refers to a preference of a node to attach to other nodes that are similar or different. Similarity is often but not necessarily expressed in terms of a nodes degree, i.e. in social networks, highly connected nodes prefer to attach to other highly connected nodes (assortativity). The opposite effect can be observed in technological and biological networks, where highly connected nodes tend to attach to low degree nodes (disassortativity).
Assortativity is measured as correlation between two nodes. The most common measures are assortativity coefficient and neighbor connectivity. The assortativity coefficient is a Pearson correlation coefficient between pairs of nodes. The range of the measure \( r \) is from -1 for perfect assortative mixing patterns to 1 for completely disassortative.

### 2.2 Two typical complex network

Two well-known and much studied classes of complex networks are scale-free networks (Barabási and Albert, 2003) and small-world networks (Watts and Strogatz, 1998) whose discovery and definition are canonical case-studies in the field.

A network is named scale-free if its degree distribution, i.e., the probability that a node selected uniformly at random has a certain number of links (degree), follows a particular mathematical function called a power law. The power law implies that the degree distribution of these networks has no characteristic scale. In contrast, networks with a single well-defined scale are somewhat similar to a lattice in that every node has (roughly) the same degree. Examples of networks with a single scale include the Erdös–Rényi (ER) random graph and hypercubes. In a network with a scale-free degree distribution, some vertices have a degree that is orders of magnitude larger than the average-these vertices are often called "hubs", although this is a bit misleading as there is no inherent threshold above which a node can be viewed as a hub. If there were such a threshold, the network would not be scale-free.

Interest in scale-free networks began in the late 1990s with the reporting of discoveries of power-law degree distributions in real world networks such as the World Wide Web, the network of Autonomous systems (ASs), some networks of Internet routers, protein interaction networks, email networks, etc. Most of these reported "power laws" fail when challenged with rigorous statistical testing, but the more general idea of heavy-tailed degree distributions—which many of these networks do genuinely exhibit (before finite-size effects occur)—are very different from what one would expect if edges existed independently and at random (i.e., if they followed a Poisson distribution). There are many different ways to build a network with a power-law degree distribution. The Yule process is a canonical generative process for power laws, and has been known since 1925. However, it is known by many other names due to its frequent reinvention, e.g., The Gibrat principle by Herbert A. Simon, the Matthew effect, cumulative advantage and, preferential attachment by Barabási and Albert for power-law degree distributions. Recently, Hyperbolic Geometric Graphs have been suggested as yet another way of constructing scale-free networks.

Some networks with a power-law degree distribution (and specific other types of structure) can be highly resistant to the random deletion of vertices—i.e., the vast majority of vertices remain connected together in a giant exponent. Such networks can also be quite sensitive to targeted attacks aimed at fracturing the network quickly. When the graph is uniformly random except for the degree distribution, these critical vertices are the ones with the highest degree, and have thus been implicated in the spread of disease (natural and artificial) in social and communication networks, and in the spread of fads (both of which are modeled by a percolation and branching process). While random graphs (ER) have an average distance of order \( \log N \) between nodes, where \( N \) is the number of nodes, scale free graph can have a distance of \( \log \log N \). Such graphs are called ultra small world networks.

A network is called a small-world network by analogy with the small-world phenomenon (popularly known as six degrees of separation). The small world hypothesis, which was first described by the Hungarian writer Frigyes Karinthy in 1929, and tested experimentally by Stanley Milgram (1967), is the idea that two arbitrary people are connected by only six degrees of separation, i.e. the diameter of the corresponding graph of social connections is not much larger than six. In 1998, Duncan J. Watts and Steven Strogatz published the first small-world network model, which through a single parameter smoothly interpolates between a random graph and a lattice. Their model demonstrated that with the addition of only a small number of long-range links, a regular graph, in which the diameter is proportional to the size of the network, can be transformed into a "small world" in which the average number of edges between any two vertices is very small (mathematically, it should grow as the logarithm of the size of the network), while the clustering coefficient stays large. It is known that a wide variety of abstract graphs exhibit the small-world property, e.g., random graphs and scale-free networks. Further, real world networks such as the World Wide Web and the metabolic network also exhibit this property.

In the scientific literature on networks, there is some ambiguity associated with the term "small world." In addition to referring to the size of the diameter of the network, it can also refer to the co-occurrence of a small diameter and a high clustering coefficient. The clustering coefficient is a metric that represents the density of triangles in the network.
the network. For instance, sparse random graphs have a vanishingly small clustering coefficient while real world networks often have a coefficient significantly larger. Scientists point to this difference as suggesting that edges are correlated in real world networks.

3. AIRPORT RUNWAY SECURITY RISK EVOLUTION MODEL

In this section, we introduce a risk evolution model that generates small-world networks with scale-free properties. The BA model is based on a simple principle of preferential attachment. The probability that an old node receiving links is linearly proportional to its degree. It assumes that every new node has the complete information about the whole network, which is unrealistic for real network formations. As a matter of fact, many networks have their topology influenced by the environmental constraints.

In our model, nodes $k_i$ represent every possible risk factor, edges $e_i$ represent risk induced process. Initially, the network is composed of $m_0$ ($m_0 \geq 2$) fully connected nodes. At each subsequent time, we grow the network according to the following prescription: (a) At each increment of time, a new node $n$ is built or created by one of the existing vertices, and assume the probability that the new node established by node $i$ is proportional to the degree $k_i$, more precise, the probability of node $i$ to build new node at one step time is:

$$P_{cr}(i) = \frac{k_i}{\sum_j k_j}$$  

Eq. (1) indicates that nodes with large degrees have large probability to build new nodes. (b) Once the new node is established by node $i$, $m=m_0$ edges are distributed to $i$ and its nearest neighbors. One edge connects node $i$ and the other $(m-1)$ edges are attached to the nearest neighbors. Here we assume the $(m-1)$ links are distributed to the nearest neighbors of node $i$ uniformly, thus the conditional probability that one of the nearest neighbors $j$ connecting the new node established by node $i$ is:

$$P(j|i) = \frac{m-1}{k_i}$$  

These steps are repeated sequentially, creating a network with a temporally growing number of nodes $t$. We note that, since the network size $t$ is increased by one in each discrete time step, $t$ can be used as a system size or a time variable.

The growing network model can be shown in Figure 2.

![Figure 2. Illustration of our growing network model](image-url)

We now consider the dynamics of degree $k_i$ of a given node $i$ to calculate the degree distribution in our model. The degree $k_i$ will increase when a new node is established by node $i$ or by its nearest neighbors. Consequently, $k_i$ satisfies the following dynamical equation:
\[ \frac{dk_i}{dt} = 1 \cdot P_{cr}(i) + \sum_{l \in \Gamma'(i)} p(i|l) \cdot p_{cr}(l) \]  

(3)

Where \( \Gamma'(i) \) is the set of nearest neighbors of node \( i \). The first term on the right-hand side corresponds to the random selection of node \( i \) as a creator of the new node with probability \( P_{cr}(i) \), while the second term corresponds to the selection of the nearest neighbors of node \( i \) as a creator. Substituting \( P_{cr}(L) \) and \( P(i|l)=m-l/k \) into Eq. (3), we have

\[ \frac{dk_i}{dt} = m \sum_j k_j \]

(4)

Eq. (4) indicates that the growth and linear preferential attachment are preserved in our model. This equation can be solved with the initial condition \( k_i(t=t)=m \), yielding

\[ k_i(t) = m \sqrt{\frac{t}{t_i}} \]

(5)

The evolution of the degree \( k_i \) is the same as that in the BA model, therefore the degree distribution of our model is identical to that of the BA model.

Figure 3 shows \( k_i \) of our model versus that of the BA model for \( t=10000 \) and \( m=2 \).

From Figure 4 we can see that the dashed line is a power-law \( p(k) \sim k^{-3} \).

![Figure 3](image1.png)  
**Figure 3.** Degree \( k_i \) of our model versus that of the BA model

![Figure 4](image2.png)  
**Figure 4.** Degree distributions for our model and BA model

The clustering \( C_i \) of node \( i \) is defined by

\[ C_i = \frac{2E_i}{k_i(k_i-1)} \]

(6)
where \( E_i \) is the total number of links between the \( k_i \) neighbors of node \( i \). When a new node is established at time \( t \), the total number of edges \( E_i(t) \) between the nearest neighbors of node \( i \) can increase either if the new node is built by \( i \) or by its nearest neighbors.

The evolution equation for \( E_i \) is thus given by

\[
\frac{dE_i(t)}{dt} = (m-1) \sum_j k_j + \sum_{l \in \Gamma(i)} p(l | i) \cdot p_{<\nu}(k_l) = 2(m-1) \sum_j k_j
\]

(7)

Considering that there are at least \( m-1 \) links among the nearest neighbors of node \( i \) when it is established, the initial condition of \( E_i \) can be written as \( E_i(t=0) \geq m-1 \), where the equality holds only for \( m=2 \).

Therefore Eq. (7) can be readily integrated as

\[
E_i(t) \geq \frac{2(m-1)k_i(t)}{m} - (m-1)
\]

(8)

Figure 5 shows the clustering spectrum for \( t=10000 \) and \( m=2 \), which agrees well with the analytical prediction of Eq. (8).

![Figure 5. The degree dependent clustering coefficient for \( m=2 \) and \( t=10000 \)](image)

The open circles in Figure 6 show \( L \), the shortest path length between pairs of nodes averaged over all node pairs of single growing network realizations, on a linear scale versus \( t \) on a logarithmic scale.

![Figure 6. Semi logarithmic graph of the average path length vs the system size t for our model and BA model](image)

The data shows a linear trend, demonstrating the average path length increase logarithmically with the network size \( t \). In addition, from Figure 6, we can conclude that the local restriction of edges makes the average path length of our model larger than that of the BA model.
Since the network has a high clustering as $t \rightarrow \infty$ and the average path length scales as $L \sim \ln t$, our model displays the small-world properties.

4. RISK EVOLUTION TOPOLOGY MODEL

There are 27 risk and 51 evolution chain in the risk evolution model. These risk factors are more complex, they can be divided into risk from the air and risk from the ground.

In this model, in-degree and out-degree, the number of nodes and the number of branches can indicate the importance of risk. These topological features of some important risk factors are shown in Table 1.

<table>
<thead>
<tr>
<th>Risk</th>
<th>in-degree</th>
<th>out-degree</th>
<th>number of nodes</th>
<th>number of branches</th>
</tr>
</thead>
<tbody>
<tr>
<td>Departmental communication problems</td>
<td>1</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Loopholes in management</td>
<td>0</td>
<td>7</td>
<td>12</td>
<td>16</td>
</tr>
<tr>
<td>Bad weather</td>
<td>0</td>
<td>5</td>
<td>10</td>
<td>15</td>
</tr>
<tr>
<td>Bird pest</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>Pilot mistakes</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Runway incursion</td>
<td>3</td>
<td>1</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>Aircraft vehicle collision</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>Lack of safety awareness</td>
<td>1</td>
<td>1</td>
<td>7</td>
<td>10</td>
</tr>
<tr>
<td>Ground staff violation</td>
<td>2</td>
<td>4</td>
<td>11</td>
<td>15</td>
</tr>
<tr>
<td>Communication equipment fault</td>
<td>2</td>
<td>1</td>
<td>3</td>
<td>6</td>
</tr>
</tbody>
</table>

From Table 1 we can see that Pilot mistakes, Lack of safety awareness of the ground staff, Ground staff violation and Bad weather are the key nodes (factors) of the risk evolution topology model.

5. CONCLUSION

In this paper, on the basis of risk source identification, the airport runway risk evolution model based on complex network is proposed. The airport runway risk evolution mathematical model is described from clustering coefficient, average path length and degree distribution. From the perspective of modeling, this research only constructs the model of the topology structure of the risk evolution, and the model of the relationship between the risk evolution factors is still to be improved.

REFERENCES