Biodiversity as a security approach in ad hoc networks

1. Research Objective
Maintaining security within computer networks is a continuing problem. In scenarios such as digital virus epidemics, few operating systems and protocols can exacerbate the problem. Ecology research has found that undesirable disturbances to an ecosystem, such as the spread of viruses, can be reduced by increasing biodiversity. This research explores the effects of biodiversity as a security approach in ad hoc computer networks.

2. Ad Hoc Networks
An ad hoc network is characterised by devices connected in an arbitrary manner to form a network without a central controller. Messages are passed around the network in a series of hops. Ad hoc networks of the future are likely to interconnect applications such as home robots, wearable computers, and sensor networks. There are similarities between ad hoc networks and natural communities due to their movement and short range communication patterns making them a good candidate for studying the effects of biodiversity as a security mechanism.

3. The Biodiversity Benefit
Ecology research has found that biodiversity promotes resistance to disturbances against the functioning of the ecosystem. In an ad hoc network environment security attacks can create destructive disturbances at the individual (I), community (C) or the ecosystem (E) scale affecting the functioning of the services provided by the network.

4. Security Attack Disturbances
Common security attack disturbances causing effects at the community scale are shown here where network behaviours are affected.

<table>
<thead>
<tr>
<th>Attack Disturbances</th>
<th>Community Scale Effects</th>
</tr>
</thead>
<tbody>
<tr>
<td>Denial of Service</td>
<td>Reduced Availability for Network Communication</td>
</tr>
<tr>
<td>Impersonation</td>
<td>Excessive Network Delays</td>
</tr>
<tr>
<td>Message Modification</td>
<td>Increased or Bursts in Network Traffic</td>
</tr>
<tr>
<td>Message Replay</td>
<td>Sections of the Network Infrastructure Compromised</td>
</tr>
<tr>
<td>Black hole</td>
<td>Distorted Routing Behaviours</td>
</tr>
<tr>
<td>Eavesdropping</td>
<td>Little or no Change at the Community Level</td>
</tr>
</tbody>
</table>

5. Three Scale Biodiversity Strategy and Classification System
Measuring and applying biodiversity strategies within an ad hoc network ecosystem requires classification and measurements at different scales.

6. Community Scale Species Taxonomy
At the community scale one method of classification of ad hoc nodes is by a taxonomy system, similar to how species are classified.

7. Individual Scale Genotype & Phenotype
At the individual scale where genetic diversity is measured genotype classification can be used to classify differences in software and hardware composition. A binary vector can be used to identify the presence (1) or absence (0) of a particular software or hardware component (x1-x9).

Alternatively phenotype classification can be used to classify differences in the traits and characteristics of each node such as the communication frequency or migration rate. Each characteristic can be represented as a dimension with a scale representing the strength, so that each node will be a point in the vector space.

By applying biodiversity strategies at different scales, it is hypothesised that the destructive effects from security attacks can be tolerated to maintain ecosystem function.

Name: Jennifer Jackson – Complexity Science
Supervisors: Sadie Creese - WMG & Mark Leeson - Engineering
June 2010

Security Disturbances
Destructive E I
Constructive E C
Function & Services
Resilience
Biodiversity Strategies

Biodiversity Scales
Large scale: (Ecosystem)
Ecological Diversity
Classification of ad hoc network application environment
Diversity between clusters of large network or networks, between application environments or ecosystem services. Diversity changes over time

Medium scale: (Community)
Species & Functional Diversity
Taxonomy classification of ad hoc node types according to device product lines
Functional classification of ad hoc node types according to similarities in their processes
Quantification of different ad hoc node types, their distribution and topology

Small scale: (Individual)
Genetic Diversity
Structural classification of software & hardware composition
Behavioural classification of traits & characteristics

Biodiversity Measurements

Biodiversity Strategies
Environmental & habitat changes
Biodiversity belts around homogeneous communities
Increase resources available
Provide incentives and benefit sharing schemes

Evolution & natural selection
Distributed complementary species attributes
Complementary functional groups
Introduce predators, competitors, or pathogens
Change the density of certain communities
Introduce varieties of a single species
Introduce a sacrificial species
Introduce a species that attracts beneficials
Employ species rotation or intermingling
Avoid hosts with similar vulnerabilities
Replace species with more resistant variety

Complementary functional groups
Introduce predators, competitors, or pathogens
Change the density of certain species
Introduce varieties of a single species
Introduce a sacrificial species
Introduce a species that attracts beneficials
Employ species rotation or intermingling
Avoid hosts with similar vulnerabilities
Replace species with more resistant variety

Node A difference vs Node B