A Flock-Based Model for Ad-Hoc Communication Networks

Christian Carling¹
Pontus Svenson²
Christian Mårtenson²
Henrik Carlsen¹

¹Division of Defence Analysis
²Division of Command and Control Systems
Swedish Defence Research Agency
S-172 90 Stockholm, Sweden
E-mail: carling@foi.se, ponsve@foi.se,
cmart@foi.se, hencar@foi.se
Vulnerability of Command and Control Networks

- In network-centric forces, the network itself will presumably be a prime target of enemy attacks.
- Need to assess vulnerabilities of different designs.
- Standard methods of Network Reliability unsuited for highly dynamic, mobile networks.
- Connectivity measures, Performability measures
- Probability of finding functional chains, small subgraphs more relevant for Network-centric operations.
Mobile Ad-Hoc Communication Networks

- Distributed communication system
- Messages routed through intermediate nodes
- Complexity caused by
  - Constant movement of units
  - Units enter and leave area of operations
Model structure

<table>
<thead>
<tr>
<th>Reliability</th>
<th>Diffusion</th>
<th>Resource allocation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time series analysis</td>
<td>Random graph model</td>
<td></td>
</tr>
</tbody>
</table>

Connectivity

Mobility model
Classes of mobility models

• Random models
  – random walk,
  – random waypoints

• Deterministic models
  – Rule-based,
  – predefined movement path
  – real mobility trace

• Hybrid models
Local neighbourhood for flocking behaviour
Basic steering rules

Separation: avoid collision towards average
Alignment: Steer towards the average heading of flock mates.
Cohesion: Steer position of flock mates.
Mobility regimes
Connectivity graphs
Results

- $p(k, t) = \#\text{nodes with } k \text{ neighbours}$
- Quick transient behaviour
Global efficiency

- Latora and Marchiori:
  \[
  E_{\text{glob}} = \frac{1}{n(n-1)} \sum_{i \neq j} \frac{1}{d_{ij}}
  \]
  where \(d_{ij}\) is the shortest distance
- Works for unconnected graphs
- Quick decay, stabilizes at value characteristic for phase.
Number of isolated nodes

- Fluctuates strongly—many units are periodically out of contact for a short while before they reconnect.
- Reaches stationary behaviour slower
Different communication ranges $d$

- Large $d = \text{almost complete graph}$
- Small $d = \text{isolated nodes}$
- Global efficiency for $d=0.5 \ r$ at $d=2r$ using “SOF dir”.
- Order of magnitude difference
- Very important to be able communicate longer!
- But this leads to increased risk of detection
Other types of motion

- Direction important
- CGF and SOF dir similar
- Stable against small perturbations
Summary of work so far

- Flocking model can simulate various behaviours
- Communication range d gives graphs
- Graphs differ for different behaviours
- Graphs are dynamic
- d has large impact on global efficiency
Future work

• Different types of units, Enemy units
• Network reliability
• Diffusion of information
• Random graph modelling
  – Define ensemble of communication graphs for different behaviours instead of simulating
• Resource allocation
  – functional chains
  – sensor-to-shooter
Vulnerability to attacks

- Physical attack
- Functional attack
- Semantic attack

- Remove nodes or edges
- Nodes change role in time
- Where should we attack enemy’s communication nets?
- Hijacking – feeding false data to information fusion node
Diffusion of information

- System is dynamical – nodes change characteristics
- Edges have lifetimes
- Information can spread not only through the connections, but also via physical movement of the nodes
- Give information to node, measure time needed to propagate to all fusion nodes
- Red and blue teams competing for information