### Objective

Automated Game Theoretic algorithm for detecting and preventing attack (injection of malicious packages) against a Wireless Sensors Network (WSN). In this way, Network Operators (Defender) follow the defending strategy that minimizes the impact of an attack by an Attacker.

### Model Analysis

#### 3.1. Intrusion Detection Model

This model determines the best strategy (i.e., optimal number of sensors and optimal tolerance) that the defender could choose in order to better protect the network.

- Decided by Attacker
- Decided by Defender
- Predetermined (reflect credibility of every sensor)
- Nash Equilibrium of matrix will be found

#### 3.2. Intrusion Prevention Model

Best strategy for the defender is found (i.e., optimal number of sensors and sensor recoveries).

- Decided by Attacker
- Decided by Defender
- Nash Equilibrium of that matrices will be found

### Results

#### Intrusion Detection Model

<table>
<thead>
<tr>
<th>Significance Coefficients</th>
<th>Optimal # of Sensors</th>
<th>Optimal Tolerance</th>
<th>Optimal # of Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>All equal to 1</td>
<td>511</td>
<td>0.8</td>
<td>400</td>
</tr>
<tr>
<td>Uniform (1,4)</td>
<td>503</td>
<td>0.85</td>
<td>400</td>
</tr>
<tr>
<td>Normal (2.5, 0.25)</td>
<td>500</td>
<td>0.85</td>
<td>400</td>
</tr>
</tbody>
</table>

#### Intrusion Protection Model

<table>
<thead>
<tr>
<th>Non-Iterated / Iterated</th>
<th>Optimal # of Sensors</th>
<th>Optimal # of Recoveries</th>
<th>Optimal Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-Iterated</td>
<td>200</td>
<td>1</td>
<td>Expon.(mean: 92.5)</td>
</tr>
<tr>
<td>Iterated</td>
<td>200</td>
<td>1</td>
<td>Poisson(mean: 65)</td>
</tr>
</tbody>
</table>

*At the iterated IPM, the number of rounds is determinant*

### Further Work

- Forecasting
- Investigate model's applicability in networks of varying densities and its scalability with increasing network size

Similar methods can be applied to Military Systems, Battlespace, Environmental or Infrastructure Monitoring etc.

### Sensomax

Sensomax and the simulations run with it are made by Mo Haghigi (Mo.Haghigi@bristol.ac.uk)

Sensomax is an agent-based WSN middleware, which supports concurrent execution in multiple applications, integrates different mechanisms for different operational paradigms, and facilitates application developers with a component-based architecture for seamless development process.

### References
