Challenges

• Security solution for mobile Ad Hoc networks
  ◆ Infrastructureless network
  ◆ Open and insecure wireless communication
  ◆ Highly dynamic due to mobility, channel error, node failure, node’s arrival and departure
  ◆ Occasional break-ins
  ◆ Security is a chain; it is as secure as the weakest link.
  ◆ In theory there is no difference between theory and practice. In practice, there is…

System Framework

Authentication

• Intrusion tolerant security solution set

Functionality | Design
---|---
Prevention | Localized authentication, Proactive protection
Detection | Local intrusion detection, Collaborative consensus
Reaction | Two-tie alarming

Design Goals

• Network performance centric security design
  ◆ Scalability
  ◆ Availability
  ◆ Robustness
  ◆ Communication overhead
  ◆ Computation complexity

• Intrusion tolerant security solution set
  ◆ Proactive prevention
  ◆ Intrusion detection
  ◆ Reactive protection

Intrusion Detection

• Local intrusion detection based on overhearing
  ◆ Suitable for ad hoc networks due to the lack of central monitoring point
  ◆ Inherent imprecision
  ◆ Tradeoff between detection probability and false detection probability

Authentication

• Network performance of different authentication schemes

<table>
<thead>
<tr>
<th></th>
<th>Centralized</th>
<th>Peer-to-Peer</th>
<th>Localized</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scalability</td>
<td>Bad</td>
<td>Bad</td>
<td>Good</td>
</tr>
<tr>
<td>Availability</td>
<td>Bad</td>
<td>Good</td>
<td>Good</td>
</tr>
<tr>
<td>Robustness</td>
<td>Bad</td>
<td>Good</td>
<td>Good</td>
</tr>
<tr>
<td>Communication</td>
<td>Centralized</td>
<td>Distributed</td>
<td>Localized</td>
</tr>
<tr>
<td>Computation</td>
<td>Heavy</td>
<td>Light</td>
<td>Light</td>
</tr>
<tr>
<td>Security Strength</td>
<td>Weak</td>
<td>Weak</td>
<td>Strong</td>
</tr>
</tbody>
</table>

• Localized authentication scheme

Alarming

• Two-tie alarming
  ◆ The bridge between authentication and intrusion detection
  ◆ Proposed for localized authentication and local intrusion detection
  ◆ The monitors send the intrusion detection result to the previous authenticators.
  ◆ The new authenticators acquire this result from the previous authenticators