**Sensor Networks**

- Functions
  - Sensing
  - In-network Processing
  - Ad-hoc Communication
- Applications
  - Military Surveillance
  - Homeland Security

**Node Compromises**

- Unattended, harsh, hostile environment
- Temper-resistant hardware is expensive
- Insider attacks become possible
- Behavior-based detections are error-prone
- Millions of checksum computations to generate distinguishable time difference
- Untrustworthy mobile verifier to enter sensor’s transmission range
- Remote attestation from BS can be affected by network channel collision and multi-hop distance

---

**Our Solutions – Distributed Software-based Attestation**

**Scheme I: Threshold Secret Sharing**

- Share Distribution
- Seed Recovery
- Attestation

**Scheme II: Majority Voting**

- Information Distribution
- Attestation

---

**Security Analysis and Performance Evaluation**

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Detection Rate</th>
<th>False Positive</th>
<th>Attacker Reward</th>
<th>Eavesdrop</th>
<th>Repaly</th>
<th>Message Dropping</th>
<th>Compromised Neighbors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheme I</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes, except to compromised cluster head</td>
</tr>
<tr>
<td>Scheme II</td>
<td>Higher</td>
<td>Lower</td>
<td>Lower</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Prototype Implementation**

- ROM space: 21KB out of 128KB program memory
- RAM space: 1KB out of 4KB data memory