Introduction

What:
- Developed a comprehensive attacker model for analyzing and comparing routing protocols.
- Developed an implementation of AODV for TelosB sensor motes (MoteAODV) and PC’s + PDA’s (xAODV).

Why:
- Focus on categorizing attackers instead of attacks.
- Earlier attacker models did not allow comparison of protocols.
- Previous AODV implementations did not include security.

How:
- Attacker model focuses on categorizing attackers by capabilities.
- Attacker model is protocol and topology agnostic allowing comparison of routing protocols and their security.
- MoteAODV includes timer-based events in AODV and supports AES-128, hash functions (MD5, SHA-256), and trust mechanisms.
- xAODV includes an extensible framework for testing future protocol modifications.

Attacker Model

Existing Models:
- Proposed for specific protocol, not general use.
- Categorize attacks, then transfer categorization to attackers.
- New attacks might require requiring new categorization.

Our New Model:
- Categorizes attackers based on their capabilities.
- Communication:
  - Receive (passive) vs. send (active)
  - Single node vs. colluding attackers vs. Dolev-Yao equivalent
- Computation:
  - Ability to encrypt/decrypt messages
  - Knowledge
  - Collusion

Advantages of New Model:
- Easier to model more general attacker.
- Yields necessary and sufficient capabilities for an attack.
- Easily evaluate new protocol for vulnerability to known attack.

MoteAODV

Implementation:
- Route expiry, HELLO message, micro-ack alternative.

Security Using Pre-Shared Keys and Trust:
- Implements AES-128, MD5, SHA-256, and trust mechanisms.
- Benchmarks for individual operations (AES-128):

<table>
<thead>
<tr>
<th>Operation</th>
<th>Textbook</th>
<th>Improved</th>
<th>Assembler</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption</td>
<td>1.9944 ms</td>
<td>1.6377 ms</td>
<td>1.3001 ms</td>
</tr>
<tr>
<td>Decryption</td>
<td>2.3652 ms</td>
<td>1.9964 ms</td>
<td>1.6855 ms</td>
</tr>
<tr>
<td>Enc/Dec (CTR)</td>
<td>3.5411 ms</td>
<td>2.9900 ms</td>
<td>2.3769 ms</td>
</tr>
</tbody>
</table>

- Benchmarks for MoteAODV protocol performance:

xAODV

Implementation:
- Cross-platform runs on Zaurus SL-5500 and standard PC’s.

Security Using ECC and Trust:
- Implements Elliptic Curve Cryptography and trust mechanisms.
- Benchmarks for individual operations (ECC):

<table>
<thead>
<tr>
<th>Curve</th>
<th>Sig. Gen. w/o Opt. (ms)</th>
<th>Sig. Gen. w/ Opt. (ms)</th>
<th>Sig. Verif. (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>sect163k1</td>
<td>30.704</td>
<td>0.404</td>
<td>59.986</td>
</tr>
<tr>
<td>prime192v1</td>
<td>43.216</td>
<td>0.416</td>
<td>52.840</td>
</tr>
<tr>
<td>secp224r1</td>
<td>60.202</td>
<td>0.452</td>
<td>73.840</td>
</tr>
<tr>
<td>prime256v1</td>
<td>83.458</td>
<td>0.494</td>
<td>103.322</td>
</tr>
</tbody>
</table>

- Benchmarks for xAODV protocol performance:

Future Work
- Analyze and compare various routing protocols in our new model.
- Test additional protocol extensions for MoteAODV and xAODV.