Vehicle Safety Communications - Applications (VSC-A) Project: Security for Vehicle Safety Messages

Sue Bai
Honda Research Americas, Inc.
Security for V2V Safety Messages

- **Overall objective:** Improve existing vehicle-to-vehicle (V2V) communication security schemes
  - Efficient authentication of V2V safety communications (>1000 received messages per second)
  - Dealing with privacy concerns due to periodic V2V safety communications (10 messages per second)

- Extend IEEE 1609.2 and VII-C results regarding V2V safety communication security

- Conform to IEEE 1609.2 and rely on VII-C results regarding infrastructure and management
Activities

• Cost / run-time performance
  • Avoid dedicated hardware
    • Cost handicaps market penetration
    • Security updates are cumbersome
  • Potentially piggy-back on existing processor to run security solution

• Over-the-air (OTA) bandwidth overhead
  • Bandwith is an issue, even regardless of security
  • Can bandwidth overhead due to security be reduced without loss of security and reliability?
Activities (continued)

Privacy protection

- Adapt privacy protecting mechanisms for V2V safety applications
- Utilize VIIC solutions
- Potentially, consider deployment without supporting infrastructure (RSEs)
## Time Schedule

<table>
<thead>
<tr>
<th>2007</th>
<th>2008</th>
<th>2009</th>
</tr>
</thead>
<tbody>
<tr>
<td>Definition of Threat Model</td>
<td>Definition of Security Requirements</td>
<td>Implementation, Refinement, and Evaluation of Security Protocol</td>
</tr>
<tr>
<td>Selected Protocols for Level I Test Bed</td>
<td>Definition and Evaluation of Potential Protocols</td>
<td>Level I Test Bed Implementation</td>
</tr>
<tr>
<td>Definition of Interface between OBE and Security Module</td>
<td>Implementation, Refinement, and Evaluation of Security Protocol</td>
<td>Level II Test Bed Implementation</td>
</tr>
<tr>
<td>Definition of Over-the-Air Message Format</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Implemented Security Protocols

- Certificate distribution
  - Do not attach certificate to each message
  - Balance availability of certificates and OTA bandwidth

- Authentication protocols:
  - Reference protocol: IEEE 1609.2 / ECDSA\(^1\)
  - TESLA\(^2\) [3, 4, 5, 6]
  - TADS (TESLA Authentication and Digital Signatures) [1]
  - Verify-on-Demand [2]

\(^1\)ECDSA: Elliptic Curve Digital Signature Algorithm
\(^2\)TESLA: Timed Efficient Stream Loss-tolerant Authentication
## Implemented Security Protocols

<table>
<thead>
<tr>
<th>Properties</th>
<th>ECDSA (IEEE 1609.2)</th>
<th>TESLA</th>
<th>TADS</th>
<th>Verify-on-Demand</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Standardized</td>
<td>Two-step protocol</td>
<td>Combination of ECDSA and TESLA</td>
<td>Only verify messages that have actual impact</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Time-dependent</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Computation</td>
<td>Demanding</td>
<td>Highly efficient</td>
<td>Highly efficient</td>
<td>Efficient</td>
</tr>
<tr>
<td>Time delay</td>
<td>Medium / Deterministic</td>
<td>Varies (very low – higher than ECDSA)</td>
<td>Reasonable / Adjustable</td>
<td>Reasonable / Deterministic</td>
</tr>
<tr>
<td>OTA overhead</td>
<td>Reasonable</td>
<td>Varies</td>
<td>Slightly higher</td>
<td>Reasonable</td>
</tr>
</tbody>
</table>
Next Steps

• Evaluate performance/scalability of potential protocols through extensive network simulations

• Adapt security module software to run on same CPU as safety applications

• Bring in expertise and results to IEEE 1609.2 (DSRC Security Standard)

• Decide on one security protocol

• Perform third-party evaluation of protocol
Open Issues

• Public Key infrastructure
  • How to organize the keys
  • Detection of malicious vehicles
  • Revocation of vehicles

• Privacy
  • Technical challenges
  • Governance issues
Thank You