Misbehavior detection in C-ITS

Secure Cooperative Autonomous systems (SCA) project approach

Arnaud Kaiser (arnaud.kaiser@irt-systemx.fr)
ETSI ITS Workshop – 4-6 March 2019 – Sophia Antipolis
SCA project overview

Misbehavior detection
  • Overview
  • 3-steps process
    o Local detection
    o Reporting
    o Global detection

SCA project current status and next-steps
SCA project overview

- **SCA Start**: July 1, 2017
- **SCA End**: July 1, 2020

Timeline:
- **2017**
  - T1
  - T2
  - T3
  - T4
  - **SCA Start**

- **2018**
  - T1
  - T2
  - T3
  - T4
  - **Protection Profiles**

- **2019**
  - T1
  - T2
  - T3
  - T4
  - **Use Cases**

- **2020**
  - T1
  - T2
  - T3
  - T4
  - **Tests and Evaluation**

- **Today**

Use Cases, V2X stack, PKI, Authority, Demonstrator, Risk analysis, Architecture, Misbehavior Authority, Demonstrator, Tests and Evaluation.
SCA key challenges

Use cases cooperative autonomous vehicle
- Use cases C-ITS
- Risk analysis
- Performance criteria
- C-ITS privacy
- Evaluation

Crypto-agility & Business continuity
- Misbehaviour detection
- Crypto-agility
- Updates over-the-air

Compliance assessment & Penetration tests
- Test tools development
  - Security conformity
  - Penetration testing
- Dimensioning evaluation in a real case

Interoperability & Scalability
- End-to-end hybrid networks security
- Interoperability with C-ITS entities (IoT-like)
- PKI scalability and dynamic dimensioning
C-ITS privacy
- Pseudonym change policies / lifecycle
- Privacy threats: social & legal issues
- Security performance, privacy technology assessment

Misbehaviour detection
- Embedded side (OBU) and infrastructure side (MA)

PKI dynamic dimensioning
- On-demand dimensioning
- Impact of pseudonym change policies (pseudonym reload)

E2E security for hybrid networks
- Multiple connectivity in ITS-S: ITS-G5, LTE, Wi-Fi, etc.
- Multiple patterns to support application requirements
- Fulfill security requirements

Crypto-agility
- Design of crypto-agile security protocols
- Fulfill performance requirements especially for embedded systems
**Current C-ITS system:**
- RSUs and OBUs
- Communication based on:
  - ITS-G5
  - 5G
- Messages:
  - Beacon (CAM)
  - Warning (DENM)
- A Backend
  - PKI, MA
- PKI infrastructure:
  - Long- and short-term certificates

**C-ITS System overview**
Misbehavior detection

Objective: Reliable identification of bad actors

Two different levels:

- **Local MBD**: The process of identifying misbehavior at the device level
- **Global MBD**: The process of identifying misbehavior at a backend
Step 0: State-of-the-art analysis (1)

- **MBD largely studied in the scientific literature (2006 -> present)**
  - Some of the proposed solutions may not be appropriate

- **Classification & evaluation of state-of-the-art solutions**
  - Evaluation criteria:
    - Regulations/privacy compliance
    - Compatibility with what had been standardized
    - Requires specific HW equipments
  - Detected attacks:
    - Sybil
    - Bogus info

'Misbehavior detection’ trend according to google scholar
Summary of the feasibility challenges

<table>
<thead>
<tr>
<th>Detection Method</th>
<th>Current feasibility</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Standard</td>
</tr>
<tr>
<td>Path History</td>
<td></td>
</tr>
<tr>
<td>RSU linkability</td>
<td>+</td>
</tr>
<tr>
<td>Neighbor List</td>
<td>+</td>
</tr>
</tbody>
</table>

**Beacon Messages**

<table>
<thead>
<tr>
<th>Sybil &amp; Bogus</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>RSU triangulation</td>
<td>✓</td>
</tr>
<tr>
<td>Signal Properties</td>
<td>✓</td>
</tr>
<tr>
<td>Data-Centric</td>
<td>✓</td>
</tr>
<tr>
<td>Info Exchange</td>
<td>✓</td>
</tr>
</tbody>
</table>

**Warning Messages**

<table>
<thead>
<tr>
<th>Bogus Info</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Reputation-Based</td>
<td>×</td>
</tr>
<tr>
<td>Cooperative</td>
<td>×</td>
</tr>
<tr>
<td>Data-Centric</td>
<td>×</td>
</tr>
<tr>
<td>Pseudonym Linking</td>
<td>✓</td>
</tr>
</tbody>
</table>

✓: Compatible, -: Requires Adjustment/Study, ×: Incompatible

- **Regulations/Privacy requirements**
  Most difficult to adopt even if they present big advantages.

- **Standard incompatibilities**
  Changes in standards could be committed if the advantages are significant.

- **Equipment**
  Subject to the tradeoff between equipment costs and provided benefits.

**Publication**: J. Kamel, A. Kaiser, I. B. Jemaa, P. Cincilla and P. Urien, “Feasibility study of misbehavior detection mechanisms in cooperative intelligent transport systems (c-its)”, IEEE VTC Spring, 2018
CAM-based local checks (Speed, Position, Range, …)

- **Plausibility checks**: Verification on the data accuracy based on a CAM
- **Consistency checks**: Verification of the data accuracy based on two consecutive CAMs

### Step 1: Local detection (2)

<table>
<thead>
<tr>
<th>App</th>
<th>Scenario Detectors</th>
<th>Evaluation Metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Recall</td>
<td>Precision</td>
</tr>
<tr>
<td><strong>Threshold</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Legacy</td>
<td>0.3976</td>
<td>0.9504</td>
</tr>
<tr>
<td>CaTch</td>
<td>0.4203</td>
<td>0.9457</td>
</tr>
<tr>
<td></td>
<td>△5.7%</td>
<td>△-0.5%</td>
</tr>
<tr>
<td>F₁ Score</td>
<td>BM</td>
<td>MCC</td>
</tr>
<tr>
<td>Legacy</td>
<td>0.5607</td>
<td>0.3834</td>
</tr>
<tr>
<td>CaTch</td>
<td>0.5819</td>
<td>0.4038</td>
</tr>
<tr>
<td></td>
<td>△3.8%</td>
<td>△5.3%</td>
</tr>
<tr>
<td><strong>Machine Learning</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Legacy</td>
<td>0.3928</td>
<td>0.9498</td>
</tr>
<tr>
<td>CaTch</td>
<td>0.7961</td>
<td>0.9102</td>
</tr>
<tr>
<td></td>
<td>△102.7%</td>
<td>△-4.2%</td>
</tr>
<tr>
<td>F₁ Score</td>
<td>BM</td>
<td>MCC</td>
</tr>
<tr>
<td>Legacy</td>
<td>0.5556</td>
<td>0.3783</td>
</tr>
<tr>
<td>CaTch</td>
<td>0.8494</td>
<td>0.7424</td>
</tr>
<tr>
<td></td>
<td>△52.9%</td>
<td>△96.2%</td>
</tr>
</tbody>
</table>

(b) Sybil Attack Scenario
### Security layer local checks, based on TS 103 096-2 and TS 103 097

#### Security profile
- **Version**
- **Signer**
  - Certificate
    - The certificate is an AT
    - The parent certificate is known
    - The parent certificate is an AA
    - Region
    - Certificate validity
    - Ascending order of header fields
    - Presence of aid ssp list
    - No duplicate AID
    - AID in certificate are also in the parent certificate
  - Certificate chain
- **Digest**
  - The corresponding certificate is known
- **Verification depending of the type**
  - **CAM security profile**
    - signer_info, generation_time and its_aid are not duplicated
    - Ascending order of header fields
    - No Forbidden header fields
    - The payload is present and its length is not null
    - The trailer is present and contains only the signature
- **DENM security profile**
  - signer_info, generation_time, generation_location and its_aid are not duplicated
  - Ascending order of header fields
  - No Forbidden header fields
  - The signer is a certificate
  - Location
  - The payload is present and its length is not null
  - The trailer is present and contains only the signature
- **Generic**
  - idem ci-dessus

#### Step 1: Local detection (3)

- **Structure (deserialization)**
- **Time stamp (generation_time)**
- **Security profile**
  - **Digest**
    - The corresponding certificate is known
  - **Verification depending of the type**
    - **CAM security profile**
      - signer_info, generation_time and its_aid are not duplicated
      - Ascending order of header fields
      - No Forbidden header fields
      - The payload is present and its length is not null
      - The trailer is present and contains only the signature
    - **DENM security profile**
      - signer_info, generation_time, generation_location and its_aid are not duplicated
      - Ascending order of header fields
      - No Forbidden header fields
      - The signer is a certificate
      - Location
      - The payload is present and its length is not null
      - The trailer is present and contains only the signature
    - **Generic**
      - idem ci-dessus

- **Signature**
  - Structure of the signature
Step 2: Reporting (1)

Our initial requirements:

1. Specify the sender and the reported identities
2. Specify the type of misbehavior
3. Specify the evidence
4. Reduce overhead
The proposed report protocol includes multiple key features:

1. Reducing overhead by linking reports
2. Authenticating the sender and reported ITS-S with a pseudonym certificate
3. Specifying the type of the detection
4. Specifying the evidence required by misbehavior type

**Misbehavior report key information:**
- Security header,
- Report ID,
- Related Report ID,
- Generation Time,
- Report Metadata,
- Reporter Information,
- Reported Message,
- Detection Type,
- Evidence

Level 1:
- One message

Level 2:
- N inconsistent messages

Level 3:
- Map of the Area
- Neighbors Messages

Level 4:
- One reported Message
- Sender sensor information (using the same objects as CPM)
Step 2: Reporting (4)

ASN.1 format

```
BEGIN
IMPORTS
TimestampTs, StationType, ReferencePosition, Heading, Speed, DriveDirection, VehicleLength, VehicleWidth, Curvature, LongitudinalAcceleration, CurvatureCalculationMode, YawRate, PerceivedObjectContainer, FieldOfViewContainer FROM ITS-Container { itu-t (0) identified-organization (4) etsi (9) itsDomain (5) wgl (1) ts (102894) cdd (2) version (1) }

EtsiTs10397Data, EtsiTs10397Certificate FROM EtsiTs10397Module { itu-t (0) identified-organization (4) etsi (0) itsDomain (5) wgs (5) ts (10397) v1 (0) }

-- The root data frame for report messages
Report ::= SEQUENCE {
  reportMetadataContainer ReportMetadataContainer, reportContainer ReportContainer
}

ReportMetadataContainer ::= SEQUENCE {
  reportID IASString, generationTime TimestampTs, relatedReportContainer RelatedReportContainer OPTIONAL
}

RelatedReportContainer ::= SEQUENCE {
  relatedReportID IASString, omittedReportsNumber OmittedReportsNumber
}

ReportContainer ::= SEQUENCE {
  reportedMessageContainer ReportedMessageContainer, detectionTypeContainer DetectionTypeContainer, evidenceContainer EvidenceContainer OPTIONAL
}

ReportedMessageContainer ::= CHOICE { certificateIncludedContainer CertificateIncludedContainer, certificateAddedContainer CertificateAddedContainer
```
Step 3: Global detection (1)

Some examples of use cases

Reporting ITS-S

Misbehaving ITS-S

Falsified CAM
MB Report

Falsified AT requests
MB Report

Reporting PKI
The global misbehavior detection is performed by the MA and consists of the following steps:

- **Correlation**: Cross-reporting and validation of reports structure
- **Decision**: Misbehavior accuracy and classification
- **Reaction**: Response to the misbehaving ITS station (Revocation, Suspension, Notification, ...)

**Misbehavior authority process**

Incoming MB Reports → Correlation → Decision → Reaction
Step 3: Global detection (3)

- **Correlation / Decision**
  - Artificial Intelligence (AI) techniques.
  - Machine Learning algorithms for misbehavior classification.

- **Reaction:**
  - **Long-term reaction:** Revocation of misbehaving ITS stations by notifying the PKI (EA) to reject all their new authorization requests. This is also called *passive revocation*.
  - **Short-term reaction:** Revocation of pseudonyms (ATs) at the level of ITS stations by providing a CRL with a list of certificates to be ignored during V2X communications. This is also called *active revocation*.
Framework For Misbehavior Detection (F²MD)

- F²MD is a VEINS Module. (Omnet++, Sumo)
- This project is open source and available at:
  - https://github.com/josephkamel/F2MD
  - https://www.irt-systemx.fr/f2md/
  - https://veins.car2x.org/documentation/modules/#f2md
## Misbehavior detection & PKI V2 evaluation

<table>
<thead>
<tr>
<th>Current status</th>
<th>PKI V2</th>
<th>Misbehavior Detection</th>
</tr>
</thead>
<tbody>
<tr>
<td>PoC implemented (on-table)</td>
<td>First tests by simulation</td>
<td></td>
</tr>
<tr>
<td>PKI V2 deployed</td>
<td>Contributions to TR 103 460 (State of art, MBR)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TODO</th>
<th>PKI V2</th>
<th>Misbehavior Detection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Validation at ETSI plugtests 2019</td>
<td>PoC implementation (on-table)</td>
<td></td>
</tr>
<tr>
<td>Evaluation in real experimentations</td>
<td>Evaluation in real experimentations</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Real experim.</th>
<th>PKI V2</th>
<th>Misbehavior Detection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance evaluation</td>
<td>Performance evaluation</td>
<td></td>
</tr>
<tr>
<td>Logs generation for privacy evaluation (AT change policies)</td>
<td>Logs generation to improve ML algorithms (training)</td>
<td></td>
</tr>
</tbody>
</table>

### Timeline

- **2017**: SCA Start, July 1, 2017
- **2018**: Use Cases, Protection Profiles
- **2019**: V2X stack, PKI v2, Risk analysis, Misbehavior Authority, Demonstrator
- **2020**: Tests and Evaluation, SCA End, July 1, 2020