

Certificate Revocation List Distribution in Vehicular Communication Systems

Panos Papadimitratos, Ghita Mezzour, and Jean-Pierre Hubaux
{panos.papadimitratos, ghita.mezzour, jean-pierre.hubaux}@epfl.ch

Laboratory of Computer Communications and Applications (LCA-1)
EPFL, Switzerland

Context

- Vehicular Communications (VCs)
- Large-scale and multi-domain VC systems
- Secure VC architecture
- Faulty, compromised, or illegitimate VC devices should be evicted

Problem at Hand

- Distribute Certificate Revocation Lists (CRLs) to all vehicles within a domain in a timely manner

Challenges

- Scalability
 - Numbers of circulating and revoked vehicles
 - Multiple regions and Certification Authorities (CAs)
- Vehicular communication
 - Road-Side infrastructure Units (RSUs) are not pervasive
 - Short vehicle-RSU contact times
 - Bandwidth constraints

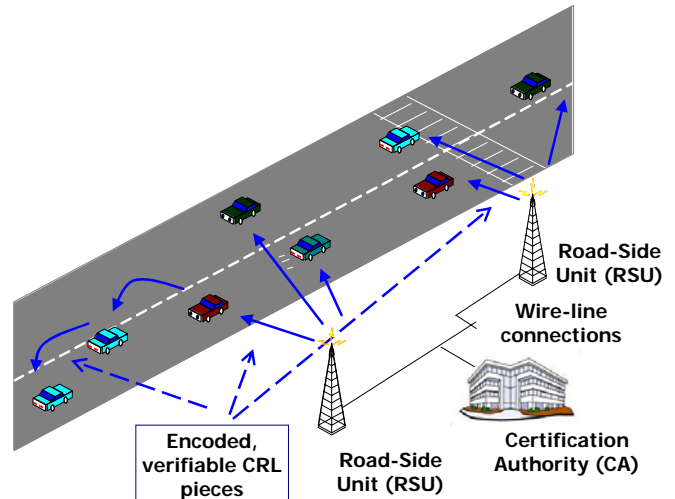


Illustration of the CRL distribution

System Operation

- Collaboration between domains (regional CAs)
 - Regional CRLs
 - Issuance of Foreigner Certificates
- Encoded, verifiable CRL pieces
 - Erasure or Fountain codes
 - M segments of the CRL encoded into $N > M$ or a stream of pieces
 - Piece authentication and integrity
- Multi-RSU CRL distribution
 - Uncoordinated broadcast of CRL pieces, at rate r_B kbps by each RSU, within its range R meters
 - Average RSU spacing D meters

Conclusions

- Robust CRL distribution within an average commute time
- Low overhead and simple operation
 - CRLs transmitted at few kbps
 - No RSU – RSU interactions
 - Minimal CA – RSU interactions
- Future work
 - Design trade-offs
 - Vehicle-to-vehicle CRL dissemination complement

System Performance

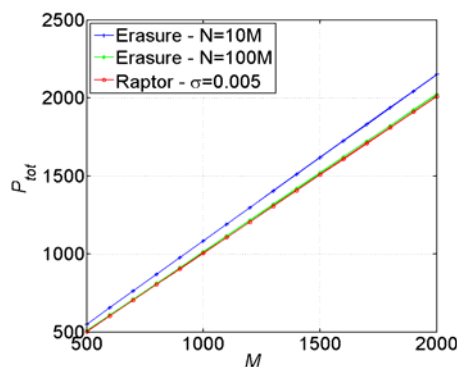
- Practically all ($x\% \rightarrow 1$) vehicles in a region should receive in a timely manner the most up-to-date CRL
- Recovery (with high probability) of the entire CRL (M segments) after receiving P_{tot} encoded pieces

- Erasure codes:
$$P_{tot} = \sum_{i=1}^M \frac{N}{N-i} + 3.9 \sqrt{N \sum_{i=1}^M \frac{i}{(N-i)^2}}$$

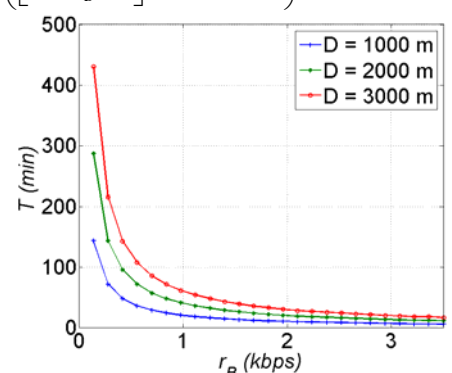
- Raptor codes:
$$P_{tot} = (1 + \sigma)M$$

- Average time to complete the CRL, for piece size sz bits and average vehicle velocity v meters/sec:

$$T = \frac{1}{v} \left(\left[P_{tot} \frac{sz \cdot v}{r_B \cdot R} \right] (R + D) + R \right)$$



Number of pieces to be received (P_{tot}) vs. number of original CRL pieces (M)



Acquisition delay (T) for a 200 Kbyte CRL vs. broadcast bandwidth (r_B)