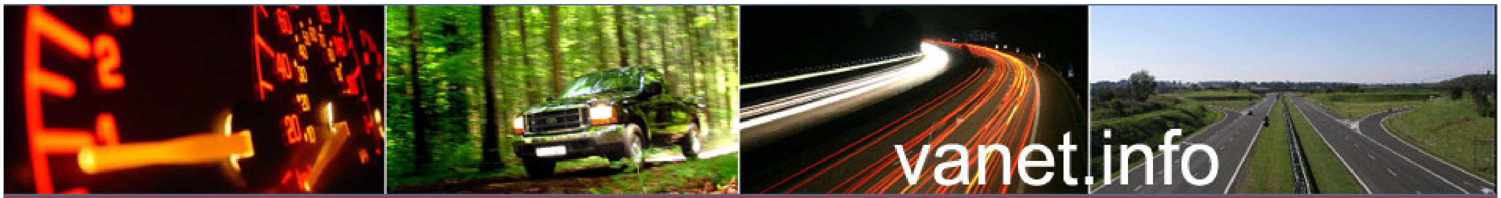


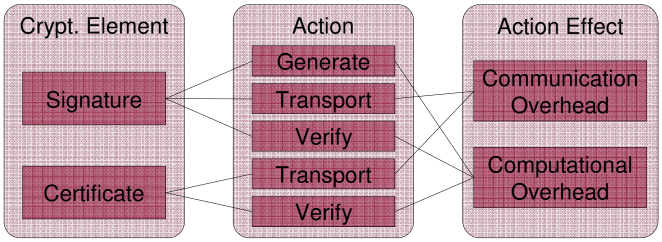
Secure and Efficient Beaconing for Vehicular Networks

Frank Kargl, Elmar Schoch, Björn Wiedersheim – Ulm University
Tim Leinmüller – DENSO Automotive Deutschland GmbH

Problem

Securing beacon messages creates overhead

Adding *cryptographic integrity protection* to beacon messages *enlarges packets* and *requires additional computations* by sender and receiver. Packets need to carry the packet signature and certificate of the sender. When using efficient Elliptic-Curve-Cryptography, this requires about *160 extra bytes per beacon*. Senders must calculate the signature; receivers must verify the signature and the certificate.


Crypt. Element
Signature
Certificate
Action
Generate
Transport
Verify
Transport
Verify
Action Effect
Communication Overhead
Computational Overhead

Solution

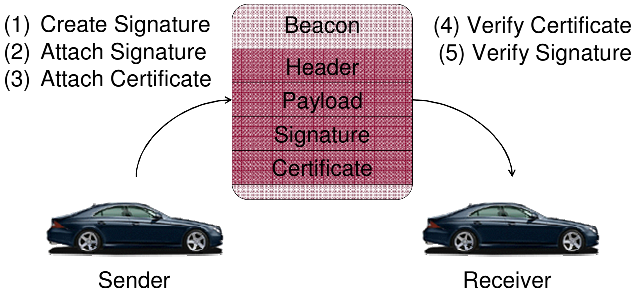
Signature and certificate omission strategies

Omit certificates (3) and certificate verification (4)

If receivers already know the sender's certificate, the certificate does not need to be attached to the beacon(3). If receivers have verified the certificate in earlier beacons, the verification can be skipped (4).

In critical cases new neighbors receive beacons that do not contain a certificate without having received this certificate earlier. This leads to "not instantly verifiable beacons" that can later be verified after receiving the certificate.

We propose a Neighbor-based Certificate Omission strategy where nodes attach certificates to a beacon whenever their neighbor table has changed.


(1) Create Signature
(2) Attach Signature
(3) Attach Certificate
Beacon
Header
Payload
Signature
Certificate
(4) Verify Certificate
(5) Verify Signature
Sender
Receiver

Omit signature verification (5)

All beacons carry signatures and certificates. To save computational overhead, a receiver decides to verify only a certain percentage of beacon signatures. Selection of beacon signatures to be verified can be periodic, context-adaptive, or situation-aware.

Context-adaptive signature verification:

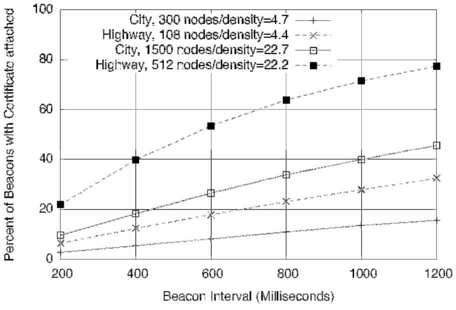
1. predict future movement of neighbor vehicles (e.g. using Kalman filter)
2. if observed movement deviates significantly from expected behavior, verify signature
3. else omit signature verification

Omit signatures (2) (5)

Periodic signature omission: sign only every n^th^ packet. Signed packets provide trusted information that is filled up with untrusted information that is sent at a higher rate. If untrusted information deviates significantly from trusted data, it may be disregarded.

Situation-based signature omission: All beacons are unsigned by default. If vehicles detect potentially dangerous situation (e.g. two vehicles approaching each other at high speeds) subsequent beacons are signed.

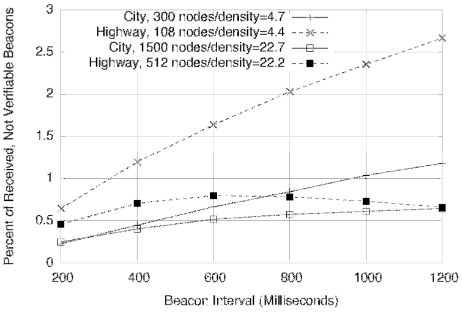
Evaluation



Neighbor-based Certificate Omission:
Percentage of beacons with attached certificates

Simulation-based evaluation of neighbor-based certificate omission shows that 20% to 95% of certificates can be omitted. At the same time, less than 3% of beacons where not instantly verifiable due to missing certificates at the receiver.

Simulation settings: JiST/SWANS; STRAW/highway mobility model; node velocity 25 m/s (city), 40 m/s (highway); 60 / 300 s simulation time; 5 / 10 runs per parameter set.



Neighbor-based Certificate Omission:
Percentage of not instantly verifiable beacons

Contact

For more information please contact: Frank Kargl | Institute of Media Informatics | Ulm University | frank.kargl@uni-ulm.de