**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.

---

**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.

---

**Evaluation**

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.

---

**Contact**

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