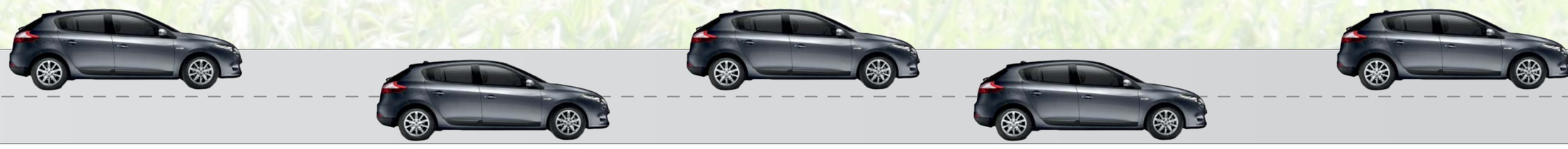
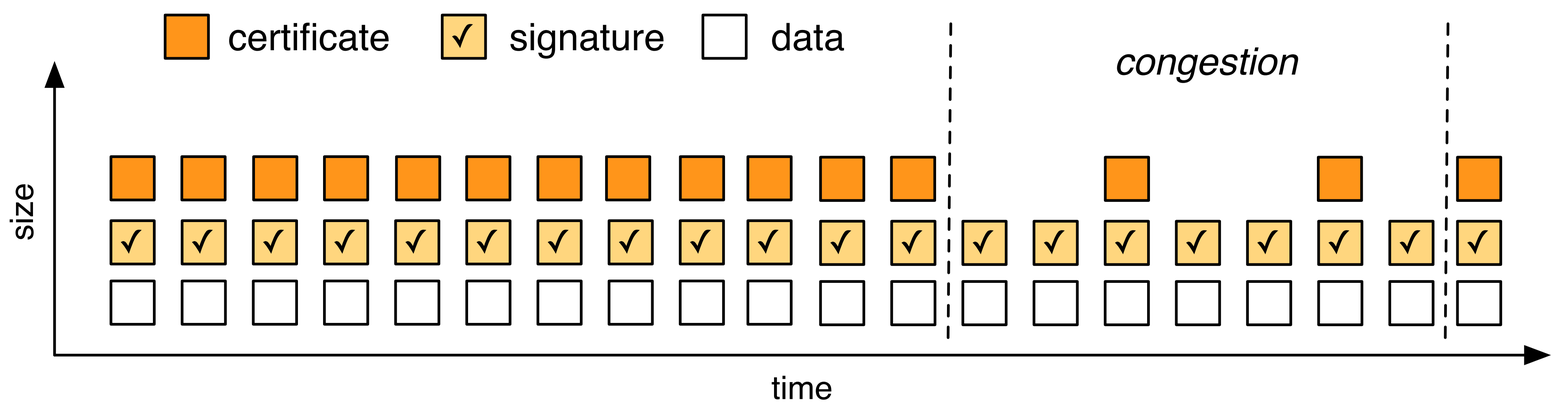
Pre-distribution of certificates for pseudonymous broadcast authentication in VANET

Michael Feiri
Rolf Pielage
Jonathan Petit
Nicola Zannone
Frank Kargl

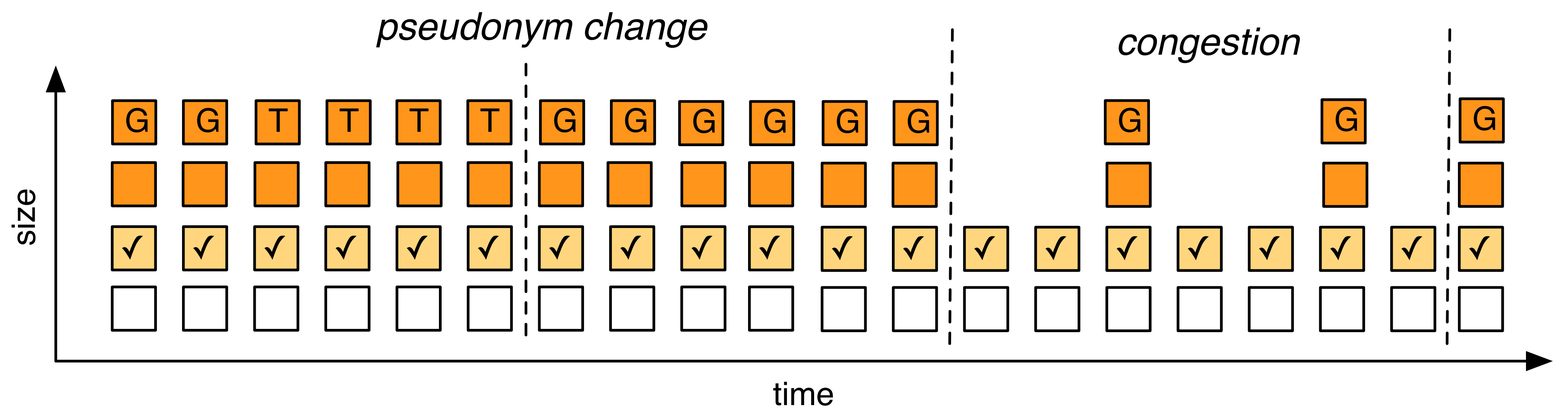


Secure communication consumes extra bandwidth for certificates

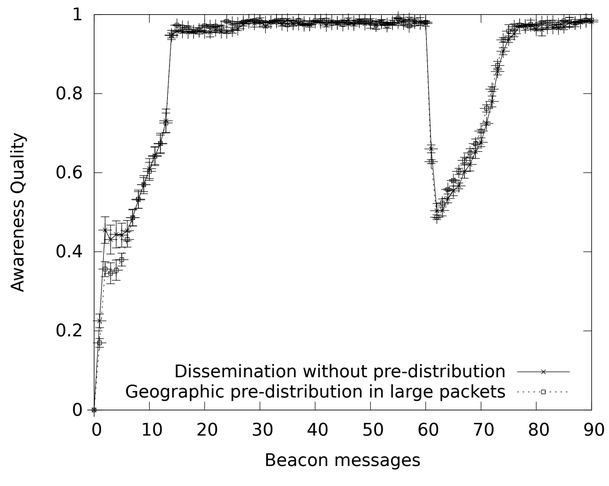
Vehicular ad-hoc networking (VANET) uses digital signatures to authenticate messages. However exchanging pseudonymous certificates creates communication overhead. **Omission** of certificates can reduce this overhead, but can introduce **cryptographic packet loss** when a certificate is not available immediately.

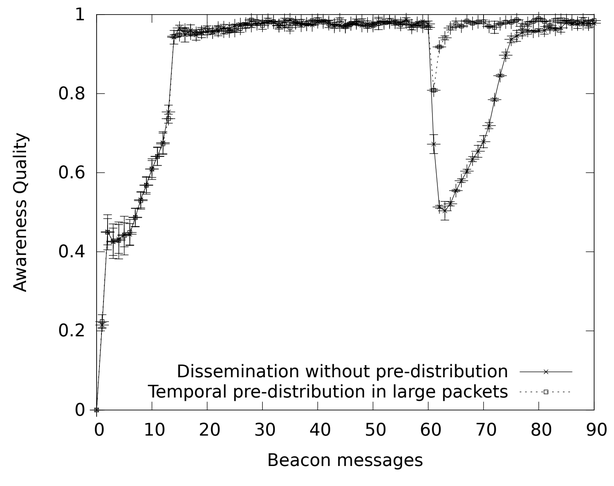


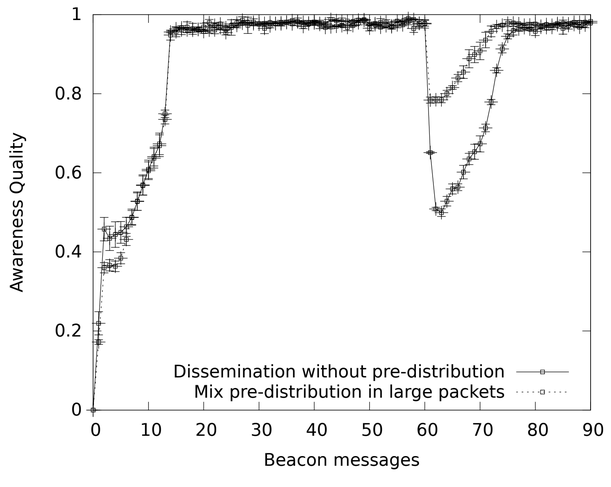
Times of low congestion can be used to **geographically** G pre-distribute certificates to avoid cryptographic packet loss later. Similarly certificates can be pre-distributed **temporally** T when the sender knows that a certificate will change soon.



Certificate omission and pre-distribution reduce information loss







We used application level **awareness quality** to evaluate the performance of certificate pre-distribution. A simulation study showed that **geographic** pre-distribution over **one-hop** has only minimal effects. More elaborate dissemination techniques, such as **multi-hop**, need to be evaluated. Temporal pre-distribution was very effective at minimizing cryptographic packet loss due to pseudonym changes. **Temporal pre-distribution makes pseudonym changes safe**.

Technische Universiteit Eindhoven University of Technology
University College Cork, Ireland Coláiste na hOllscoile Corcaigh
Deloitte.
UNIVERSITÄT ULM · SCIENDO · DOCENDO · CURANDO
UNIVERSITY OF TWENTE.

Supported by the **PRESERVE** project, which is part of the Seventh Framework Programme of the European Commission
Duration: 01/2011–06/2015
Reference: IST-269994