Secure and Efficient Beaconing for Vehicular Networks

Frank Kargl*, Elmar Schoch*, Björn Wiedersheim*, Tim Leinmüller+
*Ulm University, Institute of Media Informatics, Ulm, Germany
+DENSO Automotive Deutschland GmbH, Eching, Germany
givenname.surname@uni-ulm.de, t.leinmueller@denso-auto.de

ABSTRACT

The basis for many VANET applications are periodic beacons carrying information like location, heading and speed. In order to secure beaconing, messages should be signed and carry a certificate to attest valid network participants. In order to reduce the significant communication and computational overhead created by this, we propose to skip signatures or certificates in certain situations.

Categories and Subject Descriptors: C.2.0 [Computer-Communication Networks]: General

General Terms: Security, Reliability, Performance.

Keywords: Vehicular ad hoc networks (VANETs), Security, Efficiency

1. INTRODUCTION

Looking at recent standardization efforts and fields tests it becomes clear that beaconing will initially be a cornerstone for upcoming C2X eSafety applications. With beaconing we denote the periodic transmission of packets containing a vehicle's position and other information as a (single-hop) link-layer broadcast to all neighboring vehicles or road-side units. Implemented in an insecure way, beaconing opens opportunities for abuse. To address these problems, many security solutions suggest to use signatures based on asymmetric cryptographic mechanisms like ECDSA together with more mechanisms [2, 3]. The basic strategy is to equip vehicles with asymmetric cryptographic key pairs (VK, SK) and certificates $(Cert)$ issued by a trusted certification authority (CA). Then all beacons get signed using the vehicle's signature key SK and receivers verify them using the verification key VK. Signature and certificate containing VK are attached to the beacon. This mechanism introduces two significant problems:

1. Adding signatures and certificates to the beacons creates a notable **protocol overhead**. Even when using an ECC-based solution with comparatively small overhead, signature plus certificate require at least $150 - 160$ bytes [2].
2. Creating and verifying signatures causes significant **computational overhead**. Every sent beacon needs one signature generation and two verifications (signature plus certificate). Assuming a maximum neighbor number of 200 vehicles and a beaconing rate of 10Hz, a vehicle needs to generate 10 signatures and verify 4000 signatures per second, which exceeds the capacity of typical vehicle on-board units. As cost constraints in vehicle manufacturing are high and on-board units need to be cheap, this cannot be addressed only by using more powerful hardware.

VANET'08, September 15, 2008, San Francisco, California, USA.
ACM 978-1-60558-191-0/08/09.

2. EFFICIENT SECURE BEACONING STRATEGIES

Aiming at reduction of protocol and computational overhead, we propose the following approaches:

Omitting Certificates and Certificate Verifications: When verifying the validity of a certificate, this corresponds to one signature verification. By storing already verified certificates locally, subsequent beacons containing the same certificate can be verified without cryptographic operation. This already cuts the computational costs of handling received packets almost by half, yet to the cost of some more memory.

Additionally, storing certificates opens up the opportunity to omit the certificate in subsequent packets from the same node. If the signature and an ID allowing the identification of the corresponding verification key is contained in a beacon, a receiving node can use the verification key out of the previously retrieved and checked certificate to verify the signature of the new packet. In summary, one can omit attaching certificates to every packet without reducing security if communication partners have already exchanged their certificates previously.

However, omitting certificates in beacons may lead to the situation that a node receives a packet from a neighbor without having received a certificate earlier. In this case, such a packet must be regarded as invalid or signature verification must be delayed until the verification key VK is available. But as the omission of a certificate saves more than 100 bytes per packet, we suggest to analyze strategies where certificates can be omitted while minimizing the described situation of unverifiable packets.

The approach in [1] proposes to leave out certificates on a periodic schedule, which means that only every n^{th} beacon packet contains a certificate. This approach saves a constant amount of bandwidth, but it does not consider the current vehicle context. Therefore, we propose a neighbor-based scheme that takes into account topology changes explicitly. The idea is to utilize the fact that every node knows its

neighbors in wireless transmission range through beaconing. Therefore, a node can monitor neighborhood changes and base the decision whether to attach a certificate or not on these changes. If new neighbors have been added to the neighbor table since the last beacon, the next beacon gets attached a certificate, otherwise not. The evaluation of this scheme in Section 3 shows how effectively it adapts to topology changes and beacon interval.

Omitting Signatures: Omitting not only the certificates but also the signatures has the big advantage to reduce communication overhead and computation overhead for some beacons to almost zero, obviously to the disadvantage that forging and modification attacks on beacons become possible. The assumption behind the idea to omit signatures is that not all beacons will trigger safety related applications but are used in less safety critical use-cases. So it might be acceptable to selectively activate signatures, e.g. following a periodic schedule or depending on the situation.

Different strategies for omitting signatures include periodic signing, where only every n^{th} beacon is signed. This provides something like a reliable movement pattern for every vehicle, filled with additional unreliable information for the path in between the secured steps.

The major drawback of the periodic omission is that in potentially dangerous situations, the rate of trustworthy information that a vehicle can base potentially safety critical decisions on decreases to the rate of available signed beacons. To better address this issue, we propose situation-based signature omission. In this approach, all beacons are unsigned by default. Only in case that a vehicle detects a potentially dangerous situation, it starts to sign its beacons. Neighboring vehicles are expected to act likewise.

Potentially dangerous situations can be detected using insecured beacons, but only if the source of the previously unsigned beacons switches to secured beacons as well, the situation is actually taken into account by the safety applications. The detection could work by considering a certain safety distance that two vehicles must not fall short of. Another approach is to predict potential collisions based on current movement vectors.

Omitting Signature Verification: Assuming that signatures are attached to all of the beacons, their cryptographic verification is computationally expensive. Computational load is more or less exclusively determined by signature verifications and not by signature generations. On the one hand, this is due to the characteristics of ECDSA, where a signature verification is about three times more costly than a generation. Even more severe, in dense traffic a vehicle will receive a magnitude more packets than it sends and will thus have to do much more signature verifications than generations.

The idea of signature verification omission is that it is up to the receiver to decide, which packet signatures it will actually verify. This has the advantage that the receiver can control its computational load based on the current situation. The drawback is of course that an attacker might inject spoofed packets with invalid signatures hoping that receivers will not check them.

The question remains how to select packets to be verified. Here, strategies include *periodic verification*, *context-adaptive verification*, and *situation-aware verification* which will be described in more detail in future work. To highlight the idea of context-adaptive verification: vehicles can use linear predictions (e.g. based on Kalman filters) to extrapolate future positions, speed, etc. for each neighbor vehicle.

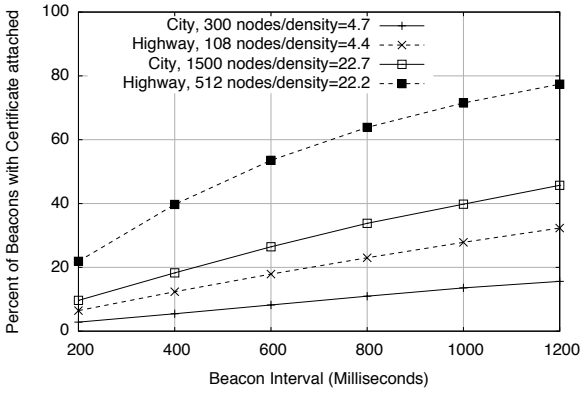

Figure 1: Percent of beacon packets of all sent beacons, where a certificate was attached

If future beacons from such a neighbor are sufficiently close to the predictions, the vehicle "behaves as expected" and signature verifications may be omitted. If prediction and actual values differ significantly, the neighbor vehicle makes unexpected movements and the signatures will be checked. For new neighbors, signatures will always be checked.

3. EVALUATION

In order to show the effectiveness of our approaches, we conducted extensive simulations that show the savings in terms of communication and/or computational overhead and also the rate of unverifiable packets. Whereas full details of this evaluation will be given in future work, we want to highlight some of our results shown in Figure 1. For this simulation, we have implemented certificate omission based on neighbor changes. As shown in Figure 1, depending on traffic model (city or highway traffic), traffic density, and beacon intervals, the number of beacons with certificates is significantly reduced. With small beacon intervalls, which are often recommended for faster reaction times of eSafety applications, more than 80% of certificates can be omitted, resulting in large bandwidth saving. At the same time, analysis of simulation results shows that the number of beacons that are not instantly verifiable due to unknown certificates is in the order of 1%.

Our other results are also promising and indicate, that the degree of security that is lost by our schemes is by magnitudes smaller than the performance and bandwidth gain. The freed resources can be used to increase beaconing rate and build cheaper on-board units. This will increase reliability of safety applications and the deployment rate of eSafety systems while still providing systems that are hard to attack.

4. REFERENCES

[1] Giorgio Calandriello, Panos Papadimitratos, Jean-Pierre Hubaux, and Antonio Lioy. Efficient and robust pseudonymous authentication in VANET. In *VANET '07*, pages 19–28, New York, NY, USA, September 2007. ACM.

[2] IEEE Standard for Information Technology. IEEE P1609.2 - Standard for Wireless Access in Vehicular Environments (WAVE) - Security Services for Application and Management Services, June 2006.

[3] SEVECOM Project. Security Architecture and Mechanisms for V2V/V2I (Deliverable 2.1). Technical report, 2007.