

Security Certificate Revocation List Distribution for VANET

Kenneth P. Laberteaux
Toyota Technical Center
Ann Arbor, MI, U.S.A.
klaberte@acm.org

Jason J. Haas and Yih-Chun Hu
Dept. of Electrical and Computer Engineering
University of Illinois — Urbana-Champaign
Urbana, IL, U.S.A.
jjhaas2@crhc.uiuc.edu,
yihchun@crhc.uiuc.edu

ABSTRACT

In a VANET, a certificate authority issues keys and certificates to vehicles. Each vehicle distributes these certificates to other VANET participants and subsequently signs messages against these certificates. If the certificate authority needs to revoke a certificate (e.g. due to a breach of trust), it universally distributes a certificate revocation list. We propose a method for car-to-car epidemic distribution of certificate revocation lists which is quick and efficient. Large-scale simulations based on realistic mobility traces show that this epidemic model significantly outperforms methods that only employ road side unit distribution points.

Categories and Subject Descriptors: C.2.0 [Computer-Communication Networks] General: Security and protections, (e.g., firewalls); C.2.1 [Computer-Communication Networks] Network Architecture and Design: Wireless communication

General Terms: Security, Performance, Design

Keywords: Security, VANET, CRL, revocation, simulation

1. INTRODUCTION

The literature [1, 2], and various government and industry-based working groups¹, anticipates that future VANET deployments will use wireless messages, e.g. periodic safety beacons, to distribute vehicle state information (e.g. position, speed, ...) to nearby vehicles. Surrounding vehicles will use this information to inform their drivers of safety-critical situations. VANETs will thus improve safety by increasing driver awareness. The IEEE 1609.2 standard [3] specifies security protocols for VANETs and requires the use of public key certificates for signing messages.

Due to misbehavior, intentional or otherwise, a radio's certificates may need to be revoked in order to limit the risk that that radio poses to the rest of the network. For example, an attacker could misrepresent his observations in order to gain an advantage (e.g. a vehicle falsely reports that its desired road is stopped with traffic, thereby encouraging others to avoid the desired road and providing a less-congested trip for the attacker). An attacker could also impersonate other vehicles or road side units (RSUs) in order to trigger safety hazards. For car-to-car (C2C) safety applications to succeed, received information must be trustworthy. Security

¹e.g. Crash Avoidance Metrics Partnership (CAMP), Vehicle Infrastructure Integration Consortium (VII-C) partnership

threats could be reduced by creating networks of trust and ignoring, or at least distrusting, information from untrusted senders.

For two nodes to communicate securely, each must possess a copy of the other's credentials in the form of a certificate. To mitigate situations such as those described above, a universally-trusted *Certificate Authority* (CA), which provides vehicles with signed certificates, must revoke the certificate(s) that it previously signed. Typically, the CA adds the identification of the revoked certificate(s) to a *Certificate Revocation List* (CRL).² The CA then publishes the updated CRL to all VANET participants, instructing them not to trust the revoked certificate. The CA employs a set of infrastructure nodes (in the case of VANET, a set of RSUs) to broadcast this CRL to all mobile nodes as they pass.

We propose an epidemic C2C method for distributing an updated CRL that allows the CRL to spread very quickly despite a minimal deployment of RSUs. Our simulations (presented below) demonstrate that CRL propagation is much faster and requires fewer RSUs than the typical methods for CRL distribution, thereby lowering deployment cost.

2. CRL DISTRIBUTION

As discussed above, for a CA to invalidate a vehicle's certificates, the CA appends the certificate identities to the CRL. The CA then distributes the CRL so that vehicles can identify and distrust the newly revoked vehicle. The distribution should spread quickly to every vehicle in the system.

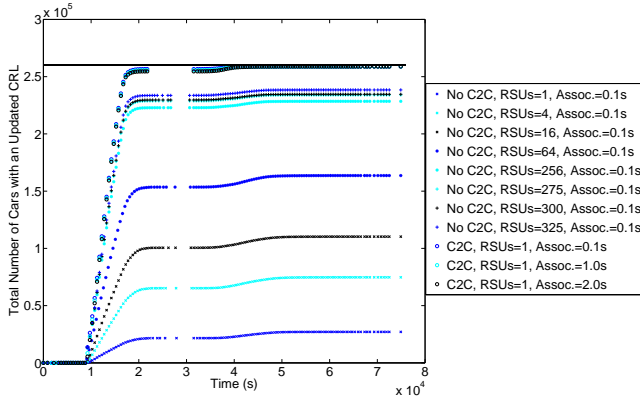
Previous work assumed that CRLs will be distributed by broadcasting updates from RSUs [4]. Distributing a CRL quickly to all vehicles in the system would require a very large number of RSUs to be deployed and maintained by the CA, incurring substantial deployment costs. Another significant challenge to RSU-only distribution is many vehicles may rarely encounter a RSU providing CRL updates, e.g. in rural areas.

Our proposal improves the distribution speed and spread of the CRL by using vehicles to distribute the CRL in an epidemic fashion. A CRL update could be broadcast by a small number of RSUs in high vehicle density locations. The RSU then *infects* each passing vehicle with the CRL update. Each infected vehicle, in turn, infects every vehicle it encounters. This infection propagates very quickly in an epidemic fashion (as verified by the simulations presented below). In order to reduce network load, storage requirements and ex-

²Using an online certificate status protocol is possible with PKI but impractical due to inconsistent connectivity inherent in VANETs.

Table 1: Simulation Parameters

| | |
|-------------------|---------------------------|
| Number of RSUs | 1,4,16,64,256,275,300,325 |
| Association time | 0.1s, 1.0s, 2.0s |
| C2C communication | Disabled, enabled |

**Figure 1: A comparison of the number of vehicles in possession of a CRL released at 9000s.**

cessive computation for distributing, storing and processing a CRL, we propose that incremental updates to a CRL be shared; that is, a source vehicle should only share the part of the CRL which the recipient does not have but the source does (we omit further details for space reasons).

3. METHODOLOGY

In order to evaluate the performance of C2C epidemic CRL passing as compared to the performance of CRLs being distributed exclusively by RSUs, we obtained realistic traces of car movements for simulation. The trace we used was based on the area surrounding the city of Zurich, Switzerland [5]. This trace contains nearly 260,000 vehicles and covered approximately 354km x 263km. In order to handle the massive size of this trace, we built a highly-parallel, custom simulator to track encounters between vehicles. This simulator uses a simple infection criteria, described below. It does not attempt to emulate packet-level communication. We believe our simulations to be the largest simulations of CRL distribution thus far reported in the literature.

In the simulator, vehicles are given velocities and destinations based on the events in the trace file. The positions of the vehicles are sampled every 0.1s. Every 0.1s, a list of neighbors is generated for each vehicle. For the simulations where we did not consider C2C communication, the neighbor list consists of only nearby RSUs. For the simulations where we did consider C2C communication, the neighbor list included nearby RSUs and nearby cars. We consider the CRL update to be exchanged if two neighbors (one possessing the CRL update) are within 100m of each other for at least the simulated association time, which we varied.

We placed RSUs at the center of the densest areas of the trace, based on off-line calculations. Using a visualizer for our simulations, we discovered that there are what appear to be a morning rush hour and an evening rush hour, where cars generally move into the city and move out of the city, respectively. Table 1 summarizes the parameters that we used in our simulations.

4. RESULTS

Figure 1 shows the total number of cars in the simulation

Table 2: Comparison of the percentage of vehicles with the updated CRL at the end of the 76000s simulation.

| | |
|--------------------------------------|----------|
| C2C, RSUs=1, Assoc. time = 2.0s | 99.5811% |
| No C2C, RSUs=325, Assoc. time = 0.1s | 91.7035% |
| No C2C, RSUs=1, Assoc. time = 0.1s | 10.4036% |

that received the CRL up to a given time. The CRL update was released at 9000s. Gaps in each data set occur when there are no new vehicles receiving the CRL update during that time interval. The gaps between 22000s and 32000s correspond to a period of time when very few vehicles move in the trace, i.e., between the rush hours. After this plateau, the CRL update distribution progresses again around 35000s as more vehicles begin to move. Figure 1 shows that the C2C CRL update passing method outperforms the method where CRL updates are distributed solely by RSUs (No C2C) in both total coverage (the number of cars with the CRL update at the end of the simulation) and speed of coverage (the rate at which cars obtain the CRL update). This remains true even when the No C2C case uses 325 RSUs while the C2C case uses only one RSU. To stress the C2C case even further, we increased the association time from 0.1s to 2.0s (all No C2C cases were run with an association time of 0.1s). This increase in association time made little impact on the efficacy in passing CRL updates in the C2C cases.

Table 2 shows the number of vehicles with the CRL update at the end of the simulation as a percentage of the total number of vehicles. The case of 1 RSU using C2C passing results in superior CRL update coverage for any length of association time as compared to any number of RSUs simulated with C2C CRL update passing disabled.

5. CONCLUSION

To summarize, we propose that vehicles be employed to spread CRL updates in an epidemic fashion. We further propose that only the required CRL update sections be communicated, thereby minimizing communication bandwidth usage. Our simulation results show the performance obtained from using epidemic C2C passing of CRLs obtains better performance for a single deployed RSU than the performance of 325 RSUs without epidemic C2C passing of CRLs. In other words, for deploying RSUs, the cost savings of using a system with epidemic C2C CRL passing is greater than a factor of 325 when compared to an RSU only system.

6. REFERENCES

- [1] C. L. Robinson, L. Caminiti, D. Caveney, and K. Laberteaux. Efficient coordination and transmission of data for cooperative vehicular safety applications. In *VANET '06: Proceedings of the 3rd international workshop on Vehicular ad hoc networks*, pages 10–19, New York, NY, USA, 2006. ACM.
- [2] Yih-Chun Hu and Kenneth P. Laberteaux. Strong VANET security on a budget. *Proceedings of the 4th Annual Conference on Embedded Security in Cars (escar 2006)*, November 2006.
- [3] IEEE 1609.2-Standard for Wireless Access in Vehicular Environments (WAVE) - Security Services for Applications and Management Messages, available from ITS Standards Program, <http://www.standards.its.dot.gov/StdsSummary.asp>.
- [4] Vehicle Infrastructure Integration-VII Architecture and Functional Requirements, v1.1, <http://www.vehicle-infrastructure.org>, 2008.
- [5] Valery Naumov, Rainer Baumann, and Thomas Gross. An evaluation of inter-vehicle ad hoc networks based on realistic vehicular traces. In *MobiHoc '06: Proceedings of the 7th ACM international symposium on Mobile ad hoc networking and computing*, pages 108–119, New York, NY, USA, 2006. ACM.