Michele Weigle
CS 795/895, Spring 2007

Summary of "The Security of Vehicular Ad Hoc Networks"

Maxim Raya and Jean-Pierre Hubaux
ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN) 2005

In this paper, the authors detail their approach to achieving security in VANETs while maintaining driver privacy. The main idea is to use digital signatures to ensure that messages originate with valid senders. This approach requires the use of a tamper-proof device in the vehicle to store private keys used for the digital signature. To maintain privacy and avoid tracking, the authors suggest changing private keys at various intervals. This requires the storage of many keys (estimated to be 43,800 per year) in the tamper-proof device. In addition to private keys, vehicles must store certificates corresponding to those private keys. These certificates will be issued by a trusted certificate authority (CA) and include the public key corresponding to each private key used for the digital signature.

The authors focus on safety messages, which they break down into traffic information messages, general safety-related messages (including collision avoidance warnings), and liability-related messages, which would help law enforcement determine fault in the event of an accident. Messages in their system model are broadcast, are not encrypted, and do not contain any explicit vehicle identification.

The authors describe a simple protocol based on work published by Yang *et al*. [33] and describe attackers and possible attacks in a manner similar to the later Parno and Perrig paper [PP05]. The authors also describe basic requirements for a secure VANET system, including authentication, verification of data consistency, availability, non-repudiation (a vehicle cannot deny that it send a specific message), privacy, and real-time constraints.

The authors also discuss various implementation issues regarding the number of keys needed in a year, the lifetime of certificates, and the size of the digital signature. A further investigation involves the feasibility of public key cryptography for VANETs. For a particular scenario, they calculate a worst-case processing delay of 2.5 ms per message when vehicles are not congested. On a congested roadway, they calculate a maximum processing delay of 2.78 ms.

The authors ran ns-2 simulations to investigate the message delay (seconds), number of received messages per vehicle (msgs/sec), and the system throughput (Mbps). They use these simulations to show that public key cryptography does meet the worst-case per-message processing demands.

The authors only mention future work in that "we intend to further develop this proposal", which is not very informative. There is also a short discussion on the use of GPS and secure positioning, but it appears to largely just be a mention. This may be an area for future work.

References (Note: Numerical reference numbers correspond to those in the original paper.)

[33] X. Yang, J. Liu, F. Zhao, and N. Vaidya. A vehicle-to-vehicle communication protocol for cooperative collision warning. In *First Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous 2004)*, August 2004.

[PP05] B. Parno and A. Perrig. Challenges in securing vehicular networks. In *Proceedings of HotNets*, 2005.

Other Possibly Interesting References

[10] S. Duri, M. Gruteser, X. Liu, P. Moskowitz, R. Perez, M. Singh, and J.-M. Tang. Framework for security and privacy in automotive telematics. In *Proceedings of the 2nd International Workshop on Mobile Commerce*, pages 25-32, 2002.

[15] L. Gollan and C. Meinel. Digital signatures for automobiles. In *Systemics, Cybernetics, and Informatics (SCI)*, 2002.

[23] K. Matheus, R. Morich, I. Paulus, C. Menig, A. Lbke, B. Rech, and W. Specks. Car-to-car communication – market introduction and success factors. In *ITS 2005: 5th European Congress and Exhibition on Intelligent Transportation Systems and Services*, 2005.

Questions/Comments

- How/when does the vehicle communicate with the CA? Does it need to communicate with the CA once the CA's public key and all of the necessary private keys and certificates have been loaded?
- Is there a way that the many private keys can be used to mount a Sybil attack?
- **Figure 4 comment**: Some data lies on the scale-line rectangle making those points difficult to read.