A communication protocol for securing connected vehicle platoons using joint hardware-software means

Peijing Li[1], Neda Masoud[2]

1 -- Computer Science and Engineering, College of Engineering, University of Michigan, Ann Arbor, MI; corresponding author email: peijli@umich.edu

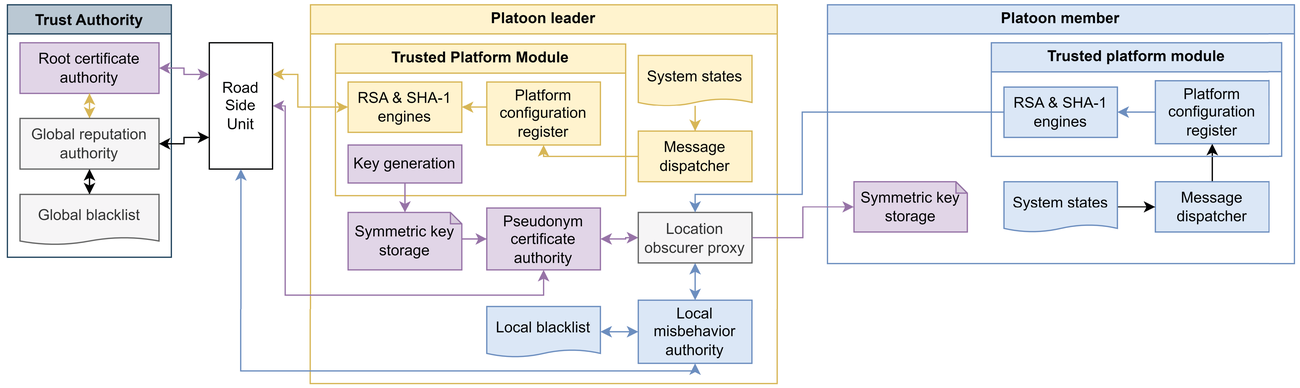
2 -- Civil and Environmental Engineering, College of Engineering, University of Michigan, Ann Arbor MI

Abstract

Both the security of vehicular ad-hoc networks (VANETs) and the communication topologies within platoons of connected vehicles have been studied with increased interest over the past two decades. However, existing protocols do not specifically account for vehicular platoons and may make the process of both authentications and securing succeeding communication packets unnecessarily complex. In the meantime, given the exclusive focus on software solutions in research over the past decade, potentials for dedicated hardware such as Trusted Platform Modules (TPMs) have not been fully explored concerning their impacts on authentication and message integrity checks. The purpose of this study is to address the issue of improving the efficiency of secured communication within connected vehicle platoons while maintaining the goals of authentication, privacy, and data integrity during the entire process of electing leaders, establishing trust, securing connections, and managing misbehaviors. We propose a new protocol that features the following: (a) a two-level trust system, respectively between an external trust authority and a platoon's leader, and between the leader and the remaining members of the platoon; (b) a communication scheme that enables more efficient communication between trusted platoon members via symmetric cryptography; (c) a challenge-response scheme for misbehavior detection that relies upon TPMs of each vehicle to report its operational state to be assessed by a superior in the trust system; (d) a reputation scheme based on the results of said TPM functionalities to determine new leaders of platoons.

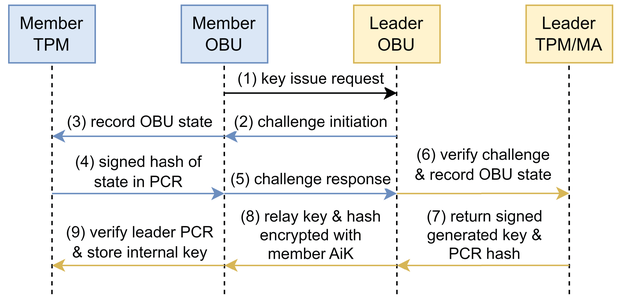
Introduction

1. Platooning of connected vehicles is a promising way to improve traffic efficiency and safety.
2. Characteristics of vehicular platoons: small headway, similar speed, potential integral mutual trust (i.e., due to belonging to the same organization)
3. Goals of VANET security: authentication, data consistency, privacy, real-time
4. No research specifically consider intentionally formed vehicular platoons and their security characteristics (only focusing on geographical “groups” of mutually untrusted vehicles)
5. State of the art in VANET security: Public key infrastructure with elliptic curve digital signature algorithm (PKI/ECDSA), high computational cost; symmetric cryptography (e.g., AES) is less secure but is less computationally expensive
6. **Research question: given the unique characteristics of vehicular platoons and functionalities of hardware like trusted platform modules (TPMs), how can one reduce the number of PKI-based communications and replace them with more efficient symmetric cryptography between “trusted” vehicles instead?**
7. Protocol design with platoon-specific use cases: **establishing and renewing trust, leader election, communication, and leaving a platoon.**



Establishing/Renewing trust

Note that this process is repeated for each new member in platoon and every 5-10 minutes for each current member.



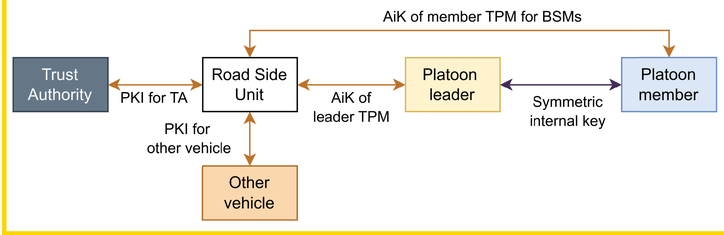
Platoon leader election

We wish to identify “trustworthy” vehicles with “reputation” scores, aggregated from other vehicles’ past communication results with the prospective group leader.

For each prospective group leader: Use TPM to verify the integrity of each component, and share integrity verification report with authorities via road-side units (RSU). The trust authorities compute reputation score of each component for each vehicle using weighted arithmetic averages over different points in time.

The trust authority wold only assign group leader role to vehicles meeting a certain “reputation” threshold.

Communication scheme



Leaving a platoon

Generally speaking, vehicles leaving a platoon involve a “refresh” of the internal symmetric keys of the platoon, where the new keys are made available to the remaining platoon members but not to vehicle that left.

Actions are required for different entities given the different types of vehicles leaving a platoon. When a platoon member leaves, such an action – and subsequent key regeneration – would be handled by its platoon leader. When a platoon leader leaves, such an action – and subsequent leader election and key regeneration – would be handled by the TA communicating through RSUs.

There are two different ways a vehicle can leave a platoon. It can either voluntarily leave the platoon by petitioning its superior (either platoon leader or the TA) and receiving a positive response, or it can be forcibly ejected by its superior upon detection of anomalous behaviors and have its AiK in its TPM added to the blacklist of both the TA and all platoon leaders.

Validation

We wish to utilize the following tools to simulate and validate this protocol:

1. SUMO: road traffic simulation
2. OMNet++: network simulation
3. Veins: integrates SUMO and OMNet++ for vehicular network simulation
4. Plexe: extension to Veins to enable platoon networking simulation

We would compare the system latency of this new protocol against existing ones, e.g., PKI/ECDSA. We would also observe the response of the systems to different forms of attacks.

Acknowledgement

The primary author wishes to thank Dr. Neda Masoud and Yiyang Wang in mentoring the project and providing valuable insights on research trends and background knowledge.

References

[1]A. A. Wagan, B. M. Mughal, and H. Hasbullah, “VANET Security Framework for Trusted Grouping Using TPM Hardware,” in 2010 Second International Conference on Communication Software and Networks, Feb. 2010, pp. 309–312. doi: 10.1109/ICCSN.2010.115.

[2]A. Studer, F. Bai, B. Bellur, and A. Perrig, “Flexible, extensible, and efficient VANET authentication,” Journal of Communications and Networks, vol. 11, no. 6, pp. 574–588, Dec. 2009, doi: 10.1109/JCN.2009.6388411.

[3]G. Guette and C. Bryce, “Using TPMs to Secure Vehicular Ad-Hoc Networks (VANETs),” in Information Security Theory and Practices. Smart Devices, Convergence and Next Generation Networks, Berlin, Heidelberg, 2008, pp. 106–116. doi: 10.1007/978-3-540-79966-5_8.

[4]M. Raya and J.-P. Hubaux, “The security of vehicular ad hoc networks,” in Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks, New York, NY, USA, Nov. 2005, pp. 11–21. doi: 10.1145/1102219.1102223.

[5]A. A. Wagan and L. T. Jung, “Security framework for low latency vanet applications,” Kuala Lumpur, Malaysia, Jun. 2014, pp. 1–6. doi: 10.1109/ICCOINS.2014.6868395.

[6]S. Sharma, A. Kaul, S. Ahmed, and S. Sharma, “A detailed tutorial survey on VANETs: Emerging architectures, applications, security issues, and solutions,” Int J Commun Syst, vol. 34, no. 14, Sep. 2021, doi: 10.1002/dac.4905.

[7]H. Hu, R. Lu, Z. Zhang, and J. Shao, “REPLACE: A Reliable Trust-Based Platoon Service Recommendation Scheme in VANET,” IEEE Transactions on Vehicular Technology, vol. 66, no. 2, pp. 1786–1797, Feb. 2017, doi: 10.1109/TVT.2016.2565001.