Poster: Securing Vehicular Platoon Membership

Mikael Asplund

Linköping University Post Print

N.B.: When citing this work, cite the original article.

©2015 IEEE. Personal use of this material is permitted. However, permission to reprint/republish this material for advertising or promotional purposes or for creating new collective works for resale or redistribution to servers or lists, or to reuse any copyrighted component of this work in other works must be obtained from the IEEE.

Mikael Asplund, Poster: Securing Vehicular Platoon Membership, 2014, Proceedings of IEEE Vehicular Networking Conference (VNC), 119-120.

<http://dx.doi.org/10.1109/VNC.2014.7013324>

Postprint available at: Linköping University Electronic Press

<http://urn.kb.se/resolve?urn=urn:nbn:se:liu:diva-114294>

Poster: Securing Vehicular Platoon Membership

Mikael Asplund

Department of Computer and Information Science,
Linköping University, SE-581 83 Linköping, Sweden
mikael.asplund@liu.se

Abstract—Vehicular platoons have the potential to bring considerable fuel-savings and increase traffic efficiency. A key component for the next generation platoon systems is a secure membership component which can accommodate membership changes in a dynamic and potentially hostile environment. In this poster paper we analyse the conditions for creating a secure membership protocol which is resilient to attacks and faults in the communication protocols.

I. INTRODUCTION

In a recent report by the US National Highway Traffic Safety Administration [3] the readiness of Inter-Vehicular Communication (IVC) is assessed. It appears that while many issues remain, large-scale deployment of this technology is no longer in the distant future. The next big research challenge for IVC-systems is to enable efficient *coordination* among vehicles to further increase the safety and efficiency. In particular for heavy-duty vehicles the ability to drive in platoons can present significant fuel-savings as well as increase safety.

We argue that secure group membership is a crucial component for future vehicular coordination systems. We define a platoon membership view as an ordered sequence of identifiers that represent all the vehicles that participate and are physically present in the platoon. Accurate and up-to-date membership views are needed in platoons for two main reasons, (1) reliable group communication (2) for the leader to make safe and appropriate driving decisions. The key challenges to implementing accurate membership for vehicular environments are the unreliable nature of wireless communication, the high level of dynamism in node movements, interaction with non-automated vehicles [5], and the possibility of malicious actors. As computer systems in vehicles become increasingly complex and interconnected, they also become more vulnerable to security threats such as viruses and trojans.

In this poster paper we analyse the security implications for membership management in vehicular platoons given different attack detection capabilities. There is a rich literature on security in VANETs relevant to this work (e.g., [6], [2], [4]), well beyond what can be summarised here, but to our knowledge we are the first to consider specific attacks on platoon membership views and possible mitigation strategies.

II. BASIC SETTING

Figure 1 shows the basic setting with one leader vehicle (L) pilot two follower vehicles (F1 and F2). Platoon members

are equipped with sensing capabilities to detect objects and vehicles in front and behind, as well as IVC (thus, each participating vehicle is also a node in a wireless network). A membership protocol should be able to provide all participating nodes with a consistent view of which other vehicles that participate and are physically present (i.e., in this case the view [L,F1,F2]). Such a protocol will need to account for both unexpected and normal membership changes, disruptions in the communication, faults in the software of the vehicles and finally malicious attempts by outsiders to fool the system.

Fig. 1. Platoon formation showing sensor and IVC for F1

We assume the existence of a simple membership protocol (not described here for reasons of brevity), where the platoon configuration is periodically broadcasted by the leader vehicle. Joins and leaves are handled by requests to the leader vehicle which also periodically collects sensor data from all participating vehicles. In line with current standardisation efforts [1], we assume signed messages (hindering spoofed messages from already known nodes). Our focus in this poster paper is to analyse how the membership views of the participating vehicles can be corrupted by malicious actors in the system. We consider a membership view to be false if the physical configuration along the road does not match the membership view. Note that a malicious vehicle does not necessarily mean malicious driver, since there is a possibility that the platoon management software system is infected with malicious code (or contains non-malicious bugs which amounts to seemingly malicious behaviour).

III. ATTACK SCENARIOS AND ANALYSIS

We now proceed to describe six distinct attack scenarios which represent typical cases where one or more malicious agents try to cause fair nodes to form false membership views. The scenarios are illustrated in Figure 2 and their descriptions follow.

- 1) Node A initiates a platoon and node B joins, causing A's membership view to be [A,B]. B secretly initiates a new platoon, which is joined by C. A still has the membership view [A,B] and C has the view [B,C]. Both views are inconsistent with the physical configuration [A,B,C].
- 2) Nodes A, and B form a platoon with membership views [A,B]. C initiates a new platoon, falsely claiming to be in B's position. The result is that D believes it has joined

Thanks to Henrik X. Pettersson from Scania CV AB for his valuable input to this work.

Fig. 2. Platoon membership attack scenarios

platoon [C,D], when in fact it is part of a three-vehicle formation [A,B,D].

- 3) A is a regular vehicle without IVC capabilities. B initiates a platoon falsely claiming to be in A's position. C and D join the platoon which they believe consists of the nodes [B,C,D] when in fact the platoon is physically led by A.
- 4) Node B (the tail of a 2-vehicle platoon) spuriously creates join requests for non-existing nodes C and D, making A falsely believe that the platoon is composed of four nodes.
- 5) Similar to scenario 4, A creates a platoon and B joins. In this scenario, the third member is a physical entity but it does not physically join the platoon.
- 6) Similar to scenario 1, the leader and tail nodes believe to part of 2-vehicle platoons, but in this case three malicious nodes are colluding. Node B pretends to be a tail node, C is silent and D pretends to be a leader node.

Of these six scenarios, 1, 2 and 6 are the most severe since they result in vehicles believing that the platoon is composed of fewer vehicles than are physically present. The attacks in scenarios 2 and 3 can be performed from a node which is not itself part of the platoon, whereas the attacks in scenarios 5 and 6 require colluding nodes. Given only the basic assumptions in Section II all six attack scenarios can happen unless further security measures are taken. While some of the cases might be detected by a human operator, this requires an additional level of supervision, and should ideally not be required for a next generation platooning system.

To mitigate the attacks in these scenarios we consider three important security mechanisms that can be added to the system.

Neighbour Identity Verification (NIV) assumes that vehicles can verify the identity of neighbouring vehicles that are directly in front or behind (e.g., by checking license plates).

Message Consistency Check (MCC) assumes that vehicles will overhear all communication in their vicinity and construct a local world model of their surroundings (thus detecting two-faced nodes).

TABLE I
ATTACK SCENARIOS POSSIBLE FOR VARYING SECURITY MECHANISMS

	No NIV		NIV	
	No MCC	MCC	No MCC	MCC
No SD	1,2,3,4,5,6	3,4,5,6	1,4,5,6	4,5,6
SD	1,2,3,5,6	3,5,6	1,5,6	5,6

Sybil Detection (SD) assumes that vehicles are capable of detecting nodes that try to masquerade as multiple nodes (i.e., a Sybil attack [7]).

In Table I we identify which attack scenarios that are possible under different combinations of these capabilities. In terms of the most severe attack scenarios (1, 2 and 6) we see that MCC seems to be a crucial mechanism (as well as relatively easy to implement). Moreover, the attack-from-the-side attack in scenario 3 can be easily avoided with the help of NIV, which although requiring additional hardware still seems like a reasonable component for a platooning architecture. Sybil detection avoids scenario 4. Finally, as far as we have been able to determine, if NIV, MCC, and SD are all implemented, then the only way of fooling the fair nodes in terms of membership views is by colluding attackers.

IV. CONCLUSIONS AND ONGOING WORK

Beside basic capabilities such as IVC and the ability to sense distance to vehicles in front and behind, we could see that it is crucial that all nodes continuously try to make their own map of the vehicles in the vicinity to rule out two-faced behaviour. Moreover, the ability to verify the identity of vehicles in front and back eliminates some otherwise easy attacks. Detection of Sybil attacks further reduce the possible attack surface.

However, even with all three additional security capabilities we described, colluding nodes can still fool fair nodes into adopting a false membership view. We are currently investigating how platoon rotation can mitigate the effect of such attacks and also possibly replace some of the functionality provided by other security mechanisms. Moreover, we are formalising the scenarios and capabilities described in this paper in order be able to formally prove the (non-)possibility of certain attacks.

REFERENCES

- [1] IEEE std 1609.2-2013, IEEE standard for wireless access in vehicular environments security services for applications and management messages, 2013.
- [2] M. Feiri, J. Petit, R. Schmidt, and F. Kargl. The impact of security on cooperative awareness in VANET. In *Vehicular Networking Conference (VNC), 2013 IEEE*, 2013. doi: 10.1109/VNC.2013.6737599.
- [3] J. Harding, G. Powell, R. Yoon, J. Fikentscher, C. Doyle, D. Sade, M. Lukuc, J. Simons, and J. Wang. Vehicle-to-vehicle communications: Readiness of v2v technology for application. National Highway Traffic Safety Administration (NHTSA), Report no. DOT HS 812 014, 2014.
- [4] N. Lyamin, A. Vinel, M. Jonsson, and J. Loo. Real-time detection of denial-of-service attacks in IEEE 802.11p vehicular networks. *Communications Letters, IEEE*, 18(1), 2014. doi: 10.1109/LCOMM.2013.102213.132056.
- [5] M. Segata, B. Bloessl, S. Joerer, F. Dressler, and R. Lo Cigno. Supporting platooning maneuvers through IVC: An initial protocol analysis for the join maneuver. In *Wireless On-demand Network Systems and Services (WONS)*, 2014. doi: 10.1109/WONS.2014.6814733.
- [6] A. Studer, M. Luk, and A. Perrig. Efficient mechanisms to provide convoy member and vehicle sequence authentication in VANETs. In *Third International Conference on Security and Privacy in Communications Networks (SecureComm)*, 2007. doi: 10.1109/SECCOM.2007.4550363.
- [7] B. Yu, C.-Z. Xu, and B. Xiao. Detecting sybil attacks in VANETs. *Journal of Parallel and Distributed Computing*, 73(6), 2013. doi: 10.1016/j.jpdc.2013.02.001.