On the Impact of Sybil Attacks in Cooperative Driving Scenarios

Felipe Boeira*, Marinho P. Barcellos*, Edison P. de Freitas*, Alexey Vinel† and Mikael Asplund‡

*Federal University of Rio Grande do Sul, Brazil
f.boeira@ufrgs.br
{marinho, edison.pignaton}@inf.ufrgs.br

†Halmstad University, Sweden
alexey.vinel@hh.se

‡Linköping University, Sweden
mikael.asplund@liu.se

***Abstract*—Platooning employs a set of technologies to manage how a group of vehicles operates, including radar, GPS and Inter-Vehicular Communication (IVC). It uses broadcasted information such as acceleration, position and velocity to operate vehicle members of the platoon. Cooperation among vehicles allows platoons to reduce fuel consumption and risks associated with driver mistakes. In spite of these benefits, the use of IVC to control vehicles exposes a relevant attack surface that can be exploited by malicious actors. In this paper we study the impact of vulnerabilities associated with the Sybil attack (through falsification of multiple identities) and message falsification in vehicular platooning. Simulation results show that this attack may impact the longitudinal control and compromise the entire platoon control.**

I. Introduction

The development of Cooperative Intelligent Transport Systems (C-ITS) allows the use of innovative technology such as platooning to improve transportation. A platoon is a group of vehicles that takes advantage of Inter-Vehicular Communication (IVC) to reduce the distance (headway time) between them while traveling on a highway. The headway time can be shortened as a result of repeatedly sharing information among the vehicles via *beaconing*. Beaconing consists in the platoon members periodically broadcasting a message that conveys information such as vehicle identification, speed, position and acceleration. It enables the platoon to achieve cooperative awareness and operate a longitudinal control law that dictates the behavior of the vehicles.

While beacons must include sender information, vehicles should ideally not broadcast their real identities in order to preserve their privacy. Pseudonyms are a mechanism used to protect identity privacy, as proposed in [1]. The use of pseudonyms, however, permits a single entity to present itself with multiple identities, which is known as a Sybil attack [2].

In this paper we analyze the impact of introducing Sybil vehicles to the formation of a platoon and then performing message falsification to interfere with the longitudinal control algorithm. There is literature that shows the impact of message falsification in platoons, but to our knowledge we are the first to consider Sybil and message falsification attack combination in the context of platooning.

ISBN 978-3-901882-94-4 © 2017 IFIP

II. System Model

We consider a vehicle platoon as a string of vehicles that collaborate by sharing information in order to maintain string stability. To cooperate, the vehicles use inter-vehicular communication to broadcast beacons and convey information about the physical state of the vehicle such as speed, acceleration and position. We assume that the communication is based on the IEEE 802.11p vehicular communication standard.

We assume that the vehicles adjust their acceleration based on information from the beacons broadcasted from platoon members. Each platoon member executes an instance of the controller algorithm. For each iteration of the control algorithm, the acceleration of the vehicle is adjusted if necessary. We use a longitudinal control algorithm called Consensus [3] that takes information from both the preceding vehicle and leader in order to apply its control law. Consensus is a state-of-the-art controller proposed to operate platoons based on IVC only. It has been shown to outperform other control algorithms with regard to stability under strong interference, delays, and fading conditions. In practice a combination of several different sensors (radar, camera, ultra sound) should be used. Other sensors might exhibit other weaknesses, which in combination with the attacks studied in this paper could cause considerable damage.

III. Attack Scenarios Simulation

Our experiments are conducted using the Plexe [4] platoon extension for Veins, a VANET simulator that integrates both realistic network and vehicular traffic modeling. We assume that a platoon composed of eight cars operated by the Consensus controller is traveling on a 10 km stretch of highway in which the cars move west to east for 120s or until a collision is detected. The nodes communicate using IEEE 802.11p by sending beacons with a frequency of 10 Hz. The simulations use free space path loss model ($\alpha = 2.0$) and Nakagami-m ($m = 3$) fading model.

A. Attack Scenario 1

The first scenario consists in inserting two Sybil nodes at positions that enable them to collude and control the behavior of two legitimate platoon members. In the case that it is possible to manipulate the acceleration of two vehicles, an accident

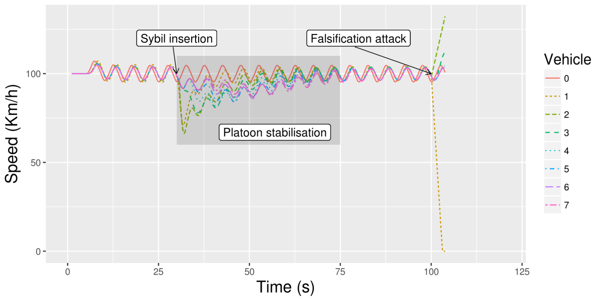

Fig. 1: Collusion attack scenario 1

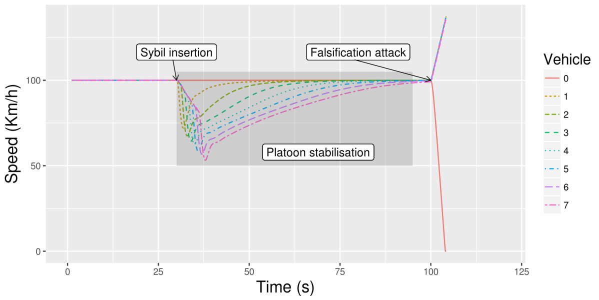

Fig. 2: Collusion attack scenario 2

can be caused. The Sybil nodes are inserted at simulation time 30s and start to manipulate its following vehicles at simulation time 100s, after a stabilisation period. The Sybil node inserted between the leader and *vehicle 1* forges its position subtracting 250m from its actual position so that the *vehicle 1* begins to decelerate. The Sybil node inserted between *vehicle 1* and *vehicle 2* also performs a position falsification adding 250m to its actual location, causing *vehicle 2* to accelerate. This behavior is represented in Figure 1. A high speed accident is caused, during 3.81 seconds the *vehicle 1* applies a strong deceleration while *vehicle 2* speeds up to 132.19 km/h, at the time a rear-end collision occurs.

B. Attack Scenario 2

In this scenario, we evaluate the message falsification effects during an emergency braking. A braking scenario is defined in which the platoon travels for 100s at 100km/h when the leader applies an emergency brake. At the time the leader starts to strongly decelerate, the Sybil nodes begin to falsify their position in order to induce the platoon members to accelerate. A Sybil node is inserted between all legitimate nodes so that the attacker can interfere with the acceleration of all followers. The behavior is assessed using a 250m position falsification by the Sybil nodes. This attack causes the vehicles to collide at high speed in a chain-reaction crash. As can be observed in Figure 2, while the leader is applying an emergency brake, the platoon members charge up to ≈137 km/h until there is a rear-end crash. The time elapsed from the beginning of the emergency brake until the crash was only 4.21 seconds, which provides little reaction window for a driver to reclaim the control of the vehicle.

C. Attack Scenario 3

While the falsification of a large position error may impact more aggressively on the acceleration of the preceding vehicle, it may be easy to detect this anomaly if a behavior analysis is being performed. In order to simulate a plausible behavior, we increase the position error falsification over time. It would be reasonable to expect that the impact of the position error in this scenario would be lower when compared with the attack scenarios 1 and 2. However, a collision can still be caused by Sybil nodes that grow the position error progressively, which makes it not trivially detectable by simple anomaly analysis. Figure 3 illustrates how the members react, the collision occurs after 17.11 seconds of progressive falsification and causes a crash between *vehicle 2* at 94.79 km/h and *vehicle 1* at 81.38 km/h.

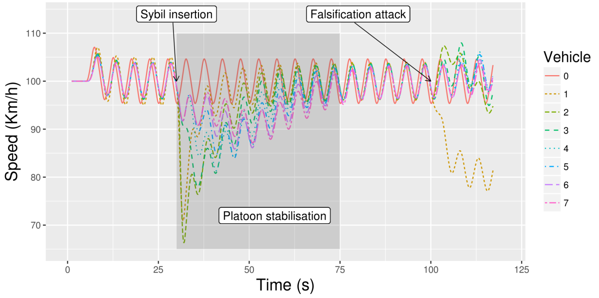

Fig. 3: Collusion attack scenario 3

IV. Conclusion

This paper has shown that the Sybil and message falsification attacks can pose a threat to the vehicular platooning. The performed simulations show that the insertion of Sybil nodes that collude in a message falsification attack may compromise the platoon's string stability if governed mainly by IVC-based information. The position falsification directly affects the longitudinal control algorithm and may result in the breach of the control law. The experiment results show that, in a IVC-based platoon, vehicle accidents at high speed may be caused by nodes that collude with carefully crafted beacons.

References

[1] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Secur.*, Jan. 2007.

[2] J. R. Douceur, "The sybil attack," in *Revised Papers from the First International Workshop on Peer-to-Peer Systems*, ser. IPTPS '01, 2002.

[3] S. Santini, A. Salvi, A. Valente, A. Pescape, M. Segata, and R. L. Cigno, "A consensus-based approach for platooning with inter-vehicular communications," in *2015 IEEE Conference on Computer Communications (INFOCOM)*. IEEE, 2015.

[4] M. Segata, S. Joerer, B. Bloessl, C. Sommer, F. Dressler, and R. Lo Cigno, "PLEXE: A Platooning Extension for Veins," in *6th IEEE Vehicular Networking Conference (VNC 2014)*. IEEE, December 2014.

The work of Felipe Boeira and Alexey Vinel has been partially supported by the ELLIIT Strategic Research Network.