Mitigating Position Falsification Attacks in Vehicular Platooning

Felipe Boeira*, Mikael Asplund*, and Marinho P. Barcellos†
*Dept. of Computer and Information Science
Linköping University, Sweden
†Institute of Informatics
Federal University of Rio Grande do Sul, Brazil

***Abstract*—As connected vehicles are envisioned to provide novel intelligent transportation systems, cyberattacks and security schemes are becoming an increasing concern. Several studies have shown that algorithms that make use of location information from other vehicles, such as vehicular platoon controllers, are vulnerable to message falsification attacks. Moreover, the ability for an attacking vehicle to appear as several vehicles through a so-called Sybil attack can significantly increase the severity of the attack. In this paper, we investigate how these attacks can be detected using Vouch location proof scheme (by identifying false location messages) and propose several reaction strategies to mitigate them. We also show through simulation that it is possible to prevent collisions by reacting appropriately to the false beacons in time while not reacting to false positives coming from the detector.**

I. Introduction

Inter-vehicular Communication (IVC) has the potential to improve traffic management, increase passengers comfort and reduce accidents. In the first generation of IVC systems vehicles share information about their current state, such as the velocity, acceleration and location through beacons. By leveraging information in beacons a variety of novel applications can be established, namely intelligent intersections and roundabouts, traffic jam management systems and vehicular platooning.

A vehicular platoon is composed of a group of vehicles that travel together in a highway (or rural road) with reduced distance between them. In many envisaged platooning scenarios, a leader is driven by a human and dictates the behavior of the following members. These vehicles employ a platooning controller algorithm that adapts its behavior according to data received in beacons from the platoon members.

In previous work, we have shown that the falsification of positioning information shared through IVC is a relevant threat to correct platooning vehicle control and the use of multiple false nodes increases the severity of collisions [1]. Similarly, Heijden et al. [2] studied the effects of falsifying speed, acceleration and position across a set of controllers and also found that attackers may cause instabilities in the platoon operation. A controller-based mitigation to position falsification was proposed based on distancing discrepancies between platoon members [3]. This is an improvement in the controller which can be complementary to our approach.

In this paper we return to the attack scenarios presented in [1] to investigate how they can be mitigated by using the Vouch location proof scheme [4]. The idea of Vouch is to use the built-in ability of the upcoming fifth generation cellular networks to locate mobile clients independently of the information provided by the client. With the help of cryptographic mechanisms and a component for countering the adverse effect of high mobility on location services, Vouch allows vehicles to *detect* location falsification attacks with low overhead and reasonable detection performance. The purpose of this paper is to go from detection to mitigation.

Designing appropriate mitigation mechanisms is not a trivial task. The premise of this work is that a vehicle that participates in a platoon where it can no longer trust the other platoon members should abort its participation in the platoon. The question then becomes, to what extent should you trust your peers when you suspect they are lying to you? Waiting too long in presence of malicious actors can result in unsafe situations, whereas prematurely abandoning the cooperation due to temporary disturbances or benign faults is almost as bad. We discuss several different reaction strategies in this paper and evaluate a timeout-based strategy for when to stop trusting a vehicle that transmits falsified beacons.

The evaluation shows that while the detector sometimes gives false alarms, having a relatively short timeout of 1 second for when to stop trusting other nodes is enough to avoid reacting unnecessarily. Moreover, we investigate how inaccuracies in the location proofs affect the ability to react to the attacks in time. Our results show that while the reaction time is heavily dependent on the attack scenario (i.e., whether the attack is subtle or not), all attacks presented in [1] can be safely addressed in time by the proposed reaction schemes.

The rest of this paper is organized as follows: Section II briefly describes the design of Vouch and Section III presents an overview of the attack scenarios. Section IV proposes reaction strategies against information deemed implausible. Section III discusses the results and Section VI outlines our findings.

II. Vouch: A Proof-of-Location Scheme

As position falsification clearly threatens correct vehicle control, we have designed Vouch: a proof-of-location scheme that provides location assurance [4]. Vouch uses Roadside

Units (RSUs) infrastructure to provide trusted location proofs for vehicles. A proof essentially is digitally signed data that enables a vehicle to attest its position to neighbors in a secure and trusted manner, i.e. proofs can not be forged or manipulated. Proofs may be acquired and disseminated in distinct frequencies, which determines the amount of overhead it will introduce in the system. When neighbor vehicles broadcast beacons, Vouch employs a plausibility model to classify the received positions according to the proofs that have been disseminated by those entities. It models the movement dynamics of vehicles and determines if a position is plausible to be achieved by a vehicle based on such proofs. Succinctly, Vouch classifies every beacon as plausible or implausible based on a mobility model and trusted proofs created by RSUs, which are disseminated by vehicles to their neighbors.

III. Attack Scenarios Overview

To evaluate the proposed reaction strategy, we employ attack scenarios studied in previous work [1]. The attacks consist of five scenarios in which an attacker travels in a lane beside the platoon and inserts false nodes into its formation. The attacks are mainly divided into two phases: in the first phase, false nodes are introduced and abide by the controller algorithm, while in the second a position falsification is carried out to cause a crash between legitimate vehicles. Each scenario is further divided into two variants: one with a single false node, and the other with multiple colluding nodes.

Given that results will refer to the distinct attack scenarios, a brief explanation for each of them is included in the list below:

- **Falsification (F).** In variant **(a)**, the attacker inserts two false nodes, one between the first pair of legitimate members (i.e. between the leader and the first legitimate follower), and the other between the second pair (i.e. between the first and the second legitimate followers). In the second phase, the attacker manipulates the first false node by falsifying its position to 250 m aheadwhile the second false node falsifies the position by the same value but in contrary direction. In variant **(b)** only the first false node is used.
- **Covert Falsification (CF).** The false nodes are distributed like the first scenario, for both variants **(a)** and **(b)**. In the second phase of the attack, the false nodes progressively increase their distance error in order to conduct a more stealthy falsification.
- **Emergency Braking Obstruction (EBO).** This scenario considers an emergency braking scenario. In variant **(a)** a false node is introduced between every pair of legitimate vehicles. In variant **(b)**, there is a single false vehicle following the leader. When the emergency braking begins, the false nodes increase their position by 250 m to cause legitimate members to accelerate.
- **Vehicle Position Hijacking to Falsify Leader (VPHFL).** The false node is falsified at the position of an innocent vehicle that travels on a highway and is not part of the platoon. This could make the attack harder to detect, provided that other sensors would attest the presence of the vehicle. In variant **(a)**, one false node is the leader and the second one takes the position of the innocent vehicle. In variant **(b)**, there is a single false node, which takes the position of the innocent vehicle as the platoon leader (i.e. the attacker starts a platoon by falsifying a node at the position of the innocent vehicle, which will become the platoon leader once other members join).
- **Vehicle Position Hijacking to Falsify Member (VPHFM).** As in the previous scenario, an innocent vehicle that is not part of a platoon is used to deploy a false node. Variant **(a)** places two adjacent false nodes, one after the other, in the middle of the platoon. The second node takes the position of an innocent vehicle that was travelling close to the platoon. In variant **(b)**, a single false node is used, which takes the position of an innocent vehicle.

IV. Reacting to Implausible Information

Vouch classifies every beacon as plausible or implausible. A vehicle must still decide how to react when a message reporting an implausible location is received. In this section, we propose three strategies to determine when a neighbor should be distrusted.

In addition to these three strategies, we propose two techniques to handle beacons with apparently implausible positions, while the sender vehicle remains trusted.

A. Reaction Strategies

Vehicles that operate without human interaction must have strategies to decide when the environment has become unsafe due to faults or malicious attacks. In vehicular platooning, such conditions could mean that the control has to be reclaimed by the driver and the platoon disbanded. Based on the classification of beacons, we propose three strategies to determine when manual control should be reclaimed, as follows.

Time without plausible positions. A vehicle may decide that it is unsafe to continue operating under the platoon when a certain timeout is achieved without the reception of a beacon that contains plausible location of a given member.

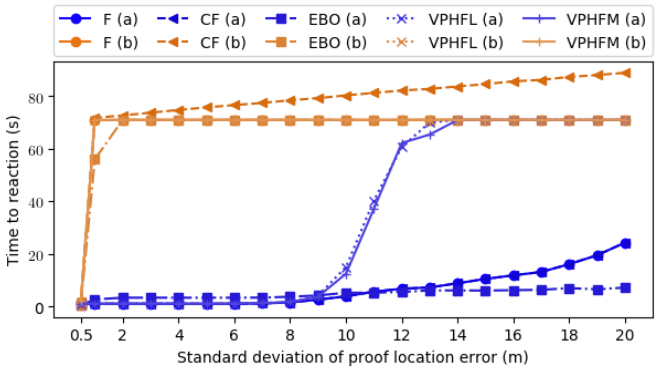
Frequency of implausible positions. A vehicle may decide to disband the platoon when a member receives plausible positions mixed with implausible ones.

Distance error threshold. A vehicle may decide to leave the platoon if a distance reported by an implausible beacon exceeds a certain threshold.

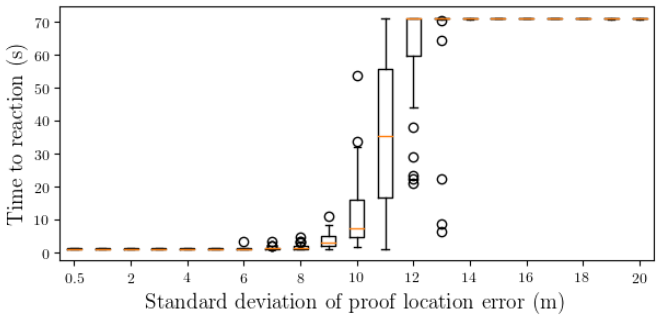
In addition to determining when to have the human driver to reclaim manual control, the vehicle may handle implausible beacons in distinct manners. We consider two techniques, as follows.

Drop. Implausible beacons are dropped altogether, in practice it behaves like packet loss.

Adjust to position boundary. This technique leverages the mobility model in Vouch that estimates the plausible position boundaries a vehicle could have achieved since the last proof.



(a) Average reaction time



(b) Results for VPHFM (a)

Fig. 1: Detection results

Using this technique does not result in the loss of the beacon but in the adjustment to plausible limits.

Even though the three strategies and two techniques listed above are orthogonal to each other and might be combined into more complex strategies, in this short paper we focus on the *time without plausible position* strategy and *dropping* implausible beacons technique.

B. Performance Metrics

To evaluate the strategies and mechanisms we define the following metrics. First, safety is a necessary condition to be satisfied: crashes that would be caused by attacks against the platooning scheme must be prevented. We measure the performance of the reaction strategy in multiple scenarios through the time to react to attacks and the number of times a vehicle left a platoon incorrectly.

V. Results

This section presents the setup that was employed in the simulations and the results obtained.

A. Simulation Environment

The experiments are conducted using Plexe [5], a vehicular platooning extension to Veins [6]. Veins couples the Omnet++ network simulator with the SUMO mobility simulator to enable vehicular networks experiments. To perform actual cryptographic operations required by Vouch, we introduced an external module based on the OpenSSL library. The remainder of the simulation components are modeled as Plexe extensions.

The *time without plausible positions* parameter indicates for how long a vehicle should continue trusting a member that has not provided plausible beacons. For the present study, we considered the hypothesis that packet loss is 20%, which results in one false reaction due to packet loss for one million seconds of operation, approximately. In that case, ten consecutive beacons were lost.

Based on results shown in [4] we have chosen to adopt the 5 Hz proof dissemination frequency with a 4 σ plausibility check threshold. We study the impact of positioning accuracy in multiple attack scenarios, and the way it affects how fast vehicles react. The accuracy is evaluated by varying *position noise standard deviation* values, from the most accurate to the least. For statistical robustness, each combination of parameters was evaluated with 33 runs, which resulted in 4158 iterations in total. Table I includes the detailed simulation parameters.

TABLE I: Simulation parameters

Freeway length	10 km
Number of lanes	4
Car speed	100 km/h
Platoon size	8 cars
Platooning car max acceleration	2.5 m/s^2
Platooning car mass	1460 kg
Platooning car length	4 m
Headway time	0.8 s
Longitudinal control algorithm	Consensus [7]
Simulation time	200 s
Beaconing frequency	10 Hz
Communication interface	802.11p
Radio frequency	5.89 GHz
Path loss model	Free space ($\alpha = 2.0$)
Transmission power	20 mW
Standard deviation of proof location error σ	0.5, 1, 2, 3, ..., 20 m
Time without plausible positions	1 s
Proof size	100 bytes
Proof frequency	5 Hz
Plausibility check threshold	4 σ

B. Results

Recall from Section III that attacks are divided into two phases: introduction of false nodes into the formation, and manipulating other vehicles (through position falsification – represented in Figure 1 at 70 s) to cause crashes. In the experiments, the attacker travels steadily in the lane beside the position of the first false node it introduced. This can be considered to be the best case for the attacker, since the smaller the distance it travels from the false node, the harder it is to detect inconsistencies in the location reported.

Figure 1a shows the average time until a member leaves the platoon in each attack scenario, varying the accuracy of the positioning information (by means of standard deviation of proof location error, defined in the previous subsection). It is

possible to observe four main groups of behavior, as follows. The first one corresponds to the blue lines at the bottom, which represents variants (a) of the attacks (i.e, with multiple false nodes). As shown in [1], this considerably increases the severity of the crashes caused by the attacks. Results in Figure 1a show that while the attack severity is higher, it is also easier to be detected due to the distance between the attacker and the additional false nodes.

In the second group, reaction time becomes increasingly longer (worse) as the position accuracy is degraded, specially for a standard deviation greater than nine. The attacks that present this behavior are the variants (a) of scenarios VPHFL and VPHFM, given that in these attacks the false nodes are close to each other.

The third group shows steady detection during the second phase of the attack for variants (b) of all scenarios. Proofs that have location standard deviation errors above 0.5 make it hard to react to the insertion of the false node, since the attacker travels close to this node. Nonetheless, the attack is detected once the second phase starts.

The last group consists of a linear increase in reaction time for scenario CF, variant (b). Since the false node increases its position error progressively, it is intuitive that as the position accuracy degrades, the reaction time increases. We observe that the worst case, i.e. the highest reaction time, happens with the covert falsification attack. Fortunately, the proposed scheme can react safely within time, since it would take $\approx$37 s to cause a crash [1].

Figure 1b provides reaction time statistics for the VPHFM, variant (a). It is possible to observe that as the positioning accuracy degrades to more than 10 σ, the scheme begins to present varying reaction times from the beginning of the attack until the second phase of the attack. When the standard deviation exceeds 14 σ the attack is no longer detected during the first phase. Still, once the second phase of the attack begins, the attacker is detected and distrusted.

Results have shown that all attacks can be timely mitigated, avoiding crashes. During the experiments, no incorrect reactions (false positives) were executed by platoon members. We observed that even though false positives occurred in the classification of beacons [4], the high beaconing frequency (10 Hz) makes consecutive false positives harder to be accumulated. The reaction times are tightly related to the type of attack being carried out, with the most severe variants having the best mitigation performance. Variants that yielded higher reaction times were still timely detected in the second phase of the attacks. Reaction times during the first phase of variants (b) of the scenarios were shown to be feasible, however, the positioning accuracy error must be small enough so that broadcast locations identify correctly the lane in which the vehicle is travelling.

VI. Conclusion

In this paper we investigated how a location detection scheme (in this case, Vouch) can be used to mitigate an ongoing location falsification attack before it can cause a crash among the set of coordinating vehicles. Results show that even with non-perfect detection performance (i.e. the location proof scheme yields false positives in the classification of beacons), the fact that location beacons are sent at a relatively high frequency (10 Hz) allows the reaction module to accumulate a number of false beacons before reacting, thereby reducing the risk of unnecessary reaction while still keeping the reaction time low. All the attack scenarios that were presented in [1] can be aborted at a very early stage of the attack. However, we also demonstrate that this is true only as long as the ability to provide accurate location proofs is maintained. If the error in the location proofs is too high, then the ability to react quickly is reduced, in particular for subtle attacks where at first the false beacons are very close to reality.

References

[1] F. Boeira, M. P. Barcellos, E. P. de Freitas, A. Vinel, and M. Asplund, "Effects of colluding sybil nodes in message falsification attacks for vehicular platooning," in *2017 IEEE Vehicular Networking Conference (VNC)*, Nov 2017, pp. 53–60.

[2] R. van der Heijden, T. Lukaseder, and F. Kargl, "Analyzing attacks on cooperative adaptive cruise control (cacc)," in *2017 IEEE Vehicular Networking Conference (VNC)*, Nov 2017, pp. 45–52.

[3] A. Petrillo, A. Pescap, and S. Santini, "A collaborative control strategy for platoons of autonomous vehicles in the presence of message falsification attacks," in *2017 5th IEEE International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS)*, June 2017, pp. 110–115.

[4] F. Boeira, M. Asplund, and M. P. Barcellos, "Vouch: A secure proof-of-location scheme for vanets," in *21st ACM International Conference on Modelling, Analysis and Simulation of Wireless and Mobile Systems (MSWIM '18), October 28-November 2, 2018, Montreal, QC, Canada*, Oct 2018.

[5] 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, pp. 53–60.

[6] C. Sommer, R. German, and F. Dressler, "Bidirectionally Coupled Network and Road Traffic Simulation for Improved IVC Analysis," *IEEE Transactions on Mobile Computing*, vol. 10, no. 1, pp. 3–15, January 2011.

[7] 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, pp. 1158–1166.