Effects of Colluding Sybil Nodes in Message Falsification Attacks for Vehicular Platooning

Felipe Boeira*†‡, Marinho P. Barcellos*, Edison P. de Freitas*, Alexey Vinel† and Mikael Asplund‡
*Institute of Informatics
Federal University of Rio Grande do Sul, Brazil
†School of Information Technology
Halmstad University, Sweden
‡Dept. of Computer and Information Science
Linköping University, Sweden

***Abstract*—This paper studies the impact of vulnerabilities associated with the Sybil attack (through falsification of multiple identities) and message falsification in vehicular platooning. Platooning employs Inter-Vehicular Communication (IVC) to control a group of vehicles. It uses broadcast information such as acceleration, position, and velocity to operate a longitudinal control law. Cooperation among vehicles allows platoons to reduce fuel consumption and risks associated with driver mistakes. In spite of these benefits, the use of network communication to control vehicles exposes a relevant attack surface that can be exploited by malicious actors. To carry out this study, we evaluate five scenarios to quantify the potential impact of such attacks, identifying how platoons behave under varying Sybil attack conditions and what are the associated safety risks. This research also presents the use of location hijacking attack. In this attack, innocent vehicles that are not part of a platoon are used as a way to create trust bond between the false identities and the physical vehicles. We demonstrate that the ability to create false identities increases the effectiveness of message falsification attacks by making them easier to deploy and harder to detect in time.**

I. Introduction

The emergence of Inter-Vehicular Communication (IVC) leads to a myriad of opportunities in the development of intelligent transportation systems, which are capable of enhancing driving safety, traffic control and also providing infotainment for passengers. The advancement and standardisation of IVC technology allows vehicles to collectively share information and enables the establishment of Cooperative Intelligent Transport Systems (C-ITS).

The development of C-ITS provides the opportunity to improve transportation through the use of platooning and other innovative technologies. A platoon is a group of vehicles that takes advantage of IVC to reduce the distance (headway time) between them while traveling on a highway. The headway time can be shortened by sharing information among the vehicles via *beaconing*: platoon members periodically broadcast 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.

Although there are known benefits on the use of platooning, such as fuel consumption reduction [1] and increased driving comfort [2], cyberattacks must be considered. There has been interest in investigating attacks on cooperative driving scenarios given the potential impact that they have. A particular dangerous scenario consists on the exploitation of the broadcast environment in platooning to simulate fraudulent vehicle beaconing [3].

Douceur [4] first describes the Sybil attack, in the context of P2P networks, as a malicious entity presenting itself via multiple identities to control a substantial part of a system. The Sybil attack may be conducted in the Vehicular ad hoc Network (VANET) environment in two ways: by a rational attacker in order to achieve self benefit, or a malicious attacker seeking to cause harm. The Sybil attack in the VANET context is conducted by falsifying multiple vehicle identities so that events can be generated by these false nodes to interfere with legitimate vehicles. A rational (selfish) attacker might use multiple identities to simulate a congestion, leading neighbor vehicles to take detour routes unnecessarily, and freeing the road which otherwise would not be possible for the attacker. A malicious attacker may use multiple identities to compromise other drivers safety. By inducing drivers to make wrong decisions, the attacker may cause traffic congestion, passenger discomfort and, in the worst case, collisions.

The Sybil attack in the platoon context may be conducted by introducing falsified vehicle identities to the platoon formation. Multiple identities may be used by an attacker to join a platoon, overloading the leader, which has to manage falsified members. The attack causes loss of efficiency and may lead to a denial of service condition, if legitimate vehicles are not able to join. A more dangerous scenario is the use of falsified members at strategic platoon locations, which collude to send erroneous beacons, potentially causing a road accident.

An important aspect of platooning control is how different information sources can be combined using sensor fusion algorithms to provide reliable object tracking. It is clear that IVC will be necessary for platooning applications in order to preserve string stability [5] and therefore it is interesting to study the effects of malicious messages on the system. While sophisticated on-board sensors might ameliorate some of these effects, there is currently a lack of research on the potential combination effects of normal sensor uncertainty

and noise in adverse conditions together with false IVC-based information. Such studies will require realistic models of on-board sensor systems together with realistic network simulation environments, and is out of scope for this work. In this paper we focus on a state-of-the-art IVC-based control algorithm in order to study the general impact of Sybil nodes for attacks against IVC-enabled platoons. We analyse several different scenarios, including those where a radar system would potentially not be able to detect a problem in time. The purpose of this study is not only to investigate whether it is possible to cause collisions (which depends on a large number of factors, including non-technical ones), but mainly to analyse how the ability to use colluding Sybil nodes affect the severity of the attacks and to quantify these effects.

The contributions of this work can be summarized in two main points:

- We design a set of Sybil attack scenarios for vehicular platooning that takes into account both IVC-only and IVC-radar enabled vehicles. We show how an IVC-only platoon could be compromised as well as how to leverage third-party vehicles on a highway to conduct a Sybil attack.

- We perform a set of experiments to quantify the impact of Sybil and message falsification attacks for the defined scenarios. The purpose of these experiments is to investigate to what extent that message falsification interferes with the acceleration of legitimate nodes, and how the ability to provoke an accident in a platoon is affected by colluding Sybil nodes. We show that the use of Sybil nodes significantly increases the attack severity.

The remainder of this paper is organized as follows. In section II, we discuss related work and show the novelty of this study. In section III, we present the system and threat models, including simplifying assumptions. In section IV, we describe the evaluation methodology, input parameters and metrics chosen for the considered attack scenarios. In section V, we present simulation results and safety risks analysis. Section VI concludes and outlines future work.

II. Related Work

Although privacy and authentication may seem contradicting at first, they are key aspects that need to be considered in VANETs. The use of pseudonyms, an authentication scheme that derives a temporary identification from a private key [6], is considered in many cases as an authentication and privacy enabler [7], [8]. Unfortunately, as messages are broadcast frequently, it lets a passive eavesdropper track a vehicle. To address this limitation, researchers use the concept of Mix Zones [9] to ensure that vehicles are not traceable [10]–[12]. While pseudonyms aim at providing both privacy and authentication, the availability of multiple pseudonyms allows a single entity to present itself via multiple identities, i.e. to perform a Sybil attack. Although the authentication model proposed in [13] considers authentication, non-repudiation and location privacy, a node can still obtain a number of identities to conduct a Sybil attack (albeit the identity can be traced afterwards by trust authorities). A rogue node detection model, proposed in [14], attempts to identify attacks by considering the relationship between vehicle density, speed and flow. However, we show in this study that just a couple of false identities placed at specific platoon positions are enough to cause an accident. Even though Sybil attacks have already been considered in the VANET context [15], the study of the impact of Sybil attacks in platoon environments remains an open subject.

Unlike in the general VANET case, vehicular platoons tend to follow a well-defined formation. As the vehicles travel sequentially one after another and the control law is known, it is possible to estimate the behavior of a platoon member. A voting technique that takes this concept into consideration is proposed in [3] to mitigate malicious effects. It collects broadcast information by other vehicles and estimates the average inter-vehicular distance. Then, if the difference between the average and the actual inter-vehicular distance exceeds the system threshold, an attack is detected. The author analyses (using a simulator called PLEXE [16]) platoon behavior when an attacker vehicle performs message falsification on its position. While these techniques can mitigate some security attacks against platoons, voting mechanisms are susceptible to weaknesses if the attacker can control the majority of nodes through Sybil nodes, for example.

Message falsification in platooning can directly influence other members. A malicious insider can negatively influence the platoon by forging data or disrespecting the platoon's control law. An adversarial platooning environment is considered in [17] as a scenario where an insider attacker aims at destabilising as well as taking control of the platoon. The authors state that by modifying the vehicle's gain and applying a sinusoidal acceleration, it is possible to interfere with the platoon's string stability and potentially cause accidents. In [18], the authors examine the application of a sliding mode control scheme on the adversarial platooning environment. They propose the use of two sliding mode controllers that are decentralised and do not take network communication into consideration. Rather, the authors assume that the vehicles have front and rear radars that are used for decision making and reaction purposes. Then, the sliding mode controllers are modeled so that defending cars are able to maintain a desired distance from the attacking vehicle.

In [19], the authors model security attacks in VENTOS [20], an open source VANET simulator, and discuss security design decisions that could be used to mitigate the threats. The authors propose attacks on the application and network layers, system level attacks and privacy leakage attacks. Simulations are performed on the application and network layers by a fixed attacker on the road. The application layer attack consists in modifying CACC beacon messages in order to interfere with the string stability. The authors also consider radio jamming attack. As a result, three potential countermeasures

are enumerated. Two of the approaches are used to identify faulty sensors on the owned vehicle itself by verifying if the reported location is plausible and by using available wearables and mobile devices' sensors as a verifier of the vehicle's reported data.

Other internal attacks are investigated in [21]. The authors define a set of internal attacks in platooning that are originated by misbehavior or equipment malfunction. They consider both a greedy driver that wants to reduce air drag and a distrusting driver that wants to increase the distance to the next car. The authors propose a model to estimate the state other members in the platoon and to compare with reported information to determine whether the member is malicious or not.

In [22], the authors design and evaluate a control strategy to detect and counteract message falsification attacks. In this work, the authors propose the estimation of the average distancing under the ideal assumption that the information broadcast by the other members are correct, i.e. they have not been marked as malicious. The calculated distancing belief is then compared to the distance of nodes based on broadcast information. If a discrepancy greater than a threshold exists, the respective member is marked as malicious and its beacons are not exploited in the control algorithm. This research does not consider colluding nodes or malicious platoon leaders.

Some of the aforementioned efforts have considered Sybil attacks in VANETs and discussed the presence of adversaries in a platoon environment. However, to our knowledge, this is the first paper to identify and evaluate the impact of vulnerabilities associated with the Sybil attack coupled with message falsification in platoons.

III. Sybil Attacks against Vehicular Platoons

This section describes (i) the general system model we adopt to evaluate the impact of attacks through simulation, and (ii) the scenarios we investigate. We specify the platoon topology, network communication details and assumptions. We then describe the attack model used to measure the impact of Sybil and message falsification attacks.

A. System Model

We consider a vehicle platoon as a group of vehicles that travel governed by a common longitudinal control law. To cooperate, vehicles use inter-vehicular communication to share information about their physical state, such as speed, acceleration and position. We assume that the communication is based on the IEEE 802.11p vehicular communication standard. The wireless channel model employs Nakagami-m fading and a free-space path loss to take into account the signal power attenuation. Our model uses a platoon composed of eight cars traveling on a 10 km stretch of highway at 100 km/h and an attacker that travels in a different lane. In some scenarios, we also consider the presence of a non-platoon car traveling on the highway, as will be detailed later.

Messages between vehicles are broadcast in beacons at 10 Hz frequency and contain information about the node. Figure 1 depicts the structure of the beacon. The *vehicleId*

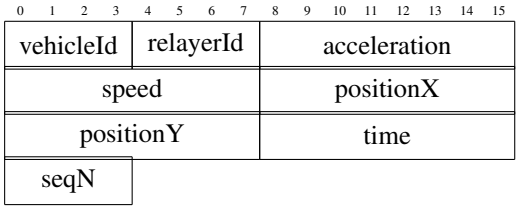


Fig. 1: Platoon beacon structure

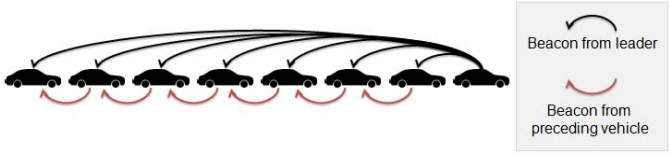


Fig. 2: Platoon topology based on beacons from the leader and preceding vehicles

member is the identification of a vehicle in the platoon, while *relayerId* is disregarded and is set the same as the *vehicleId*. The *acceleration*, *speed* and *time* are self explanatory. The coordinates are represented by *positionX* and *positionY*. A sequence number, *seqN*, is increased at every beacon. We assume that each platoon member runs an instance of a control algorithm that uses information from the beacons broadcast from other nodes. For each iteration of the control algorithm, the acceleration of the vehicle is adjusted if necessary.

We use Consensus [23], a state-of-the-art IVC-based platoon controller. Consensus operates a longitudinal control algorithm and we consider to use the Leader- and predecessor-following topology, which leverages information from both preceding vehicle and leader (see Figure 2). Consensus has been shown to outperform other control algorithms in terms of stability under strong interference, delays, and fading conditions. We do not consider maneuvers for platoon management (e.g. join, split, merge, and lane change), these might present other attack opportunities that we leave for future work.

B. Attack Model

In order to study the potential impact that can be caused by misbehaving entities, we include a model of an attacker whose objective is to cause instabilities to the vehicle platoon. We assume that the attacker is within communication range of the targeted platoon. The attacker is represented by a vehicle in the simulation that travels in a different lane and is not a member of the platoon.

Multiple peers in a distributed environment may act in collusion to achieve a certain objective. We consider a form of collusion attack in a platooning context where multiple Sybil nodes act in a coordinated manner to influence the behavior of other vehicles. As it can be observed in Figure 3, multiple Sybil nodes may falsify messages to influence their preceding vehicles. The Sybil vehicles, represented in red, are falsified nodes injected into the platoon formation by the attacker.

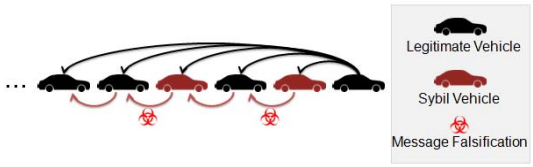


Fig. 3: Influence of Sybil nodes through message falsification

In this attack model, we assume that the owner of the identity of a vehicle is able to interfere with the content of the beacons transmitted to other members, i.e., the attacker is able to falsify information sent through IVC. This is a feasible assumption since an attacker may be able to manipulate the equipment or even build his own, based on public standards or by reverse engineering proprietary assets. In the present model, we consider tampering (interception and falsification of data) to be possible on the beacon structure represented by Fig. 1.

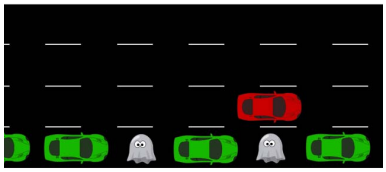
Our model combines the Sybil attack with the falsification of information in order to influence the behavior of other members of the platoon. While performing message falsification and identity theft would potentially allow an attacker to exploit the platoon in similar ways, we consider that only the owner of an identification is able to generate the corresponding beacons.

C. Attack Scenarios

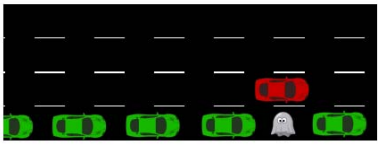
In this study, we evaluate the use of leader- and predecessor-following topology to assess how Sybil nodes may interfere with other members' behavior. We design attack scenarios for both IVC-only and IVC/Radar-based vehicular platooning. We present the scenarios 1, 2 and 3 for pure IVC-based platoons. The purpose of these scenarios is to illustrate the effect of simultaneous acceleration and braking of Sybil nodes, as well as opportunistic attacks in the event of a legitimate emergency braking by a platoon leader. We expand the possibilities of attack in scenarios 4 and 5 by allowing the attacker to make use of vehicles that are not members of a platoon, and falsify vehicle positions to impersonate these non-members. As the following vehicle's radar detects the car in front, the platooning controller may trust that it is a valid node. The Sybil node can later engage on a falsification attack to destabilize the platoon or even cause accidents. This allows an attacker to also target IVC/Radar-based platoons (since the radar might not detect any inconsistency until very late). Moreover, if the control algorithm does not have a robust method for resolving conflicting information it might trust the wrong source. For each of the scenarios, we evaluated the use of multiple colluding Sybil nodes (scenario variants (a)) and the use of only one false node (scenario variants (b)).

1. Falsification. The attack simulation in scenario 1 (a) consists on inserting two Sybil nodes at logical positions within the platoon that enable the attacker to control the behavior of two platoon members. An accident can be caused by manipulating the beacons during a short period so that the preceding vehicle decelerates and the following vehicle accelerates. In scenario 1 (b), only one false node is used in order to compare the impact of using colluding nodes and one malicious node only.

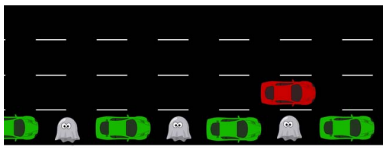
(a) Legend



(b) Attack scenarios 1 (a) and 2 (a) on IVC-based platoon



(c) Attack scenarios 1 (b), 2 (b) and 3 (b) on IVC-based platoon



(d) Attack scenario 3 (a) on IVC-based platoon

Fig. 4: IVC-based Sybil scenarios

2. Covert falsification. In this scenario, we evaluate the impact of a message falsification attack that makes the position error grow progressively. 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 scenario 2 (a), the use of colluding Sybil nodes is evaluated. The Sybil between the leader and vehicle 1 uses the deceleration profile while the other uses the acceleration profile. In scenario 2 (b) the use of only one malicious node is assessed by using the acceleration profile between the leader and vehicle 1.

In order to simulate a plausible behavior, we increase the position error over time. The attacking node's following vehicle will start to adjust its acceleration based on this

progressive error increase. We defined two simple formulas, represented by equations 1 and 2, that add a position error based on a desired acceleration and deceleration falsification.

$$D_{err} = (A_{con} - (D_{des})) * 0.1 \quad (1)$$

$$A_{err} = (A_{con} - (A_{des})) * -1 * 0.1 \quad (2)$$

Where:

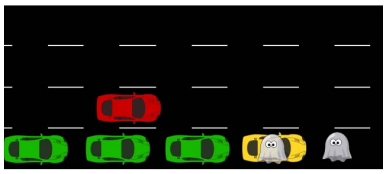
D_{err} = Deceleration distance error (m)
A_{err} = Acceleration distance error (m)
A_{con} = Controller acceleration (m/s^2)
D_{des} = Desired deceleration (m/s^2)
A_{des} = Desired acceleration (m/s^2)

We define D_{des} as -5 and A_{des} as 2.5, which represent plausible acceleration and deceleration values. The error fraction is adjusted to the 10 Hz beaconing frequency and the total error sum is added to the actual position over time, in the pace that the beacons are being broadcast.

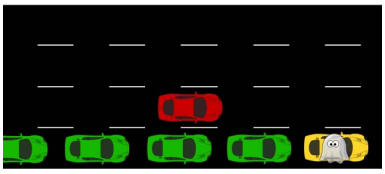
3. Emergency braking obstruction. Emergency braking is a critical event that is sensitive to faults or attacks. In scenario 3 (a), we assume that an attacker has managed to introduce a Sybil node between every pair of platoon members. This allows the attacker to manipulate the members by forging beacons, causing a chain-reaction car accident when an emergency braking is performed by the leader. In 3 (b) we assess how the emergency braking scenario would react to one malicious node only.

4. Vehicle position hijacking to falsify leader. In this scenario, we consider that the attacker is able to claim the position of another non-platoon vehicle that is traveling on the highway. The attacker may become the leader of a platoon should other vehicles request to join. Once a platoon is formed using the third-party vehicle, an attack could be conducted. While the same kind of attack could be performed by a malicious leader, using a Sybil node has the advantage that the attacker does not need to be involved in the accident. In scenario 4 (a), the attacker introduces two Sybil nodes by exploiting the fact that joining vehicles are not able to verify if nodes on front of the third-party vehicle really exist (by using the front radar). In 4 (b), the impact of using only the node at the third-party vehicle is assessed.

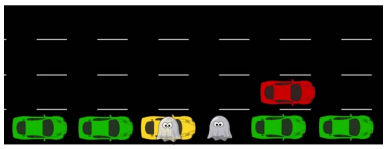
5. Vehicle position hijacking to falsify member. In this scenario, again a non-platoon vehicle is employed so that it is identified by the joining platoon member's radar. The introduction of Sybil nodes would also be possible in an already formed platoon, should a non-platoon vehicle travel close to it. The attacker may introduce a Sybil node at the non-platoon vehicle's position and wait until more members join the platoon, which will start to follow the Sybil nodes. The attacker is then able to conduct an attack. In 5 (a), the use of two Sybil nodes are assessed and in 5 (b) the use of one malicious node only.



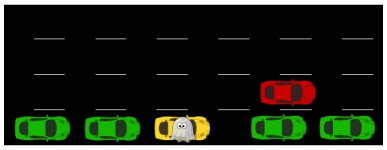
(a) Attack scenario 4 (a) on IVC/Radar-based platoon



(b) Attack scenario 4 (b) on IVC/Radar-based platoon



(c) Attack scenario 5 (a) on IVC/Radar-based platoon



(d) Attack scenario 5 (b) on IVC/Radar-based platoon

Fig. 5: IVC/Radar-based Sybil scenarios

IV. Evaluation Methodology

In this section, we briefly describe the simulation model and software (PLEXE) employed to implement the attack model defined in Section III. We also show the detailed simulation parameters and the metrics used to quantify the impact of the attacks in the platoon environment.

Our experiments are conducted using the PLEXE platoon extension for Veins, a VANET simulator that integrates both realistic network and vehicular traffic modeling. Veins uses the OMNet++ framework to simulate the network and to model the IEEE 802.11p vehicular communication standard. The road traffic simulation is performed by SUMO. Both simulators are executed in parallel, connected through a protocol called Traffic Control Interface (TraCI).

A. Simulation Parameters

The traffic scenario is based on a highway in which the cars move west to east for 200 s or until a collision is detected. The beaconing is performed under the default 10 Hz frequency and transmitted with an 802.11p network card modeled by the Veins framework. The simulation parameters are detailed in Table I.

TABLE I: Traffic 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 [23]
Simulation time	200 s
Beaconing frequency	10 Hz
Communication Interface	802.11p
Radio frequency	5.89 GHz
Path loss model	Free space ($\alpha = 2.0$)
Fading model	Nakagami-m ($m = 3$)

B. Metrics

As the key metric, we identify if an accident can be caused, which is the primary objective of the attacks. In order to quantify the impact, we measure the time taken to cause the collision as well as the speed difference of the vehicles that collided. The metrics are collected for scenarios using colluding Sybil nodes and one false node only.

V. Results

The results in this section show how platoons react to Sybil and message falsification attacks, discussing the impact and how severe the accident is in each scenario.

In the following subsections, we present the attack results of introducing Sybil nodes that falsify their positions. Given that we are not considering platoon maneuvers such as join (cf. attack model previously described), we inject the vehicles in the platoon and wait for it to stabilize. This way we guarantee that the disturbances introduced by abruptly modifying the platoon formation do not interfere with the results of the attacks. The message falsification parameters are 250 m for position and 20 m/s^2 for speed (leading Sybil node scenario 4). These falsification amounts result in high acceleration by the vehicles that exploit the false data in the controller. An overview of the results can be observed in Table II.

A. Falsification

In 1 (a), Sybil nodes are inserted at simulation time 30 s and start to manipulate their following vehicles after a stabilisation period, at simulation time 100 s. The Sybil node inserted between the leader and vehicle 1 forges its position subtracting 250 m from its actual position so that vehicle 1 begins to decelerate. The Sybil node inserted between vehicles 1 and 2 also performs a position falsification, adding 250 m to its actual location and causing vehicle 2 to accelerate. During 3.9 seconds the vehicle 1 applies a strong deceleration while vehicle 2 speeds up to ≈135 km/h, at the time a rear-end collision occurs. As result, it takes less than 4 s to cause a high speed accident. In 1 (b), only one node is used in the attack and the impact is greatly reduced, as can be observed in Table II.

B. Covert falsification

In this scenario we use a progressive position error increase on the falsification of beacons. It would be reasonable to expect that the impact of the position error in this scenario would be lower when compared with the attack scenario 1. However, a collision can still be caused by Sybil nodes that make the position error grow progressively, which could avoid detection by simple anomaly analysis. The collision occurs after 19.2 seconds of progressive falsification and causes a crash between vehicle 2 at 96.2 km/h and vehicle 1 at 83.5 km/h. Not using Sybil colluding nodes in 2 (b) presented a great disadvantage for the attacker. The accident takes 37.4 seconds to occur and the speed difference is even lower, which indicates a lower severity.

C. Emergency braking obstruction

In this scenario, we evaluate the message falsification effects during an emergency braking. In the braking scenario, the platoon travels for 100 s at 100 km/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 in 3 (a), which enables the attacker to interfere with the acceleration of the whole platoon, except the leader. The behavior of the platoon is assessed using a 250 m position falsification by the Sybil nodes.

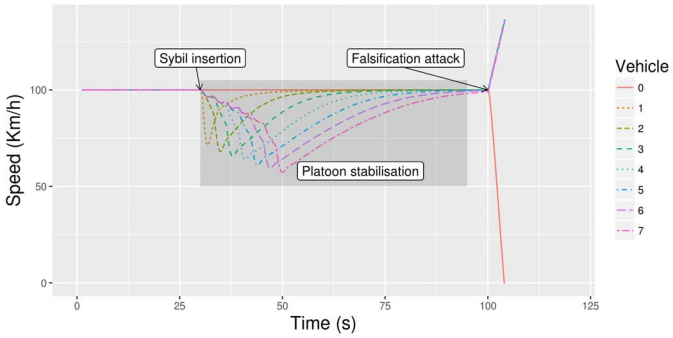
The impact of this attack affects all platoon members, which collide at high speed in a chain-reaction crash. While the leader is applying an emergency brake, the platoon members accelerate to as high as ≈137 km/h until there is a rear-end crash. Like in the previous attack, the time elapsed from the beginning of the emergency brake until the crash is short: just 4.2 seconds. It provides little reaction window for a driver to reclaim the control of the vehicle. In [21], the authors simulate a similar scenario in which a malicious platoon member falsifies its acceleration profile in order to make its following vehicle accelerate.

While the follower is speeding up, the attacker aggressively brakes. This differs from our scenario in which the attacker is not involved in the accident, instead, it uses the Sybil nodes to inject the falsified data.

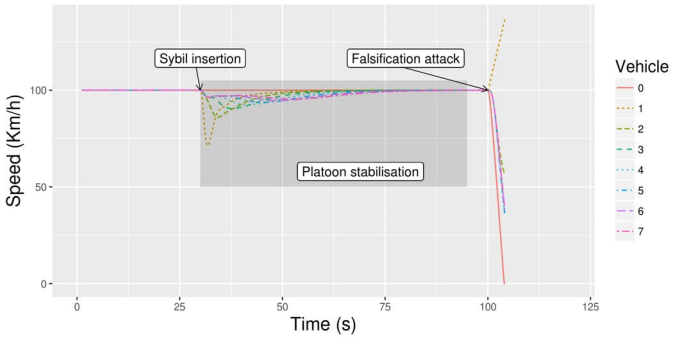
In terms of time to collision and speed difference at collision (see Table II), scenarios 3 (a) and (b) are very similar. The main difference is that, by inserting a Sybil node between every pair of vehicles, the attacker is able to make all members accelerate. This behavior can be observed in Figures 6 (a) and (b).

TABLE II: Attack scenarios results comparison

Scenario	Variant	Time until collision	Sybil nodes	Speed difference at collision	Collision Type
Falsification	(a) (b)	3.9 s 7.9 s	2 1	134.7 km/h 70.6 km/h	Between platoon members
Covert falsification	(a) (b)	19.2 s 37.4 s	2 1	12.6 km/h 8.2 km/h	Between platoon members
Emergency braking obstruction	(a) (b)	4.2 s 4.2 s	7 1	137.3 km/h 137.3 km/h	Between platoon members
Vehicle position hijacking to falsify leader	(a) (b)	2.6 s 5.8 s	2 1	105.8 km/h 30.2 km/h	Between platoon members
Vehicle position hijacking to falsify member	(a) (b)	5.5 s 5.5 s	2 1	49.5 km/h 49.3 km/h	Member crashes non-platoon vehicle



(a) Attack scenario 3 (a) on Emergency Braking



(b) Attack scenario 3 (b) on Emergency Braking

Fig. 6: Platoon member's speed in the Emergency Braking scenario

D. Vehicle position hijacking to falsify leader

We consider that platoon members will potentially use a radar to confirm whether the preceding vehicle exists before incoming data is accepted from it. Each member must trust that its preceding car will verify that the car on front actually exists (creating a trust chain). However, once an attacker is able to introduce a Sybil using a third-party car, as illustrated in Figure 5 (a), any other subsequent identities may be forged without requiring additional physical vehicles. In this scenario, the attacker broadcasts to a platoon with the position of a non-platoon vehicle. Once other members join the platoon, the attacker may falsify the beacons in a way that may cause an accident. We simulate a platoon of eight members and consider the leader to be malicious (the Sybil vehicle). In the scenario 4 (a), the attacker starts to falsify the leader's speed by increasing 20 m/s^2 and the following Sybil node by decreasing its position 250 m. Since the leader has an effect on all the members, all vehicles begin to accelerate. Vehicle 2 is under the effect of the position falsification of the Sybil vehicle 1, though, and decelerates. First of all, by using two colluding Sybil nodes, we reduce the time necessary to cause a crash: only 2.6 s. Second, the two vehicles that collide are vehicles 2 and 3 which are both honest nodes that provide truthful information of their position, but still collide due to conflicting information which is not handled properly by the control algorithm. In 4 (b), the platoon member crashes into the leader (a non-platoon vehicle whose position is being used by the attacker) in 5.8s at ≈149 km/h. In this case, only the leader identity is used. The absence of multiple colluding Sybil nodes results in the inability to control more than one vehicle in distinct ways (e.g. induce one to accelerate and the pther to decelerate), which results in a higher time to collision in 4 (b).

E. Vehicle position hijacking to falsify member

In this last scenario, we explore the attack by means of a non-platoon vehicle traveling close to an already formed platoon. Like scenario 4, we consider that a driver who is not a member of the platoon is impersonated by an attacker. In scenario 5 (a), the attacker introduces a Sybil node to the position of the third-party car and another Sybil on front of it, to fill the gap of the driver following the platoon. In 5 (b), only one node (occupying the non-platoon car) is used. The scenarios 4 (a) and (b) are similar by the reason that the Leader- and predecessor-following topology is used. This scenario could be interesting to be investigated in other topologies, such as bidirectional, which we leave for future work.

VI. Concluding Remarks

This paper has shown that the Sybil and message falsification attacks are a threat not only to VANETs in general, but also specifically to the platoon context. The experiments performed show that the insertion of Sybil nodes that collude

in a message falsification attack can indeed compromise the platoon's string stability if governed mainly by IVC-based information. The falsification directly affects the longitudinal control algorithm and may result in the violation of the control law. Moreover, we show that using Sybil nodes provide significant advantages to a malicious actor since there is no involvement of the attacker on the accident, the time to accident can be reduced compared to having a single attacking nodes, and accidents can be caused between vehicles that provide truthful information about their position to each other.

We also present the position hijacking attack, in which is possible to use non-platoon vehicles traveling close to the platoon so that Sybil nodes are less detectable by radar-enabled vehicles. In addition, a less detectable falsification using position error progression is presented. While this enables more reaction time for a driver to reclaim control of the vehicle, the scenario is also relevant in the context of driverless truck platoons, for example.

Another important aspect to consider is the combination with sensor data that the control algorithm can use. Our work has shown that the IVC-part of a platoon controller is highly susceptible to Sybil and message falsification attacks. This knowledge is important as an input when making a dependability assessment on the entire platoon logic. In particular, it demonstrates the need to study the effects of combination of effects of normal sensor uncertainty and noise in adverse conditions together with an IVC-based attack, with particular attention to timing characteristics since one of the attacks in this work resulted in a collision in as little as 2.6 seconds.

Even though the analysis of platooning maneuvers is not performed in this research, the security assessment of such protocols is also relevant as they present a threat surface that may also be exploited by the use of Sybil or message falsification attacks. We leave the analysis of this subject for a future work.

VII. Acknowledgments

This work was partially supported by the Excellence Center at Linköping-Lund in Information Technology (ELLIIT) strategic research environment.

References

[1] M. P. Lammert, A. Duran, J. Diez, K. Burton, and A. Nicholson, "Effect of platooning on fuel consumption of class 8 vehicles over a range of speeds, following distances, and mass," *SAE International Journal of Commercial Vehicles*, vol. 7, no. 2014-01-2438, pp. 626–639, 2014.

[2] A. Vahidi and A. Eskandarian, "Research advances in intelligent collision avoidance and adaptive cruise control," *Trans. Intell. Transport. Sys.*, vol. 4, no. 3, pp. 143–153, Sep. 2003.

[3] D. Vitelli, "Security Vulnerabilities of Vehicular Platoon Network," Master's thesis, Universita degli studi di Napoli Federico II, 2016.

[4] J. R. Douceur, "The sybil attack," in *Revised Papers from the First International Workshop on Peer-to-Peer Systems*, ser. IPTPS '01. London, UK, UK: Springer-Verlag, 2002, pp. 251–260.

[5] J. Ploeg, D. P. Shukla, N. van de Wouw, and H. Nijmeijer, "Controller synthesis for string stability of vehicle platoons," *IEEE Transactions on Intelligent Transportation Systems*, vol. 15, no. 2, pp. 854–865, April 2014.

[6] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Secur.*, vol. 15, no. 1, pp. 39–68, Jan. 2007. [Online]. Available: http://dl.acm.org/citation.cfm?id=1370616.1370618

[7] T. B. M. de Sales, A. Perkusich, L. M. de Sales, H. O. de Almeida, G. Soares, and M. de Sales, "Asap-v: A privacy-preserving authentication and sybil detection protocol for {VANETs}," *Information Sciences*, vol. 372, pp. 208 – 224, 2016.

[8] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in vanet," in *Proceedings of the Fourth ACM International Workshop on Vehicular Ad Hoc Networks*, ser. VANET '07. New York, NY, USA: ACM, 2007, pp. 19–28.

[9] A. R. Beresford and F. Stajano, "Location privacy in perversive computing," *IEEE Pervasive Computing*, vol. 2, no. 1, pp. 46–55, Jan. 2003.

[10] L. Buttyán, T. Holczer, A. Weimerskirch, and W. Whyte, "Slow: A practical pseudonym changing scheme for location privacy in vanets," in *2009 IEEE Vehicular Networking Conference (VNC)*. IEEE, 2009, pp. 1–8.

[11] J. Freudiger, M. Raya, M. Félegyházi, P. Papadimitratos *et al.*, "Mix-zones for location privacy in vehicular networks," 2007.

[12] B. Ying, D. Makrakis, and H. T. Mouftah, "Dynamic mix-zone for location privacy in vehicular networks," *IEEE Communications Letters*, vol. 17, no. 8, pp. 1524–1527, 2013.

[13] K. Zaidi, Y. Rahulamathavan, and M. Rajarajan, "Diva - digital identity in vanets: A multi-authority framework for vanets," in *2013 19th IEEE International Conference on Networks (ICON)*, Dec 2013, pp. 1–6.

[14] K. Zaidi, M. Milojevic, V. Rakocevic, and M. Rajarajan, "Data-centric rogue node detection in vanets," in *2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications*, Sept 2014, pp. 398–405.

[15] P. Kafil, M. Fathy, and M. Z. Lighvan, "Modeling sybil attacker behavior in vanets," in *2012 9th International ISC Conference on Information Security and Cryptology*, Sept 2012, pp. 162–168.

[16] 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)*. Paderborn, Germany: IEEE, December 2014, pp. 53–60.

[17] S. Dadras, R. M. Gerdes, and R. Sharma, "Vehicular platooning in an adversarial environment," in *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*, ser. ASIA CCS '15. New York, NY, USA: ACM, 2015, pp. 167–178.

[18] I. Sajjad, D. D. Dunn, R. Sharma, and R. Gerdes, "Attack mitigation in adversarial platooning using detection-based sliding mode control," in *Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy*, ser. CPS-SPC '15. New York, NY, USA: ACM, 2015, pp. 43–53.

[19] M. Amoozadeh, A. Raghuramu, C. n. Chuah, D. Ghosal, H. M. Zhang, J. Rowe, and K. Levitt, "Security vulnerabilities of connected vehicle streams and their impact on cooperative driving," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 126–132, June 2015.

[20] M. Amoozadeh, H. Deng, C.-N. Chuah, H. M. Zhang, and D. Ghosal, "Platoon management with cooperative adaptive cruise control enabled by vanet," *Vehicular Communications*, vol. 2, no. 2, pp. 110–123, 2015.

[21] B. DeBruhl, S. Weerakkody, B. Sinopoli, and P. Tague, "Is your commute driving you crazy?: A study of misbehavior in vehicular platoons," in *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, ser. WiSec '15. New York, NY, USA: ACM, 2015, pp. 22:1–22:11.

[22] 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.

[23] 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.